

Identity and Access Management Standard

Version 2.0 · Issued 13 October 2026 · Global Converged Security Board (GCSB)

Document control

Field	Value
Identifier	GCSB-ST-CSF-IAM-001
Title	Identity and Access Management Standard
Document type	Standard
Version	2.0
Status	Issued
Issue date	13 October 2026
Effective date	13 October 2026
Next scheduled review	13 October 2027
Issuer	Global Converged Security Board (GCSB)

Author	Prof. Dr. Vladimir Bunic
Owners	Prof. Dr. Vladimir Bunic and Global Converged Security Board (GCSB)
Reviewed by	Certification and Standards Committee
Approved by	Governing Council; approved for issue by Prof. Dr. Vladimir Bunic, President & Chair, 13 October 2026
Classification	General Use
Registered office	GCSB UK, Office 10595, 321-323 High Road, Chadwell Heath, Essex, RM6 6AX, United Kingdom
Published at	https://gcsb.uk/standards/csf-iam-001-identity-access

Contents

- 1. Foreword, status and intended use
- 2. Purpose, scope and applicability
- 3. Normative references and related documents
- 4. Terms and abbreviations
- 5. Roles, responsibilities and governance
- 6. Numbered identity requirements
- 7. Implementation and transition
- 8. Evidence, monitoring and corrective action
- 9. Exceptions, escalation and review
- 10. Document control and revision history

1. Foreword, status and intended use

1.1 Intended use

This standard connects identity proofing, authentication, authorisation, lifecycle, privileged access, federation, monitoring and continuity across cybersecurity, physical security and operational technology (OT) within an adopter's documented scope. It supports the Main, Strategic, Governance, Risk and Technology Integration and Architecture standards and interfaces with Data Protection and Privacy, Incident Response and Business Continuity, Training and Awareness, and the CCSO Policy.

1.2 Issuer and adopter

GCSB issues standards and makes recognition decisions under its certification arrangements. The adopter implements controls through its governing body, Chief Converged Security Officer (CCSO) or equivalent cross-domain executive, business owners, identity administrators and competent domain specialists. The adopter's IAM committee, Enterprise Risk Management Committee, Board Risk Committee and any corporate portal are adopter bodies and systems, not GCSB bodies or systems.

GCSB is not a training, consulting or audit provider. Adoption of this standard does not itself confer a credential, Trustmark Award, accreditation, statutory approval or any external certification (including under NIST, FIDO or ISO schemes). Certification of an individual authenticator or product is not certification of an entire deployment.

1.3 Drafting convention

"Shall" states a requirement, "should" states a recommendation, "may" states a permission and "can" states a capability. This standard applies lawful proportionality, vendor neutrality, safe OT operation and evidence-based requirements throughout.

2. Purpose, scope and applicability

2.1 Purpose

The purpose is accountable identity and access decisions, coordinated cross-domain lifecycle control and resilience, supported by lawful processing and verifiable evidence, expressed as outcome-based requirements rather than guarantees of eliminated vulnerability or specific business benefit.

2.2 Scope

The adopter shall document organisational entities, users, workforce and external identities, service/workload identities, facilities, systems, resources, security domains and material identity dependencies. Scope shall distinguish human authentication, machine access and physical entry, and identify systems where identity controls cannot safely use a common implementation.

Cloud, mobile, hybrid, voice/video/data integration and third-party access shall be addressed where present. An absent OT estate shall be explained, not invented. Joint ventures, vendors and downstream partners shall not be deemed wholly controlled simply because they access systems. Lawful agreements shall bound verification, information sharing, access rights, remediation and incident cooperation.

2.3 Applicable obligations

The adopter shall identify binding legal, regulatory, contractual and scheme obligations by entity, jurisdiction, sector and processing activity. UK and EU GDPR, NIS2 implementing measures, DORA, eIDAS (including the amended European Digital Identity framework under Regulation (EU) 2024/1183 where applicable), phased CRA/AI Act provisions and relevant North American instruments shall each be assessed on their own terms and shall not be treated as universal equivalents of one another.

NIST guidance is not automatically a statute or certification programme. Instruments such as FISMA, FICAM, CMMC/CUI requirements, HIPAA, state privacy and financial rules, and Canadian federal and provincial laws have distinct scopes and shall be verified for applicability rather than assumed.

A "most restrictive" formula cannot resolve laws that differ in jurisdiction, object or actual conflict. Required changes shall meet binding effective dates; a post-effective-date allowance is not a grace period for unlawful non-compliance.

3. Normative references and related documents

3.1 Controlled reference approach

Each reference used by the adopter shall be identified by exact title, edition, applicable provisions, normative or informative status and availability. Reference names do not incorporate entire frameworks or establish a conformity scheme by themselves.

Reference	Role
GCSB-ST-CSF-001	Master scope and baseline identity requirements
GCSB-CSF-STRAT and GCSB-ST-CSF-GLA-001	Direction, adopter oversight and delegated authority
GCSB-ST-CSF-RMA-001	Risk, coverage, business impact analysis, response and competence interface
GCSB-ST-CSF-TIA-001	Architecture, SIEM/PSIM integration, safe OT operation and technology assurance
GCSB-ST-CSF-DPP-001, GCSB-ST-CSF-IRBC-001, GCSB-ST-CSF-TRA-001 and GCSB-POL-CSF-CCSO-001	Privacy, incident response and continuity, competence, and executive role
Associated guidance, where issued by GCSB	Terminology and supporting implementation material
NIST SP 800-63 series (current edition), SP 800-207, SP 800-53, SP 800-30, IR 8286, as applicable	Identity, zero trust, control and risk guidance
ISO/IEC 27001:2022, ISO 31000:2018, ISO 22301:2019, ISO/IEC 29115, ITU-T X.1254	Management, risk, continuity and assurance references
SAML, OpenID Connect, OAuth, SCIM, WebAuthn/FIDO2, LDAP, TLS	Federation, authorisation, provisioning and authenticator/transport specifications

The adopter shall select exact revisions and profiles of the protocols and guidance above and keep pace with current security guidance; these are distinct specifications and are not interchangeable.

3.2 Mapping and authenticity

Mappings between this standard and external frameworks (for example NIST CSF outcomes or ISO/IEC 27001:2022 Annex A controls) shall use the current edition of each framework and checked clause-level evidence, not a mechanical label change. OAuth addresses authorisation; OpenID Connect addresses identity authentication built on OAuth; SCIM addresses provisioning; a JWT is a token representation. FIDO2/WebAuthn authenticator capability does not by itself establish a particular NIST authenticator assurance level, general federation capability, or universal passwordless multi-factor use. Identity assurance, authenticator assurance and federation assurance are separate dimensions. No specific availability or success benchmark is attributed to NIST or FIDO without supporting evidence; any such figures used by the adopter are illustrative examples, not commitments or guarantees.

4. Terms and abbreviations

Term	Meaning
Converged security	Coordinated cybersecurity, physical security and OT security within documented scope
CCSO	Chief Converged Security Officer or equivalent cross-domain executive
Identity proofing	Evidence-based establishment of an identity within a defined assurance process
Authentication / authorisation	Establishing control of authenticators / determining permitted actions and access
IAL / AAL / FAL	Identity-proofing / authentication / federation assurance dimensions under the adopted guidance edition
MFA	Authentication using distinct factor categories; not simply two steps of the same factor
IdP / federation	Identity provider / scoped trust and assertion arrangements between parties
Provisioning / deprovisioning	Authorised lifecycle creation or change of access / removal or disabling of access, not necessarily immediate deletion of records
Privileged access	Elevated capability requiring accountable approval, bounded use and appropriate monitoring
Coverage	Accepted integrations divided by a defined eligible population, with documented evidence
Availability / success / accuracy	Service accessibility / completed authentication or workflow outcomes / correctness against defined evidence; distinct measures
Hybrid / systemic / cascading	Risk or incident types, separate from severity and command level
Exception	Authorised deviation within lawful bounds; neither a statutory exemption nor a recognition entitlement

5. Roles, responsibilities and governance

5.1 Issuer control

Development and review of this standard sit with the Certification and Standards Committee; institutional approval sits with the Governing Council. Recognition decisions follow the single GCSB certification procedure; appeals go to the Appeals body established under the GCSB Governance Charter.

5.2 Adopter accountability

The governing body shall oversee identity risk and reserved material decisions. The CCSO shall coordinate cross-domain identity and access management through lawful delegation, reporting to the chief executive or equivalent leadership with regular direct board communication.

The adopter shall maintain a Cross-Domain IAM Governance Committee, including competent domain, risk, legal/compliance, HR and business representation, meeting monthly with recorded decisions and monthly reporting to the CCSO. The committee's policy approval authority and the CCSO's final authority shall be distinguished from governing-body reservations and emergency delegation.

Business owners shall approve access need and reviews; HR or other authoritative sources shall provide timely lifecycle events. IT, physical, OT, safety, identity, privacy and legal owners retain their competent responsibilities, and independent assurance shall be distinguishable from control operation. A data protection officer, where appointed, advises and monitors; controller decision accountability and the independence of that advisory role shall both be preserved, and approval of privacy impact assessments shall remain a controller decision informed by that advice.

5.3 Governance changes

Emergency operational changes shall stay within lawful authority. The adopter shall define and document its own approval, expedited review and consultation timeframes for governance changes, proportionate to risk. A mandatory statutory action shall not wait for an administrative consultation window.

6. Numbered identity requirements

6.1 Identity architecture and authoritative sources

6.1.1 The adopter shall maintain identity/resource inventories, architecture, data flows, trust boundaries, dependencies and accountable owners covering scoped human, third-party and machine identities.

6.1.2 Authoritative sources and reconciled identity mappings shall be documented with conflict handling and privacy controls. The adopter shall define and document its identity platform architecture, identifier strategy and provisioning model. A shared identifier shall not confer access automatically or justify unrestricted cross-domain tracking.

6.1.3 The adopter shall define and document platform support, integration coverage, capacity and performance targets proportionate to its scale, using vendor-neutral and capacity-proportionate criteria.

6.2 Authorised lifecycle control

6.2.1 Provisioning and changes shall follow authoritative triggers, business justification, role/segregation checks, appropriate approvals and recorded evidence. Emergency or manual provisioning shall be validated promptly against those criteria.

6.2.2 Lifecycle timing shall distinguish request approval, completed provisioning, attribute propagation, access suspension and detailed deprovisioning. The adopter shall define and document its own timeframes for standard and critical provisioning, modifications, reconciliation, discrepancy resolution and termination revocation, proportionate to risk.

6.2.3 Planned-departure preparation shall be bounded by actual notice availability. Leave and role changes shall receive lawful, need-based access decisions and shall not automatically receive the same treatment as termination. Disabled records, evidence and eventual deletion shall be governed separately.

6.2.4 Cross-domain consistency shall be validated with failure alerts, reconciliation and safe remediation. Any automated rollback on failed synchronisation shall not silently restore revoked access or compromise emergency egress or OT safety.

6.3 Authentication and credential protection

6.3.1 The adopter shall establish documented assurance and multi-factor authentication controls for resources and users, distinguish factor categories and authenticator assurance, and evidence phishing resistance where required, including safe treatment of legacy, OT and emergency interfaces. No bypass of these controls is authorised by this standard.

6.3.2 Authentication shall address binding, recovery, compromise, rate limits and sessions. The adopter shall adopt a current password and credential policy consistent with current NIST SP 800-63B guidance (or an equivalent current standard it selects and documents), rather than fixed composition and rotation rules that may conflict with current guidance.

6.3.3 Session, assertion and token lifetimes shall be defined coherently by service and protocol capability. Secure logout, revocation and step-up authentication decisions shall reflect actual service and protocol capability, not an unsupported universal instantaneous federated logout.

6.3.4 Biometric deployment shall address lawful basis, any required special-category condition, necessity, accessible alternatives, template protection and presentation-attack resistance. Consent and enrolment timing shall follow the adopter's documented, lawful process. Template protection shall use technically effective methods; an ordinary one-way hash does not by itself provide biometric fuzzy matching or guaranteed non-reconstruction, and legal permission and technical effectiveness are separate questions to be addressed together.

6.4 Authorisation, roles and segregation

6.4.1 Access decisions shall enforce least privilege, documented business need, role boundaries and segregation of conflicting duties across relevant domains, with explicit emergency and small-estate safeguards.

6.4.2 Elevated access shall be approved, bounded, logged and revoked. The adopter shall define and document standard, emergency and recovery-token access periods appropriate to risk. Annual role revalidation and dormant-role revocation shall be scoped so that unused emergency roles and service identities are not removed unsafely by inference.

6.4.3 Reviews shall be owner-performed with remediation evidence. The adopter shall define and document review frequencies for standard, privileged and critical access appropriate to risk; an annual strategic review does not waive a more frequent operational review where risk requires it.

6.5 Privileged and emergency access

6.5.1 Privileged identities shall have inventory, individual accountability, approved use, protected credentials, appropriate session oversight, separation of approval from use and monitored third-party access. No self-approval is permitted, and multi-person authorisation shall apply where proportionate.

6.5.2 Privileged access management (including vaulting of privileged credentials, encryption, rotation, session oversight and monitoring) shall be implemented in a manner proportionate to risk and consistent with privacy obligations. No

general right to inspect unrelated worker data is created by this standard.

6.5.3 Break-glass access shall remain bounded and traceable, with prompt notification to accountable roles, timely review and restoration. Offline emergency credentials shall not become an indefinite, unreviewed route around controls.

6.6 Federation and secure integration

6.6.1 Federation shall define trust, actual assurance, accepted assertions, attribute purpose and minimisation, signatures, audiences, replay handling, expiry, revocation capabilities, keys and agreement responsibilities. External providers shall receive periodic risk and security review, with assessment rights bounded by law and contract.

6.6.2 Provisioning, authentication and authorisation protocols shall be selected for their actual functions and current versions. Protocol selection shall not authorise collecting passwords, tokens or excessive personal data in logs.

6.6.3 Integrations shall be tested before production and compatibility validated periodically. Safe change, rollback, failover, partial-failure behaviour and dependency recovery shall be documented, including assurance equivalence and continuity where secondary identity providers are used.

6.7 Monitoring, analytics and risk response

6.7.1 Relevant identity events shall be monitored and correlated across scoped domains with lawful evidence, restricted access, validated alerts, incident authority and investigation records. Identity risks shall be assessed at least annually and registers updated quarterly or on material change.

6.7.2 Where analytics or automated tooling, including AI/ML, are used, the adopter shall address representative data, model limitations, drift, uncertainty, error rates and accountable human authority. No specific accuracy or false-positive figure is mandated by this standard; any figures the adopter publishes are illustrative examples, not commitments or guarantees.

6.7.3 Incident handling shall distinguish incident type (for example hybrid, systemic or cascading), category (for example credential, cross-domain or systemic) and impact severity. Immediate suspension and automated quarantine shall be authorised, safety-aware and linked to continuity. The adopter shall define and document risk-ranked remediation timeframes proportionate to likelihood and impact.

6.8 Privacy, retention and information control

6.8.1 The adopter shall document actual controller/processor responsibilities, lawful bases, applicable special-category conditions, transparency, rights, contracts, privacy safeguards and data protection officer advice. The decision to conduct a data protection impact assessment shall distinguish legal high-risk triggers from any stricter internal rule the adopter chooses to apply.

6.8.2 Records shall receive sensitivity-appropriate classification, integrity, access, purpose-based retention and validated disposal. Retention periods shall be set by the adopter to meet its legal and operational needs and are not automatically a statutory minimum. Deletion from backups, logs and distributed stores shall follow a feasible disposal, isolation, lawful-hold and restoration process, rather than either an instant-erasure promise or indefinite retention.

6.8.3 International transfers shall use applicable UK and EU transfer mechanisms and risk assessments appropriate to the destination and transfer, selected from the lawful mechanisms available at the time.

6.8.4 Breach assessment shall distinguish controller-to-regulator, processor-to-controller and high-risk affected-person communication, with legal awareness events and conditions applied correctly. Cross-domain investigation complexity does not extend a binding statutory clock. For data-subject rights timing, the UK rule applicable at the time shall be applied; for the EU, requests shall be handled within the period set by applicable EU and Member State law. Consent withdrawal and other rights shall be honoured under applicable law; technical feasibility considerations shall not become a reason to ignore a withdrawal or continue processing without a lawful basis.

6.9 Resilience, recovery and safe OT

6.9.1 Identity recovery shall be based on documented business impact, safety, dependencies, recovery order, restored integrity and continuity interfaces. The adopter shall define and document recovery time and recovery point objectives, offline capacity and failover arrangements proportionate to criticality.

6.9.2 Recovery exercises shall be conducted periodically to validate failure, fallback, restoration and evidence, with corrective actions tracked to closure within a documented timeframe. Emergency access shall be reviewed promptly after normal operations resume, and credentials revoked on completion of recovery.

6.9.3 Zero-trust and dynamic access changes shall address device/resource capability, human authentication versus service operation, safety/egress, authorised maintenance and offline continuity. Automatic quarantine, continuous authentication and legacy replacement in OT environments shall be applied only where safe, not as unsafe automatic disconnection.

6.10 Competence, suppliers and evidence

6.10.1 Role-based competence and training shall address identity operations, privacy, cross-domain risks, response and recovery, with timeframes and assessment standards that the adopter defines and documents, aligned with the Training and Awareness standard.

6.10.2 Periodic exercises (for example phishing simulations), content updates and post-incident or post-change training refreshers shall be conducted. Training shall be accessible and appropriate to personnel and access risk. Adopter competence assessment does not itself constitute GCSB certification or continuing professional development recognition.

6.10.3 Supplier verification, sponsorship, expiry, risk assessment, periodic reviews, integration tests and lawful agreements shall be evidenced. Background checks and any third-party audit requirements (for example under SOC 2 or ISO schemes) shall be applied only where actually required by applicable law, contract or scheme, correctly attributed to the relevant regime.

6.10.4 Evidence shall support identity scope, architecture, proofing/access decisions, lifecycle events, reviews, privileges, federation, risks, legal applicability, monitoring, recovery, training, suppliers, exceptions and corrective actions. Metric definitions shall separate authentication success, service availability, record accuracy, workflow compliance and statutory compliance.

7. Implementation and transition

Full implementation is required within 12 months from certification commencement, with a gap assessment of existing systems within 6 months.

Activity	Timing from certification commencement
Initial assessment	Within 60 days
Gap analysis, roadmap and governance	Within 90 days
Identity provider in place	Month 4
Multi-factor authentication for privileged accounts	Month 5
Role-based access and HR integration	Month 6
Existing-system gap assessment	Within 6 months
Privileged access management	Month 7
Risk-based authentication	Month 8
Physical access and federation; high-risk systems compliant	Month 9
Monitoring	Month 10
Testing and training	Month 11
Full implementation	Month 12
Reports	Monthly to the CCSO; quarterly to the Enterprise Risk Management Committee; GCSB progress report every 90 days
Cutover approval	At least 30 days before cutover

Extensions are handled as exceptions under clause 9. No emergency, incident or legal obligation is automatically suspended.

8. Evidence, monitoring and corrective action

The adopter shall maintain and evidence operational review cadences for all-user, privileged and critical access, proportionate to risk, together with periodic independent risk and maturity assessment and regular compliance reporting.

Metric claims require population, calculation method, observation period, load, evidence, owner, target, exclusions and escalation path. Availability, success, accuracy, automation and compliance are distinct measures and shall not be combined into a single aggregate figure; statutory compliance cannot be reduced to a permissive aggregate percentage. Any performance or compliance figures published by the adopter are illustrative examples, not commitments or guarantees.

Certification acknowledgement, completeness review, assessment and decision timeframes, recertification, self-assessment, material-change notice and appeal periods are set by the single GCSB certification procedure referenced by this suite. Appeals may be made within 30 days of notification to the Appeals body established under the GCSB

Governance Charter. Disputes are governed by the laws of England and Wales and subject to the exclusive jurisdiction of the courts of England and Wales; the parties may agree to mediation first; no compulsory arbitration applies; statutory rights of regulators and data subjects are unaffected.

Corrective actions shall be risk-ranked, owned, tracked and validated, with timeframes that the adopter defines and documents proportionate to risk; an urgent safety or legal duty shall not wait for an administrative maximum. Independent assessments shall not portray GCSB as an audit provider.

9. Exceptions, escalation and review

The CCSO may approve temporary exceptions up to 12 months; longer exceptions only by the Board Risk Committee on recommendation of the Enterprise Risk Management Committee; all exceptions are reviewed quarterly. The CCSO may delegate in writing the approval of exceptions of up to 30 days to IT managers, with each delegation recorded, time-bounded and reviewed quarterly; the CCSO remains accountable for every delegated approval.

Exceptions affecting multi-factor authentication for privileged accounts and other critical controls shall be differentiated from ordinary exceptions by activity and risk; formal deviation does not itself permit unsafe emergency operation or waive the law. Consultation with a critical-infrastructure regulator applies only where actually required by law or contract, not as a blanket requirement.

Each exception shall record requirement, necessity, affected scope and population, risk, compensating controls, authority, duration, monitoring, remediation and closure evidence, with regular reporting to the CCSO, periodic domain assessment, quarterly review and a fresh risk assessment on renewal. Processing time or extension documentation does not create automatic approval. Emergency access remains logged, bounded, authorised and reviewed.

10. Document control and revision history

Version	Date	Change	By
2.0	13 October 2026	Version 2.0: consolidated, aligned suite edition (identifiers, approval route, law and disputes, exceptions, implementation timetable, appeals)	GCSB
Transfer edition	10 October 2026	Issuing authority, ownership, copyright and jurisdiction transferred from CSI to GCSB (UK); content unchanged; not a separate version	GCSB
1.0	2025	First edition, issued by the Converged Security Institute (CSI)	Prof. Dr. Vladimir Bunic

Superseded edition: the 10 October 2026 transfer edition.

© 2026 Prof. Dr. Vladimir Bunic and Global Converged Security Board (GCSB). All rights reserved.