

Technology Integration and Architecture

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-TIA-001
Title	Technology Integration and Architecture
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-tia-001-technology

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 technology requirements
- 7. Implementation and transition
- 8. Evidence, monitoring and corrective action
- 9. Exceptions, escalation and review
- 10. Document control and revision history

I. Foreword, status and intended use

I.1 Intended use

This standard connects architecture, monitoring, integration and authorised response across cybersecurity, physical security and operational technology (OT) within an adopter's documented scope. It supports the Main Standard, Strategic direction, Governance accountability and Risk assessments, with Identity, Data Protection, Incident Response and Training interfaces.

I.2 Issuer and adopter

GCSB issues standards and makes recognition decisions under separately authorised arrangements. The adopter implements controls through its governing body, Chief Converged Security Officer (CCSO) or equivalent cross-domain executive, technology owners and competent specialists. An adopter's SOC, architecture authority and risk committees are not GCSB bodies.

GCSB is not a training, consulting or audit provider. Technical conformity does not itself confer a credential, Trustmark Award, accreditation, ISO certification, statutory approval or product endorsement. Any recognition scheme operated by

GCSB, its criteria, availability, powers and service commitments are set out in the GCSB certification procedure, not in this standard.

1.3 Drafting convention

"Shall" denotes a requirement, "should" a recommendation, "may" a permission and "can" a capability. Proportionality, lawful data handling, safe OT operation, vendor neutrality, conditional analytics and scheme separation are substantive requirements of this standard.

2. Purpose, scope and applicability

2.1 Purpose

The purpose is accountable interoperability, coordinated monitoring and authorised cross-domain response supported by evidence of effectiveness, resilience and lawful operation. This standard states intended outcomes; it does not guarantee prediction certainty, market differentiation or automatic recognition.

2.2 Scope

The adopter shall document entities, facilities, systems, services, personnel, security domains, data flows, suppliers and material dependencies in scope. The scope shall cover relevant SIEM, physical security monitoring, interfaces, identity services, cloud/hybrid infrastructure and analytics used for security coordination. An absent OT estate shall be explained, not invented.

Exclusions, legacy limitations and externally controlled dependencies shall be recorded with risk and compensating arrangements. Joint ventures, suppliers and partnerships shall not be deemed wholly controlled solely because they access organisational systems. Information exchange, assessment access and response authority shall be bounded by actual control, contracts and applicable law.

2.3 Applicable obligations

The adopter shall maintain an applicability register by entity, jurisdiction, sector, service and processing activity, distinguishing binding law, contracts, scheme rules and voluntary technical references. UK and EU GDPR, NIS2 national implementing measures, DORA and phased CRA requirements shall not be treated as universally applicable or interchangeable retention laws.

Conflicting obligations shall be escalated for competent legal resolution; "the most restrictive requirements apply" shall not be used as a universal rule when obligations differ in object, jurisdiction or conflict. This standard does not waive law, grant regulator powers, determine court forum or create an executed agreement through technical text.

3. Normative references and related documents

3.1 Controlled reference approach

References are cited by exact title, edition, applicable provisions and normative/informative status, as recorded by the adopter. A name or assessment dimension is not blanket incorporation of an entire external framework.

Reference	Role
GCSB-ST-CSF-001	Master scope, baseline controls and adopter exception authority
GCSB-CSF-STRAT	Strategic direction and transition dependencies
GCSB-ST-CSF-GLA-001	Adopter accountability, reporting and lifecycle oversight
GCSB-ST-CSF-RMA-001	Risk criteria, integration populations, business impact analysis and control evaluation
GCSB-ST-CSF-IAM-001, GCSB-ST-CSF-DPP-001, GCSB-ST-CSF-IRBC-001, GCSB-ST-CSF-TRA-001, GCSB-POL-CSF-CCSO-001	Access, privacy, response, competence and executive role
Associated guidance, where issued by GCSB	Terminology, technical detail, implementation and response material
NIST SP 800-207 and SP 800-82 Rev. 3	Zero trust concepts and OT safety/security guidance, informative references
ONVIF; STIX/TAXII; OAuth; TLS; EN 50131; EN 50518	Specialist interfaces, exchange, authorisation and physical security references

The exact profiles, parts, editions and applicability of each specialist reference shall be selected and documented by the adopter before normative incorporation.

3.2 Reference corrections

OAuth is an authorisation framework, not by itself an identity-authentication protocol. Federation/authentication protocols and mutual TLS shall be distinguished from authorisation, with exact versions and threat models recorded. European and ISO reference labels do not by themselves specify an encryption algorithm, key-management practice or physical system grade.

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 under the Main Standard
SIEM	Security Information and Event Management capability for collection, analysis and security-event coordination

PSIM	Physical Security Information Management capability for relevant physical-system information and coordination
Cross-domain integration	Technical and operational interoperability supporting authorised monitoring, analysis and response across scoped domains
Unified platform	Coordinated capabilities and operating view, whether through a single platform or a federated architecture, as the adopter shall define and document
Hybrid / systemic / cascading	Incident and risk types, not severity levels
Zero trust	Resource-focused access decisions without implicit trust solely from network location or ownership
Coverage	Accepted integrations divided by a defined eligible population, with a measurement window and evidence
Availability	Availability of a specified service over a specified observation period with documented calculation and exclusions
Automated response	Actions performed through authorised, bounded playbooks with safety, privacy and continuity safeguards
Adopter exception / scheme concession	Internal deviation approval under the Main Standard's authority, or a separately governed assessment decision; neither waives law

5. Roles, responsibilities and governance

5.1 Issuer control

Development and review sit with the Certification and Standards Committee and relevant consultation panels; institutional approval sits with the Governing Council under its Charter. Assessment and suspension decisions follow the single GCSB certification procedure; appeals go to the Appeals body established under the GCSB Governance Charter. Issuer bodies shall not be confused with adopter committees.

5.2 Adopter accountability

The governing body shall oversee technology risk and reserved decisions. The CCSO shall coordinate cross-domain architecture and operations through lawful delegation and maintain access to executive and board oversight in line with the Governance Standard. CTO/CISO, physical security, OT, identity, privacy, safety and service owners shall retain defined domain responsibilities.

Architecture, operation, risk acceptance, independent assurance and legal advice shall be distinguishable. A Data Protection Officer's advice and monitoring shall not be equated with deciding every processing purpose or operational action. Administration privileges, emergency authority, third-party access and change approval shall be documented.

5.3 Competence and operational authority

The adopter shall evidence competence for architecture, integration, monitoring, incident coordination, data handling and safety-relevant changes. This standard does not introduce a new professional CPD quota or replace the Main Standard's, Governance Standard's or Risk/Training competence measures. Response procedures shall identify command, escalation, operational fallback and emergency authority; critical safety action shall not be delayed awaiting an issuer assessment decision.

6. Numbered technology requirements

6.1 Architecture and inventory

6.1.1 The adopter shall maintain architecture and data-flow records identifying scoped systems, owners, dependencies, interfaces, trust boundaries, identity services and shared failure points across cybersecurity, physical security and OT.

6.1.2 Architecture decisions shall document risk, continuity, safety, privacy, capacity and integration requirements with acceptance evidence. SIEM and PSIM deployment may be achieved through a coordinated or federated architecture as well as a single platform, provided equivalence is evidenced.

6.2 Cybersecurity monitoring and coverage

6.2.1 The adopter shall collect and analyse relevant cybersecurity events from the scoped network, endpoint, identity and application systems, with evidence of source identity, ingestion, time handling, completeness and authorised access.

6.2.2 The adopter shall define the eligible population of cybersecurity sources and the overall cross-domain population, which are not assumed identical, and shall set and evidence a coverage target against the defined population. Exclusions and critical uncovered dependencies shall be recorded; no aggregate percentage substitutes for unmet binding duties.

6.3 Physical security monitoring

6.3.1 The adopter shall coordinate information from relevant physical access, surveillance, intrusion, environmental and perimeter systems within lawful scope, with traceable interfaces, operational visibility and appropriate access restrictions.

6.3.2 Physical monitoring and command capability shall be outcome-based and proportionate to the estate; PSIM, all-facility centralisation, ONVIF support and EN 50131/EN 50518 application shall be applied where appropriate to the adopter's facilities, not assumed mandatory for every estate. Physical command actions shall respect emergency egress, safety and local operational authority.

6.4 Interoperability and shared operational visibility

6.4.1 The adopter shall document and validate cross-domain integration contracts, event semantics, access, integrity, error handling, supported response actions and monitoring of interface failure. Cross-domain information sharing shall apply lawful minimisation and use restricted exchange where appropriate.

6.4.2 Unified operational views shall display relevant threat information, incidents and metrics with role-based access, least privilege and traceable ownership. Any stated "real-time" capability shall be defined by task and measured latency, not assumed against an undefined common clock.

6.4.3 Interfaces shall use justified security controls and controlled credentials, authorisation, transport protection and rate limits. Mutual TLS, OAuth2, STIX/TAXII and ONVIF profiles, and SIEM platform support, shall be selected and documented according to the adopter's architecture; no specific vendor product is mandated by this standard.

6.5 Identity, least privilege and zero trust

6.5.1 Access to integrated systems shall be governed through documented identities, roles, privileged access, authentication, lifecycle and review arrangements aligned with the Identity and Access Management Standard. Shared identity services shall have continuity and recovery arrangements.

6.5.2 Zero-trust decisions, segmentation and least privilege shall address resources, users, devices, trust boundaries and context within scoped IT/OT operations. Continuous authentication and dynamic micro-segmentation shall be evaluated against safety, availability and legacy constraints before deployment and shall not displace the Main Standard's or Identity and Access Management Standard's requirements.

6.6 Analytics and model assurance

6.6.1 Where analytics support operations, the adopter shall document purpose, relevant data, lawful use, model limitations, validation, drift, error measures and accountable decision authority. Claims of detection or prediction effectiveness shall be supported by scoped evidence, not a benefit guarantee.

6.6.2 The use of artificial intelligence and machine learning shall be risk-based and conditional on the adopter's scope rather than mandatory across all domains. Dataset age alone does not prove representativeness or accuracy; live testing of such capability requires authorised safeguards.

6.7 Authorised response and resilience

6.7.1 The adopter shall maintain cross-domain response procedures for hybrid, systemic and cascading scenarios and integration failures, distinguishing incident type, severity and command/escalation level.

6.7.2 Automated playbooks, security orchestration, containment and physical/OT actions shall be bounded by documented authority, safety, privacy, continuity, logging and fallback. Cross-domain response shall align with the Risk Management Standard and the Incident Response and Business Continuity Standard.

6.7.3 The adopter shall document and exercise failure of monitoring, identity, integration and analytics services and validate safe restoration. Availability, recovery and detection targets shall be defined by service and measurement event. A 99.9% availability target, where used, is an indicative value the adopter shall confirm in its own procedures and is not a universally achievable commitment or a substitute for the Risk Management Standard's recovery time and recovery point objectives.

6.8 Privacy and information lifecycle

6.8.1 The adopter shall identify actual controllers/processors, lawful bases, applicable special-category conditions and required processing records and agreements for integrated personal data. Security monitoring is not automatically

lawful under legitimate interests; an Article 9 condition does not replace an Article 6 basis.

6.8.2 Data flows shall address necessity, minimisation, access, privacy by design and default, retention, subject rights, transfers and disposal under applicable law. Automated deletion and any data localisation shall be consistent with lawful preservation obligations and actual territorial and sectoral requirements; neither unrestricted retention nor universal EU residence is required by this standard.

6.8.3 Breach procedures shall distinguish controller regulator notification, processor-to-controller reporting and affected-person communication. In the UK, notification to the supervisory authority shall be made without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, where required by law. In the EU, notification timing is governed by the period set by applicable EU and Member State law. Legal rights shall not be denied solely because monitoring effectiveness is required.

6.9 Lifecycle, change and supplier control

6.9.1 The adopter shall maintain documented configuration, change, integration testing, supplier dependencies, operational procedures and incident evidence. Material changes shall be assessed for risk, safety, privacy, interoperability and recognition implications through actual delegated authority.

6.9.2 Technology assurance and access rights shall be lawful, necessary, bounded and independently governed where applicable. GCSB is not an audit provider; any recognition verification arrangements are set out in the GCSB certification procedure and shall not grant unrestricted technical access.

6.10 Measurement and evidence

6.10.1 Every coverage, availability, latency, correlation and effectiveness measure shall define service/population, calculation, measurement window, evidence, target, owner, exclusions and escalation. Different populations shall not share a percentage by inference.

6.10.2 Architecture, tested integrations, incidents, roles, data handling, risk decisions, exercises, supplier controls, exceptions and corrective actions shall be supported by traceable records. Progress reports, periodic performance reports and an annual self-assessment shall be maintained; duplicate presentations may be consolidated provided the underlying duty and reporting trigger are preserved.

7. Implementation and transition

This standard uses the documented extended track: full implementation within 18 months from certification commencement, with a gap assessment of existing systems within 6 months.

Activity	Timing from certification commencement
Initial architecture and existing-system gap assessment	Within 6 months
Foundation monitoring (SIEM/PSIM or approved equivalent) covering the defined population	Within 8 months
Integration development and operational readiness	Within 12 months

Full operational capability	Within 18 months
Progress reports	Every 90 days
Final assessment	Within 60 days of declared full capability
Extension request	At least 30 days before the affected milestone, handled under clause 9

Controls required by the Main Standard and the Risk Management Standard within their 12-month baseline continue to apply during the extended track; the 18-month track does not extend them.

8. Evidence, monitoring and corrective action

The adopter shall monitor controls and material changes, maintain corrective actions with owner, priority, due date, validation and escalation, and provide accurate evidence of scoped conformity, including an annual self-assessment, periodic metrics, continuous monitoring and 90-day implementation progress reporting.

Certification process timescales, including acknowledgement, completeness checks, assessment, decision, periodic certification review and policy review and amendment notice, are set by the single GCSB certification procedure. Figures used for illustration in this standard are illustrative examples, not commitments or guarantees.

Conditional certification, suspension, remediation and reapplication arrangements are governed by the GCSB certification procedure, applied proportionately and with procedural fairness. A minor deficiency does not permit breach of binding law. Certification and enforcement decisions may be appealed within 30 days of notification to the Appeals body established under the GCSB Governance Charter.

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 reviewed quarterly.

Requests for a scheme concession shall be made in writing at least 90 days before assessment with a mitigation plan, and are decided under the single GCSB certification procedure, valid for no more than two years with reapplication. Scheme concessions are separate from internal exceptions and are never granted automatically.

Each deviation shall record affected requirement, necessity, risk, compensating controls, owner, lawful authority, duration, review and remediation. Cost or convenience alone is not sufficient justification for a scheme concession; equivalence shall be evidenced, not asserted. Neither an internal exception nor a scheme concession waives binding law, authorises unsafe action or grants a recognition entitlement.

Material changes and emergency operating decisions shall be managed within lawful delegation and reviewed by competent authorities, without prejudice to earlier statutory or urgent safety duties. This document and any dispute arising from it 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.

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.