

Converged Security Framework: Strategic Standards for Unified Risk Management and Organisational Resilience

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

Document control

Field	Value
Identifier	GCSB-CSF-STRAT
Title	Converged Security Framework: Strategic Standards for Unified Risk Management and Organisational Resilience
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-strategic-standards-resilience

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. Strategic provisions and requirements structure
- 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 Strategic role

This standard describes the strategic relationship between cybersecurity, physical security and operational technology (OT) security. It connects governance, risk management, information security and business continuity to organisational objectives and dependencies. It is intended for governing bodies, executive leaders, risk and compliance personnel, security managers, IT and OT owners, and other persons responsible for organisational resilience.

The framework supports identifying and managing hybrid, systemic and cascading risks. Integration is a means of achieving coordinated decisions, proportionate controls and reliable evidence, rather than a requirement to connect every system without regard to safety, privacy or resilience.

1.2 Issuer and adopter

GCSB is the issuer. The adopting organisation is responsible for implementation within its lawful authority. Its board, executives, CCSO, CISO, committees and convergence champions are adopter roles, not GCSB appointments. External providers remain responsible for services contracted to them. GCSB is not a training, consulting or audit provider.

Adoption alone does not confer statutory authority, ISO certification, GCSB accreditation, a credential, product endorsement or a Trustmark Award. Separate scheme decisions and evidence are required for any such recognition. No adopter is described as certified merely for implementing this framework.

1.3 Drafting convention

"Shall" denotes a requirement, "should" a recommendation, "may" a permission and "can" a capability.

2. Purpose, scope and applicability

2.1 Purpose

The purpose is to align security strategy with organisational objectives, risk appetite, critical services and resilience needs. The strategic approach covers shared oversight, a unified risk view, cross-domain dependencies, coordinated response, technology governance, identity, data protection, workforce competence and measurable improvement.

Expected benefits include clearer accountability, more consistent evidence and better coordination. Cost savings, competitive advantage, uninterrupted operation or superior threat detection are not guaranteed. An organisation should assess outcomes against its own baseline rather than assume a promotional claim establishes performance.

2.2 Scope

The organisation shall document entities, services, locations, systems, data, personnel and external interfaces within scope, together with material exclusions and dependencies. Cybersecurity, physical security and OT are all included where relevant. The three-domain definition applies; it does not require an adopter without OT to invent an OT estate.

Subsidiaries, partnerships, suppliers and cloud services should be addressed according to actual control, contractual access and exposure. Third-party involvement does not create an unlimited right to obtain data or direct another organisation's operations.

2.3 Legal, territorial and sector applicability

The organisation shall identify applicable duties by jurisdiction, entity type, activity, product, sector and contractual commitment. Statutory duties cannot be displaced by this standard. Voluntary standards, technical specifications, legal instruments and recognition schemes are distinct categories.

UK GDPR and EU GDPR require separate applicability analysis. GDPR duties are not limited to consent, and compliance with an information security standard does not itself establish compliance with data protection law. NIS2 depends on scope and applicable national implementation. DORA concerns defined financial entities and the relevant ICT third-party arrangements and oversight regime, not every enterprise. The EU Cyber Resilience Act concerns products with digital elements within its legal scope and has phased application dates.

Clause 3 sets an applicability method in place of blanket sector-wide applicability assertions. Sector-specific duties shall be determined by the adopter's own legal and regulatory analysis.

2.4 Exclusions and boundaries

This standard is not a contract executed between GCSB and each adopter, a legal opinion, a licence to third-party standards text or an accreditation decision. It does not prescribe commercial suppliers merely by discussing examples. Operational safety, lawful processing and independent recognition decisions remain separate responsibilities.

3. Normative references and related documents

3.1 Normative-reference treatment

The adopter shall identify each reference's exact title, edition and binding role relevant to its scope. A mention of an external publication is not sufficient to make the entire publication mandatory. The following references apply for alignment, not blanket incorporation of every clause or amendment.

Reference	Role	Boundary
ISO 31000:2018, Risk management - Guidelines	Risk management alignment	Guidance; not itself a certifiable management-system requirements standard
ISO/IEC 27001:2022, Information security management systems - Requirements	ISMS alignment	Certification remains a separate scoped assessment; amendments require explicit edition control
ISO 22301:2019, Business continuity management systems - Requirements	BCMS alignment	A requirements standard, not simply implementation guidelines
NIST Cybersecurity Framework 2.0 (2024)	Informative cybersecurity governance and outcome mapping	Six functions; not a GCSB award or a substitute for physical/OT risk assessment

Adoption of later editions or amendments of any referenced instrument is a separate decision taken during reference control and is not automatic.

3.2 Related documents

The Main Standard GCSB-ST-CSF-001 provides the overarching requirements. Related documents include 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).

Additional external references cited in supporting tables include EN security-system series, IEC 62443, NIST SP 800-53, CIS Controls v8, COBIT 2019 and academic or institutional reports, cited by title. The adopter shall confirm the current status, edition and applicability of any such reference before relying on it; a series-level identifier does not by itself establish which technical part or edition applies. Associated guidance, where issued by GCSB, may further support implementation.

3.3 Applicability record

For each relevant external instrument or reference, the adopter shall record its identifier and edition, legal or voluntary status, applicability rationale, scoped assets or activities, responsible owner, relevant provisions, supporting evidence and review triggers. Legal dates come from the applicable instrument, not from this standard's implementation schedule.

3.4 NIST and third-party model references

NIST CSF 2.0 has six functions: Govern, Identify, Protect, Detect, Respond and Recover. GCSB's Converged Security Framework is a distinct framework from NIST's Cybersecurity Framework.

Any citation of third-party maturity-model research shall identify the authentic title, author and year, and shall not be presented as an issued certification standard.

4. Terms and abbreviations

Term	Definition or use
Converged Security Framework	A unified approach integrating cybersecurity, physical security and OT security into coordinated governance, risk management and operational controls
Hybrid risk	Risk involving exploitation of vulnerabilities across physical and digital domains, including simultaneous attack vectors
Systemic risk	Risk arising from interconnected dependencies capable of affecting multiple operational areas
Cascading risk	Risk of sequential failures propagating from an initiating event through organisational dependencies
Organisational resilience	Capacity to prepare for, withstand, respond to, recover from and adapt to disruption within defined organisational objectives
GCSB CSF / NIST CSF	Separate frameworks; the abbreviation is qualified where confusion is possible
CCSO	Chief Converged Security Officer; adopter cross-domain executive role, consistent with the Main Standard

CISO	Chief Information Security Officer; a domain role, not automatically a substitute for the CCSO's full cross-domain accountability
GRC	Governance, risk management and compliance
IT / OT / IoT	Information technology / operational technology / Internet of Things
IAM / MFA / RBAC	Identity and access management / multi-factor authentication / role-based access control
SIEM / PSIM / SOAR	Security Information and Event Management / Physical Security Information Management / security orchestration, automation and response
KPI / RTO / RPO	Key performance indicator / recovery time objective / recovery point objective
AI / ML	Artificial intelligence / machine learning

Hybrid, systemic and cascading describe risk or incident type. They are not a severity scale and do not determine statutory reporting deadlines. Terminology and mappings are read consistently with the Main Standard, the Incident Response and Business Continuity standard, and the CCSO Policy.

5. Roles, responsibilities and governance

5.1 Board-level oversight

The adopter's governing body shall align the security strategy with organisational objectives and risk appetite, oversee material exposures, allocate responsibility and consider evidence of effectiveness. Board oversight does not eliminate executive or operational accountability.

5.2 Executive coordination

The CCSO or equivalent role identified in the Main Standard shall coordinate the three-domain strategy, with defined delegated authorities and escalation routes. Domain specialists retain technical and operational responsibilities. The CCSO role does not merge a CISO, risk committee, DPO or GCSB office into itself.

5.3 Cross-functional participation

Risk, compliance, legal, IT, OT, physical security, HR, procurement and business owners should contribute to scoped decisions. Convergence champions support coordination and change management. The relationship between the adopter's Enterprise Risk Management Committee and Board Risk Committee is defined by the adopter consistent with Governance and CCSO requirements.

5.4 Assurance and independence

Implementation owners shall provide evidence without representing their own assessment as an independent certification decision. Assurance, accreditation, Trustmark, appeal and conflict-of-interest arrangements remain subject to their own rules. The DPO's independent advice and monitoring role is not executive control over all processing.

6. Strategic provisions and requirements structure

The following sets out an operational strategic structure. These provisions are guidance except where a specifically applicable Main or companion requirement already imposes a duty.

6.1 Strategy, threat context and unified risk

The organisation shall maintain a security strategy connected to business objectives, critical services, risk appetite and dependencies. It shall identify hybrid attack vectors, systemic dependencies and cascading failure scenarios using coordinated assessments rather than isolated domain registers.

A common risk view should link threats, vulnerabilities, affected assets, business impacts, controls and accountable owners. Qualitative and quantitative methods can be combined when their assumptions, limitations and data quality are understood. Risk tools and analytics support judgement; they do not guarantee predictive accuracy or justify replacing accountable decisions with automation.

6.2 Standards integration and GRC

The organisation should map relevant standards and legal duties to its scope and processes, identify overlaps and actual conflicts, and maintain consistent evidence. Integrated oversight should support decision-making and corrective action without implying that ISO alignment automatically satisfies every regulatory regime.

Unified policies, control mappings, communications and assurance planning should reduce unnecessary duplication while preserving distinct legal, operational and professional responsibilities. This standard does not set new audit frequencies or replace the Main Standard's reporting periods.

6.3 Data governance, identity and privacy

Data governance should address inventories, classification, ownership, stewardship, data quality, authorised processing, retention, access, sharing, backup and recovery. Data criticality and business dependency should guide protection and continuity decisions.

IAM shall support named accountability, least privilege, appropriate authentication, lifecycle changes and controlled physical/digital interfaces. HR integration should support timely provisioning and removal of access no longer authorised. Identity analytics, biometrics and cross-domain monitoring require applicable lawful processing, necessity, proportionality and security safeguards.

Rights, lawful bases and limitations are set out in the Identity and Access Management and Data Protection and Privacy standards. For the United Kingdom, data-subject rights timing follows the applicable UK statutory period; for the European Union, data-subject rights shall be met within the period set by applicable EU and Member State law.

6.4 Technology, open architecture and IT/OT

Technology shall be governed as a cross-domain resilience capability with recorded ownership, dependencies and evidence. Integration design should consider SIEM/PSIM coordination, interfaces, access controls, interoperability, logs and response workflows as relevant to scope and risk.

Open standards and modularity can reduce lock-in and support interoperability, but an open interface is not inherently secure. The organisation shall assess authentication, authorisation, integrity, availability, vendor support and data exposure. No mandatory vendor product is named by this standard.

IT/OT integration shall preserve operational safety, availability and change control. Network connection, patching, automation or shared identity changes should be evaluated against operational constraints rather than assumed safe because IT controls are effective elsewhere.

AI/ML, blockchain, 5G and VR are illustrative capabilities, not evidence of compliance or prerequisites imposed by this standard. Human oversight, model limitations, privacy, failure modes and safe fallback should guide technology evaluation.

6.5 Coordinated incident response and continuity

The organisation shall coordinate preparation, detection, analysis, containment, eradication, recovery and lessons learned across affected domains. Plans shall identify responsibilities, authority, communications, dependencies and escalation interfaces, including third parties where relevant.

Business continuity should reflect critical services and dependencies, with scoped RTOs and RPOs established through impact assessment. Incident response targets are not the same as legal notification clocks. Incident type, severity, regulatory reportability and recovery priority should be separately recorded. Response and recovery clocks not otherwise set by applicable law are indicative values that the adopter shall confirm in its own procedures.

6.6 People, culture, stakeholder engagement and training

Leadership shall demonstrate accountability and support cross-functional cooperation. Change management should address resistance, resources, skills, role clarity and feedback. ADKAR or another suitable method may be used as informative guidance.

Training should be role-appropriate, cover relevant cross-domain dependencies and include practical exercises. Participation, knowledge, practical competence and operational outcomes should be evaluated separately. A participation rate does not establish a pass rate, and completion alone does not confer a GCSB credential or approved CPD credit. Training clocks not otherwise set by applicable law are indicative values that the adopter shall confirm in its own procedures.

Stakeholder communications should be timely, authorised and appropriate to recipients. Intelligence sharing with peers or regulators shall respect legal authority, confidentiality, privacy and operational sensitivity.

6.7 Measurement, improvement and learning

The organisation should define metrics that connect security activities to critical services, risk reduction and resilience objectives. Records should identify the metric, scope, denominator where applicable, baseline, target, data source, owner, period and decision use. Qualitative evidence can complement numerical indicators.

Any cost, savings, benefit, adoption-rate or similar figure used as an example is illustrative only and is not a commitment or guarantee. Distinct measures and denominators shall not be combined into a single percentage without a documented basis.

Incidents, exercises, assurance findings and stakeholder feedback should lead to tracked improvement decisions. Any scenario used for illustration that is not independently evidenced shall be labelled as illustrative.

7. Implementation and transition

7.1 Source schedule

The following sequence is a suggested implementation sequence, not a set of separate binding deadlines. The binding period is the suite baseline set out in 7.2.

Suggested milestone	Period
Comprehensive risk assessment across all domains	Months 1-2
Unified governance with executive sponsorship	Month 3
Technological integration including SIEM/PSIM	Months 4-6
Cross-functional response protocols and training	Months 7-9
Continuous monitoring and improvement	Months 10-12 and ongoing

A six-step method may also be used: current-state assessment; target architecture; roadmap; controlled pilot; scaled deployment; monitoring and improvement.

7.2 Starting event and dependencies

A documented adoption date is the starting event, consistent with the Main Standard. The binding periods are the suite baseline: full implementation within 12 months and an existing-system gap assessment within 6 months of the documented adoption date. The 18-month extended track applies only to the requirements of the Governance, Technology and Training standards. This standard does not redefine recertification and does not imply that technology integration must precede governance and operational safety controls.

7.3 Implementation evidence

A roadmap should identify scope, baseline, accountable owners, resources, milestones, dependencies, interim controls, testing and acceptance evidence. Pilots should have defined safeguards and evaluation criteria. Monitoring and improvement continue after initial implementation.

8. Evidence, monitoring and corrective action

Evidence should include the strategy and approved scope, risk and dependency records, applicability/control mappings, responsibility assignments, architecture and interface records, incident/continuity plans, exercise results, role-based training evidence, metrics and improvement records.

Metrics should be reviewed for decision usefulness and data quality. Recovery measures, detection measures, workforce competence and stakeholder perceptions should not be conflated. External benchmark statistics require a source, date, population, method and relevance statement; they are not automatic performance requirements.

Corrective actions shall identify an owner, priority, supporting risk rationale, completion evidence and escalation route. The Main Standard's audit and reporting duties remain unaffected. This standard creates no alternative reporting frequency, waiver duration or retention period.

9. Exceptions, escalation and review

Exceptions to an applicable Main or companion requirement shall follow that requirement's controlled authorisation process. A departure from informative strategic guidance is distinguished from a waiver of a binding requirement. No exception permits breach of applicable law or confers recognition by default.

The CCSO may approve temporary exceptions of up to 12 months; longer exceptions require approval by the Board Risk Committee on the recommendation of the Enterprise Risk Management Committee, and all exceptions are reviewed quarterly. This standard does not give the issuer authority over each adopter's operational exceptions.

Material changes in threats, legal duties, services, technology or organisational structure shall trigger review of the strategy and affected evidence, in addition to the scheduled review set out in document control.

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.

Reference to this standard shall accurately attribute its title and edition. An adopter's local implementation material shall be distinguished from this issued text. Citation of this standard alone does not imply accreditation or endorsement by GCSB.

This document is governed by the laws of England and Wales and is 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.

Certification and enforcement decisions arising under this standard 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.

