SCOPE Framework: Identity & Access 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 Identity & Access Management (IAM) domain establishes the comprehensive framework for governing and enforcing how identities are created, managed, authenticated, and authorized across enterprise systems. This domain ensures that access to systems, data, and resources is based on verified identity, enforced through context-aware access controls, and continuously monitored to prevent misuse or unauthorized access. By incorporating robust mechanisms such as role- and attribute-based access control, identity federation, single sign-on, privileged access governance, multi-factor authentication, and secure credential management, this domain minimizes identity-related risk while enabling secure digital interactions. Effective implementation of IAM strengthens user accountability, limits the blast radius of compromise, and ensures only the right individuals and entities have access to the right resources at the right time for the right reasons.

Section 1. Access Controls (ACN)

The Access Controls (ACN) control family establishes requirements for the implementation, enforcement, and ongoing management of access permissions to systems, applications, and data based on established access control models. These controls are foundational to the confidentiality, integrity, and availability of information and should align with business objectives and risk tolerance levels. This control family includes Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC) frameworks.

1.1 ACN-01: Access Control Policy

The organization shall develop, document, and maintain an access control policy that defines the methodology and criteria for granting, reviewing, and revoking access to systems, applications, and data. The policy shall include model selection (RBAC, ABAC, PBAC), approval workflows, access provisioning requirements, and segregation of duties principles.

1.2 ACN-02: Role-Based Access Control (RBAC) Implementation

The organization shall implement Role-Based Access Control where access rights are assigned based on user roles aligned to job functions. Roles shall be clearly defined, documented, and approved, with minimal privileges required for task execution (principle of least privilege).

1.3 ACN-03: Attribute-Based Access Control (ABAC) Framework

Where applicable, the organization shall employ ABAC mechanisms to evaluate access decisions based on user attributes, resource characteristics, and environmental conditions (e.g., location, device trust level). ABAC policies shall be centrally managed and reviewed for consistency and effectiveness.

1.4 ACN-04: Policy-Based Access Control (PBAC) Integration

The organization shall utilize PBAC models to manage access decisions using defined policy rules that dynamically evaluate multiple criteria beyond identity or role alone. Policies shall be granular, support context-aware decisioning, and be tested prior to production deployment.

1.5 ACN-05: Access Authorization Procedures

The organization shall enforce formal access request and approval procedures, requiring documented justification, supervisor or system owner approval, and alignment to authorized roles or access policies. Temporary or emergency access must follow defined exception handling workflows.

1.6 ACN-06: Access Recertification

The organization shall perform access reviews at regular intervals, not to exceed 90 days for high-privilege or sensitive systems and 180 days for standard users. The reviews shall validate user need-to-know, privilege level appropriateness, and current employment or contract status.

1.7 ACN-07: Access Revocation

The organization shall revoke user access within defined timeframes upon role change, separation, or access expiration. Automated triggers from HR systems or termination events shall be integrated into revocation workflows where feasible.

1.8 ACN-08: Default Deny Enforcement

The organization shall configure all access control mechanisms to default to deny unless explicitly permitted by policy. Systems and services must be configured to prevent unauthorized access by default, including for APIs, backend systems, and privileged interfaces.

1.9 ACN-09: Access Control Exception Management

The organization shall establish a process to handle access control exceptions, including documentation of the rationale, risk acceptance, expiration date, and compensating controls. All exceptions must be reviewed and approved by designated risk owners.

1.10 ACN-10: Service & System Account Restrictions

The organization shall define and enforce access control rules for service accounts, system accounts, and non-human identities to ensure access is limited to required functions. These accounts must not be used for interactive logins unless explicitly authorized and logged.

1.11 ACN-11: Access Logging & Reporting

The organization shall log access control events, including authentication attempts, authorization decisions, and access changes. Reports must be generated and reviewed regularly to detect anomalies, policy violations, or indicators of unauthorized access.

1.12 ACN-12: Access Control Testing & Validation

Access controls shall be tested at least annually and after any significant system change to validate enforcement, policy adherence, and alignment with organizational requirements. Testing should include negative testing scenarios to evaluate default deny and policy edge cases.

Section 2. Identity Federation & Single Sign-On (SSO)

The Identity Federation & Single Sign-On (SSO) control family establishes the governance, implementation, and assurance mechanisms required to securely enable identity portability and seamless access across systems, organizations, and trust domains. These controls ensure that federated identity systems and SSO implementations maintain integrity, interoperability, and strong assurance without compromising access boundaries or increasing risk exposure. Controls in this family specifically address configurations, trust frameworks, session behaviors, and identity brokerage.

2.1 SSO-01: Federated Identity Governance

The organization shall establish a governance model for federated identity that defines responsibilities, trust criteria, and risk tolerances associated with accepting or asserting identities across organizational boundaries.

2.2 SSO-02: Trust Framework Alignment

Federated identity implementations shall align with recognized trust frameworks (e.g., SAML, OpenID Connect, WS-Federation, FIDO2) and must document all protocol versions, endpoints, and configurations in use.

2.3 SSO-03: Identity Provider (IdP) Authorization

The organization shall formally authorize any external Identity Provider (IdP) prior to integration, based on an assessment of security practices, compliance posture, and contractual obligations including incident handling and liability.

2.4 SSO-04: Service Provider (SP) Integration Controls

The organization shall implement a consistent method for onboarding Service Providers (SPs) into the federated ecosystem, including metadata validation, binding method verification, and endpoint assurance prior to enabling SSO.

2.5 SSO-05: Single Sign-On Policy Definition

The organization shall develop, document, and enforce a Single Sign-On policy defining the scope of SSO implementations, systems in-scope, session timeouts, and acceptable usage patterns.

2.6 SSO-06: Assertion Integrity Verification

The organization shall implement controls to verify the cryptographic integrity and authenticity of identity assertions or tokens received from IdPs, including signature validation and expiration checks.

2.7 SSO-07: Audience & Scope Restriction

All SSO assertions or tokens must include audience restrictions and scoped claims that limit use to the intended relying party or service, preventing assertion re-use or injection into unintended services.

2.8 SSO-08: Identity Mapping & Claim Normalization

The organization shall implement identity claim normalization processes to map federated identities to internal access models, roles, or entitlements without assuming parity of attributes or authorization levels.

2.9 SSO-09: Cross-Domain Identity Assurance

Federated identity implementations shall require identity assurance levels (IAL) appropriate to the sensitivity of the target system, including adherence to NIST 800-63 or similar identity proofing standards.

2.10 SSO-10: Session Security for SSO

The organization shall enforce session security parameters for SSO transactions, including time-based expiration, IP validation, inactivity timeouts, and re-authentication for privileged functions.

2.11 SSO-11: Federation Metadata Integrity

All federation metadata files must be signed, validated, and rotated periodically in accordance with organizational policy and vendor recommendations to mitigate stale trust configurations.

2.12 SSO-12: IdP & SP Certificate Management

The organization shall maintain an inventory and lifecycle management process for all certificates used in federation and SSO transactions, ensuring timely renewal and revocation.

2.13 SSO-13: SSO Logout Propagation

The organization shall configure SSO systems to propagate logout events to all participating services when feasible, or document compensating controls for sessions that remain valid post-logout.

2.14 SSO-14: Identity Federation Testing

Federated SSO configurations must undergo functional and security testing before deployment, including simulated assertion tampering, token replay attempts, and invalid issuer scenarios.

2.15 SSO-15: Just-in-Time (JIT) Provisioning Controls

Where Just-in-Time provisioning is used, the organization shall implement controls to limit access until post-provisioning checks are completed, such as role validation and policy alignment.

2.16 SSO-16: Federation Drift Monitoring

The organization shall monitor for federation drift, including expired metadata, broken links, or updated IdP/SP configurations that are not reflected in the trust relationship.

2.17 SSO-17: Multi-IdP Support Assurance

Where multiple IdPs are supported, the organization shall ensure routing logic, IdP discovery, and failover handling are implemented securely, without revealing unnecessary user information or introducing ambiguity in authentication paths.

2.18 SSO-18: Third-Party Federation Agreements

All external identity federation arrangements must be governed by agreements outlining responsibilities, liabilities, incident response coordination, privacy requirements, and dispute resolution mechanisms.

2.19 SSO-19: Audit Logging of Federation Events

The organization shall log federation-related events, including authentication requests, token issuance, signature verification results, and errors, storing logs in accordance with organizational retention and monitoring policies.

2.20 SSO-20: SSO Availability & Resilience

The organization shall design SSO components with appropriate redundancy, failover, and service degradation capabilities to ensure authentication continuity in the event of IdP or SP unavailability.

2.21 SSO-21: Federation Boundary Enforcement

The organization shall enforce logical boundaries between federated identity systems and internal IAM processes, ensuring that federated identity assertions do not bypass internal controls, validations, or approvals.

2.22 SSO-22: SSO Usability & Error Feedback

The organization shall ensure user-facing SSO mechanisms provide clear, non-technical feedback for authentication issues, and do not disclose sensitive error information that could be leveraged by an attacker.

Section 3. Privileged Access Management (PAM)

The Privileged Access Management (PAM) control family establishes the policies, processes, and technical mechanisms required to govern, monitor, and secure access granted to privileged accounts and identities. These controls are designed to mitigate risks associated with administrative access, elevated permissions, and non-repudiable actions across critical infrastructure, systems, and data. This control family is limited to elements directly pertaining to the lifecycle, use, and oversight of privileged access and should be implemented distinctly from general access controls.

3.1 PAM-01: Privileged Access Policy

The organization shall develop, approve, and maintain a privileged access policy that defines criteria for privileged role assignment, usage boundaries, and accountability measures for all elevated access types, including local, domain, application, and cloud-native roles.

3.2 PAM-02: Privileged Role Classification

All privileged accounts shall be classified according to risk and scope of access (e.g., root, domain admin, hypervisor admin, database admin) with documented responsibilities, separation requirements, and authorized users.

3.3 PAM-03: Least Privilege Enforcement for Admins

Privileged accounts shall be provisioned with the minimum level of access necessary to perform their defined administrative functions and shall not retain standing access beyond their operational scope.

3.4 PAM-04: Dedicated Administrative Accounts

The organization shall require users with privileged access to use separate, dedicated administrative accounts that are not used for daily operations, email, or internet access.

3.5 PAM-05: Privileged Session Isolation

All privileged sessions shall be brokered, isolated, or tunneled through secure PAM infrastructure to prevent direct access to target systems and enable monitoring, session recording, and command restriction.

3.6 PAM-06: Just-In-Time Privileged Access

The organization shall implement just-in-time (JIT) mechanisms for granting temporary privileged access, with automated expiration, usage logs, and reapproval requirements for subsequent access.

3.7 PAM-07: Privileged Access Request Workflow

A formal request workflow shall be required for all new or temporary privileged access grants, including justification, manager/system owner approval, expiration dates, and periodic reassessment criteria.

3.8 PAM-08: Privileged Credential Vaulting

Privileged credentials, including root, service, and break-glass accounts, shall be stored in an encrypted, access-controlled credential vault that supports access logging, password rotation, and policy enforcement.

3.9 PAM-09: Automated Password Rotation

Privileged credentials managed by the vault shall be rotated automatically on a scheduled basis and immediately following any use event, account change, or suspected compromise.

3.10 PAM-10: Command Filtering & Restrictions

The PAM solution shall enforce command-level restrictions on privileged sessions based on role, environment, and system sensitivity to prevent misuse or accidental execution of high-risk commands.

3.11 PAM-11: Dual Control for High-Risk Access

The organization shall implement dual control (two-person integrity) for access to sensitive systems or actions deemed high-risk, such as root access to production databases or changes to security configurations.

3.12 PAM-12: Privileged Session Recording

Privileged sessions shall be recorded in full or in part (e.g., keystroke logging, video capture) for forensic investigation, compliance, and operational auditing. Recordings shall be stored securely with integrity validation.

3.13 PAM-13: Emergency Access Controls

Emergency or “break-glass” privileged access shall be tightly controlled, monitored in real time, require post-use review, and include automated revocation and alerting mechanisms to ensure immediate accountability.

3.14 PAM-14: Third-Party Privileged Access Management

Privileged access granted to external vendors, contractors, or managed service providers must be provisioned through PAM infrastructure, time-bound, auditable, and restricted to necessary functions only.

3.15 PAM-15: Privileged Access Review Cadence

The organization shall review all privileged access assignments at least monthly, validating continued business need, role appropriateness, usage history, and adherence to policy.

3.16 PAM-16: Inheritance & Role Creep Prevention

Controls shall be implemented to prevent privilege accumulation through role inheritance or organizational changes. Users promoted or reassigned shall have previous access reviewed and removed where no longer applicable.

3.17 PAM-17: Non-Repudiation of Privileged Actions

Privileged access systems shall ensure non-repudiation by associating all administrative actions with uniquely attributable credentials, and by disallowing anonymous or shared use of privileged accounts.

3.18 PAM-18: Cloud-Native Privileged Role Governance

The organization shall implement governance controls specific to cloud-native privileged roles, ensuring principle of least privilege, role scoping, and monitoring are enforced natively.

3.19 PAM-19: High-Risk Activity Alerting

The organization shall configure real-time alerts for privileged actions or patterns indicative of misuse, compromise, or insider threat—including privilege escalation, lateral movement, and changes to audit settings.

3.20 PAM-20: Privileged Access Termination Procedures

Upon termination, reassignment, or contract conclusion, privileged access shall be revoked immediately, including account disabling, session termination, credential revocation, and removal from vault access groups.

3.21 PAM-21: Privileged Account Lifecycle Documentation

A complete lifecycle record of each privileged account—including creation, ownership, changes, usage logs, reviews, and decommissioning—shall be maintained for audit and investigation purposes.

Section 4. Multi-Factor Authentication (MFA)

The Multi-Factor Authentication (MFA) control family defines the specific requirements for implementing, enforcing, and maintaining strong authentication mechanisms based on multiple factors—typically something the user knows (knowledge), has (possession), and is (inherence). These controls address MFA strategy, enforcement criteria, authentication factor validation, and the security and usability of the MFA experience. All controls herein are unique to MFA and do not duplicate broader access control or identity governance mechanisms.

4.1 MFA-01: MFA Strategy & Policy

The organization shall develop, document, and maintain a multi-factor authentication (MFA) policy that defines enforcement criteria, approved factors, fallback procedures, and user populations subject to MFA requirements.

4.2 MFA-02: Risk-Based MFA Enforcement

MFA shall be enforced based on risk level, including user role, sensitivity of the accessed resource, location, device context, and time of access. Systems must support risk-adaptive MFA triggers.

4.3 MFA-03: MFA for External Access

All access to organizational systems from external networks—including VPN, remote desktops, cloud platforms, and web applications—shall require MFA regardless of user privilege level.

4.4 MFA-04: MFA for Administrative Access

All privileged and administrative accounts must use MFA for every login session, regardless of network location, including break-glass, cloud console, and local root-level access.

4.5 MFA-05: MFA Factor Diversity

Authentication mechanisms must be based on at least two distinct factor types (knowledge, possession, inherence). Use of two factors from the same category shall not be permitted unless compensating controls are in place and documented.

4.6 MFA-06: Approved MFA Technologies

The organization shall maintain a list of approved MFA technologies (e.g., FIDO2 tokens, TOTP apps, smart cards, biometrics) and shall prohibit use of deprecated or insecure methods such as SMS or email-based OTP unless required by system limitations and explicitly approved.

4.7 MFA-07: MFA Registration Process

MFA registration for new users shall be subject to identity verification, system logging, and administrative oversight. MFA setup processes must verify possession of enrolled factors through a secure channel.

4.8 MFA-08: MFA Enrollment Limitations

Users shall not be permitted to enroll multiple MFA methods without business justification. Each method must be uniquely identifiable and traceable to the user.

4.9 MFA-09: MFA Factor Expiration & Review

The organization shall define expiration periods for certain MFA factors (e.g., certificates, physical tokens), requiring periodic review and renewal of registered devices or methods.

4.10 MFA-10: Secure Storage of MFA Secrets

Secrets used in the generation or validation of MFA (e.g., TOTP seeds, private keys) shall be stored in cryptographically protected, access-controlled environments with appropriate separation of duties.

4.11 MFA-11: Offline MFA Considerations

Where offline access to systems is required, the organization shall implement mechanisms for secure, time-bound use of MFA such as cached one-time codes or hardware-based authenticators with audit logging.

4.12 MFA-12: MFA Fallback & Recovery Procedures

The organization shall implement secure recovery procedures for lost or unavailable factors, requiring secondary identity verification and logging of recovery events for audit review.

4.13 MFA-13: MFA Challenge Logging

Each MFA challenge and response attempt (successful and failed) shall be logged with timestamp, user, source IP, factor used, and device metadata. These logs shall be protected and monitored.

4.14 MFA-14: Device Binding for MFA

Where feasible, MFA systems shall support and enforce device binding (e.g., hardware tokens, biometrics tied to a specific endpoint) to prevent reuse on unauthorized systems.

4.15 MFA-15: Third-Party MFA Integration

When using third-party identity or authentication providers, MFA enforcement shall be verified through contracts, configuration audits, and test assertions. External MFA implementations must meet or exceed organizational requirements.

4.16 MFA-16: Biometric MFA Security

Biometric MFA methods must be locally stored, encrypted, and processed within a secure enclave or equivalent architecture. Biometric data must never be transmitted or stored in centralized databases.

MFA-17: MFA for Federated Logins

Federated authentication methods must enforce MFA before releasing authentication assertions. The organization must verify that external IdPs enforce MFA in alignment with internal policies.

4.17 MFA-18: Time Synchronization for TOTP

All systems supporting Time-Based One-Time Passwords (TOTP) must maintain accurate and synchronized system clocks using authenticated NTP sources to ensure reliable MFA validation.

4.18 MFA-19: MFA Usability & Accessibility

MFA methods must account for users with disabilities, limited device access, or connectivity constraints. The organization shall provide alternative methods that maintain equivalent security assurance.

4.19 MFA-20: Denial of Access Without MFA Completion

Access to systems, services, or applications shall be denied if MFA challenges are not completed successfully. Partial access, limited functionality, or read-only access shall not be granted unless explicitly approved through a documented risk exception.

4.20 MFA-21: Continuous MFA Innovation Review

The organization shall conduct annual reviews of its MFA mechanisms to evaluate emerging threats (e.g., push fatigue attacks, MFA bombing), assess new technologies, and update approved factors accordingly.

Section 5. Credential & Secrets Management (CSM)

The Credential & Secrets Management (CSM) control family defines the organizational requirements for the generation, storage, rotation, distribution, and revocation of digital credentials and secrets, including passwords, API keys, tokens, certificates, and cryptographic material. These controls ensure that authentication artifacts are managed securely across systems, environments, and application layers without duplicating access enforcement or privileged management mechanisms addressed in other families.

5.1 CSM-01: Credential Lifecycle Policy

The organization shall establish a formal policy governing the lifecycle of credentials and secrets, including issuance, rotation, expiration, revocation, and archival, in accordance with security best practices and compliance requirements.

5.2 CSM-02: Secure Credential Generation

All system-generated credentials must be created using cryptographically secure random functions or approved key generation algorithms. Default credentials must be immediately changed upon system deployment.

5.3 CSM-03: Centralized Secrets Management Platform

The organization shall deploy and maintain a centralized secrets management platform capable of secure storage, fine-grained access control, automated rotation, and audit logging for all secrets.

5.4 CSM-04: Secrets Scope Restriction

Each secret shall be scoped to the minimum necessary set of applications, environments, or systems. Secrets must not be reused across environments (e.g., dev/test/prod) or across organizational boundaries.

5.5 CSM-05: Secrets Transmission Protection

All credentials and secrets must be transmitted only over encrypted channels (e.g., TLS 1.2 or higher) and must not be passed via URL parameters, unencrypted headers, or plain-text email.

5.6 CSM-06: Secrets Storage Encryption

All stored secrets and credentials must be encrypted at rest using FIPS-validated or NIST-approved cryptographic algorithms, with keys stored and managed separately using a key management system (KMS).

5.7 CSM-07: Secrets Access Authorization

Access to stored credentials and secrets must be restricted based on least privilege, with access granted only to identities or services that require use for specific, documented operational functions.

5.8 CSM-08: Secrets Rotation Policy

Secrets and credentials must be rotated at regular intervals defined by policy, with immediate rotation required after suspected compromise or upon changes in associated personnel, systems, or integrations.

5.9 CSM-09: Application Secrets Handling

Applications shall be prohibited from hardcoding credentials or secrets within source code, configuration files, container images, or deployment manifests. Secrets must be injected securely at runtime using environment variables or secure API calls.

5.10 CSM-10: Secrets Expiration & Revocation

All secrets shall have defined expiration dates. Expired or deprecated secrets must be automatically invalidated and purged from the management system and dependent systems promptly.

5.11 CSM-11: Logging of Secret Access Events

All access to secrets must be logged with timestamp, calling identity, secret identifier (non-sensitive), and originating system. Logs shall be stored in a tamper-evident format and reviewed regularly.

5.12 CSM-12: Non-Human Secrets Governance

Secrets used by service accounts, automation scripts, CI/CD pipelines, and APIs shall be subject to the same control rigor as human credentials, including unique generation, rotation, and auditing.

5.13 CSM-13: Secrets Sprawl Detection

The organization shall implement tooling or scanning mechanisms to identify secrets accidentally exposed in repositories, logs, containers, or runtime memory. Identified exposures must trigger immediate remediation actions.

5.14 CSM-14: Certificate & Key Pair Governance

The organization shall manage certificates, SSH keys, and asymmetric cryptographic key pairs under a defined lifecycle process that includes issuance, storage, expiration, renewal, and revocation via Certificate Authorities (CAs) or approved tools.

5.15 CSM-15: API Key Management Controls

All API keys shall be generated with scoped permissions, tied to specific systems or users, and managed through a secure issuance, expiration, and rotation process with monitoring for misuse.

5.16 CSM-16: Secrets Injection Assurance

The organization shall verify that secrets injection mechanisms (e.g., sidecar containers, secret stores, secure environment provisioning) are functioning properly in each environment and are not by passable.

5.17 CSM-17: Break-Glass Credential Controls

Emergency-use credentials shall be stored securely, segregated from standard secrets, and governed under additional access controls, including dual authorization, time-based access, and post-use audit requirements.

5.18 CSM-18: Secrets Usage Pattern Monitoring

Systems shall monitor and baseline normal usage patterns for high-sensitivity secrets. Deviations—such as unusual access frequency, geolocation, or source identity—shall trigger alerts or automatic blocking.

5.19 CSM-19: Third-Party Credential Handling

Third-party vendors or external systems granted credentials or secrets must adhere to organization-defined handling and protection requirements. Contracts must stipulate technical and procedural controls for safeguarding credentials.

5.20 CSM-20: Secrets Decommissioning Process

When systems, applications, or integrations are decommissioned, all associated secrets and credentials shall be revoked, scrubbed from memory and storage, and removed from the secrets management platform.

5.21 CSM-21: Segregation of Duties in Secrets Administration

Administrative access to secrets platforms must be separated from access to the systems that consume those secrets. No single individual shall have unrestricted control over both storage and consumption pipelines.

5.22 CSM-22: Developer Education on Secrets Hygiene

Developers shall receive training and documentation on secure secrets handling, including avoidance of common mistakes, such as embedding secrets in code repositories, using shared accounts, or misconfiguring vault access.