

Governance and Leadership Framework

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-GLA-001
Title	Governance and Leadership Framework
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-gla-001-governance

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. Governance 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 addresses governing-body oversight and executive coordination of cybersecurity, physical security and operational technology security. It connects the Main Standard's cross-domain requirements with the Strategic Standard's organisational direction and companion operational standards. It is intended for adopter governing bodies, executive leaders, CCSOs, domain owners, risk and compliance personnel and business-unit representatives.

I.2 Issuer, adopter and service providers

GCSB issues the standard. The adopting organisation implements it within its lawful organisational and contractual authority. The adopter's board, CEO, CCSO, risk committees and champions are not GCSB appointments. The GCSB Governance Charter governs the issuer; it does not automatically supply voting rules or employment conditions to every adopter.

GCSB is not represented as a training, consulting or audit provider. Adoption alone does not confer statutory authority, ISO certification, GCSB accreditation, a credential, a product endorsement or a Trustmark Award. Recognition decisions

remain subject to their separate schemes and independent decision safeguards.

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 establish accountable cross-domain governance: oversight, delegated executive authority, coordination, risk decisions, competence, evidence, change control and continuity. Benefits shall be assessed against a documented baseline, using evidence-based evaluation rather than promising outcomes no governance structure can guarantee.

2.2 Organisational scope

The adopter shall document entities, business units, services, assets, data, personnel and external interfaces within scope, and the justification for exclusions. Cybersecurity, physical security and OT security shall be addressed where present or materially connected to the organisation's risk. An organisation without OT need not invent an OT estate; the scope record shall explain that absence and relevant external dependencies.

Subsidiaries and controlled entities shall be addressed according to actual authority. Joint ventures, partners and suppliers shall be governed through applicable law, agreements and the adopter's lawful access rights. Access to systems or data does not confer unlimited management powers over another entity. Detailed operational procedures remain in companion standards; their governance and escalation remain within this standard.

2.3 Legal and territorial boundaries

The adopter shall identify applicable statutory, regulatory, contractual and scheme duties by jurisdiction, entity type, sector and activity. A voluntary standard cannot displace binding law or create powers for a regulator. Conflicts shall be referred for qualified advice and documented resolution.

UK GDPR and EU GDPR require distinct scope analyses. NIS2 duties depend on applicable national implementation and entity/activity scope. DORA applies within its defined financial-sector and ICT arrangements. PCI DSS is not an EU statute. A reference to a legal instrument does not incorporate all its provisions as universal duties.

This standard is not an executed agreement, appointment contract, liability allocation, arbitration agreement or universal governing-law instrument. Genuine contracts require identified parties, authority, consent and appropriate legal review.

3. Normative references and related documents

3.1 Referenced documents

The adopter shall identify each normative reference's exact title, edition, relevant provisions and availability. References to external standards, legal instruments, products and schemes are not blanket incorporation. Associated guidance, where issued by GCSB, supports but does not replace this standard's requirements.

Reference	Role
GCSB-ST-CSF-001 Main Standard	Master scope and overarching requirements
GCSB-CSF-STRAT Strategic Standard	Strategy and organisational alignment
GCSB-ST-CSF-RMA-001, GCSB-ST-CSF-TIA-001, GCSB-ST-CSF-IAM-001, GCSB-ST-CSF-DPP-001, GCSB-ST-CSF-IRBC-001, GCSB-ST-CSF-TRA-001 and GCSB-POL-CSF-CCSO-001	Domain requirements and role policy
ISO 31000:2018	Risk management guidance
ISO/IEC 27001:2022	ISMS requirements alignment
ISO 22301:2019	BCMS requirements alignment
NIST Cybersecurity Framework 2.0	Informative cybersecurity outcome mapping, including the Govern function
COBIT 2019, CMMI and ISO/IEC 38500:2015	Informative governance and assessment references
GCSB Trustmark and certification scheme published at gcsb.uk	Scheme interface where applicable; adoption of this standard creates no endorsement, certification or Trustmark Award

3.2 External legal references

A legal applicability register shall distinguish legislation, delegated or implementing measures, regulator guidance and voluntary standards. Legal reporting triggers and clocks shall be taken from the applicable current instrument.

4. Terms and abbreviations

Term	Meaning
Adopting or implementing organisation	Entity implementing the framework within its defined scope and authority
Governing body / board-level oversight	Adopter's highest accountable governing body, or an authorised oversight committee; statutory responsibilities are not displaced by delegation
CCSO	Chief Converged Security Officer or equivalent cross-domain executive role under the Main Standard

CISO	Chief Information Security Officer; a domain role, not automatically the whole cross-domain CCSO role
Converged Security Governance Committee	Adopter's cross-functional coordinating body, chaired by the CCSO under documented terms of reference
Convergence champion	Designated business-unit liaison for cross-domain implementation and reporting
Unified risk management	Coordinated identification, assessment, treatment and monitoring of risks across scoped security domains
Hybrid / systemic / cascading	Risk or incident types; not severity levels or reporting-clock triggers
KPI	Indicator with documented purpose, owner, baseline, population, calculation, target, escalation and evidence
Competent authority	Authority identified under applicable law
RTO / RPO	Recovery time / recovery point objective, scoped to the relevant service and business impact
RACI	Responsible, Accountable, Consulted, Informed; an optional accountability notation, not a transfer of legal duties

5. Roles, responsibilities and governance

5.1 Issuer control

This standard is reviewed by the Certification and Standards Committee and approved by the Governing Council under the GCSB Governance Charter.

5.2 Adopter accountability

The adopter's governing body retains oversight of strategy, risk appetite, material exposures, executive appointment and investment priorities. The CEO or equivalent executive establishes delegated operating authority. The CCSO coordinates cybersecurity, physical security and OT security within that delegation. Domain owners retain specialist competence, safety and operational responsibilities.

The coordination committee and champions support delivery and escalation without displacing board accountability. Risk, legal, compliance, HR, procurement, IT, OT and physical security participate according to scope. Assurance and independent review remain distinct from ownership of the controls reviewed. The data protection officer's advice and monitoring must not be equated with deciding the purposes and means of all processing.

5.3 Risk committee relationship

The adopter's Enterprise Risk Management Committee and Board Risk Committee may be different bodies. Their authority, delegation, reserved decisions and reporting shall be documented. For exceptions, the Enterprise Risk Management Committee recommends and the Board Risk Committee approves any exception longer than 12 months.

6. Governance requirements

6.1 Board-level oversight

6.1.1 The adopter shall appoint at least one board member or authorised committee with specific converged security oversight responsibility. Responsibilities shall include policy and strategy approval, risk appetite review, CCSO appointment and performance oversight, review of security evidence, and approval of security investment priorities and allocations.

6.1.2 Board-level oversight shall meet at least quarterly and receive monthly written reports covering the scoped domains. All oversight decisions and follow-up actions shall be recorded and retained under a documented lawful retention schedule.

6.1.3 The adopter shall provide annual converged security training for board members with oversight responsibilities and establish escalation for material cross-domain incidents and risks.

6.2 CCSO appointment, authority and performance

6.2.1 The adopter shall appoint a CCSO or equivalent executive with demonstrable cross-domain authority and competence, subject to board-level approval. The role shall report to the CEO or equivalent senior executive and have regular direct communication with board-level oversight. The delegation shall record policy, personnel, budget, assessment, remediation, incident and emergency decision powers and reserved decisions.

6.2.2 The CCSO shall maintain the converged security strategy, unified risk processes, committee coordination, champions network, KPIs, board reports, applicable compliance coordination and cross-domain incident coordination. The role shall undergo annual board-level performance review.

6.2.3 Competence shall be evidenced through an approved role specification and verified qualifications and experience. The adopter shall define and document the applicable qualification requirements and any accepted equivalent experience.

6.2.4 Planned CCSO succession shall begin at least 90 days before anticipated departure. The adopter shall define and document interim and emergency appointment periods and notification arrangements proportionate to the role and its authority.

6.3 Cross-functional coordinating committee

6.3.1 The adopter shall establish a Converged Security Governance Committee chaired by the CCSO, including senior representatives with decision authority from the scoped IT security, physical security, OT, enterprise risk, compliance and business operations functions. Representation and any absent domain shall be justified by scope.

6.3.2 The committee shall convene at least monthly and keep written minutes, decisions, owners and action records. Terms of reference shall define delegated decisions, board-reserved matters, quorum, voting, remote participation, conflicts, recusals, escalation and decision tracking, as the adopter defines and documents them.

6.3.3 The committee shall coordinate cross-domain policy proposals, incident governance, KPI review, resource-conflict resolution and investment recommendations. It may create subject-specific subcommittees under bounded

delegation. Members shall receive regular converged security training. Technology, transcription and sentiment-analysis tools shall not replace accountable deliberation or lawful handling of meeting records.

6.4 Convergence champions

6.4.1 The adopter shall designate at least one champion in each scoped business unit, with documented role, authority, competence, access to business-unit leadership and communication with the CCSO. Champions shall complete the CCSO-specified training within 90 days of designation.

6.4.2 Champions shall coordinate implementation, identify risks and gaps, communicate across domains, participate in governance coordination and report resource needs. The CCSO shall maintain monthly network meetings, quarterly champion performance assessments and annual strategic planning. Champions shall provide monthly reports to business-unit leadership.

6.4.3 The adopter shall provide necessary resources and continuity during reassignment. The CCSO may replace or reassign a champion in consultation with business-unit leadership with written notice.

6.5 KPIs and management reporting

6.5.1 The adopter shall establish a unified KPI framework developed with the coordinating committee and approved by the CCSO. It shall address detection and response, incidents and impacts, risk treatment, applicable compliance, integration and coordination, training and competence, resource efficiency, hybrid risks, IT/OT dependencies and applicable access-control architecture.

6.5.2 Each KPI shall have a defined measurement population and denominator, owner, calculation, evidence source, baseline window, target and escalation threshold. A compliance percentage shall not be used to excuse an unmet binding legal duty. Quantitative targets require a defensible method and scoped baseline.

6.5.3 Committees and champions shall review KPI data monthly. The CCSO shall report KPI results quarterly to board-level oversight, including variances, corrective actions and uncertainty. These quarterly analyses do not replace the monthly board security reports required under clause 6.1.2.

6.5.4 Authorised disclosure to a competent regulator shall follow applicable law and secure handling. The adopter shall define and document its KPI alert thresholds and annual improvement expectations against a defensible baseline.

6.5.5 The adopter shall maintain a unified view of hybrid, systemic and cascading risks with documented ownership, appetite, escalation and board visibility. Risk assessment, treatment, monitoring and specialist model validation shall be conducted in accordance with GCSB-ST-CSF-RMA-001 rather than replaced by KPI analytics. No unsupported correlation establishes causal proof or an acceptable risk decision.

6.6 Training and competence

6.6.1 The adopter shall define, fund and maintain governance role competence and cross-functional training that addresses dependencies across cybersecurity, physical security and OT. Board, CCSO, committee and champion training shall be evidenced separately from any professional credential or member continuing professional development requirement.

6.6.2 Completion, attendance, examination pass rate and demonstrated competence shall be treated as different measures. The CCSO shall coordinate training requirements with GCSB-ST-CSF-TRA-001. Training may be delivered

through appropriate independent providers; this clause does not appoint GCSB as the provider.

6.6.3 Personal certification milestones apply to individuals holding governance roles, as personal skills deadlines separate from the implementation timetable in clause 7: foundational certification within 12 months of taking up the role; committee-member certification within 18 months; CCSO-level certification within 12 months and advanced CCSO certification within 24 months of appointment; a minimum of 60 annual continuing-education hours for the CCSO, with subject allocations defined by the adopter; and a 120-hour initial champion programme with quarterly updates. These personal deadlines run from the individual's role start or appointment date and are not shortened, extended or superseded by the organisational implementation track in clause 7.

6.7 Technology and resource governance

6.7.1 The adopter shall govern technology integration, access-control architecture, evidence, procurement and operational safety against the Main Standard and applicable domain requirements. Resource decisions shall consider scoped risks, dependencies, competence, continuity and total cost, with approved spending delegations.

6.7.2 Vendor-neutral, outcome-based governance does not waive the Main Standard's retained AI/ML obligations or the requirements of GCSB-ST-CSF-TIA-001 and GCSB-ST-CSF-IAM-001. No automatic or AI-generated action shall be described as exempt from delegated authority, safety and lawful processing.

6.7.3 Budget envelopes and financial thresholds shall be approved against organisational scope and authority, as the adopter defines and documents them. Any cost, savings or return-on-investment figures referenced in supporting material are illustrative examples only, not commitments or guarantees.

6.8 Applicable compliance and notifications

6.8.1 The adopter shall maintain an applicability register, accountable owners, evidence, change monitoring and procedures for the binding duties that apply. NIS2, DORA and GDPR shall not be combined into one universal notification deadline, entity threshold, recovery objective or budget rule.

6.8.2 Notification procedures shall separately record the legal trigger, awareness or detection event, responsible person, recipient, required content, deadline, follow-up and proof of submission. Internal reporting and response clocks shall be distinguished from external legal clocks and are indicative values that the adopter shall confirm in its own procedures unless law sets them. Hybrid, systemic and cascading types shall be mapped separately from severity and legal significance under GCSB-ST-CSF-IRBC-001.

6.8.3 Privacy governance shall identify the actual controller or processor responsibilities for each processing activity, lawful basis, rights procedures, retention, security and applicable transfer safeguards, in accordance with GCSB-ST-CSF-DPP-001. For data-subject rights timing, the UK GDPR statutory period applies in the United Kingdom; in the European Union, requests shall be handled within the period set by applicable EU and Member State law. GCSB is not automatically the controller of adopter data.

6.9 Succession and governance continuity

6.9.1 The adopter shall maintain a CCSO succession plan, documented interim authority, knowledge transfer and continuity of board oversight, committees, champions and reporting. Planned succession shall begin at least 90 days before anticipated departure. Board approval shall govern transitions.

- 6.9.2 The adopter shall define and document interim appointment periods, emergency appointment arrangements, permanent replacement timescales and any applicable regulator notification period, proportionate to the role and organisational scope.
- 6.9.3 Emergency governance shall preserve essential oversight, secure communications, delegated decisions and incident coordination. Emergency powers shall remain bounded by law, scope and delegation and be documented for subsequent oversight. Force majeure does not automatically suspend statutory reporting, excuse security failures or grant unlimited CCSO powers.

6.10 Governance information protection

- 6.10.1 The adopter shall classify governance information, control authorised access, protect records and communications, review access rights quarterly and maintain appropriate audit evidence. Information shall be shared only under lawful authority, confidentiality obligations and applicable safeguards.
- 6.10.2 Suspected or confirmed breaches of confidential governance information shall be reported to the CCSO within 24 hours of discovery, with immediate containment and remediation. This is an internal indicative timescale, confirmed by the adopter in its own procedures, and is not a substitute for any applicable legal notification clock under GCSB-ST-CSF-IRBC-001.
- 6.10.3 Personnel shall receive relevant confidentiality and security training before access. Retention, disposal, legal holds and cross-border transfers shall be governed by documented purpose and applicable law. Information classification labels shall not imply state security clearances.

6.11 Governance change control

- 6.11.1 Proposed governance changes shall be recorded, assessed for security, privacy, safety, resources and cross-document impact, consulted on and approved by the competent delegated or board authority before implementation. Change records shall include rationale, implementation, validation, rollback and communication.
- 6.11.2 The adopter shall define and document consultation, notice and emergency-modification periods for governance changes. Emergency governance shall not displace binding law. A regulator's prior approval shall be required only where an applicable duty creates that requirement.

7. Implementation and transition

7.1 Implementation timetable

Event	Period or criterion	Status
Gap assessment	Within 6 months of certification commencement	Suite baseline
Full implementation (extended track)	Within 18 months of certification commencement	Extended track for this standard

Phase 1 governance establishment, including CCSO appointment	Within 6 months	Read within the 18-month track
Phase 2 operational integration	Within 9 months, minimum 90% training completion of in-scope personnel	Cumulative from certification commencement
Remediation plan after gap assessment	Within 90 days of assessment completion	Plan deadline, not completion of remediation
KPI development and approval	Within 90 days of certification commencement	Aligned with operational baseline collection

This implementation timetable governs organisational rollout. It is distinct from the personal certification deadlines in clause 6.6.3, which run from each individual's role start or appointment date and are not shortened, extended or superseded by this timetable.

7.2 Controlled implementation record

The adopter shall document the adoption decision, scope, gap assessment, accountable owners, resources, dependencies, interim risk controls and approved milestones within the 18-month extended track. Any further extension requires an exception under clause 9.1 and shall not be presented as full conformity before applicable requirements are satisfied.

8. Evidence, monitoring and corrective action

The adopter shall maintain board and committee records, role appointments and delegations, competence evidence, champions records, risk and applicability registers, KPI definitions and data, incident and escalation evidence, change records, succession plans and corrective-action evidence appropriate to scope.

Annual CCSO and committee reviews shall include independent assessor input, stakeholder feedback, quantitative and qualitative evidence, written findings and recommendations. Interim CCSO and committee assessments shall occur quarterly. Results shall be reported to board oversight within 30 days of completion, as an indicative value the adopter shall confirm in its own procedures, and improvement plans shall be produced within 90 days of deficiency identification. Disclosure to a regulator depends on applicable duties.

Corrective actions shall identify owner, due date, risk treatment and follow-up evidence. Independence requires real conflict management, not merely a purchased certification label or self-generated accuracy score. No unsupported benefit, correlation, maturity or predictive result is accepted as evidence of conformity.

9. Exceptions, escalation and review

9.1 Bounded exceptions

Exceptions shall identify affected requirement, rationale, risk, compensating controls, approver, expiry and review. The CCSO may approve temporary exceptions not exceeding 12 months. Longer exceptions may be approved only by the

Board Risk Committee on recommendation of the Enterprise Risk Management Committee. All exceptions are reviewed quarterly. No exception waives statutory duties.

9.2 Decisions, disputes and emergency arrangements

Governance disputes within the adopter shall be escalated through documented organisational routes with conflict management and continuity of essential functions. Any dispute arising from this standard is 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, and no compulsory arbitration applies. Statutory rights of regulators and data subjects are unaffected. Certification and enforcement decisions by GCSB 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. Internal adopter governance disputes, GCSB scheme appeals and external litigation are distinct processes. Contract terms on termination, liability and force majeure apply only where agreed between identified parties.

9.3 Review

Review shall respond to material legal, organisational, incident, technology and suite changes.

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.