Defensible10

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Defensible 10

Annex F (Normative): D06-Identity & Access Security Architecture

Technical Standards

Standards Committee
12-19-2025

About ISAUnited

The Institute of Security Architecture United is the first dedicated Standards Development Organization (SDO) focused exclusively on cybersecurity architecture and engineering through security-by-design. As an international support institute, ISAUnited helps individuals and enterprises unlock the full potential of technology by promoting best practices and fostering innovation in security.

Technology drives progress; security enables it. ISAUnited equips practitioners and organizations across cybersecurity, IT operations, cloud/platform engineering, software development, data/AI, and product/operations with vendor-agnostic standards, education, credentials, and a peer community—turning good practice into engineered, testable outcomes in real environments.

Headquartered in the United States, ISAUnited is committed to promoting a global presence and delivering programs that emphasize collaboration, clarity, and actionable solutions to today's and tomorrow's security challenges. With a focus on security by design, the institute champions the integration of security into every stage of architectural and engineering practice, ensuring robust, resilient, and defensible systems for organizations worldwide.

Disclaimer

ISAUnited publishes the ISAUnited Defensible 10 Standards Technical Guide to provide information and education on security architecture and engineering practices. While efforts have been made to ensure accuracy and reliability, the content is provided “as is,” without any express or implied warranties. This guide is for informational purposes only and does not constitute legal, regulatory, compliance, or professional advice. Consult qualified professionals before making decisions.

Limitation of Liability

ISAUnited - and its authors, contributors, and affiliates - shall not be liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive damages arising from the use of, inability to use, or reliance on this guide, including any errors or omissions.

Operational Safety Notice

Implementing security controls can affect system behavior and availability. First, validate changes in non-production, use change control, and ensure rollback plans are in place.

Third-Party References

This guide may reference third-party frameworks, websites, or resources. ISAUnited does not endorse and is not responsible for the content, products, or services of third parties. Access is at the reader’s own risk.

Use of Normative Terms (“Shall,” “Should,” “Must”)

- Must / Shall: A mandatory requirement for conformance to the standard.
- Must Not / Shall Not: A prohibition; implementations claiming conformance shall not perform the stated action.
- Should: A strong recommendation; valid reasons may exist to deviate in particular circumstances, but the full implications must be understood and documented.

Acceptance of Terms

By using this guide, readers acknowledge and agree to the terms in this disclaimer. If you disagree, refrain from using the information provided.

For more information, please visit our Terms and Conditions page.

License & Use Permissions

The Defensible 10 Standards (D10S) are owned, governed, and maintained by the Institute of Security Architecture United (ISAUnited.org).

Practitioner & Internal Use (Allowed):

- You are free to download, share, and apply this standard for non-commercial use within your organization, departments, or for individual professional, academic, or research purposes.
- Attribution to ISAUnited.org must be maintained.
- You may not modify the document outside of Sub-Standard authorship workflows governed by ISAUnited, excluding the provided Defensible 10 Standards templates and matrices.

Commercial Use (Prohibited Without Permission):

- Commercial entities seeking to embed, integrate, redistribute, automate, or incorporate this standard in software, tooling, managed services, audit products, or commercial training must obtain a Commercial Integration License from ISAUnited.

To request permissions or licensing:
info@isaunited.org

Standards Development & Governance Notice

This standard is one of the ten Parent Standards in the Defensible 10 Standards (D10S) series. Each Parent Standard is governed by ISAUnited's Standards Committee, peer-reviewed by the ISAUnited Technical Fellow Society, and maintained in the Defensible 10 Standards GitHub repository for transparency and version control.

Contributions & Collaboration

ISAUnited maintains a public GitHub repository for standards development. Practitioners may view and clone materials, but contributions require:

- ISAUnited registration and vetting
- Approved Contributor ID
- Valid GitHub username

All Sub-Standard contributions must follow the Defensible Standards Submission Schema (D-SSF) and are peer-reviewed by the Technical Fellow Society during the annual Open Season.

Obsolete and withdrawn documents should not be used; please use replacements.

Abstract

The ISAUnited Defensible 10 Standards provide a structured, engineering-grade framework for implementing robust and measurable cybersecurity architecture and engineering practices. The guide outlines the frameworks, principles, methods, and technical specifications required to design, build, verify, and operate reliable systems.

Developed under the ISAUnited methodology, the standards align with modern enterprise realities and integrate Security by Design, continuous technical validation, and resilience-based engineering to address emerging threats. The guide is written for security architects and engineers, IT and platform practitioners, software and product teams, governance and risk professionals, and technical decision-makers seeking a defensible approach that is testable, auditable, and scalable.

This document includes a series of Practitioner Guidance, Cybersecurity Students & Early-Career Guidance, and Quick Win Playbook callouts.

Practitioner Guidance- Actionable steps and patterns to apply the technical standards in real environments.

Cybersecurity Student & Early-Career Guidance- Compact, hands-on activities that turn each section's ideas into a small, verifiable artifact.

Quick Win Playbook- Immediate, evidence-driven actions that improve posture now while reinforcing good engineering discipline.

Together, these elements help organizations translate intent into engineered outcomes and sustain long-term protection and operational integrity.

Foreword

Message from ISAUnited Leadership

Cybersecurity is at a turning point. As digital systems scale, reactive and checklist-driven practices do not keep pace with adversaries. The ISAUnited position is clear: security must be practiced as engineered design, grounded in scientific principles, structured methods, and defensible evidence. Our mission is to professionalize cybersecurity architecture and engineering with standards that are actionable, testable, and auditable.

ISAUnited Defensible 10 Standards: First Edition is a practical framework for that shift. The standards in this book are not theoretical. They translate intent into measurable specifications, controls, and verification, and enable teams to design and operate resilient systems at enterprise scale.

About This First Edition

This edition publishes 10 Parent Standards, one for each core domain of security architecture and engineering. Sub-standards will follow in subsequent editions, contributed by ISAUnited members and reviewed by our Technical Fellow Society, to provide focused, technology-aligned detail. Adopting the Parent Standards now positions organizations for seamless integration of Sub Standards as they are released on the ISAUnited annual update cycle.

Why “Defensible Standards”

Defensible means the work can withstand technical, operational, and adversarial scrutiny. These standards are designed to be demonstrated with evidence, featuring clear architecture, measurable specifications, and verification, so that practitioners can confidently stand behind their designs.

Contents

Annex F (Normative): Identity & Access Security Architecture

ISAUnited's Defensible 10 Standards
Parent Standard: D06-Identity & Access Security Architecture
Document: ISAU-DS-IAM-1000
Last Revision Date: December 2025
Peer-Reviewed By: ISAUnited Technical Fellow Society
Approved By: ISAUnited Standards Committee

Section 1. Standard Introduction

The Identity & Access Security Architecture Parent Standard (ISAU-DS-IAM-1000) defines the technical identity plane that secures enterprise infrastructure across on-premises, cloud, and hybrid environments. It specifies how core identity components—enterprise Identity Providers (IdPs), directories, federation gateways, token services, Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), privileged access boundaries, and telemetry pipelines—are designed and integrated into a defensible architecture. Identity is established within clear trust boundaries: authentication and token lifecycle management are enforced by hardened services; well-structured RBAC/ABAC models govern authorization; privileged actions are confined to scoped, time-bounded elevations using Privileged Access Management (PAM) with Just-in-Time (JIT) elevation and Privileged Session Monitoring (PSM). No fail-open behaviors are permitted in authentication, token issuance, or enforcement paths.

The architecture emphasizes authenticated-by-default entry points, protocol-conformant federation (SAML 2.0, OAuth 2.0, OpenID Connect), cryptographically secure token handling, device trust and posture validation before session creation, and continuous identity-centric monitoring via Identity Threat Detection & Response (ITDR). It extends to Service & Machine Identities—service accounts, machine workloads, APIs, and bots—through unique identity objects, credential vaulting and automated rotation, mutual TLS (mTLS), and signed token exchanges, keeping these identities governed, auditable, and traceable.

As a Parent Standard, ISAU-DS-IAM-1000 establishes core architectural expectations and invariants that downstream sub-standards operationalize through controls-as-code, test specifications, and evidence artifacts. Delivery teams use it to design identity trust zones, place PDPs/PEPs, rigorously route authentication and token flows, and instrument the identity plane for continuous Verification & Validation (V&V).

Objective

Define a rigorous, Zero-Trust-aligned identity and access security architecture that:

1. Establishes explicit identity trust boundaries and standardizes authentication and token flows across all human and machine entry points.
2. Enforces strong (including passwordless) authentication and context-aware authorization using RBAC/ABAC, with least-privilege demonstrated as a measurable outcome in V&V.
3. Constrains and monitors privileged activities via PAM, implementing JIT elevation and PSM for Tier-0 actions, with deny-by-default enforcement.
4. Secures Service & Machine Identities with unique objects, credential vaulting and rotation, mTLS, and signed token exchanges, validated through repeatable tests.

5. Provides resilience for identity services (IdP, federation, directories, token services, PAM/IGA) through high-availability topologies, protected keys, documented rotation/recovery, and validated failover—no fail-open.
6. Produces audit-ready, immutable identity logs, session traces, and policy-as-code histories to support independent verification, incident forensics, and evidence production.

These objectives map to the Requirements (Section 5) and Technical Specifications (Section 6) and are validated in Section 12 through adversary-aware testing of identity flows and privileged pathways.

Justification

In modern distributed enterprise environments, identity is the control plane that governs access between users, services, and data. Network-centric controls alone are insufficient as applications, APIs, automation, and administrative access originate from diverse locations and devices. Common breach paths—credential theft, privilege escalation, unmanaged service accounts, token replay, and federation misconfigurations—exploit architectural weaknesses in identity flows and trust boundaries.

A policy-only approach is inadequate; the identity and access security architecture must be engineered as a hardened plane with:

- Clear trust zoning for where authentication occurs, where tokens are minted, and where authorization decisions are enforced.
- Standards-based federation and token lifecycle controls (issuance, rotation, audience/issuer validation, replay protections).
- Robust privileged boundary design (JIT elevation, session recording, scoped command/action allow-lists).
- Service & Machine Identity governance (unique identities, vaulting, scheduled rotation, certificate-based mutual trust).
- Resilience engineering for critical key material and identity services—explicitly eliminating fail-open behaviors.
- Comprehensive telemetry and ITDR to surface anomalous identity use and support rapid, defensible response.

This Parent Standard closes the gap between “IAM as processes” and Identity & Access Security Architecture as a measurable, testable, auditable technical plane. It provides the blueprint for delivery teams to unify authentication, authorization, privileged access, federation, and identity telemetry into a cohesive, resilient, Zero-Trust-aligned infrastructure.

Section 2. Definitions

These definitions ensure consistent interpretation within this Parent Standard (ISAU-DS-IAM-1000) and its IAM sub-standards. Terms are framed for architecture and infrastructure design, not policy operations.

Access Token / Refresh Token / ID Token — Short-lived bearer or proof-of-possession artifacts conveying authorization (access), renewal capability (refresh), or authentication claims (ID), bound to audience, issuer, scopes, and expiry.

Attribute-Based Access Control (ABAC) — An authorization model that evaluates attributes (user, resource, action, and context, such as device posture, location, time) for dynamic, context-aware decisions.

Authentication Assurance Level (AAL) — Strength of an authentication event as defined by assurance criteria (AAL 2 minimum for privileged/admin; AAL 3 preferred where feasible).

Claims — Signed identity and authorization attributes carried in assertions or tokens (for example, subject, issuer, audience, scopes, assurance level, device posture).

Claim Propagation — Preservation and forwarding of required claims across service hops so downstream enforcement can maintain continuous authorization context; stripping or injection is treated as an invalid request.

Clock Skew — Permitted time difference between systems used when validating token timestamps; skew bounds must be defined and enforced.

Conditional Access — Policy-driven access evaluation using context (device posture, location, risk signals) to require step-up authentication, restrict sessions, or deny access.

Credential Vault — A hardened store for secrets, keys, and certificates with controlled retrieval, auditing, automated rotation, and just-in-time issuance.

Device Trust / Posture Validation — Evaluation of device compliance (OS, patch, EDR, disk encryption, jailbreak/root status) as a precondition for session establishment or privilege activation.

Directory — The attribute and entitlement store (for example, users, groups, service principals) synchronized with the IdP and used by PDPs/PEPs for authorization decisions.

Federation Gateway — The boundary service that brokers trust between identity domains (internal, partner, SaaS), translating and validating assertions across SAML 2.0, OAuth 2.0, and OpenID Connect.

Federation Metadata — Signed configuration describing federation endpoints, keys, entity identifiers, and protocol settings used to establish trust between parties.

High Availability (HA) — Redundant architecture that maintains identity services during component failure.

Identity Governance and Administration (IGA) — Lifecycle governance for identities and entitlements, including provisioning/de-provisioning, access review, certification, and role or entitlement management.

Identity Plane — The set of components that establish and enforce identity trust: Identity Providers (IdPs), directories, federation gateways, Security Token Services (STS), PDPs/PEPs, PAM/JIT/PSM controls, and identity telemetry.

Identity Provider (IdP) — The authoritative authentication service that verifies identities and issues tokens and claims for relying applications and services.

Identity Threat Detection & Response (ITDR) — Detection, investigation, and automated containment of identity-centric threats (credential theft, account takeover, privilege escalation, anomalous SSO or token usage).

Immutable Log Store — Tamper-resistant, time-synchronized storage for identity events, privileged session traces, and enforcement decisions used for V&V and forensics.

Just-in-Time (JIT) Elevation — Time-bounded privilege activation granted on approved request and automatically revoked on task completion or timeout.

Mean Time to Detect (MTTD) / Mean Time to Respond (MTTR) — Time to detect an identity compromise and time to contain or remediate it, measured against defined objectives.

Multi-Factor Authentication (MFA) — Authentication requiring two or more factors (something you know, have, are); includes phishing-resistant methods (for example, FIDO2, smart cards).

Mutual TLS (mTLS) — Certificate-based, bidirectional authentication between services; often combined with signed tokens for defense in depth.

OAuth 2.0 / OpenID Connect (OIDC) / SAML 2.0 — Open protocols for delegated authorization and federated authentication. OIDC provides an identity layer on OAuth 2.0; SAML 2.0 provides assertion-based federation.

Policy Decision Point (PDP) — The component that evaluates access requests against policies (RBAC/ABAC, conditional access) and renders allow/deny decisions.

Policy Enforcement Point (PEP) — The component on the request path that enforces PDP decisions (for example, an API gateway, proxy, application middleware, or an admission controller).

Privileged Access Management (PAM) — Controls and services that constrain, broker, and monitor high-risk operations and administrative access.

Privileged Session Monitoring (PSM) — Recording and inspection of privileged activity (commands, screens, API calls) with searchable, timestamped evidence.

Proof-of-Possession (PoP) / Demonstration of Proof-of-Possession (DPoP) — Mechanisms that bind a token to a client-held key to reduce replay; DPoP is an OAuth-based PoP method using signed proof.

Recovery Time Objective (RTO) / Recovery Point Objective (RPO) — Target time to restore service after failure (RTO) and acceptable data loss window (RPO).

Risk-Based Authentication (RBA) — Adaptive authentication that steps up, blocks, or limits access based on assessed risk (device posture, geo-velocity, behavior anomalies).

Role-Based Access Control (RBAC) — Authorization model that maps permissions to roles and roles to principals for predictable, static entitlements.

Security Token Service (STS) — A hardened service that issues, validates, and exchanges tokens (access, refresh, ID) with defined lifetimes, audiences, and claims.

Separation of Duties (SoD) — Governance constraint ensuring no single actor can request, approve, and execute privileged access or policy changes end-to-end.

Service Account Governance — Lifecycle controls for non-human identities: unique accounts, least privilege, vaulting and rotation of credentials, activity monitoring, and revocation.

Service & Machine Identities — Non-human identities (service accounts, workloads, APIs, bots) with unique principals, scoped entitlements, and governed credentials.

Single Sign-On (SSO) — Centralized authentication flow allowing principals to access multiple applications via federated trust with the IdP.

System for Cross-domain Identity Management (SCIM) — Standard protocol for automated provisioning and de-provisioning between IdPs/directories and relying applications.

Tier-0 — Highest-sensitivity identity scope (for example, IdP, directory, federation, key services) requiring AAL 2+ authentication, JIT elevation, and full PSM.

Token Replay Protection — Mechanisms that prevent token reuse (for example, nonces, PoP/DPoP, rotating refresh tokens, strict audience/issuer validation, short TTLs).

Section 3. Scope

Identity & Access Security Architecture defines the engineered identity plane for enterprise systems: how authentication, authorization, and privileged boundaries are designed, integrated, and enforced across on-premises, cloud, and hybrid environments. This scope covers the placement and hardening of Identity Providers (IdPs), directories, federation gateways, Security Token Services (STS), Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), privileged access controls, and identity telemetry needed to produce measurable, auditable outcomes. The focus is on architectural and infrastructure components, not on policy administration.

Applicability

- **Identity types:** Human users and Service & Machine Identities (service accounts, workloads, APIs, bots) that authenticate and request authorization.
- **Enterprise and academic environments:** Security architects, engineers, and platform owners building and operating identity trust boundaries.
- **Hybrid and multi-platform:** First-party data centers, public cloud, SaaS, and partner domains requiring federation and consistent enforcement.

Key Focus Areas

- **Identity governance and lifecycle:** Single source of truth for identities and entitlements; automated provisioning and de-provisioning (prefer System for Cross-domain Identity Management (SCIM)); orphaned account detection;

periodic access certifications supplying attributes for RBAC/ABAC evaluation at PDPs.

- **Authentication and authorization:** Phishing-resistant MFA; Authentication Assurance Level (AAL) 2 minimum (AAL 3 preferred) for privileged access; risk-adaptive controls; centralized decisions at PDPs with in-path enforcement at PEPs; re-authentication on elevation.
- **Identity context propagation:** PEPs preserve and forward required subject attributes and claims (for example, subject ID, assurance level, device posture, scopes) so downstream services maintain continuous authorization; claim stripping, injection, or downgrade is denied and logged.
- **Privileged access boundaries:** PAM with JIT elevation and PSM for Tier-0 operations; command and action allow-lists as code; break-glass that is time-boxed and audited with immediate post-use rotation.
- **Federation and SSO:** Standards-conformant SAML 2.0, OAuth 2.0, OpenID Connect; assertion and token validation for audience, issuer, signature, and age; device-posture-bound SSO with step-up or revoke on posture change.
- **Token security**: STS issuing short-lived tokens; rotating refresh tokens; anti-replay controls such as nonces and proof-of-possession (PoP/DPoP) where feasible; documented clock-skew handling; strict audience and issuer validation.
- **Service & Machine Identity security:** Unique principals, scoped entitlements, credential vaulting with automated rotation, certificate-based mutual authentication (mTLS), and signed token exchanges.
- **Identity Threat Detection & Response (ITDR):** End-to-end identity telemetry, IdP and STS events, PDP decisions, PEP outcomes, PSM replays—normalized into SIEM; automated containment that can disable identities, revoke tokens, and terminate sessions.
- **Resilience and recovery:** High-availability topologies for IdP, federation, directories, STS, PAM, and PDP/PEP paths; HSM-protected keys with rotation, escrow, and recovery drills; no fail-open in authentication, token, or enforcement paths; quarterly failover tests with evidence.
- **Evidence and auditability:** Centralized, tamper-resistant, hash-verified immutable log store for identity events, token traces, PDP decisions, PEP outcomes, and privileged session artifacts that support V&V and forensics.

Outcomes

Architectures conforming to this standard are:

- **Defensible:** Explicit trust boundaries, centralized decisions, deny-by-default enforcement, and no fail-open behaviors.
- **Measurable:** Quantified objectives (AAL targets, token TTLs, JIT windows, idle timeouts, MTTD, and MTTR) evidenced in immutable telemetry and replayable sessions.

- **Adaptive:** Context-aware controls (device posture and behavioral baselines) and protocol-conformant federation that evolve without redesign.
- **Aligned:** Consistent with enterprise objectives and risk posture, and ready for Verification and Validation as defined in Section 12.

This scope establishes the architectural boundaries and enforcement responsibilities of the identity plane—what is in, what is out, and how components interact to produce defensible outcomes. It anchors the inputs in Section 5 and the technical outputs in Section 6, and it establishes the evidence expectations verified in Section 12.

Section 4. Use Case

This use case demonstrates how Identity & Access Security Architecture eliminates credential-driven attack paths by redesigning the identity plane—not merely adding policies. It highlights explicit trust boundaries, centralized decisions at PDPs, in-path enforcement at PEPs, short-lived tokens from an STS, deny-by-default privileged boundaries (PAM with JIT/PSM), device-posture-bound SSO, and immutable evidence to support Verification & Validation.

Table F-1:

Use Case Name	**Securing Enterprise Identities and Privileged Access Against Credential Theft**
Objective	Eliminate standing admin privileges, prevent credential theft/replay, and improve identity threat detection via Zero-Trust enforcement, PAM (JIT/PSM), risk-adaptive authentication, centralized PDP/PEP control, and short-lived tokens from an STS—using open, vendor-neutral standards and policy-as-code.
Scenario	A global manufacturer across cloud and on-premises suffers repeated credential-based intrusions that bypass perimeter controls. Audits reveal shared admin accounts, password-only authentication for privileged users, inconsistent federation validation, and no centralized identity governance, resulting in excessive entitlements and uneven enforcement.
Actors	IAM Architect; Security Engineer; Identity Governance Administrator; Privileged Access Administrator; SOC Analysts; Cloud Security Engineer.
Challenges Identified	• Persistent privilege (standing admin rights)

	• Weak authentication for Tier-0 • Credential sprawl and stale secrets across AD and cloud IdPs • Federation drift (audience/issuer/age not consistently validated) • Limited real-time visibility into anomalous auth/privilege events
Technical Solution	Zero-Trust Identity Enforcement: MFA (phishing-resistant for Tier-0); passwordless where feasible; AAL 2 minimum, AAL 3 preferred; device-posture-bound SSO with step-up or revoke on posture change. Centralized Decisions & Enforcement: Policies as code at PDPs—RBAC/ABAC expressed in open standards or open policy languages such as XACML or OPA/Rego; in-path PEPs (API gateways, open-source proxies, or admission controllers) enforce. Required subject claims (ID, assurance level, device posture, scopes) are propagated; claim stripping/injection is denied and logged. Token Security (STS): Short-lived access tokens; rotating refresh tokens; strict audience/issuer/signature and clock-skew handling; proof-of-possession (PoP/DPoP) where feasible; no fail-open on issuance/validation. Controls use open, vendor-neutral protocols (OAuth 2.0, OIDC, SAML 2.0). Privileged Access Management (PAM): Replace standing rights with JIT elevation (dual-control approval for Tier-0); auto-revoke on completion/timeout; PSM records privileged activity; command/action allow-lists managed as code and tested in CI. Identity Governance & Administration (IGA): Centralize lifecycle with automated provisioning/de-provisioning (prefer SCIM, an open standard); quarterly access certifications; orphaned account detection with 24-hour remediation; unique Service & Machine Identities; secrets/keys/certs vaulted and rotated. Identity Threat Detection & Response (ITDR): Normalize IdP/STS/PDP/PEP/PSM telemetry in the SIEM; detect impossible travel, refresh token abuse, abnormal consent grants, and federation trust drift; automate containment (disable identities, revoke tokens, terminate sessions). All telemetry and decision trails are written to tamper-resistant, hash-verified, immutable repositories for audit, verification and validation (V&V).
Expected Outcome (targets)	• 100 % Tier-0 actions require approved JIT; elevation ≤ 60 minutes unless approved exception • ≥ 95 % reduction in successful privileged logons without MFA • 100 % critical apps validate audience/issuer/signature and token age • MTTD ≤ 15 minutes; MTTR ≤ 60 minutes with automated containment • Access certification closure ≤ 30 days; orphaned/admin-equivalent accounts remediated ≤ 24 hours; rotation SLOs met • Privileged access certifications and PAM audit artifacts align with CIS Control 6.8 and CSA CCM IAM-14/15/16 (measured via evidence packs).
Evidence for V&V	Immutable evidence repositories containing: PDP policy-as-code with approvals; PEP enforcement logs with decision IDs; STS token traces (TTL, audience/issuer) and negative-test denials; DPoP/PoP proofs where implemented; PAM JIT requests (dual-control) and PSM replays linked via correlation IDs; SCIM provisioning logs; access certification reports; vault rotation logs; retention/hash manifests; incident timelines showing automated containment.

Key Takeaways

Obsolete and withdrawn documents should not be used; please use replacements.

- Treat identity as an engineered plane: centralize decisions at PDPs, enforce at in-path PEPs, and prohibit fail-open in auth, token, or enforcement paths.
- Replace standing privilege with PAM + JIT elevation and full PSM on Tier-0; make least privilege measurable (elevation windows, idle timeouts, approval trails).
- Issue short-lived tokens from an STS; validate audience/issuer/signature and clock skew; prefer PoP/DPoP for high-risk APIs.
- Bind SSO to device posture and re-evaluate on posture change; use phishing-resistant MFA with AAL2 minimum for privileged access (AAL3 preferred).
- Govern Service & Machine Identities with unique principals, vaulting, automated rotation, and mTLS or signed tokens for service-to-service calls.
- Normalize IdP/STS/PDP/PEP/PSM telemetry in SIEM and automate containment; target MTTD ≤ 15 minutes and MTTR ≤ 60 minutes.
- Store all evidence (logs, policies, certifications, session replays) in tamper-resistant, hash-verified, immutable repositories to support V&V and audit.

Practitioner Guidance:

- Map entry points and trust boundaries first, then place PDPs and PEPs; document token flows and elevation paths before changing controls.
- Express RBAC/ABAC as policy-as-code using open standards or open policy languages (for example, XACML, OPA/Rego); validate in CI and promote via controlled pipelines.
- Prefer open, vendor-neutral protocols (OAuth 2.0, OIDC, SAML 2.0; System for Cross-domain Identity Management (SCIM) for provisioning); avoid proprietary appliances—use API gateways, open-source proxies, or admission controllers.
- Make privileged boundaries real: dual-control JIT for Tier-0, PSM required, command/action allow-lists as code, immediate post-use rotation.
- Propagate required claims (subject, assurance level, device posture, scopes) across microservices; deny and log any claim stripping or injection.
- Define evidence up front: for each control, specify the artifact, its immutable-store location, and the success metric (for example, token TTLs, JIT window, certification SLA).
- Anchor outcomes to frameworks rather than products: measure against CIS Control 6.8 and CSA CCM IAM-14/15/16, and record results as Evidence Pack IDs.
- Use phishing-resistant MFA and set Authentication Assurance Level (AAL) 2 minimum (AAL 3 preferred) for privileged access; re-authenticate on elevation and bind SSO to device posture with step-up or revoke on posture change.
- For high-risk APIs, enable proof-of-possession (PoP/DPoP) and run negative tests (replay, wrong audience/issuer, over-TTL) as pipeline gates.

Section 5. Requirements (Inputs)

To implement an Identity & Access Security Architecture, the following baseline architectural and environmental conditions must be met. These inputs enable the defensibility and enforceability of the Technical Specifications (§6) and subsequent sub-standards.

5.1 Centralized Identity Provider (IdP) Integration
An enterprise IdP is established and federates identities across on-premises, cloud, and SaaS using open, secure protocols (SAML 2.0, OAuth 2.0, OpenID Connect).

5.2 Multi-Factor Authentication (MFA) & Authentication Assurance
All privileged/administrative accounts are MFA-enabled, supporting phishing-resistant methods (e.g., FIDO2, smart cards). Tier-0 access meets Authentication Assurance Level (AAL) 2 minimum; AAL 3 preferred where feasible. Adaptive/risk-based challenges are supported.

5.3 Privileged Access Management (PAM)
A PAM platform brokers privileged access with Just-in-Time (JIT) elevation, Privileged Session Monitoring (PSM), command/action allow-lists, dual-control approval for Tier-0, and automatic revocation on task completion or timeout.

5.4 Identity Governance & Administration (IGA)
Automated provisioning/de-provisioning (prefer SCIM), role/entitlement management, periodic access certifications, and orphaned account detection for all human and Service & Machine Identities.

5.5 Identity Threat Detection & Response (ITDR)
Security monitoring ingests identity telemetry (IdP/STS, PDP decisions, PEP enforcement, PSM events), correlates it in the SIEM, and detects anomalous identity activity, with automated containment available.

5.6 Device Trust Validation
Conditional access evaluates device posture (compliance, EDR, encryption, jailbreak/root) before session creation and at elevation.

5.7 Audit-Ready Logging Infrastructure
Identity events, authentication attempts, token issuance/validation, authorization decisions, and access changes are centrally logged with retention aligned to policy and legal requirements.

5.8 Service & Machine Identity Governance

All non-human identities (service accounts, workloads, APIs, bots, CI/CD) are uniquely identifiable, inventoried, and scoped to least privilege; credentials (secrets, keys, tokens, certificates) are vaulted, rotated, and monitored. mTLS and/or signed token exchanges are enforced for service-to-service calls where feasible.

5.9 Separation of Duties (SoD) for IAM Administration
Distinct roles perform design, enforcement, and approval/review. No individual may propose and approve the same privilege grant or policy change. JIT elevation requires dual control with auditable trails.

5.10 IAM Availability Objectives
Target RTO/RPO for identity services (IdP, federation, directory, PAM, IGA) are defined and tested at least quarterly. Key material (signing/encryption) and configuration state are backed up, protected (e.g., via an HSM), and recoverable in accordance with stated objectives.

Additional Architectural Prerequisites (supporting §6)

5.11 Security Token Service (STS)
A hardened STS issues, validates, and exchanges short-lived access/refresh/ID tokens with strict audience/issuer/signature checks, rotating refresh tokens, documented clock-skew handling, and no fail-open on issuance or validation. Proof-of-possession (PoP/DPoP) is supported for high-risk APIs where feasible.

5.12 Policy Decision/Enforcement Placement (PDP/PEP)
Locations of Policy Decision Points (PDPs) and in-path Policy Enforcement Points (PEPs) are documented for every entry point/trust boundary (human and machine). Authorization policies are expressed as policy-as-code (for example, XACML or OPA/Rego); PEPs must enforce PDP decisions on the request path.

5.13 Protocol Conformance & Time Synchronization
Federation paths pass SAML 2.0/OAuth 2.0/OIDC interoperability and negative tests. All identity services are time-synchronized (NTP) to maintain token validity windows.

5.14 Immutable Evidence Repositories
All identity-relevant artifacts—logs, token traces, PDP decisions, PEP outcomes, PSM replays, policy-as-code, certification reports, rotation logs—are stored in tamper-resistant, hash-verified, immutable repositories for audit and V&V.

Practitioner Guidance:

Unify identity under the enterprise IdP and IGA first; then close gaps in federation, provisioning, device posture, PAM/JIT/PSM, and centralized telemetry before layering advanced controls. Confirm AAL targets, STS short-lived tokens, PDP/PEP placement, and immutable evidence are operational. If any prerequisite is missing or non-functional, downstream specifications in §6 will not be defensible, measurable, or auditable.

Section 6. Technical Specifications (Outputs)

Technical specifications define the concrete, defensible outputs that must be implemented to satisfy this standard. Each output is a required engineering area that transforms policy into measurable, actionable security outcomes. Together, these specifications establish a resilient foundation for identity and access security across on-premises, cloud, and hybrid environments.

Outputs must be:

- **Measurable:** validated by scans, logs, audits, or tests
- **Actionable:** implementation-ready, not policy slogans
- **Aligned:** traceable to §5 Requirements and sub-standards

6.1 Identity Governance & Lifecycle Management

- **Automated provisioning and de-provisioning:** Implement centralized lifecycle automation for all human and Service & Machine Identities; prefer System for Cross-domain Identity Management (SCIM) where supported.
- **Periodic access certifications:** Run automated access reviews at least quarterly to confirm role assignments, enforce least privilege, and detect privilege creep; Tier-0 entitlements recertified ≤ 14 days.
- **Orphaned account detection:** Continuously detect inactive or unlinked accounts (including non-interactive) and remove them within 24 hours.
- **Delegated administration controls:** Enforce granular, least-privilege delegation; document delegated scopes.
- **Centralized identity repository:** Maintain a single source of truth for attributes and entitlements synchronized to PDPs for RBAC/ABAC evaluation.
- Access review SLAs: Access certification closure ≤ 30 days; orphaned/non-interactive remediation ≤ 24 hours.

6.2 Authentication & Authorization Security

- **Multi-Factor Authentication (MFA):** Enforce MFA for privileged, administrative, and high-risk accounts; support phishing-resistant methods (FIDO2, smart cards) and passwordless where feasible.
- **Risk-based adaptive authentication:** Adjust requirements using context (device posture, geo-velocity, behavior baselines); step-up or deny at elevated risk.
- **RBAC/ABAC via PDP/PEP:** Express authorization policies as code (for example, XACML or OPA/Rego). PDPs render decisions; in-path PEPs (API gateways, open-source proxies, and admission controllers) enforce them.
- **Session management controls:** Re-authenticate on elevation; terminate inactive or suspicious sessions; privileged idle timeout ≤ 15 minutes.
- **Delegated authorization protocols:** Standardize on OAuth 2.0, OpenID Connect, and SAML 2.0 for federated authorization.
- **Authentication assurance & privileged session boundaries:** Enforce Authentication Assurance Level (AAL) 2 minimum (AAL 3 preferred) for privileged/admin access. Bind sessions to device posture; re-evaluate posture on materially changed conditions.
- **Token protections:** Access token TTL ≤ 60 minutes; rotate refresh tokens on use; validate audience/issuer/signature; document allowed clock-skew; support proof-of-possession (PoP/DPoP) for high-risk APIs; strictly prohibit fail-open on token issuance/validation.

6.3 Privileged Access Management (PAM)

- **Just-in-Time (JIT) access:** Provision privileged rights only when required; auto-revoke on completion/timeout; dual-control approval for Tier-0.
- **Privileged Session Monitoring (PSM):** Record privileged activity (commands/screens/API calls) with searchable, timestamped logs; index with correlation IDs.
- **Command and action filtering:** Maintain allow/deny lists as code; validate in CI before deployment.
- **Break-glass procedures:** Time-boxed, auditable emergency access; immediate post-use credential rotation and session review.
- **Privileged credential vaulting:** Store credentials in a vault with automated rotation and access logging; prefer short-lived, STS-issued credentials for retrieval-less flows.
- **Elevation limits & Tier-0 recording:** JIT elevation duration ≤ 60 minutes unless approved exception; PSM required for all Tier-0 actions.

6.4 Federated Identity & Single Sign-On (SSO)

- **Federation protocol compliance:** Enforce SAML 2.0, OAuth 2.0, OIDC; perform interoperability and negative tests for each federation path.
- **Centralized authentication:** Require authentication via approved, monitored IdPs/STS; log assertion/token details to the immutable evidence store.
- **Cross-domain trust validation:** Validate audience, issuer, signature, token age; reject tokens outside allowed skew or with claim anomalies.

Obsolete and withdrawn documents should not be used; please use replacements.

- **Device posture checks for SSO:** Bind SSO to device posture; trigger step-up or revoke on posture change.
- **SSO session auditing:** Detect impossible travel, token substitution/replay, anomalous consent grants.
- **Token security & replay protections:** Access token TTL ≤ 60 minutes; rotate refresh tokens on use; enforce audience/issuer validation; support PoP/DPoP where feasible; no fail-open.

6.5 Identity Threat Detection & Response (ITDR)

- **Anomaly detection:** Model credential theft, privilege escalation, refresh-token abuse, abnormal consent grants, and federation trust drift using behavioral analytics.
- **Identity event logging:** Log all authentication attempts, access grants/denials, privilege escalations, PDP decisions, and PEP enforcement outcomes to a tamper-resistant, hash-verified immutable repository.
- **Correlation with SIEM:** Normalize IdP/STS/PDP/PEP/PSM telemetry and correlate with infrastructure/application signals for cross-domain detection.
- **Automated containment:** On high-risk events, disable identities, revoke tokens (including refresh), terminate sessions, and force step-up challenges.
- **Post-incident forensics:** Retain PSM replays, token traces, and decision trails; support replayable timelines.
- **Response objectives:** Identity-compromise MTTD ≤ 15 minutes; MTTR ≤ 60 minutes with automated containment.

6.6 Identity Service Resilience & Recovery

- **High-availability topologies:** Deploy IdP, federation gateways, directories, PAM/IGA, STS, and PDP/PEP paths in redundant, multi-AZ/clustered configurations with quorum and health checks.
- **Key & token continuity:** Protect signing/encryption keys in HSM or equivalent; document rotation, escrow, and recovery; ensure token issuance continues during node loss; fail-open is prohibited.
- **RTO/RPO targets:** Meet or exceed §5.10 (for example, IdP RTO ≤ 30 minutes, RPO ≤ 15 minutes).
- **Failover & DR testing:** Conduct at least quarterly controlled failovers; demonstrate uninterrupted authentication flows and policy enforcement during/after failover, and that no auth/token/enforcement path fails open.
- **Operational runbooks:** Maintain runbooks for component failure, region loss, key rotation/recovery, token revocation at scale, and rollback; assign owners and update cadence.

Practitioner Guidance:

- Start with a baseline architecture map: entry points, trust boundaries, PDP/PEP locations, token flows, elevation paths, and device-posture gates.

	• Express RBAC/ABAC as policy-as-code (for example, XACML or OPA/Rego); validate in CI; deploy via controlled pipelines with approvals. • Prefer open, vendor-neutral protocols (OAuth 2.0, OIDC, SAML 2.0; SCIM for provisioning); avoid proprietary appliances—use API gateways, open-source proxies, or admission controllers. • Make privileged boundaries concrete: dual-control JIT, PSM required for Tier-0, allow-lists as code, immediate post-use rotation. • Define evidence up front: for each specification, name the artifact, target metric (TTL, AAL, JIT window, idle timeout, MTTD/MTTR), and where it lives in the immutable repository.

	**Quick Win Playbook**: **Title:** Replace Standing Admin with Dual-Control JIT + Full PSM on One Tier-0 Path **Objectives** 1. Eliminate standing privileged access on a single Tier-0 admin path. 2. Require dual-control Just-in-Time (JIT) elevation for every privileged action. 3. Capture 100 % of Tier-0 sessions with Privileged Session Monitoring (PSM). 4. Enforce command/action allowlists as code; deny and alert on out-of-scope commands. 5. Produce immutable evidence suitable for V&V under Evidence Pack EP-06.01. **Target:** Replace standing admin rights with dual-control JIT and full PSM for Tier-0; enforce command/action allow-lists as code (§6.2, §6.3). **Component/System:** PAM platform; PEP-enforced admin channels; credential vault. **Protects:** Privileged operations from persistent privilege, misuse, and untracked activity. **Stops/Detects:** Unauthorized elevation, unapproved commands, unrecorded emergency access. **Action:** Remove standing admin; require dual-control JIT for Tier-0; mandate PSM on all Tier-0 sessions; deploy allowlists via a CI-validated policy bundle; rotate credentials immediately after use. **Test**: non-JIT elevation = deny; approved JIT = allow + record; disallowed command = deny + alert. **Proof:** PAM policy-as-code commit/diff + approved JIT tickets + PSM recording excerpt + allow-list CI report + rotation logs → Evidence Pack EP-06.01.

	Metric: 100 % Tier-0 actions via approved JIT; elevation ≤ 60 minutes; 100 % Tier-0 sessions recorded; unauthorized command attempts result in deny + alert = 100 %. **Rollback:** Reinstate prior role bindings only under a time-bounded exception; archive superseded artifacts in EP-06.03 (indexed from EP-06.00).

Section 7. Cybersecurity Core Principles

The following ISAUnited Cybersecurity Core Principles anchor the design and operation of the identity plane. They guide how trust boundaries are defined, how decisions are centralized at PDPs and enforced at PEPs, how tokens are issued and validated, and how privileged boundaries are engineered and verified.

Purpose and Function

Principles in this Parent Standard are engineering constraints, not slogans. They ensure the Technical Specifications in §6 are implemented as measurable, testable behaviors that withstand real-world identity threats.

Table F-2. Principles and IAM-Domain Applicability:

Principle Name	Code	Applicability to Identity & Access Security Architecture
Least Privilege	ISAU-RP-01	Scope entitlements to the minimum required; replace standing admin with JIT elevation; enforce command/action allow-lists as code; attest with PDP decisions and PSM evidence.
Zero Trust	ISAU-RP-02	Continuously verify human and Service & Machine Identities; bind SSO to device posture; re-challenge on risk; do not infer trust from network location.
Complete Mediation	ISAU-RP-03	Every request is evaluated by PDP policies (RBAC/ABAC) and enforced at in-path PEPs; deny unvalidated or claim-stripped calls; prohibit bypass paths.
Defense in Depth	ISAU-RP-04	

Principle Name	Code	Applicability to Identity & Access Security Architecture
		Layer phishing-resistant MFA, adaptive authentication, token PoP/DPoP, PAM JIT/PSM, and ITDR correlation; eliminate single points of failure in authentication/enforcement.
Secure by Design	ISAU-RP-05	Place IdP/STS, PDP/PEP, and privileged boundaries in the architecture phase; express policies as code; validate in CI before production.
Minimize Attack Surface	ISAU-RP-06	Reduce exposed authentication endpoints; remove unused accounts; constrain token TTLs; quarantine non-compliant devices at PEPs.
Secure Defaults	ISAU-RP-10	Deny-by-default policies; no fail-open for authentication, token issuance/validation, or enforcement paths.
Evidence Production	ISAU-RP-15	Write IdP/STS/PDP/PEP/PSM telemetry to tamper-resistant, hash-verified, immutable stores; produce replayable timelines for V&V and forensics.
Protect Confidentiality	ISAU-RP-18	Use phishing-resistant MFA; encrypt credentials; validate token audiences, issuers, and signatures; prefer mTLS and signed tokens for service-to-service calls.
Protect Availability	ISAU-RP-20	Engineer HA for IdP/federation/STS/PAM; protect keys in HSM; meet RTO/RPO; verify no fail-open during failover drills.

Implementation note: A compact traceability matrix can show how each principle maps to specific outputs in §6 and to control mappings in §9.

Practitioner Guidance:

- Link principle → spec → proof. For each item in Table F-2, note the matching §6 specification(s), assign a §12 Test-ID (positive and negative paths), and record the Evidence Pack location (for example, policy commit, token trace, PSM replay) under EP-06.xx.
- Put numbers on intent. Convert each principle into a threshold (for example, RP-01: ≥ 99 % deny on out-of-scope commands; RP-02: 100 % Tier-0 at AAL 2+; RP-20: DR drill meets stated RTO/RPO with no fail-open).

	• Treat change as a re-test trigger. Any shift in trust boundaries, token TTLs, device posture rules, or entitlement models must ship with synchronized policy updates, tests, and evidence in the same change set. • Prove end-to-end. Capture IdP/STS decision_id and PEP outcomes for the same request; attach the joined trail to the Evidence Pack so auditors can replay authorization from entry to enforcement. • Keep a living register. Maintain a one-row ledger per principle: Principle → §6 control → §12 Test-ID → EP-06.xx; review after incidents and quarterly to prevent drift.

Section 8. Foundational Standards Alignment

Internationally recognized frameworks from NIST and ISO/IEC establish baseline expectations for identity assurance, access control, and trustworthy systems. Identity & Access Security Architecture builds on these foundations, integrating them into a defensible, engineering-focused model that addresses modern hybrid architectures, federated trust, and measurable implementation.

Purpose and Function

- Demonstrate alignment with globally accepted NIST/ISO practices for identity, authentication, authorization, and resilience.
- Bridge compliance baselines to ISAUnited's architecture-and-engineering methodology (identity plane, PDP/PEP, STS, PAM/JIT/PSM).
- Enhance credibility and traceability for adoption and audit readiness.
- Provide a consistent baseline for clause-level mapping in sub-standards.

Table F-3. Applicable Foundational Standards:

Framework	Standard ID	Reference focus
NIST	SP 800-53 Rev. 5	Security and privacy controls (AC, IA, AU) for access control, identification/authentication, and audit/accountability.
NIST	SP 800-63 (all parts), esp. 800-63B	Digital identity: identity proofing, Authentication Assurance Levels (AAL), federation assertions and lifecycle.
NIST	SP 800-207	Zero Trust Architecture: continuous verification, least privilege, and explicit Policy Decision Point (PDP)/Policy Enforcement Point (PEP) patterns.

Framework	Standard ID	Reference focus
NIST	SP 800-160 Vol. 1	Systems security engineering practices for designing and verifying trustworthy identity services.
ISO/IEC	27001:2022	ISMS requirements encompass identity, access, and logging within risk management.
ISO/IEC	27002:2022	Code of practice for implementing access control, authentication, and event logging.
ISO/IEC	29115	Entity authentication assurance framework supporting risk-appropriate authentication.
ISO/IEC	24760 (series)	Identity management framework and terminology for identities, attributes, and lifecycle concepts.

NOTE: ISAUnited Charter Adoption of Foundational Standards.

Per the ISAUnited Charter, the institute formally adopts the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) and the National Institute of Standards and Technology (NIST) as its foundational standards bodies, consistent with their public encouragement of organizational adoption. Parent Standards align to ISO/IEC and NIST for architectural grounding and auditability, and this alignment flows down to Sub-Standards as invariant and minimum requirements that may be tightened but not weakened. ISAUnited does not restate or speak on behalf of ISO/IEC or NIST; practitioners shall consult the official publications and terminology of these organizations, verify scope and version currency against the latest materials, and implement controls in a manner consistent with ISAUnited security invariants and the requirements of this standard.

Sub-Standard Expectations

Sub-standards under ISAU-DS-IAM-1000 must:

- Cite specific clauses from Table F-3 (for example, NIST SP 800-53 AC-6, NIST SP 800-63B AAL 2, ISO/IEC 27002:2022 control 5.x/8.x) for each normative output they extend.

Obsolete and withdrawn documents should not be used; please use replacements.

- Convert those clauses into testable engineering behaviors (policy-as-code / control-as-code) with defined verification/validation in §12.
- Document any divergence with compensating controls, a risk-based rationale, and a sunset date; store passing artifacts under the Evidence Pack ID.
- Include a concise mapping table: §6 Output → Framework → Clause → Test-ID(s) → Evidence Pack ID.

Practitioner Guidance:

- Map at clause level only: for each §6 output (for example, 6.2 Authentication & Authorization, 6.3 PAM/JIT/PSM, 6.4 Federation/SSO), add a row Spec → NIST/ISO clause → how enforced (policy/code) → Evidence Pack ID.
- Keep mappings current: when a control or policy changes (AAL targets, token TTLs, PDP policy), update the NIST/ISO citation in the same change and store the diff in the Evidence Pack.
- Multi-regime environments: where multiple clauses could apply, adopt the strictest applicable requirement and record the rationale once in the mapping sheet.
- Scope discipline: do not list CSA/CIS/OWASP in this section; place them in §9 with their testable control mappings.

Section 9. Security Controls

This section identifies technical control families and references that the Identity & Access Security Architecture Parent Standard directly supports or enforces. These mappings translate architectural intent into testable safeguards and provide traceability to widely used industry frameworks.

Purpose and Function

Security controls translate the identity plane design into measurable behaviors, including strong authentication, centralized authorization (PDP) with in-path enforcement (PEP), privileged boundaries (JIT/PSM), device posture binding, short-lived tokens with replay protection, and identity-centric detection/response.

By mapping to CSA CCM, CIS Controls v8, OWASP, and MITRE ATT&CK, ISAUnited ensures:

- Clear alignment with broadly recognized best practices.

Obsolete and withdrawn documents should not be used; please use replacements.

- Interoperability across diverse platforms and operating models.
- Reuse of controls in sub-standards and straightforward validation and audit.

Implementation Guidance

- Reference at least three concrete, implementation-level controls from recognized frameworks.
- Provide the framework acronym, control ID, and a concise, implementation-focused description.
- Align every selected control to one or more §6 specifications and (optionally) a principle code from §7 to aid traceability.
- Favor controls that are verifiable via logs, policy-as-code diffs, token traces, and PSM artifacts.

Table F-4. Control Mappings for Identity & Access Security Architecture:

Framework	Control ID	Control name/description	Aligns to §6
CSA CCM v4	IAM-05	Least Privilege — employ least privilege for information system access; supports RBAC/ABAC enforcement.	6.1, 6.2
CSA CCM v4	IAM-06	User Access Provisioning — define and implement user access provisioning with authorization and recording.	6.1
CSA CCM v4	IAM-08	User Access Review — review and revalidate user access (least privilege and SoD) on a defined cadence.	6.1
CSA CCM v4	IAM-14	Strong Authentication — implement multi-factor authentication for administrative and remote access.	6.2, 6.4
CIS Controls v8.1	5.3	Disable Dormant Accounts — delete or disable accounts after a defined inactivity period.	6.1
CIS Controls v8.1	5.5	Inventory of Service Accounts — establish and maintain an inventory; review regularly.	6.1
CIS Controls v8.1	6.3	Require MFA for Externally-Exposed Applications.	6.2, 6.4
CIS Controls v8.1	6.4		6.2

Framework	Control ID	Control name/description	Aligns to §6
		Require MFA for Remote Network Access.	
CIS Controls v8.1	6.5	Require MFA for Administrative Access.	6.2, 6.3
OWASP ASVS v4.x	V2	Authentication verification requirements — centralized, strong authentication patterns.	6.2, 6.4
OWASP ASVS v4.x	V3	Session management verification requirements — secure tokens, expiration, revocation, and replay protections.	6.2, 6.4
OWASP API Security Top 10 (2023)	API2:2023	Broken Authentication — harden API auth (OAuth 2.0/OIDC, token TTL/rotation, PoP/DPoP), prevent replay/substitution.	6.2, 6.4

NOTE: Use of External Control Frameworks.

ISAUnited maps to external control frameworks to provide alignment and traceability, but does not speak on behalf of those organizations. Practitioners shall consult and follow the official practices, recommendations, and implementation guidance of the Center for Internet Security (CIS), the Cloud Security Alliance (CSA), and the Open Worldwide Application Security Project (OWASP) when applying controls. Always verify control identifiers, scope, and version currency against the publishers' latest materials. Where wording differs, use the framework's official documentation while maintaining consistency with ISAUnited security invariants and this standard's requirements.

Additional References

As the identity domain evolves, authors may include supplementary, implementation-level controls from these frameworks to maintain robustness and relevance.

Sub-Standard Expectations

Sub-standards developed under this Parent Standard must:

- Select and enforce explicit technical controls relevant to the scope (e.g., MFA, PAM/JIT/PSM, IGA/SCIM, federation/SSO, token protections, ITDR).

Obsolete and withdrawn documents should not be used; please use replacements.

- Provide a concise mapping for each control—§6 Output → Framework → Control ID → Test-ID(s) (§12) → Evidence Pack ID—and keep it current.
- Document and justify any deviation from the control families referenced here, including compensating controls and a review/sunset date.

Practitioner Guidance:

- Build a mini-map for each control: §6 Output → Framework (CSA/CIS/OWASP/ATT&CK) → Control ID/Technique → Test-ID (§12) → Evidence Pack (EP-06.xx). Keep it to one row per behavior (for example, token TTL, JIT elevation).
- Prefer implementation checks over prose: verify via policy-as-code diffs, PDP decision logs, PEP enforcement logs, token traces, PSM replays—not screenshots.
- Anchor MFA where it matters: map CIS 6.3/6.4/6.5 to the exact entry points (externally exposed apps, remote network access, administrative access) and prove with auth telemetry showing Authentication Assurance Level (AAL) and factor type.
- Tie least privilege to RBAC/ABAC evidence: map CCM IAM-05 and show denied out-of-scope actions and SoD review closures; include the CI report for allow-lists.
- Treat service accounts as first-class: map CIS 5.5 and CCM IAM-06/08 to SCIM jobs, orphan detection, and vault rotation logs; show mTLS or signed-token proofs for service-to-service calls.
- Validate tokens like an adversary would: map OWASP ASVS V2/V3 and API2:2023; run negative tests for replay, wrong audience/issuer, and over-TTL; include PoP/DPoP verification records.
- Add ATT&CK realism: include at least one test against T1078 (Valid Accounts) or T1550 (Use of Stolen Tokens) with expected auto-containment results.
- Keep scope discipline: reserve NIST/ISO for §8; use CSA/CIS/OWASP/ATT&CK here only. When a control or spec changes, update the mapping and re-run the linked §12 tests in the same change set, recording the new EP-06.xx.

Section 10. Engineering Discipline

This section defines the architectural thinking, rigorous engineering processes, and disciplined operational behaviors required to implement Identity & Access Security Architecture (ISAU-DS-IAM-1000). ISAUnited's Defensible Standards are not compliance checklists; they are engineered systems, grounded in systems thinking,

critical reasoning, and Verification & Validation (V&V), that produce measurable, auditable, defensible outcomes across identity providers, federation paths, authorization points, and privileged boundaries.

10.1 Purpose & Function

Purpose. Establish a repeatable, auditable way of working that integrates systems thinking, lifecycle controls, adversary-aware design, and measurable outcomes for identity and access security.

Function in D10S. Parent Standards set expectations and invariants. Sub-Standards convert them into policies-as-code/controls-as-code, test specifications, and evidence artifacts embedded in delivery and operations.

10.2 Systems Thinking

Goal: Make the identity system legible end-to-end—trust boundaries, flows, interfaces, and dependencies—so controls bind where risk actually manifests.

10.2.1 System Definition & Boundaries

- Declare system purpose, scope, stakeholders, and in-/out-of-scope assets (IdP, directories, federation gateways, STS, PDPs/PEPs, PAM/JIT/PSM, device posture service, SIEM/ITDR, credential vault/HSM).
- Model trust zones and boundary crossings (user/device → IdP, service → STS, app/API → PEP/PDP, partner/SaaS → federation, admin → PAM gateway, workload→workload with mTLS/signed tokens).

10.2.2 Interfaces & Identity/Token Contracts

- Maintain Interface Control Documents (ICDs) for authN/authZ paths (SAML/OIDC/OAuth flows, token exchange, API gateway enforcement, admin channels via PAM).
- For each interface, specify: principal type (human vs Service & Machine Identity), required AAL, RBAC/ABAC policy context, device-posture requirement, token format/TTL/scopes/audience/issuer, replay/PoP/DPoP settings, error/deny semantics, telemetry fields (trace_id, decision_id, policy_version), retention/time-sync requirements, and invariants (e.g., “no fail-open,” “Tier-0 requires JIT+PSM,” “claim propagation required across service hops”).

10.2.3 Dependencies & Emergent Behavior

- Map shared services (time sync/NTP, HSM/keys, vault, SIEM/ITDR, posture provider, CI/CD, evidence store).
- Identify emergent risks from composition (e.g., long-lived tokens + missing audience checks → token reuse, permissive PEP bypass routes → unenforced calls, shared admin accounts + weak MFA scope → lateral movement; absent claim propagation → downstream authorization drift).

10.2.4 Failure Modes & Safeguards

- For critical paths, document failure modes (token over-TTL, audience/issuer not validated, JIT bypass, PSM disabled, clock skew, posture downgrade, federation misconfig) and safeguards (deny-by-default, negative tests, PoP/DPoP, dual-control elevation, immutable logging, quarterly failover with no fail-open).
- Required Artifacts (min): Context diagram with trust boundaries; identity flow map (auth/token/elevation); ICD set; invariants register.

10.3 Critical Thinking

Goal: Replace assumptions with explicit reasoning that survives review, attack, and audit.

10.3.1 Decision Discipline

- Use Architecture Decision Records (ADRs): problem → options → constraints/assumptions → trade-offs → decision → invariants → test/evidence plan (who/when/how measured).

10.3.2 Engineering Prompts

- **Boundaries**: What are the identity trust boundaries and why? Where are PDP/PEP placed?
- **Interfaces**: What must always be true at each identity interface (invariants)? How is it tested (positive/negative)?
- **Adversary**: Which identity-centric techniques are credible here (credential theft, token replay/substitution, consent abuse, JIT bypass)? What is the shortest attack path?
- **Evidence**: Which objective signals prove this control works today and after change (token traces, decision logs, PSM replays)?
- **Failure**: When this fails, does it fail safe (deny, revoke, quarantine, immutable log)? What is the operator's next action?

Required Artifacts (min): ADRs; assumptions & constraints log; evidence plan per decision.

10.4 Domain-Wide Engineering Expectations

Secure System Design

- Define identity boundaries (IdP/STS, federation routes, PDP/PEP paths, PAM/JIT/PSM, device posture, SIEM/ITDR, vault/HSM).
- Validate boundaries and trust relationships via structured reviews using §10.2 artifacts; ensure protections bind to AAL targets, token contracts, and privilege boundaries at each hop.

Implementation Philosophy — "Built-in, not bolted-on."

- Integrate MFA/AAL, RBAC/ABAC, token protections (TTL, rotation, audience/issuer, PoP/DPoP), device posture, and PAM/JIT/PSM at design time.
- Express controls as policy-as-code/control-as-code bound to §10.2.4 invariants (e.g., “no fail-open,” “Tier-0 requires JIT+PSM,” “posture-bound SSO”).

Lifecycle Integration

- Embed identity controls into design reviews, backlog, build/test, deployment, and operations; keep delivery mechanics in Annex J; crypto specifics in Annex I (CEK).
- Enforce version-controlled reviews with required ADRs and Evidence Pack ID updates on every change.

Verification Rigor (V&V)

- Combine automated checks (protocol conformance, token negative tests, PDP policy unit tests, PEP deny/allow suites, posture re-checks, DR/failover drills) with targeted probes (claim stripping/injection, replay/substitution, JIT bypass).
- Require continuous validation in pipelines and scheduled runtime checks tied to invariants (e.g., AAL, TTL, rotation, JIT window, idle timeout).

Operational Discipline

- Monitor for drift and unauthorized change (policy diffs, disabled PSM, extended TTLs, removed audience checks, posture scope narrowed, SoD violations); auto-remediate where safe with time-bounded exceptions.
- Maintain runbooks/SOPs for identity compromise, token abuse, JIT/PSM faults, federation errors, and DR events; record outcomes in the Evidence Pack.

10.5 Engineering Implementation Expectations

- Policies/Controls as Code. Manage RBAC/ABAC rules, conditional access, MFA/AAL scopes, token TTL/rotation, PoP/DPoP, PDP policy bundles, PEP rules, PAM/JIT/PSM policies as code with peer review and provenance.
- Structured Enforcement Path. Build → policy lint/unit/negative tests → federation/STS conformance → canary → promote/rollback (execution in Annex J; semantics here).
- Explicit Security Boundaries. Maintain diagrams and ICDs; continuously validate posture (deny-by-default, audience/issuer validation, rotation on use, JIT+PSM) with audits and smoke tests.
- Automated Security Testing. Integrate token replay/substitution tests, audience/issuer checks, clock-skew tests, PDP/PEP decision suites, elevation boundary tests, and failover no-fail-open assertions before production.

- Traceable Architecture Decisions. Link ADRs to controls, tests, and evidence; update ADRs and evidence on each change request.

Required Artifacts (min): Policies-as-code repo; enforcement/test gates; boundary/ICD set; automated test results; evidence ledger (see §10.7 and §12).

10.6 Sub-Standard Alignment (inheritance rules)

Sub-Standards must operationalize this discipline with IAM-specific detail:

- MFA & AAL (e.g., ISAU-DS-IAM-1010). AAL targets, phishing-resistant factors, posture gates; Tests: AAL detection in auth telemetry; step-up on risk.
- PAM/JIT/PSM (e.g., ISAU-DS-IAM-1020). Dual-control JIT, elevation windows, PSM coverage, allow-lists as code; Tests: JIT denial without approval; unauthorized command = deny+alert; PSM replay linkage.
- Federation & SSO (e.g., ISAU-DS-IAM-1030). Interop/negative testing (SAML/OIDC/OAuth), token TTL/rotation, audience/issuer/signature validation, PoP/DPoP; Tests: replay/substitution denials; skew handling.
- IGA/SCIM (e.g., ISAU-DS-IAM-1040). Provision/de-provision cadence, certification SLAs, orphan detection; Tests: coverage/latency; removal within SLA.
- Service & Machine Identities (e.g., ISAU-DS-IAM-1050). Unique principals, vault/rotation, mTLS or signed tokens, claim propagation safeguards; Tests: forced rotation does not break flows; stale tokens denied.
- ITDR (e.g., ISAU-DS-IAM-1060). Telemetry normalization, correlation rules, automated containment; Tests: MTTD/MTTR attainment; auto-revoke/terminate on high-risk events.

10.7 Evidence & V&V (what proves it works)

Establish an Identity Evidence Pack per system containing:

- Design Evidence: trust-boundary diagrams, identity/token flow maps with ICDs, invariants register, ADRs.
- Build Evidence: policy-as-code history (RBAC/ABAC, conditional access, PAM/JIT/PSM, token settings), federation/STS conformance results, negative-test reports (replay, wrong audience/issuer, over-TTL), CI outcomes.
- Operate Evidence: runtime allow/deny logs with trace_id/decision_id/policy_version, token traces (TTL/audience/issuer/rotation), PSM session replays, device-posture decisions, SIEM/ITDR correlations, DR/failover outcomes showing no fail-open.
- Challenge Evidence: adversary emulation (credential theft, token abuse, JIT bypass), red-team results, incident timelines with automated containment, remediation closure with re-test.

Obsolete and withdrawn documents should not be used; please use replacements.

Each control requires objective pass/fail criteria, specified test frequency, a responsible owner, and a defined retention policy. Map Evidence Pack IDs into §12 traceability.

10.8 Example: Sub-Standard Discipline Alignment (Federation & Token Handling)

Scope: ISAU-DS-IAM-1030 (Federated Identity & SSO).
Design: Define trust boundaries and invariants ("tokens short-lived," "audience/issuer must match," "no fail-open," "posture-bound SSO"). Place PDP/PEP for each entry point.
Implement: Express PDP policies and PEP rules as code; configure STS token TTL ≤ 60 minutes, rotating refresh; enable PoP/DPoP on high-risk APIs; enforce audience/issuer/signature validation; log decision_id.
V&V: Run interop and negative tests (replay, wrong audience/issuer, expired/over-TTL, skew); verify PoP/DPoP; assert denial with evidence; failover drill proves no fail-open.
Operate: Evidence Pack includes policy repo history, token traces, negative-test logs, PEP enforcement logs, SIEM correlations, and DR/failover reports.

Practitioner Guidance:

- Build and maintain a Controls → Outputs → Tests sheet per identity domain; keep it current in the same change that modifies policies (MFA/AAL, token profiles, PDP/PEP rules, PAM/JIT/PSM). Attach proofs (policy diffs, token traces, PSM excerpts, conformance reports) and record EP-06.xx.
- Favor controls expressed as code and verified automatically by §12 tests; reserve exceptions for time-bounded, owner-approved waivers with compensating controls and explicit Test-IDs/Evidence Pack IDs.

Section 11. Associate Sub-Standards Mapping

Purpose of Sub-Standards

ISAUnited Defensible Sub-Standards under Identity & Access Security Architecture are tightly scoped, engineering-driven extensions that:

- Define granular, identity-layer requirements for specialized domains (for example, MFA/AAL, PAM/JIT/PSM, Federation/SSO, IGA/SCIM, Service & Machine Identities, ITDR).
- Translate architectural intent into enforceable behaviors in platforms and policies (IdP/STS profiles, PDP/PEP rules, PAM policies, SCIM jobs).
- Specify verification/validation methods that yield test artifacts (token negative tests, JIT denial/approval logs, PSM replays, federation interop results) referenced in §12.
- Align directly to the Parent Standard's §6 outputs and §7 principles, with traceable Evidence Pack artifacts (EP-06.xx).

Interface notes (non-normative)

- Annex F (this) produces identity-layer requirements, PDP/PEP control bindings, and tests.
- Annex J ensures those tests run in CI/CD and at promotion; provenance, SBOM, and gates live there.
- Annex I (CEK) governs crypto profiles, keys, and token signing; Annex F governs correct identity-layer application (token TTL/rotation, PoP/DPoP, mTLS).
- Annex H (MDR/MDR-like) consumes identity telemetry (IdP/STS/PDP/PEP/PSM) for detection, correlation, and IR workflows.

Scope and Focus of IAM Sub-Standards

Multi-Factor & Authentication Assurance
Example Sub-Standard: ISAU-DS-IAM-1010 — MFA & Authentication Assurance

- AAL targets; phishing-resistant factors; step-up on risk/posture; re-auth on elevation.
- Maps to §6: 6.2, 6.4
- Tests: AAL detection in auth telemetry; posture downgrade → step-up/deny; factor removal → deny.

PAM with JIT/PSM & Zero-Trust Privilege
Example Sub-Standard: ISAU-DS-IAM-1020 — PAM/JIT/PSM

- Dual-control JIT; elevation window ≤ 60 minutes; PSM required for Tier-0; command/action allow-lists as code.
- Maps to §6: 6.3
- Tests: non-JIT elevation = deny; disallowed command = deny + alert; complete PSM replay linkage.

Federation & SSO Architecture
Example Sub-Standard: ISAU-DS-IAM-1030 — Federation/SSO

- SAML/OIDC/OAuth interop; short-lived tokens; rotating refresh; audience/issuer/signature validation; PoP/DPoP where feasible.
- Maps to §6: 6.4

- Tests: replay/substitution/over-TTL/clock-skew → deny; conformance/negative test suite pass.

IGA & Lifecycle (SCIM)
Example Sub-Standard: ISAU-DS-IAM-1040 — IGA & Access Reviews
- SCIM provisioning/de-provisioning; quarterly certifications; orphan remediation ≤ 24 hours.
- Maps to §6: 6.1
- Tests: SCIM coverage/latency; certification closure ≤ 30 days; orphan removal SLA.

Service & Machine Identity Security
Example Sub-Standard: ISAU-DS-IAM-1050 — SMI Governance
- Unique principals; vault/rotation; mTLS or signed tokens; claim-propagation safeguards.
- Maps to §6: 6.1, 6.2, 6.4
- Tests: forced rotation does not break flows; stale token/cert → deny; claim stripping/injection → deny + log.

Identity Threat Detection & Response
Example Sub-Standard: ISAU-DS-IAM-1060 — ITDR
- Normalized IdP/STS/PDP/PEP/PSM telemetry; automated containment (disable/revoke/terminate).
- Maps to §6: 6.5
- Tests: MTTD ≤ 15 minutes; MTTR ≤ 60 minutes; containment success rate meets target.

Table F-5. Example future sub-standards:

Identifier	Sub-Standard name	Key focus area
ISAU-DS-IAM-1010	MFA & Authentication Assurance	Strong authentication & AAL
ISAU-DS-IAM-1020	PAM with JIT/PSM & Zero-Trust Privilege	Privileged elevation & monitoring
ISAU-DS-IAM-1030	Federation & SSO Architecture	Interop, token contracts, replay defenses
ISAU-DS-IAM-1040	IGA & Access Reviews (SCIM)	Lifecycle, certifications, orphan removal

Identifier	Sub-Standard name	Key focus area
ISAU-DS-IAM-1050	Service & Machine Identity Security	SMI inventory, vault/rotation, mTLS/PoP
ISAU-DS-IAM-1060	ITDR: Detection, Correlation & Containment	Telemetry, rules, auto-containment

Development and Approval Process

ISAUnited uses an open, peer-driven annual process to propose, review, and publish sub-standards:

- Open Season Submission — Proposals must cite the §6 outputs and §7 principles they extend, plus clause-level NIST/ISO anchors from §8.
- Technical Peer Review — Evaluate engineering rigor, testability, scope clarity, and cross-domain consistency.
- Approval & Publication — Assign identifier/version and publish as an actionable extension of ISAU-DS-IAM-1000.

Sub-Standard Deliverables (normative)

Each sub-standard must include:

- **Inputs (Requirements):** Preconditions from Annex F §5 it depends on.
- **Outputs (Specifications):** Concrete identity-layer behaviors and thresholds (for example, AAL targets, token TTL/rotation, JIT windows) tied to §6.
- **Verification/Validation:** Named tests and acceptance criteria tied to §12 (for example, replay denial, elevation denial without approval, certification closure).
- **Evidence:** Artifact list and storage location (EP-06.xx).
- **Standards Mapping:** Spec → NIST/ISO clause (§8) → Controls (§9) → Test-ID (§12) → Evidence Pack ID.
- **Interfaces:** Clear delineation of what is enforced at IdP/STS/PDP/PEP/PAM (Annex F) vs. delivery mechanics (Annex J) and crypto parameters (Annex I).

Practitioner Guidance:

- Bind invariants before tests. Define the identity invariants first (AAL targets, token TTL/rotation, audience/issuer checks, JIT + PSM, posture-bound

	SSO). If any invariant lacks a named Test-ID (§12) and EP-06.xx, halt and record a tracked risk. • Make SLOs explicit and provable. Pick 1–2 SLOs per sub-standard (for example, ≥ 99 % out-of-policy denials on privileged commands; token TTL ≤ 60 minutes with 100 % audience/issuer validation; MTTD/MTTR targets) and point to the EP-06.xx that proves each. • Keep CEK separation and traceability. Say "per CEK cryptographic profiles" for token signing/keys; verify via HSM/KMS logs and conformance tests. In the mapping sheet, always include: §5 input(s) → §6 output(s) → NIST/ISO clause (§8) → control (§9) → Test-ID (§12) → EP-06.xx.

Section 12. Verification and Validation

The effectiveness and defensibility of an Identity & Access Security Architecture must be continuously verified and validated using structured, engineering-grade assessments. While detailed platform tests are defined in the IAM sub-standards, this Parent establishes the gold-standard expectations below.

> **Verification** confirms implementation against this standard's Requirements (Inputs, §5) and Technical Specifications (Outputs, §6).
>
> **Validation** proves the identity system performs under real operating conditions and withstands adversarial testing.

Core Verification Activities

- **Confirm §6 controls at trust boundaries and paths:** AAL/MFA scope; PDP policies as code with in-path PEP enforcement; PAM with JIT/PSM; STS token profiles (TTL/rotation/audience/issuer/signature/PoP/DPoP); federation/SSO interop; device-posture gates; immutable evidence plumbing.
- **Review baselines:** IdP/STS profiles; PDP/PEP rules and locations; elevation flows (dual-control JIT, idle timeouts); System for Cross-domain Identity Management (SCIM) provisioning jobs and access-review cadences; key protection (HSM) and DR runbooks; no fail-open invariants expressed as policy.
- **Verify integrations do not break identity flows:** IdP/STS ↔ apps/APIs; PDP ↔ PEP; PAM ↔ admin channels; posture provider ↔ IdP/PEPs; telemetry ↔ immutable store/SIEM—confirm enforcement points align to business-critical entry points.

Core Validation Activities

- **Adversary-informed exercises:** Simulate credential theft, token replay/substitution, consent abuse, federation misconfiguration, claim stripping/injection, and JIT bypass; require denial with explicit reasons in logs.
- **Runtime resilience:** Planned failover of IdP/STS/PDP/PEP paths proving no fail-open; RTO/RPO attainment; key rotation/escrow/recovery drills; posture downgrade triggers step-up or revoke.
- **Operational drills:** Non-JIT elevation denial and approved JIT auto-revocation; PSM coverage for all Tier-0 sessions; SIEM correlation across IdP/STS/PDP/PEP/PSM; end-to-end reconstruction using decision_id/trace_id/policy_version.

Required Deliverables

All Verification & Validation efforts must produce documented outputs that include:

1. Test Plans & Procedures — Scope, tooling, Test-IDs, owners for verification and validation phases.
2. Validation Reports — Pass/fail results, residual risk, prioritized remediation tied to §6 outputs.
3. Evidence Artifacts — Policy diffs; token traces (TTL/audience/issuer/rotation/PoP); PDP decisions and PEP enforcement logs (decision_id); JIT approvals and PSM replays; federation conformance/negative tests; failover logs and RTO/RPO proofs—each labeled with an Evidence Pack (EP-06.xx).
4. Corrective Action Plans — Time-bounded remediation for findings to be closed prior to acceptance, with re-test Test-IDs.

Common Pitfalls to Avoid

- **Checklist posture without negative tests:** No replay/substitution tests, missing audience/issuer checks, or absent PoP/DPoP on high-risk APIs.
- **Privilege controls not real:** Standing admin persists; JIT not dual-control; PSM disabled or partial.
- **Evidence that is not immutable:** Screenshots without logs, or logs not hash-verified/time-synced.
- **Fail-open during faults:** DR plans that allow authentication, token validation, or enforcement to bypass on component loss.

Table F-6. Traceability Matrix: Requirements (§5) → Verification/Validation (§12) → Technical Specifications (§6):

Requirement ID	Requirement (summary)	Verification (build-correct)	Validation (works-right)	Related §6 Outputs
5.1	Centralized IdP integration	IdP configured; federation metadata signed; SAML/OIDC/OAuth interop tests pass.	Invalid/expired/assertion-tampered flows → deny with reason	6.4
5.2	MFA & Authentication Assurance (AAL)	AAL scope present for privileged groups; phishing-resistant factors enabled	Tier-0 MFA bypass attempt → deny; elevation re-auth enforced	6.2
5.3	PAM with JIT/PSM	JIT policies and PSM enabled; dual-control approvals required	Non-JIT elevation = deny + alert; approved JIT = allow + record; idle timeout enforced	6.3
5.4	IGA/SCIM lifecycle & reviews	SCIM jobs are active; quarterly certifications are scheduled; orphan detection rules	Orphaned accounts removed ≤ 24 hours; certification closure ≤ 30 days	6.1
5.5	ITDR integration	Telemetry schemas normalized; SIEM rules deployed.	Compromise MTTD ≤ 15 minutes; MTTR ≤ 60 minutes with auto-containment	6.5
5.6	Device posture validation	Conditional access tied to posture; claims propagated	Posture downgrade → step-up/revoke; claim stripping → deny + log	6.2, 6.4
5.7	Audit-ready logging	Immutable store configured; retention/time sync verified.	Replayable auth and privileged timelines with decision_id/trace_id	6.5
5.8	Service & Machine Identity governance	Inventory; vault/rotation; mTLS/signed tokens enforced	Forced rotation does not break; stale cert/token → deny	6.1, 6.4

Requirement ID	Requirement (summary)	Verification (build-correct)	Validation (works-right)	Related §6 Outputs
5.10	IAM availability objectives	HA/DR topologies and runbooks; key escrow/rotation plans	Failover meets RTO/RPO; no fail-open on auth/token/enforcement	6.6
5.11	STS (short-lived tokens, rotation, PoP)	TTL ≤ 60 minutes; rotating refresh; audience/issuer/signature checks	Replay/substitution/over-TTL → deny; PoP/DPoP verified on scoped APIs	6.2, 6.4
5.12	PDP/PEP placement	PDP/PEP map per entry point; policy bundle loads	PEP denies when PDP denies; downstream services preserve claims	6.2, 6.4
5.13	Protocol conformance & time sync	Interop and negative tests; clock-skew bounds documented	Out-of-skew tokens rejected; audit shows skew reason	6.4
5.14	Immutable evidence repositories	Evidence store hash-verification enabled; access controls set.	Random sample reconstructs the incident with immutable artifacts	6.5

Evidence guidance

Attach (per row) to the EP-06.xx: IdP/STS configs and test outputs; AAL/MFA policy exports; token traces and negative-test logs; PDP policy bundle and PEP enforcement logs; JIT approvals and PSM replays; SCIM/certification/orphan reports; posture decisions; SIEM correlation results; DR/failover reports; immutable-store hash manifests.

How to use this matrix

- **Plan:** For each §5 requirement, define ≥ 1 Verification and ≥ 1 Validation tied to §6 outputs.
- **Execute:** Run tests; record SLO met/not met with direct artifact links in the EP-06.xx.

Obsolete and withdrawn documents should not be used; please use replacements.

- **Maintain:** When a requirement or enforcement changes, update the row and re-run impacted tests in the same change set.

Practitioner Guidance:

- Test what the invariants enforce. Start with no fail-open, AAL targets, token TTL/rotation and audience/issuer, JIT + PSM, posture-bound SSO; give each a Test-ID and EP-06.xx.
- Prefer negative tests over screenshots. Replay, substitution, wrong audience/issuer, over-TTL, claim stripping, non-JIT elevation—prove denial and log reason codes.
- Automate and gate. CI must fail on over-TTL tokens, disabled audience/issuer checks, missing PoP/DPoP where required, or PSM/JIT not enforced.
- Prove resilience. Show RTO/RPO attainment and no fail-open during failover with logs from IdP/STS/PDP/PEP and key services.
- Keep traceability alive. Maintain a simple register: §6 Output → Test-ID (§12) → EP-06.xx → Status; review after incidents and quarterly.

Quick Win Playbook:

Title: Stand Up an “STS + PDP/PEP” Replay-Resistance Smoke Suite on One Admin API

Objectives

1. Prove replay/substitution defenses (TTL, audience/issuer/signature, PoP/DPoP).
2. Prove deny-by-default at PEP when PDP denies.
3. Produce immutable evidence in EP-06.02.

Target: Admin API entry point (§6.2, §6.4).

Components: STS; PDP policy bundle; API gateway/PEP; immutable evidence store.

Protects: Admin API from stolen/forged tokens.

Stops/Detects: Over-TTL; wrong audience/issuer; tampered signature; missing PoP/DPoP.

Action: Configure STS: access token TTL ≤ 60 minutes; rotating refresh; audience/issuer/signature + skew checks; enable PoP/DPoP for admin endpoints. Configure PDP deny rules for out-of-scope actions; enforce at PEP.

	Run: valid token = allow; expired/over-TTL = deny; wrong audience/issuer = deny; no PoP on protected endpoint = deny. **Proof → EP-06.02:** STS profile export; token traces; negative-test deny logs with reason; PDP policy diff; PEP enforcement logs (decision_id). **Metric:** 100 % negative cases denied; 100 % critical endpoints validate audience/issuer/signature; PoP/DPoP active on scoped APIs. **Rollback:** Revert STS/PEP policy via approved change; keep artifacts in EP-06.02 marked superseded.

Section 13. Implementation Guidelines

This section does not prescribe vendor-specific tactics. Parent Standards are stable, long-lived architectural foundations. Here, we define how IAM sub-standards and delivery teams must translate the Parent's intent into operational behaviors that are testable, automatable, and auditable for the Identity & Access Security Architecture (Annex F/D06). Delivery mechanics (pipeline orchestration, SBOM/provenance, promotion/rollback) are governed by Annex J.

Purpose of This Section in Sub-Standards

Sub-standards must use Implementation Guidelines to:

- Translate architectural expectations from the Parent into enforceable run-time and first-boundary (gateway/edge) IAM behaviors (for example, PDP decisions enforced at in-path PEPs, posture-bound SSO, dual-control JIT, token contracts).
- Provide stack-agnostic practices that improve adoption, reduce failure, and align with ISAUnited's defensible design philosophy.
- Highlight common failure modes and how to prevent them with measurable gates and checks.
- Offer repeatable patterns (as code) that enforce controls, trust models, and engineering discipline across IdP/STS, PDP/PEP, PAM/JIT/PSM, services/microservices, partner/SaaS federation, device posture, vault/HSM, and telemetry.

Open Season Guidance for Contributors

Contributors developing sub-standards must:

- Align all guidance with this Parent's strategic posture and §6 outputs (and §7 principles).
- Avoid vendor/product terms; express controls as requirements, tests, and evidence.
- Include lessons learned (what fails, why, and how the test proves it).
- Focus on repeatable engineering patterns (policies-as-code/controls-as-code), not one-offs.
- Provide a minimal Standards Mapping: Spec/Control → NIST/ISO clause from §8 → Control(s) from §9 → Test-ID (§12) → Evidence Pack EP-06.xx.

Technical Guidance

A. Organizing Principles (normative)

1. Everything as code. PDP policies (XACML/OPA Rego), PEP rules, IdP/STS profiles (token TTL/rotation/audience/issuer, PoP/DPoP), conditional access (AAL scope, posture), PAM/JIT/PSM policies, SCIM jobs, logging schema, and runbooks must be version-controlled, peer-reviewed, and promoted on protected branches.
2. Gated change. Every merge/release must pass non-bypassable security gates tied to §6 and §12 acceptance criteria (for example, 100% token negative tests, 100% AAL coverage for privileged accounts, replay/substitution tests pass, non-JIT elevation denied, PSM health checks green).
3. Immutable, reproducible releases. No manual IAM policy/code edits post-build; releases must be reproducible and verified at the first boundary (PEP) and in IdP/STS configuration.
4. Least privilege & JIT (identity context). Identities (human and Service & Machine Identities) and admin functions must be scoped; privileged elevation must be dual-control JIT; error templates/logs must preserve confidentiality while remaining diagnostically useful.
5. Environment parity. Staging must mirror production IAM controls (PDP/PEP, token profiles, posture rules, PAM/JIT/PSM, logging schema) so tests are predictive; drift must be monitored and reconciled; identity telemetry ingest meets schema-conformance = 100 % in staging.

B. Guardrails by Pipeline Stage (normative)

1. **Pre-commit / local**
   - Secrets scanning and signed commits required.
   - Pre-commit hooks should lint PDP/PEP policies, IdP/STS profiles, and run token negative tests locally (expired, wrong audience/issuer, missing PoP).
2. **Pull request (PR) / code review**

- CODEOWNERS approval required; attach an Identity Threat-Model Delta for changes to trust boundaries (new PEP path, new federation route, new Tier-0 scope).
- Token negative gate for changed entry points; critical findings = 0.
- Authorization coverage check: changed mutating admin routes show explicit PDP decisions enforced at PEP; planned §12 Test-IDs and EP-06.xx stub recorded.

3. **Build & package**
   - Deterministic artifacts; pinned policy bundles; no ad-hoc fetch at deploy.
   - Generate PoP/DPoP validators and token-contract tests from STS/IdP profiles; package PEP rules and PAM/JIT policies as deployable config.
4. **Pre-deploy / release**
   - Config drift detection against approved policies; approvals “as code.”
   - Progressive rollout (staged/canary) for PEP rules, token profile updates, and posture gates with health SLOs and automatic rollback; include JIT/PSM health checks.
   - Positive/negative token-contract tests at first boundary; elevation re-auth tests; posture-downgrade tests.
5. **Deploy & runtime**
   - Enforce PDP decisions at in-path PEP (deny unvalidated or claim-stripped calls); per-request token validation (audience/issuer/signature, TTL, PoP/DPoP where required).
   - Posture-bound SSO for privileged surfaces; re-auth on elevation; privileged idle timeout ≤ 15 minutes.
   - Unified logging schema (timestamp, subject, source, object, action, result, assurance, device_posture, scopes, trace_id, decision_id, policy_version) → immutable storage with authenticated time sync.
6. **Post-deploy validation & operations**
   - Continuous validation: replay/substitution suites, claim stripping/injection tests, non-JIT elevation denial, PSM coverage checks, federation misconfig probes, DR/failover no fail-open drills.
   - Track IAM SLOs: token TTL distribution, refresh rotation rate, AAL coverage on privileged sign-ins, elevation re-auth rate, privileged idle timeout violations (target 0), replay/substitution deny rate (target 100 %), PSM coverage (target 100 %), MTTD/MTTR targets, failover pass rate.
   - Auto-generate child Evidence Pack(s) per release (EP-06.xx) with policy diffs, token/elevation test results, deny logs with reason codes, PSM replay hashes, posture events, and ADR links.

C. Identity, Tokens, and Secrets (normative alignment to §6.2–§6.6)

- Validate OAuth 2.0/OIDC tokens per request; enforce TTL ≤ 60 minutes, rotating refresh; audience/issuer/signature checks; PoP/DPoP on designated high-risk APIs.
- Privileged access requires Authentication Assurance Level (AAL) 2 minimum (AAL 3 preferred) with re-authentication on elevation; bind SSO to device posture and step-up/revoke on posture change.
- Secrets never in repos or images; use approved vault/HSM; rotate post-use for privileged sessions; redact secrets in logs.

D. IAM Supply-Chain Integrity (normative; mechanics in Annex J)

- Only deploy policy bundles and code that passed all IAM gates; restrict sources/namespaces for policy artifacts.
- Quarantine and verify third-party auth libraries and token middleware; enforce license and integrity checks.
- Separate build and deploy identities; forbid production writes from build jobs; treat PEP/PDP policy tamper as a release-blocking event.

E. Measurement & Acceptance (aligned to §6 and §12)

- **Token contracts:** strict validation at boundary; token negative tests pass = 100 % (expired, wrong audience/issuer, tampered, missing PoP where required).
- **Authorization:** explicit PDP decisions enforced at PEP on 100 % privileged/mutating handlers.
- **Assurance & posture:** 100 % privileged sign-ins at AAL 2+; posture-downgrade step-up/revoke = 100 %; idle timeout ≤ 15 minutes.
- **Privilege controls:** 100 % Tier-0 via dual-control JIT; elevation window ≤ 60 minutes; PSM coverage = 100 %.
- **Logging & evidence:** schema-conformant events at ingest = 100 %; immutable retention; every change linked to EP-06.xx (trace §5 → §6 → §12).

Common Pitfalls (and the engineered countermeasure)

1. Pipelines as suggestions → Enforce non-bypassable gates; block merges/releases on fails; keep failing artifacts as proof.
2. One-time scanning → Treat checks as recurring gates; require coverage for changed entry points and boundary-enforcement events.
3. Manual hot-fixes/drift → Detect & reconcile drift; forbid out-of-band edits; require ADRs and rollback plans.
4. Open admin paths/side channels → Force all admin to traverse the PEP; test for alternate routes; block on detection.
5. Weak token handling → Run replay/substitution suites; enforce audience/issuer/signature; enable PoP/DPoP where scoped.
6. Standing privilege / partial PSM → Require dual-control JIT; block elevation when PSM health is red; alert on PSM gaps.

7. No evidence → Every release must have an EP-06.xx with tests and results; immutable, hash-verified.

Practitioner Guidance:

- Bind invariants first. Define no fail-open, AAL targets, token TTL/rotation and audience/issuer, PoP/DPoP scope, JIT + PSM, posture-bound SSO—give each a Test-ID and EP-06.xx.
- Automate the deny paths. Negative tests (replay/substitution, wrong audience/issuer, over-TTL, claim stripping, non-JIT elevation) should be mandatory pipeline gates.
- Keep changes atomic. Policy change = test change = evidence link in the same commit; reject partial updates.
- Prefer open, vendor-neutral enforcement. PDP policy in XACML or OPA/Rego; enforcement at API gateways, open-source proxies, or admission controllers.
- Operate with numbers. Track AAL coverage, token TTL distribution, refresh rotation rate, JIT windows, PSM coverage, MTTD/MTTR, failover pass rate; review quarterly.

Quick Win Playbook:

Title: Enforce Deny-by-Default Privileged Elevation with Dual-Control JIT + Full PSM on One Tier-0 Path

Objectives

1. Remove standing privileged access on a single Tier-0 admin path.
2. Require dual-control JIT for every privileged action.
3. Record 100 % of Tier-0 sessions with PSM.
4. Deny and alert on out-of-scope commands via allow-lists as code.
5. Produce immutable evidence suitable for V&V in EP-06.01 (indexed by EP-06.00).

Target: Enforce deny-by-default privileged elevation with dual-control JIT and full PSM on one Tier-0 path (§6.2, §6.3, §12).

Components/System: PAM platform; API gateway/PEP for the admin channel; credential vault; immutable evidence store.

Protects: Management plane from unauthorized elevation and untracked activity.

Stops/Detects: Non-JIT elevation, unapproved commands, unrecorded emergency access.

	Action: Remove standing admin; enable dual-control JIT; require PSM for Tier-0; deploy command/action allowlists as code; rotate credentials post-use. **Smoke test:** non-JIT = deny; approved JIT = allow + record; disallowed command = deny + alert. **Proof:** PAM policy-as-code diff; JIT approval tickets; PSM replay excerpt; allow-list CI report; rotation logs → Evidence Pack EP-06.01. **Metric:** 100 % Tier-0 actions via approved JIT; elevation window ≤ 60 minutes; 100 % Tier-0 sessions recorded; unauthorized commands → deny + alert = 100 %. **Rollback:** Reinstate prior bindings only under a time-bounded exception; archive superseded artifacts in EP-06.03.

Appendices

Appendix A: Engineering Traceability Matrix (ETM)

Req ID	Requirement (Inputs) (§5)	Technical Specifications (Outputs) (§6)	Core Principles (§7)	Control Mappings (§9)	Verification – Build Correct (§12)	Validation – Works Right (§12)	Evidence Pack ID
5.1	Centralized IdP integration	§6.4 Federated Identity & SSO	RP-05 Secure by Design; RP-03 Complete Mediation	OWASP ASVS V2, V3; CSA CCM IAM-06/08	IdP configured; signed federation metadata present; SAML/OIDC/OAuth interop tests pass.	Invalid/expired/assertion-tampered flows → deny with reason; end-to-end token exchange resists substitution	EP-06.06
5.2	MFA & Authentication Assurance (AAL)	§6.2 Authentication & Authorization	RP-01 Least Privilege; RP-02 Zero Trust; RP-10 Secure Defaults	CIS 6.3/6.4/6.5; CSA CCM IAM-14; OWASP ASVS V2	AAL scope for privileged groups; phishing-resistant factors enabled; re-auth on elevation configured	Tier-0 MFA bypass attempt → deny; elevation re-auth enforced; 100 % privileged sign-ins at AAL 2+	EP-06.03
5.3	PAM with JIT/PSM	§6.3 Privileged Access Management	RP-01 Least Privilege; RP-04 Defense in Depth; RP-03 Complete Mediation	CIS 6.5; CSA CCM IAM-05	JIT policies and PSM enabled; dual-control approvals required; allow-lists as code in repo	Non-JIT elevation = deny + alert; approved JIT = allow + record; elevation window ≤ 60 minutes; 100 % Tier-0 PSM coverage	EP-06.01 / EP-06.05
5.4	IGA/SCIM lifecycle & reviews	§6.1 Identity Governance & Lifecycle	RP-06 Minimize Attack Surface; RP-10 Secure Defaults;	CIS 5.3/5.5; CSA CCM IAM-06/08	SCIM jobs active; quarterly access reviews scheduled; orphan detection rules defined	Orphaned accounts removed ≤ 24 hours; certification closure ≤ 30 days;	EP-06.07

Req ID	Requirement (Inputs) (§5)	Technical Specifications (Outputs) (§6)	Core Principles (§7)	Control Mappings (§9)	Verification – Build Correct (§12)	Validation – Works Right (§12)	Evidence Pack ID
			RP-05 Secure by Design			privilege-creep trend declining	
5.5	ITDR integration	§6.5 Identity Threat Detection & Response	RP-15 Evidence Production; RP-04 Defense in Depth	— (frameworks in §9 applied elsewhere)	Telemetry schemas normalized; SIEM rules deployed; containment playbooks linked.	Compromise MTTD ≤ 15 minutes; MTTR ≤ 60 minutes with auto-containment (disable/revoke/terminate)	EP-06.09
5.6	Device posture validation	§6.2 Authentication & Authorization; §6.4 Federation & SSO	RP-02 Zero Trust; RP-03 Complete Mediation; RP-10 Secure Defaults	OWASP ASVS V2/V3; CIS 6.3/6.4	Conditional access tied to posture; PEP requires posture claims; tests defined	Posture downgrade → step-up/revoke; stripped posture claims → deny + log; privileged idle timeout ≤ 15 minutes	EP-06.03
5.7	Audit-ready logging	§6.5 ITDR (logging & evidence)	RP-15 Evidence Production	OWASP ASVS V2/V3 (eventing aspects)	Immutable store configured; retention/hash/time sync verified; schema fields present (trace_id, decision_id, assurance, device_posture)	Replayable auth + privileged timelines reconstructed from immutable logs; random audit samples pass.	EP-06.11
5.8	Service & Machine Identity governance	§6.1 Governance; §6.4 Token/Svc trust	RP-01 Least Privilege; RP-06 Minimize Attack	CIS 5.5; CSA CCM IAM-06/08; OWASP API2:2023	SMI inventory; vault/rotation policies; mTLS/signed tokens configured	Forced rotation does not break flows; stale/forged token/cert → deny; service-to-service calls	EP-06.08

Req ID	Requirement (Inputs) (§5)	Technical Specifications (Outputs) (§6)	Core Principles (§7)	Control Mappings (§9)	Verification – Build Correct (§12)	Validation – Works Right (§12)	Evidence Pack ID
			Surface; RP-18 Protect Confidentiality			require valid certs/tokens	
5.9	Separation of Duties (SoD) for IAM admin	§6.2 Authz; §6.3 PAM	RP-01 Least Privilege; RP-10 Secure Defaults	CSA CCM IAM-08; CIS 5.5	Role maps show distinct designer/enforcer/approver; dual-control JIT required.	Self-approval attempts blocked and logged; sampled JIT requests demonstrate dual control	EP-06.05
5.10	IAM availability objectives	§6.6 Resilience & Recovery; §6.4 Federation continuity	RP-20 Protect Availability; RP-10 Secure Defaults	—	HA/DR topologies and runbooks in place; key escrow/rotation plans documented	Planned failover meets RTO/RPO; no fail-open on auth/token/enforcement during failover.	EP-06.10
5.11	STS (short-lived tokens, rotation, PoP)	§6.2 Token Protections; §6.4 Token Security	RP-02 Zero Trust; RP-10 Secure Defaults; RP-04 Defense in Depth	OWASP ASVS V3; OWASP API2:2023; CIS 6.5; CSA CCM IAM-14	STS profile: access token TTL ≤ 60 minutes, rotating refresh, audience/issuer/signature checks	Replay/substitution/over-TTL → deny; PoP/DPoP verified on scoped APIs	EP-06.04
5.12	PDP/PEP placement	§6.2 RBAC/ABAC via PDP/PEP;	RP-03 Complete Mediation; RP-06 Minimize	OWASP ASVS V2; CSA CCM IAM-05	PDP/PEP map per entry point; policy bundle loads; deny path configured	PEP denies when PDP denies; downstream services preserve required claims	EP-06.02

Req ID	Requirement (Inputs) (§5)	Technical Specifications (Outputs) (§6)	Core Principles (§7)	Control Mappings (§9)	Verification – Build Correct (§12)	Validation – Works Right (§12)	Evidence Pack ID
		§6.4 PEP auditing	Attack Surface			(no injection/stripping)	
5.13	Protocol conformance & time sync	§6.4 Federation compliance; token age/skew	RP-05 Secure by Design; RP-10 Secure Defaults	OWASP ASVS V2/V3; CSA CCM IAM-14	Interop and negative tests pass; clock-skew bounds documented	Out-of-skew tokens rejected; audit shows skew reason and denial at the boundary	EP-06.06
5.14	Immutable evidence repositories	§6.5 Logging & Evidence	RP-15 Evidence Production	—	Evidence store: hash verification enabled; access controls set; retention applied.	Random sample reconstructs incidents from immutable artifacts; hashes attest integrity.	EP-06.11

Notes

- Sub-EP entries represent future IAM sub-standards to be developed; each will inherit this EP structure and include §6/§12 mappings and Quick Win artifacts.
- For every row, practitioners should record the Test-ID(s) executed and the exact EP-06.xx link in the project's register to keep traceability current.

Appendix B: EP-01 Summary Matrix – Evidence Pack Overview

Layer	EP Identifier	Purpose	Evidence Categories Included
Parent EP	EP-06.00	Stores annex-wide IAM evidence supporting §§5, 6, 10, and 12. Acts as the index/readme for all EP-06.xx sub-packs.	• Identity trust-boundary maps, identity/token flow diagrams, PDP/PEP placement • Invariants register (no fail-open, AAL targets, token contracts, JIT+PSM, posture) • Policy-as-code repo pointers (IdP/STS, PDP/PEP, PAM/JIT/PSM, SCIM) • Unified logging schema (fields incl. assurance, device_posture, decision_id) • Quick Win index and pass/fail summaries (refs to EP-06.01/02/03)
Sub-EP	EP-06.01	Privileged boundary hardening (JIT + PSM) for one Tier-0 path (§§6.3, 12).	• PAM policy-as-code diffs; dual-control JIT approvals • PSM session replays with hash manifest • Allow-list CI reports; deny events for out-of-scope commands • Rotation logs post-use • Quick Win: “Dual-Control JIT + Full PSM” smoke test results
Sub-EP	EP-06.02	Token & enforcement path: STS + PDP/PEP replay-resistance on one admin API (§§6.2, 6.4, 12).	• STS profile export (TTL ≤ 60 minutes, rotating refresh, aud/iss/signature) • Negative-test deny logs (expired/over-TTL, wrong audience/issuer, tampered sig) • PoP/DPoP verification records on scoped endpoints • PDP policy bundle diffs; PEP enforcement logs with decision_id • Quick Win: “STS + PDP/PEP V&V Smoke Suite” evidence
Sub-EP	EP-06.03	Assurance & posture: AAL-bound privileged access with posture-bound SSO (§§6.2, 6.4, 12).	• IdP conditional-access exports (AAL 2/3 scope, re-auth on elevation) • Auth telemetry showing AAL; posture change/step-up/revoke events • Privileged idle-timeout evidence (≤ 15 minutes)

Layer	EP Identifier	Purpose	Evidence Categories Included
			• PEP deny logs for stripped/missing posture claims • Quick Win: “AAL + Posture” test set
Sub-EP	EP-06.04	Token protections suite (contract enforcement) across critical paths (§§6.2, 6.4, 12).	• Token traces (TTL, aud/iss, rotation) • Replay/substitution denials; clock-skew test outputs • Library/config attestations for validation settings • PoP/DPoP negative/positive suites
Sub-EP	EP-06.05	PAM policy artifacts & privileged controls at scale (§6.3).	• Allow/deny command lists as code with CI • Break-glass workflow tickets and post-event rotation logs • Elevation windows and exception register with sunset dates
Sub-EP	EP-06.06	Federation/SSO conformance & negative tests (§6.4).	• SAML/OIDC/OAuth interop results and signed metadata • Assertion/token age, issuer/audience validation results • Skew-bound tests, substitution/replay denials
Sub-EP	EP-06.07	IGA/SCIM lifecycle & access reviews (§6.1).	• SCIM coverage/latency reports • Quarterly certification closure (≤ 30 days) • Orphan detection and remediation (≤ 24 hours) • Role/entitlement change logs
Sub-EP	EP-06.08	Service & Machine Identity governance (§§6.1, 6.4).	• SMI inventory (unique principals) • Vault rotation schedules/logs • mTLS/signed-token proofs • Forced-rotation “no-break” tests; stale cert/token denials
Sub-EP	EP-06.09	ITDR detection, correlation, and automated containment (§6.5).	• Normalized IdP/STS/PDP/PEP/PSM telemetry samples • SIEM correlation rule packs and alert timelines

Layer	EP Identifier	Purpose	Evidence Categories Included
			• MTTD ≤ 15 minutes / MTTR ≤ 60 minutes attainment with auto-containment logs
Sub-EP	EP-06.10	Resilience & DR: HA topologies and failover drills (§6.6).	• HA diagrams; quorum/health monitors • Planned failover logs showing no fail-open on auth/token/enforcement • RTO/RPO attainment reports; key rotation/escrow/recovery drill outputs
Sub-EP	EP-06.11	Immutable evidence configuration & integrity (§§6.5, 12).	• Evidence store retention config; hash manifests; access controls • Time-sync/NTP proofs • Random reconstruction samples (end-to-end auth/privileged timelines)
Sub-EP	EP-06.12	Traceability exports and matrix snapshots (§§5→12→6).	• ETM/traceability matrix snapshots • Change-set diffs linking Spec → Test-ID → EP-06.xx • Quarterly review sign-off records
Future Sub-EPs	EP-06.13+	Reserved for future IAM sub-standards.	• Will inherit the same EP structure, including Quick Win mapping and §6/§12 linkages.

Notes for editors

- Each EP-06.xx row should reference the exact §6 outputs and §12 Test-IDs exercised by its artifacts; record the invariant(s) proven (for example, “no fail-open,” “AAL 2+,” “TTL ≤ 60 minutes,” “dual-control JIT,” “posture-bound SSO,” “PoP/DPoP on scoped APIs”).
- The Parent EP-06.00 must include a human-readable index that points to every sub-EP, its location, checksum manifest, and the latest pass/fail status for associated Quick Wins.
- Sub-EP entries represent future IAM sub-standards to be developed; each will inherit this EP structure and include §6/§12 mappings and Quick Win artifacts.

Adoption References

NOTE: ISAUnited Charter Adoption of External Organizations.

ISAUnited formally adopts the work of the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) and the National Institute of Standards and Technology (NIST) as foundational standards bodies, and the Center for Internet Security (CIS), the Cloud Security Alliance (CSA), and the Open Worldwide Application Security Project (OWASP) as security control–framework organizations. This adoption aligns with each organization's public mission and encourages use by practitioners and institutions. ISAUnited incorporates these organizations into its charter so that every Parent Standard and Sub-Standard is grounded in a common, defensible foundation.

a) **Foundational Standards (Parent level).**
ISAUnited adopts *ISO/IEC* and *NIST* as foundational standards organizations. Parent Standards align with these bodies for architectural grounding and auditability, and extend that foundation through ISAUnited's normative, testable specifications. This alignment does not supersede *ISO/IEC* or *NIST*.
b) **Security Control Frameworks (Control level).**
ISAUnited adopts *CIS, CSA*, and *OWASP* as control framework organizations. Control mappings translate architectural intent into enforceable technical controls within Parent Standards and Sub-Standards. These frameworks provide alignment at the implementation level rather than at the foundational level.
c) **Precedence and scope.**
Foundational alignment (*ISO/IEC, NIST*) establishes the architectural baseline. Control frameworks (*CIS, CSA, OWASP*) provide enforceable mappings. ISAUnited's security invariants and normative requirements govern implementation details while remaining consistent with the adopted organizations.
d) **Mapping.**
Each cited control mapping is tied to a defined output, an associated verification and validation activity, and an Evidence Pack ID to maintain end-to-end traceability from requirement to control, test, and evidence.
e) **Attribution.**
ISAUnited cites organizations by name, respects attribution requirements, and conducts periodic alignment reviews. Updates are recorded in the Change Log with corresponding evidence.
f) **Flow-downs.**

Obsolete and withdrawn documents should not be used; please use replacements.

(Parent → Sub-Standard). Parent alignment to the International *ISO/IEC* and *NIST* flows down as architectural invariants and minimum requirements that Sub-Standards must uphold or tighten. Parent-level mappings to *CIS, CSA*, and *OWASP* flow down as implementation control intents that Sub-Standards must operationalize as controls-as-code, tests, and evidence. Each flow-down shall reference the Parent clause, the adopted organization name, the Sub-Standard clause that implements it, the associated verification/validation test, and an Evidence Pack ID for traceability. Any variance requires a written rationale, compensating controls, and a time-bounded expiry recorded with an Evidence Pack ID.

Change Log and Revision History

Review Date	Changes	Committee	Action	Status
December 2025	Standards Revision	Standards Committee	Publication	Draft v1 published
November 2025	Standards Submitted	Technical Fellow Society	Peer review	Pending
October 2025	Standards Revision	Task Group ISAU-TG39-2024	Draft submitted	Complete
December 2024	Standards Development (Parent D01)	Task Group ISAU-TG39-2024	Draft complete	Complete

End of Document
IO.