

Chief Converged Security Officer (CCSO) Policy

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

Document control

Field	Value
Identifier	GCSB-POL-CSF-CCSO-001
Title	Chief Converged Security Officer (CCSO) Policy
Document type	Policy
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/ccso-policy

Contents

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

1. Foreword, status and intended use

This policy sets out a unified Chief Converged Security Officer (CCSO) governance model for adopting organisations. It describes an adopter's CCSO office, which is distinct from the GCSB CCSO membership grade. Adoption of this policy confers no GCSB membership, recognition, qualification, accreditation or Trustmark Award.

2. Purpose, scope, applicability and exclusions

Purpose: to establish unified converged security leadership under a CCSO across cyber, physical and operational technology (OT) domains, so that converged risk governance is embedded in strategic organisational decisions.

Scope: this policy applies to adopting organisations and their controlled entities that are within the scope of the adopter's certification, wherever located, including:

- 1. All organisational entities, including the parent organisation, subsidiaries, joint ventures and controlled affiliates.
- 2. All information technology systems, networks, applications and data repositories, regardless of hosting location or service provider.

3. All operational technology systems, including industrial control systems, SCADA networks, IoT devices and manufacturing systems.
4. All physical security infrastructure, including access control systems, surveillance networks, perimeter protection and facility security operations.
5. All third-party integrations, cloud services, supply chain connections and vendor relationships that access or process the organisation's data or systems.
6. All employees, contractors, consultants and temporary personnel, regardless of employment status or location.

Governance under this policy extends to all security domains, including cybersecurity, physical security, operational technology security, information security, personnel security and supply chain security.

This policy supersedes conflicting internal security policies, procedures and governance structures to the extent they conflict with unified converged security governance under CCSO authority, without overriding applicable law.

Exceptions to scope require the approval set out in clause 9.

Exclusions: this policy does not itself confer GCSB membership, recognition, qualification, accreditation or certification.

3. Normative references

GCSB-ST-CSF-001; GCSB-CSF-STRAT; GCSB-ST-CSF-GLA-001; 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.

External references, cited by title without asserting unverified edition details and treated as informative unless the adopter's own legal review states otherwise: the General Data Protection Regulation (GDPR) and UK GDPR; the Network and Information Systems Directive 2 (NIS2); the Digital Operational Resilience Act (DORA); the EU Cyber Resilience Act (CRA); the EU Artificial Intelligence Act; ISO/IEC 27001; ISO 22301; ISO 31000; IEC 62443; and the NIST Cybersecurity Framework.

Associated guidance, where issued by GCSB, may support implementation of this policy. This policy is reviewed by the Certification and Standards Committee and approved by the Governing Council.

4. Terms, definitions and abbreviations

- **Business Continuity:** the capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident, encompassing both cyber and physical recovery procedures.
- **Cascade Effect Mapping:** the systematic documentation and analysis of how security incidents in one domain may propagate to affect other interconnected systems, networks or physical infrastructure.
- **Chief Converged Security Officer (CCSO):** the executive appointed by an adopting organisation with unified authority across cyber, physical and operational technology domains, responsible for coordinated governance, resilience against hybrid threats, and alignment with applicable standards and regulatory frameworks. The adopter CCSO office described in this policy is distinct from, and does not confer, the GCSB CCSO membership grade.
- **Converged Security:** the integrated approach to managing cyber, physical and operational technology security as a unified discipline, with coordinated threat detection, response and recovery.
- **Convergence Champion:** an individual appointed by a business unit to coordinate implementation of this policy within that unit and to facilitate cross-functional security integration.

- **Hybrid Risks:** risks arising from threats that combine cyber, physical and operational technology attack vectors, often involving coordinated actions across multiple domains.
- **Systemic Risks:** risks that affect the organisation's security posture across multiple interconnected systems or domains simultaneously.
- **Cascading Risks:** risks arising where an incident in one domain propagates to affect other interconnected domains.
- **Executive Authority Hierarchy:** the adopter's defined structure of delegated decision-making authority for converged security matters, with clear accountability and escalation procedures.
- **Board Risk Committee:** the adopter's governance body responsible for strategic oversight of converged security risk.
- **Converged Security Governance Committee:** the adopter's cross-functional committee, chaired by the CCSO, responsible for coordinating implementation of this policy.
- **Identity and Access Management (IAM):** the unified system for managing digital and physical identities, authentication, authorisation and access controls across all organisational domains and systems.
- **Multi-Factor Authentication (MFA):** an authentication method requiring two or more verification factors to gain access to systems, applications or physical locations.
- **Operational Technology (OT):** hardware and software systems that monitor and control physical devices, processes and infrastructure in industrial environments, including supervisory control and data acquisition systems.
- **Physical Security Information and Management (PSIM):** a technology platform that integrates multiple security applications and devices to provide a unified approach to security management.
- **Security Information and Event Management (SIEM):** a technology platform providing real-time analysis of security alerts generated by applications and network hardware across cyber and operational technology domains.
- **Third-Party Integrations:** external service providers, suppliers, contractors and cloud services that interface with, or have access to, the organisation's cyber, physical or operational technology systems.
- **Unified Risk Register:** the consolidated record of identified risks across cyber, physical and operational technology domains, including risk ratings, treatment plans and interdependency mapping.
- **Zero Trust:** the security architecture principle requiring verification of every user and device attempting to access systems or data, regardless of location or prior authentication status.

5. Roles, responsibilities and governance

The following are adopter roles and bodies, not GCSB offices.

Board and Board Risk Committee. The adopter's Board shall establish a Board Risk Committee with oversight responsibility for converged security governance. Where the adopter's governance arrangements provide for independent directors, the Committee should include members with relevant security, risk management or technology expertise proportionate to the organisation's size and risk profile.

Chief Executive Officer (CEO). The CEO shall provide executive sponsorship for the converged security programme and ensure adequate budgetary allocation under CCSO authority.

Chief Converged Security Officer (CCSO). The CCSO shall hold authority equivalent to other C-suite officers and shall report directly to the CEO and the Board Risk Committee, with decision-making authority over converged security strategy, implementation and operations, including:

1. Budgetary control over security-related expenditure across cyber, physical and operational technology domains, consistent with clause 6, requirement R9.
2. Authority to issue security directives to business units, subsidiaries and third-party service providers.

3. Authority to require modification or suspension of business operations that pose unacceptable security risk.
4. Final authority over security incident response decisions and business continuity activation.

Converged Security Governance Committee. The CCSO shall chair a Converged Security Governance Committee comprising representatives responsible for IT security, OT security, physical security, risk management, legal and compliance, and Convergence Champions from major business units. The committee should convene on a regular cadence defined by the adopter, with provision for emergency sessions following significant security incidents.

Convergence Champions. Each business unit shall appoint a Convergence Champion as the primary liaison with the CCSO, responsible for coordinating implementation of this policy within that unit.

Business units. Business units shall comply with unified security policies, report incidents through CCSO-managed channels, participate in risk assessments, and integrate converged security requirements into operational and vendor management processes.

Employees and third parties. Employees shall comply with IAM policies, participate in training required under GCSB-ST-CSF-TRA-001, and report security incidents promptly. Third-party service providers and contractors shall comply with the organisation's converged security requirements as set out in their agreements; third-party integrations are subject to CCSO approval and ongoing monitoring.

6. Requirements

R1 CCSO appointment, authority, independence and competence. The CCSO shall be formally appointed, hold executive authority as described in clause 5, and demonstrate competence aligned with GCSB-ST-CSF-TRA-001. Appointment criteria should reflect senior security leadership experience, relevant professional certification, and a record of regulatory compliance management, without implying GCSB CCSO membership.

R2 Governance structure and reporting lines. The adopter shall maintain the governance structure set out in clause 5, with the CCSO reporting to the CEO and the Board Risk Committee, and presenting regular reports to the Board Risk Committee covering converged security posture, risk assessments, incident response activity and regulatory compliance status.

R3 Integrated risk governance and unified risk register. The CCSO shall implement a risk management framework aligned with GCSB-ST-CSF-RMA-001, maintaining a Unified Risk Register that consolidates risks across cyber, physical and operational technology domains, including cascade effect mapping and interdependency analysis, reviewed on a regular cycle defined by the adopter.

R4 Identity and access governance. The organisation shall deploy and maintain unified identity and access management aligned with GCSB-ST-CSF-IAM-001, including multi-factor authentication for critical access points, privileged access management based on least privilege, and identity lifecycle management integrated with human resources processes.

R5 Incident response tiers and business continuity. The CCSO shall establish unified incident response procedures and business continuity plans aligned with GCSB-ST-CSF-IRBC-001, including a tiered escalation structure and defined recovery objectives. Response, notification and recovery time values referenced in the organisation's procedures are indicative values that the adopter shall confirm and document in its own procedures, consistent with GCSB-ST-CSF-IRBC-001, unless a shorter or longer period is set by applicable law.

R6 Compliance and regulatory alignment. The organisation shall maintain a regulatory compliance register and procedures for monitoring regulatory change, covering frameworks applicable to it such as GDPR/UK GDPR, NIS2 and

DORA. Regulatory notification periods stated in applicable law (for example, incident notification periods under NIS2 or personal data breach notification under GDPR) apply as set by that law; where this policy or the adopter's procedures state a period for internal purposes, it is indicative unless law requires otherwise.

R7 Technology, PSIM, OT and supply-chain integration. The organisation shall integrate security information and event management (SIEM) and physical security information and management (PSIM) platforms in a vendor-neutral manner, aligned with GCSB-ST-CSF-TIA-001, extending to operational technology environments and third-party and supply-chain integrations. No specific vendor product is mandated by this policy.

R8 Audit, assurance, performance measurement and reporting. The CCSO shall establish an audit and assurance framework, including periodic independent internal audit of converged security controls and corrective action plans for identified deficiencies within a timeframe the adopter shall define and document. Performance measurement shall cover risk management, incident response, access management, regulatory compliance, and training and culture development. Any detection accuracy, false-positive, prediction-accuracy, activation-time or training-completion figures used by the adopter are illustrative examples, not commitments or guarantees, unless the adopter defines and documents its own measured targets.

R9 Resource allocation, financial accountability, communication and crisis management. The CCSO shall have defined budgetary authority for converged security expenditure, subject to thresholds set by the Board Risk Committee, with regular financial reporting. The CCSO shall maintain crisis management and communication procedures, including defined incident reporting channels and escalation to the CEO and Board Risk Committee for critical incidents. Any cost, savings or return-on-investment figures referenced by the adopter are illustrative examples, not commitments or guarantees.

R10 Change management, version control and continual improvement. The CCSO shall maintain a change management process classifying changes to this policy (for example, as emergency, standard or major), with emergency changes subject to retrospective Board Risk Committee approval within a timeframe the adopter shall define, and major changes subject to Board Risk Committee approval following impact assessment. Version control records shall be retained for a period the adopter shall define and document, consistent with its regulatory and audit obligations.

7. Implementation and transition

Implementation shall occur within 12 months of certification commencement, with a 6-month gap assessment of existing systems against this policy's requirements.

8. Evidence, monitoring, assessment and corrective action

Evidence of conformance includes records of CCSO appointment, governance committee minutes, periodic Board reports, the Unified Risk Register, performance metrics and audit records. Where the adopter uses quantitative targets (for example, for detection accuracy, false-positive rates, prediction accuracy, activation time or training completion), these shall either be supported by a defined and documented measurement method or treated as aspirational indicators, and in either case are not commitments or guarantees.

For data-subject rights timing, the UK rule applies as set out in applicable UK data protection law; for the European Union, data subject rights shall be exercised within the period set by applicable EU and Member State law, with no specific number stated in this policy.

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.

This policy, and any dispute arising from it, 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.

9. Exceptions, escalation and review

The CCSO may approve temporary exceptions to this policy for up to 12 months, supported by documented business justification and risk assessment. Exceptions longer than 12 months require approval by the Board Risk Committee on the recommendation of the Enterprise Risk Management Committee. All exceptions shall be reviewed quarterly, with a centralised exception register maintained recording business justification, compensating controls, risk evaluation and remediation progress.

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.