SCOPE Framework: Asset & Configuration Management Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Asset & Configuration Management domain ensures comprehensive visibility, control, and integrity of all enterprise technology assets and their configurations throughout the system lifecycle. This domain governs the identification, tracking, and classification of hardware and software assets; the establishment and enforcement of secure baseline configurations; the structured management of configuration changes; and the use of automated discovery to maintain an accurate, real-time inventory. It also extends oversight to mobile and remote assets operating beyond the traditional perimeter. By institutionalizing these practices, the organization reduces the risk of misconfigurations, unauthorized changes, shadow IT, and unmanaged endpoints—ultimately supporting a defensible architecture, effective incident response, and continuous alignment with security and compliance objectives.

Section 1. Hardware & Software Asset Management

Effective cybersecurity operations depend on the accurate, real-time identification, categorization, and management of all hardware and software assets authorized within the enterprise. The Hardware & Software Asset Management (HSA) control family ensures visibility, ownership, and accountability of all technology assets, minimizing the risk of unauthorized or unmanaged components within the environment. This control family establishes the foundation for asset lifecycle tracking, license compliance, and configuration alignment across the enterprise.

1.1 HSA-01: Asset Inventory Establishment

Organizations shall establish and maintain an authoritative, enterprise-wide inventory of all hardware and software assets, to include physical, virtual, cloud-based, and containerized environments.

1.2 HSA-02: Unique Asset Identification

Each asset shall be assigned a unique identifier for tracking purposes, enabling correlation across management, configuration, and monitoring systems.

1.3 HSA-03: Asset Ownership Assignment

Each hardware and software asset shall have a designated business and technical owner accountable for its use, security posture, and lifecycle status.

1.4 HSA-04: Asset Classification by Sensitivity and Function

Assets shall be categorized by sensitivity level, operational criticality, and functional role (e.g., server, workstation, network device, application software).

1.5 HSA-05: Asset Lifecycle Tracking

All assets shall be tracked from acquisition through deployment, maintenance, and eventual decommissioning, with records updated at each lifecycle phase.

1.6 HSA-06: Unauthorized Asset Detection and Handling

Processes shall be implemented to detect, alert, and respond to unauthorized or rogue hardware and software assets within enterprise environments.

1.7 HSA-07: Software License Management

All software assets shall be reviewed for proper licensing; mechanisms shall be in place to ensure compliance with vendor license terms and renewals.

1.8 HSA-08: Hardware and Software Asset Reconciliation

Asset records shall be regularly reconciled with procurement, CMDB, and configuration repositories to identify discrepancies or orphaned assets.

1.9 HSA-09: Asset Onboarding Requirements

New assets shall not be authorized for use until they have been inventoried, assigned an owner, configured to baseline standards, and registered in the asset inventory system.

1.10 HSA-10: Shadow IT Discovery Procedures

Organizations shall implement methods to detect and evaluate unsanctioned or unmanaged software and services (e.g., SaaS, cloud instances) used by business units.

1.11 HSA-11: Virtual and Cloud Asset Inclusion

Inventory practices shall extend to virtualized workloads, cloud-hosted assets, and containers, ensuring visibility regardless of hosting model or provider.

1.12 HSA-12: Portable and Removable Media Tracking

Portable devices (e.g., external hard drives, USB devices) shall be tracked through serial registration or equivalent mechanisms to prevent data leakage or loss.

1.13 HSA-13: Asset Tagging and Labeling Standards

Physical and virtual assets shall be tagged in accordance with standardized asset labeling procedures to enable streamlined tracking and identification.

1.14 HSA-14: Asset Discovery Integration with CMDB

Discovery tools shall integrate with the Configuration Management Database (CMDB) to maintain data fidelity and support configuration auditing.

1.15 HSA-15: Software Asset Whitelisting

Organizations shall establish a whitelisting process that governs what software is permitted to operate within the environment, with justification and approval workflows.

1.16 HSA-16: End-of-Life Asset Identification

Processes shall be in place to identify and flag assets that are end-of-life or end-of-support, with transition and replacement plans documented.

1.17 HSA-17: Asset Risk Profiling

Assets shall be risk-ranked based on factors such as data sensitivity, exposure to threats, business criticality, and level of user access.

1.18 HSA-18: Integration with Security Tools

Asset inventories shall be continuously synchronized with vulnerability management, SIEM, and endpoint protection platforms to ensure coverage and situational awareness.

1.19 HSA-19: Asset Inventory Access Controls

Access to asset inventory systems shall be role-based and restricted to authorized personnel, with audit logging enabled to track changes and queries.

1.20 HSA-20: Periodic Asset Inventory Validation

Organizations shall conduct periodic validation of the asset inventory through automated and manual processes to verify accuracy, completeness, and integrity.

1.21 HSA-21: Mobile Asset Tracking Integration

Mobile hardware (e.g., laptops, smartphones) shall be tracked through integration with mobile device management (MDM) solutions to maintain visibility during offsite or remote use.

1.22 HSA-22: Asset Reporting and Dashboards

Dashboards and reporting mechanisms shall be implemented to provide stakeholders with insights into asset inventory metrics, trends, and gaps across the enterprise.

Section 2. Configuration & Change Management (CCM)

Configuration & Change Management (CCM) governs how systems, applications, and infrastructure are securely configured, maintained, and modified throughout their operational lifecycle. This control family ensures standardized, documented processes for configuration baselining, authorized change approvals, rollback procedures, and version control. It is essential for minimizing misconfigurations, reducing unauthorized changes, and maintaining the security integrity of enterprise systems while supporting agile business operations.

2.1 CCM-01: Configuration Management Policy and Procedures

Organizations shall establish, document, and maintain configuration management policies and detailed procedures that govern secure baseline configurations, version control, and change approvals.

2.2 CCM-02: Authorized Configuration Baseline Enforcement

All systems and components shall be configured in accordance with formally approved baseline configurations, and deviations shall require documented risk acceptance and change approval.

2.3 CCM-03: Configuration Drift Detection

Automated mechanisms shall be employed to continuously detect, alert on, and report deviations from approved configurations (i.e., configuration drift).

2.4 CCM-04: Change Control Governance Structure

A governance body (e.g., Change Advisory Board) shall oversee proposed changes to production environments, ensuring risk evaluation and stakeholder alignment.

2.5 CCM-05: Change Request Documentation Requirements

All change requests shall include a detailed description, business justification, risk assessment, testing results, rollback plan, and implementation timeline.

2.6 CCM-06: Pre-Change Security Impact Assessments

Security impact assessments shall be conducted prior to implementing configuration or system changes to evaluate potential risks to confidentiality, integrity, and availability.

2.7 CCM-07: Change Approval Workflows

No configuration change shall be executed without documented approval through predefined workflows that consider the risk level and affected systems.

2.8 CCM-08: Emergency Change Handling Procedures

A distinct, documented emergency change process shall exist to address time-sensitive, high-priority issues, including expedited approval, validation, and post-implementation review.

2.9 CCM-09: Rollback Strategy Requirement

Every change implementation shall include a fully defined rollback strategy that can be executed if the change fails or introduces adverse effects.

2.10 CCM-10: Post-Change Validation and Review

All implemented changes shall undergo post-change validation and operational testing to confirm successful implementation and to identify any residual issues.

2.11 CCM-11: Configuration Change Logging

All configuration changes shall be logged with user identity, timestamp, system affected, and change details, and retained in accordance with log retention policy.

2.12 CCM-12: Version Control of Configuration Files

Configuration files shall be managed using version control systems that track, retain, and provide audit history of all changes.

2.13 CCM-13: Unauthorized Configuration Change Detection

Automated systems shall be in place to detect and alert on configuration changes made outside of authorized workflows.

2.14 CCM-14: Change Freeze Periods and Maintenance Windows

Change activity shall be restricted during defined change freeze periods and permitted only within approved maintenance windows to reduce operational risk.

2.15 CCM-15: Configuration Dependency Mapping

Organizations shall maintain a mapping of configuration dependencies and system interrelationships to inform change impact analysis and minimize cascading failures.

2.16 CCM-16: Segregation of Duties for Change Implementation

Configuration changes shall be subject to separation of duties, ensuring individuals requesting changes are not the same as those approving or implementing them.

2.17 CCM-17: Configuration Control of Virtualized & Cloud Resources

Configuration and change management controls shall extend to virtual machines, cloud-native infrastructure, and container orchestration systems, with change tracking enforced.

2.18 CCM-18: Baseline Revalidation and Recertification

Approved configuration baselines shall be reviewed and revalidated on a scheduled basis, especially following major system updates, to ensure continued relevance and security.

2.19 CCM-19: Controlled Use of Automation in Configuration Changes

Where automation is used for configuration changes (e.g., Infrastructure as Code), scripts shall be reviewed, tested, and version-controlled before execution.

2.20 CCM-20: System-Specific Configuration Exceptions Management

Any deviation from standard configuration baselines shall be documented, justified, approved, and periodically reviewed to assess ongoing risk and necessity.

2.21 CCM-21: Change Communication Protocols

Organizations shall define and follow standardized communication protocols to notify stakeholders of approved, upcoming, and completed changes impacting their operations.

2.22 CCM-22: Third-Party Change Integration Requirements

Changes performed by third-party vendors or managed service providers shall follow the organization’s change management requirements and be subject to internal review.

Section 3. Baseline Security Configurations

Baseline Security Configurations (BSC) define and enforce secure default settings for all systems, platforms, applications, and devices prior to deployment. These configurations reflect the minimum-security posture required to mitigate common threats and vulnerabilities, reduce the attack surface, and ensure consistent implementation across the enterprise. This control family focuses on the creation, validation, and enforcement of hardened configurations based on industry standards, without overlapping with change control or asset inventory processes.

3.1 BSC-01: Secure Configuration Baseline Development

Organizations shall develop secure configuration baselines for all technology platforms, operating systems, applications, and devices.

3.2 BSC-02: Platform-Specific Baseline Definition

Each technology platform (e.g., Windows, Linux, macOS, network devices, hypervisors) shall have its own tailored secure baseline that aligns with its unique security requirements and risk exposure.

3.3 BSC-03: Role-Specific Configuration Templates

Baselines shall be customized based on the role or function of the asset (e.g., web server, database server, end-user workstation) to balance security with operational needs.

3.4 BSC-04: Pre-Deployment Baseline Enforcement

Systems and applications shall not be deployed into production environments until verified to be configured in accordance with an approved security baseline.

3.5 BSC-05: Hardening of Default Credentials and Services

Baseline configurations shall include disabling or securing default accounts, removing unnecessary services, and modifying default configurations to eliminate known risks.

3.6 BSC-06: Administrative Interface Restrictions

Baseline configurations shall restrict access to administrative interfaces (e.g., web UI, CLI, management ports) to authorized personnel and secure network segments only.

3.7 BSC-07: Logging and Auditing Configuration Standards

Security baselines shall define required logging parameters, including which events must be logged, how logs are retained, and secure forwarding requirements.

3.8 BSC-08: Protocol and Port Hardening

Only essential ports and protocols shall be enabled in baseline configurations; unnecessary or insecure services (e.g., Telnet, SMBv1) shall be disabled.

3.9 BSC-09: Secure Authentication Settings

Baselines shall enforce strong authentication parameters including password complexity, lockout policies, session timeouts, and secure authentication protocols.

3.10 BSC-10: Baseline Validation and Testing Procedures

Secure baselines shall be validated through repeatable testing procedures in staging environments prior to enterprise-wide implementation.

3.11 BSC-11: Least Functionality by Default

Baseline configurations shall be designed to minimize functionality, enabling only the services and capabilities necessary for the system's intended purpose.

3.12 BSC-12: Secure Configuration for Remote Administration

When remote administration is required, baseline configurations shall mandate the use of secure channels (e.g., SSH, RDP over VPN), multi-factor authentication, and access logging.

3.13 BSC-13: Endpoint Security Configuration Standards

All endpoint devices shall conform to a hardened security baseline that includes antivirus, endpoint protection platform (EPP) integration, host firewall rules, and local admin rights restrictions.

3.14 BSC-14: Secure Application Configuration Defaults

Application configurations shall disable insecure features by default (e.g., debug modes, verbose error messages) and enforce secure session handling, access controls, and encryption settings.

3.15 BSC-15: Cloud Service Security Configuration Baselines

Cloud platforms shall have defined baselines for account security, resource configurations, identity services, and native logging functions.

3.16 BSC-16: IoT and OT Configuration Hardening Standards

Where IoT or OT systems are in scope, baseline configurations shall address physical and logical security concerns, including firmware versioning, disabled USB ports, and secure communications.

3.17 BSC-17: Periodic Baseline Review and Update

Secure configuration baselines shall be reviewed at least annually, or upon the release of major system changes or emerging threats, to ensure ongoing relevancy and protection.

3.18 BSC-18: Secure Configuration of Virtualized Environments

Virtual machine and hypervisor baselines shall include isolation controls, logging settings, unused interface disablement, and restrictions on inter-VM communication.

3.19 BSC-19: Baseline Exceptions Process

Exceptions to baseline configurations shall require formal approval, documented justification, compensating controls, and periodic re-evaluation of necessity.

3.20 BSC-20: Embedded and Firmware Configuration Baselines

Systems with embedded software or firmware (e.g., routers, printers, industrial controllers) shall have defined secure configuration parameters applied and validated post-deployment.

Section 4. Mobile & Remote Asset Management (MRM)

Mobile & Remote Asset Management (MRM) governs the oversight, control, and security of assets that operate outside the traditional enterprise perimeter. This includes laptops, smartphones, tablets, field-deployed equipment, and remote workstations. The MRM control family ensures these assets remain visible, compliant, and secure regardless of location or connectivity, addressing the unique risks posed by mobile workforces, BYOD environments, and remote operations. These controls focus specifically on the secure enablement and lifecycle management of remote and mobile assets without overlapping with baseline configurations, asset discovery, or device hardening.

4.1 MRM-01: Remote Asset Enrollment Process

All mobile and remote assets shall be formally enrolled into the organization's asset management system prior to being issued or granted access to enterprise resources.

4.2 MRM-02: Mobile Device Usage Policy Enforcement

A documented mobile device usage policy shall be enforced, outlining acceptable use, security requirements, and user responsibilities for organization-managed and BYOD devices.

4.3 MRM-03: Secure Provisioning of Remote Assets

Remote and mobile devices shall be securely provisioned using approved imaging or automated deployment solutions, ensuring consistency in initial configuration and access controls.

4.4 MRM-04: Remote Management Capability Requirement

All mobile and remote assets shall be configured to support secure remote management (e.g., MDM, EDR, RMM) for configuration enforcement, policy updates, and incident response.

4.5 MRM-05: Enforced Disk Encryption on Mobile Assets

Full disk encryption shall be enabled on all mobile and remote devices capable of storing organizational data to protect against data loss due to theft or unauthorized access.

4.6 MRM-06: Remote Asset Identity Verification

Remote assets shall be uniquely identified and authenticated prior to granting access to enterprise networks or resources, using device certificates, hardware IDs, or secure tokens.

4.7 MRM-07: Mobile Application Control Enforcement

Application whitelisting or containerization shall be enforced on mobile assets to prevent the installation and execution of unauthorized or malicious applications.

4.8 MRM-08: Location-Aware Access Controls

Mobile and remote asset access shall be governed by geo-fencing, IP-based restrictions, or risk-aware contextual access controls where feasible.

4.9 MRM-09: Offline Usage Restrictions

Policies shall define and enforce restrictions on offline data access, modification, or synchronization for remote and mobile devices handling sensitive information.

4.10 MRM-10: Remote Asset Patch Compliance Monitoring

The patch and update status of remote and mobile devices shall be continuously monitored, with alerts for non-compliance or failed updates.

4.11 MRM-11: Device Wipe and Lock Capabilities

All remote and mobile devices shall support and be enrolled in a capability to remotely lock, wipe, or disable the device in the event of loss, theft, or compromise.

4.12 MRM-12: Remote Asset Connectivity Logging

All remote and mobile assets shall log connectivity attempts, access to enterprise systems, and other relevant activity to a centralized log management or SIEM platform.

4.13 MRM-13: Multi-Factor Authentication on Remote Devices

All users accessing enterprise resources from remote or mobile assets shall authenticate using multi-factor authentication (MFA), including biometric or hardware-based factors where possible.

4.14 MRM-14: Separation of Personal and Enterprise Data

Mobile asset configurations shall enforce separation between personal and organizational data through containerization or profile segregation to preserve privacy and enforce security.

4.15 MRM-15: Remote Asset Decommissioning Procedures

Remote and mobile devices shall follow a formal decommissioning process upon retirement, transfer, or termination, including data sanitization and inventory removal.

4.16 MRM-16: Cellular and Wireless Security Enforcement

Remote and mobile devices shall be restricted from connecting to unsecured networks, with controls enforcing VPN usage, hotspot restrictions, and encryption of wireless traffic.

4.17 MRM-17: Remote Asset Compliance Enforcement

Remote and mobile assets found to be out of compliance with security policies shall be subject to automated remediation, access revocation, or administrative review.

4.18 MRM-18: Endpoint Detection on Mobile Devices

All remote and mobile devices shall be equipped with endpoint detection and response (EDR) or equivalent security tools capable of detecting threats and reporting in real time.

4.19 MRM-19: Device Posture Validation Prior to Access

Prior to granting access to enterprise systems, remote assets shall be assessed for posture compliance (e.g., AV enabled, updates current, encryption active) using NAC or endpoint compliance tools.

4.20 MRM-20: Usage of Organization-Approved VPN Clients

All remote and mobile asset access to internal resources shall be routed through an organization-approved VPN client configured to enforce encryption and connection monitoring.

4.21 MRM-21: Remote Peripheral and Media Control

Remote devices shall restrict or monitor the use of USB ports, peripheral devices, and removable media to prevent unauthorized data transfer or malware introduction.

4.22 MRM-22: Data Sync Controls for Remote Assets

Policies and technical controls shall restrict synchronization of enterprise data to only approved devices and locations, with restrictions on third-party cloud services and backups.