

Converged Security Framework

Main Standard

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-001
Title	Converged Security Framework Main 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-converged-security-framework

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

1. Foreword, status and intended use

This standard establishes the main requirements for integrating cybersecurity, physical security and operational technology security within a unified risk management approach. It addresses hybrid, systemic and cascading risks across organisational dependencies.

GCSB is the issuing standards and credential governance authority. The adopting organisation is responsible for implementation. Its executives, committees and security personnel are not GCSB offices merely because they implement this standard. GCSB does not act as a training, consulting or audit provider.

Adoption of this standard does not itself confer statutory authority, ISO certification, GCSB accreditation, a professional credential or a Trustmark Award. Such recognition is subject to the separately applicable scheme and independent decision processes.

2. Purpose, scope and applicability

2.1 Purpose

The standard defines minimum requirements for integrating security governance, risk assessment, technology, identity, response, continuity, training, third-party management and privacy. It supports alignment with ISO 31000:2018, ISO/IEC 27001:2022 and ISO 22301:2019 without promising a guaranteed business outcome or treating those publications as interchangeable.

2.2 Organisational scope

The scope covers organisational entities, subsidiaries and business units under direct managerial control. For joint ventures or partnerships without majority control, the relevant requirements apply to their access to, processing of or management of the organisation's systems, data or facilities, within the organisation's lawful and contractual authority.

The adopting organisation shall document its scope, interfaces and applicable legal duties. This standard does not create authority over an unrelated third party.

2.3 Systems and interfaces in scope

- IT systems and infrastructure.
- OT systems and industrial control systems.
- Physical security systems and access controls.
- Cloud services and hybrid environments.
- Third-party integrations and supply-chain security.
- Data processing and storage systems.
- Mobile devices accessing organisational resources.
- Identity and access management systems.

2.4 Legal and regulatory applicability

Applicable statutory and regulatory duties are not displaced by this standard. The organisation shall identify the jurisdictions, sectors and activities to which each duty applies. UK GDPR, EU GDPR, NIS2, DORA and PCI DSS are not automatically applicable to every adopter on the same basis; PCI DSS is an industry standard rather than a statute.

Where requirements overlap, the organisation shall meet all applicable duties and document a lawful resolution of any actual conflict. No exception to this standard authorises non-compliance with applicable law.

3. Normative references and related documents

3.1 Referenced external editions

Reference	Subject	Role in this standard
ISO 31000:2018	Risk management - Guidelines	Alignment reference for risk management; not an ISO certification specification
ISO/IEC 27001:2022	Information security management system requirements	Alignment reference for information security management

ISO 22301:2019	Business continuity management system requirements	Alignment reference for business continuity
----------------	--	---

This standard does not reproduce external standards or claim a licence to their text. Amendments or later editions of a referenced standard require an explicit applicability decision rather than automatic incorporation.

3.2 CSF companion documents

The following are related documents: GCSB-CSF-STRAT (Strategic Standards), GCSB-ST-CSF-GLA-001 (Governance), GCSB-ST-CSF-RMA-001 (Risk Management), GCSB-ST-CSF-TIA-001 (Technology Integration and Architecture), GCSB-ST-CSF-IAM-001 (Identity and Access Management), GCSB-ST-CSF-DPP-001 (Data Protection and Privacy), GCSB-ST-CSF-IRBC-001 (Incident Response and Business Continuity), GCSB-ST-CSF-TRA-001 (Training and Awareness) and GCSB-POL-CSF-CCSO-001 (CCSO Policy).

3.3 Associated guidance

Supporting implementation guidance on terminology, implementation planning, cross-domain risk assessment methodology, incident response procedures, technology integration standards and training and certification requirements is available as associated guidance, where issued by GCSB. Such guidance supports this standard but does not itself create or vary a requirement of this standard.

4. Terms and abbreviations

Term	Definition
Converged Security Framework	A unified approach integrating cybersecurity, physical security and operational technology security into a cohesive risk management strategy.
Hybrid risks	Threats exploiting vulnerabilities across physical and digital domains simultaneously.
Systemic risks	Interconnected system failures capable of affecting multiple operational areas through dependencies and network effects.
Cascading risks	Sequential failures triggered by initial incidents and propagating through organisational dependencies.
Chief Converged Security Officer (CCSO)	An adopting organisation's executive role with cross-domain security authority and unified risk management accountability.
Cross-domain integration	Technical and procedural coordination of security controls, processes and governance across the three security domains.
IT/OT convergence	Integration of information technology and operational technology systems, including their resulting security dependencies.
SIEM / PSIM	Security Information and Event Management / Physical Security Information Management.
IAM / MFA / RBAC	Identity and access management / multi-factor authentication / role-based access control.

RTO / RPO	Recovery time objective / recovery point objective.
-----------	---

Hybrid, systemic and cascading labels identify risk or incident type. They are not, by themselves, severity levels or regulatory reporting deadlines. Their mapping to impact and response priorities is addressed in the Incident Response and Business Continuity Standard and the CCSO Policy.

5. Roles, responsibilities and governance

The adopting organisation's board-level oversight, CCSO or equivalent role, cross-functional governance committee and business-unit champions are required by clauses 6.1 and 6.8.

The Enterprise Risk Management Committee and the Board Risk Committee referenced in clauses 6.11.2 and 6.12.2 belong to the adopting organisation, not GCSB. They are distinct bodies: the Enterprise Risk Management Committee receives compliance reports and recommends long exceptions; the Board Risk Committee approves exceptions longer than 12 months.

GCSB's document-development and approval route is set out in the document control table above. It does not alter the adopting organisation's operating structure or create a new GCSB advisory board.

6. Requirements

The following requirements apply to all adopting organisations.

6.1 Governance and Leadership

- 6.1.1** Organisations shall establish board-level oversight for converged security implementation with designated accountability for unified risk management across all security domains.
- 6.1.2** A Chief Converged Security Officer (CCSO) or equivalent executive role shall be appointed with authority over cybersecurity, physical security, and operational technology security functions.
- 6.1.3** Cross-functional governance committees shall be established including representatives from IT security, physical security, OT security, risk management, compliance, and business operations.
- 6.1.4** Convergence champions shall be designated within each business unit to coordinate implementation and ensure alignment with organisational security objectives.
- 6.1.5** Unified key performance indicators (KPIs) shall be established and monitored across all security domains, with regular reporting to executive leadership and board committees.

6.2 Risk Management and Assessment

- 6.2.1** Organisations shall implement a unified risk register covering cybersecurity, physical security, and operational technology risks, with clear identification of interdependencies and cascade effects.
- 6.2.2** Risk assessments shall be conducted at least annually using methodologies aligned with ISO 31000:2018, specifically addressing hybrid, systemic, and cascading risks.

6.2.3 Threat landscape analysis shall be performed quarterly, incorporating intelligence from cybersecurity, physical security, and operational technology domains.

6.2.4 Business impact analyses shall consider scenarios affecting multiple security domains simultaneously, with particular attention to IT/OT convergence risks.

6.2.5 Risk treatment plans shall be developed with coordinated controls across all affected security domains, following the principle of defence in depth.

6.2.6 Organisations shall implement specific procedures for identifying and responding to hybrid threats that exploit both physical and cyber vulnerabilities simultaneously.

6.2.7 Organisations shall develop and maintain cascade effect maps documenting dependencies between security domains, with critical interdependencies tested at least annually.

6.2.8 Risk modelling shall include scenario-based analysis of cascading failures across multiple security domains with documented containment strategies for each scenario.

6.2.9 IT/OT convergence risk assessments shall be conducted to identify vulnerabilities created by the integration of information technology and operational technology systems.

6.2.10 Predictive analytics and threat intelligence platforms shall be implemented to enable proactive identification and mitigation of emerging threats across all security domains.

6.3 Standards Integration and Compliance

6.3.1 Organisations shall implement an integrated management system aligned with ISO 31000:2018 (Risk Management), ISO/IEC 27001:2022 (Information Security Management), and ISO 22301:2019 (Business Continuity Management).

6.3.2 Compliance frameworks shall be mapped to organisational needs, with particular attention to sector-specific requirements (NIS2 Directive, DORA, PCI DSS, GDPR) and their convergence implications.

6.3.3 Internal audit programmes shall be established to verify compliance with converged security requirements, with external certification pursued where required by regulation or business necessity.

6.4 Technology Integration and Architecture

6.4.1 Organisations shall deploy unified Security Information and Event Management (SIEM) and Physical Security Information Management (PSIM) platforms with integrated monitoring capabilities across all security domains.

6.4.2 Zero-trust architecture principles shall be applied across IT and OT environments, with continuous verification of all users, devices, and network connections.

6.4.3 Artificial intelligence and machine learning capabilities shall be deployed for predictive threat analysis and automated response coordination across security domains.

6.5 Identity and Access Management Integration

6.5.1 Organisations shall implement unified identity and access management (IAM) systems covering physical access control, IT system access, and OT system access through a single identity provider.

6.5.2 Multi-factor authentication (MFA) shall be enforced for all privileged access across physical, IT, and OT environments, with biometric authentication implemented where technically feasible.

6.5.3 Role-based access control (RBAC) shall be implemented with segregation of duties enforced across all security domains, preventing privilege escalation and unauthorised access.

6.5.4 Identity lifecycle management shall be integrated with human resources systems, ensuring immediate revocation of access no longer authorised upon employment termination or role changes.

6.5.5 Privileged access management systems shall integrate across all security domains, with unified credential vaulting and session recording capabilities.

6.5.6 Access control systems shall support dynamic risk-based authentication that considers threat intelligence from all security domains.

6.6 Incident Response and Business Continuity

6.6.1 Unified incident response protocols shall be established covering cyber incidents, physical security breaches, and operational technology disruptions with coordinated response teams.

6.6.2 Incident escalation procedures shall be defined with automatic notification mechanisms and decision-making authorities clearly established for cross-domain security events.

6.6.3 Business continuity plans shall address scenarios affecting multiple security domains simultaneously, with recovery time objectives (RTO) and recovery point objectives (RPO) defined for each critical business process. RTO, RPO and related response clocks are indicative values which the organisation shall confirm in its own procedures unless a different value is set by applicable law.

6.7 Training and Awareness

6.7.1 Cross-functional security training programmes shall be implemented for all personnel, covering cybersecurity, physical security, and operational technology security awareness.

6.7.2 Specialised training shall be provided to security personnel on converged threat scenarios, hybrid attack vectors, and integrated response procedures.

6.7.3 Regular tabletop exercises and simulation drills shall be conducted, testing response to multi-domain security incidents, with lessons learned documented and incorporated into procedures.

6.7.4 Competency requirements shall be defined for all security-related roles, with certification and continuous education requirements specified and monitored. Training and recertification intervals are indicative values which the organisation shall confirm in its own procedures unless a different value is set by applicable law.

6.7.5 Security awareness programmes shall include specific training modules on recognising and reporting hybrid threats that span multiple security domains.

6.8 Organisational Structure and Governance

6.8.1 Organisations shall establish a converged security governance structure that integrates cybersecurity, physical security, and operational technology security under unified management authority.

6.8.2 Chief Converged Security Officers (CCSOs) or equivalent executive role holders shall have cross-domain authority and accountability for all security functions, with direct reporting lines to executive management and board oversight.

6.8.3 Security governance committees shall meet monthly with mandatory participation from IT security, physical security, OT security, risk management, legal, and business operations representatives.

6.8.4 All security policies shall be aligned across domains, with no conflicting requirements between cybersecurity, physical security, and operational technology security policies.

6.8.5 Organisations shall implement standardised security communication protocols across all security domains, with centralised incident reporting and response coordination.

6.8.6 Security budget allocation shall be managed centrally to prevent resource conflicts between security domains and ensure optimal allocation for converged security initiatives.

6.8.7 Security governance frameworks shall include specific provisions for managing converged security initiatives, with dedicated project management and change control processes.

6.9 Vendor and Third-Party Management

6.9.1 All vendors providing security services shall demonstrate the capability to support converged security requirements across multiple domains.

6.9.2 Third-party risk assessments shall evaluate vendor security practices for cybersecurity, physical security, and operational technology security simultaneously.

6.9.3 Vendor contracts shall include specific requirements for converged security support, incident response coordination, and compliance with this standard.

6.9.4 Supply chain risk assessments shall be conducted annually for all critical security vendors, incorporating both cyber and physical security considerations.

6.9.5 Vendor agreements shall include specific right-to-audit provisions enabling verification of security controls across all relevant security domains.

6.10 Data Protection and Privacy Requirements

6.10.1 Data classification systems shall be unified across all security domains, with consistent protection requirements applied regardless of the domain processing the data.

6.10.2 Privacy impact assessments shall consider data flows across physical, cyber, and operational technology systems with particular attention to cross-domain privacy risks.

6.10.3 Data retention policies shall be consistent across all security domains, with secure deletion procedures that account for data copies across multiple security systems.

6.10.4 Encryption standards shall be applied uniformly across all security domains, with centralised key management systems supporting cross-domain security operations.

6.10.5 Data loss prevention systems shall operate across all security domains, with unified monitoring and policy enforcement for data in transit, at rest, and in use.

6.10.6 Cross-domain data governance frameworks shall ensure consistent data handling requirements regardless of the security domain processing the information.

Where this standard affects the exercise of data-subject rights, the organisation shall observe the timescale set by UK data protection law; for EU operations, requests shall be handled within the period set by applicable EU and Member State law.

6.11 Compliance Reporting and Documentation

6.11.1 Comprehensive documentation shall be maintained for all converged security implementations, including system architectures, process flows, and control mappings.

6.11.2 Regular compliance reports shall be generated demonstrating adherence to this standard, with quarterly submissions to the Enterprise Risk Management Committee.

6.11.3 Audit trails shall be maintained for all security-related activities across domains, with centralised logging and monitoring capabilities providing comprehensive visibility into converged security operations.

6.11.4 Organisations shall establish and monitor quantifiable resilience metrics that measure the effectiveness of the converged security programme, with quarterly reporting to executive management.

6.11.5 Resilience assessments shall include recovery time testing for scenarios involving simultaneous compromise of multiple security domains.

6.11.6 Resilience benchmarking shall be conducted annually against industry standards and frameworks specific to the organisation's sector.

6.11.7 Gap analysis reports comparing converged security capabilities against threat intelligence shall be produced semi-annually, with remediation actions tracked to completion.

6.11.8 Continuous monitoring systems shall be implemented to track converged security effectiveness and identify opportunities for improvement.

6.11.9 Adaptive security frameworks shall be established to enable rapid adjustment of security controls based on changing threat landscapes and business requirements.

6.11.10 Business value assessments shall be conducted annually to evaluate the measurable security and resilience outcomes gained through converged security implementation. Any cost, savings or return-on-investment figures used in such assessments are illustrative examples, not commitments or guarantees.

6.11.11 Sector-specific compliance reporting shall be conducted according to relevant industry regulations, including NIS2 Directive for critical infrastructure and DORA for financial services.

6.11.12 KPI dashboards shall provide real-time visibility into converged security performance, with automated alerting for performance degradation across any security domain.

6.12 Exception Management and Deviations

6.12.1 Any deviations from this standard shall be formally documented with business justification and approved by the Chief Converged Security Officer.

6.12.2 Temporary exceptions shall include specific timelines for remediation. The CCSO may approve a temporary exception for up to 12 months; a longer exception may be approved only by the Board Risk Committee on the recommendation of the Enterprise Risk Management Committee.

6.12.3 All exceptions shall be reviewed quarterly with progress reports on remediation activities submitted to executive management.

7. Implementation and transition

7.1 Implementation timetable

Full implementation shall be completed within 12 months of certification commencement, and existing systems shall be assessed within 6 months. This is the suite baseline; the Governance, Technology and Training standards use a documented extended track of 18 months for their own requirements only.

7.2 Starting event

For a new adopter, the starting event is its documented adoption date, rather than the original publication date of a standard it may encounter later. The organisation shall record a baseline assessment, phased implementation plan, responsible owners, evidence and dependencies.

7.3 Application across the suite

The 12-month baseline applies to this standard and to the Risk, Identity, Data Protection and Incident Response standards and the CCSO Policy. The 18-month extended track applies only to requirements of the Governance, Technology and Training standards and does not extend any obligation of this standard.

8. Evidence, monitoring and corrective action

The evidence, reporting, audit, testing and monitoring duties in clauses 6.2, 6.3, 6.7, 6.9 and 6.11 apply. Annual risk and supplier reviews, quarterly threat analysis and reporting, monthly committee meetings and semi-annual gap analysis apply as set out in those clauses.

The evidence set should identify the scoped systems, risk register and dependency maps, assigned roles, control mappings, implementation plan, test results, training records and exception and remediation records. Metrics require defined measurement methods, scope, owners and reporting periods; promotional claims are not a substitute for evidence.

9. Exceptions and escalation

Exceptions follow clause 6.12: CCSO approval up to 12 months; longer exceptions only by the Board Risk Committee on recommendation of the Enterprise Risk Management Committee; remediation timelines; quarterly review and executive reporting.

Exceptions cannot waive applicable law, compromise an independent award or appeal decision, or be treated as automatic certification. A longer exception requires a recorded risk decision, compensating controls, a defined expiry and review, not an indefinite waiver. The same approval route applies in all suite documents.

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.

Exception decisions do not affect an appeal. Certification and enforcement decisions may be appealed within 30 days of notification to the Appeals body established under the GCSB Governance Charter. Assessment and decision clocks are set by the GCSB certification procedure referenced by all suite documents.

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.