

Training and Awareness

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-TRA-001
Title	Training and Awareness
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-tra-001-training

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 standard sets out a uniform presentation of the Training and Awareness requirements within the Converged Security Framework (CSF) suite. It does not grant, waive or recognise any individual credential, continuing professional development (CPD) hours, certification, accreditation or Trustmark Award. Organisational training and awareness activity carried out under this standard is distinct from any individual GCSB recognition, and GCSB is not positioned as a training, consulting or audit provider. Adoption of this standard confers no qualification, Trustmark Award, accreditation or certification by itself.

2. Purpose, scope, applicability and exclusions

Purpose: this standard establishes requirements for cross-functional training, security awareness and competency development across cyber, physical and operational technology (OT) domains, supporting the Main Standard (GCSB-ST-CSF-001).

Scope: this standard applies to organisations seeking GCSB Trustmark certification for training and awareness capability, and to their personnel and relevant contractors, across cybersecurity, physical security and operational technology domains. It covers cross-functional security training programmes and curricula; security awareness programmes addressing hybrid threat recognition; specialised training for security personnel; tabletop exercises and simulation drills

for multi-domain security incidents; competency requirements and assessment for security-related roles; continuing education and professional development activity; and training documentation and record-keeping.

The requirements in this standard are minimum requirements for the stated scope; informative guidance may supplement them. Where an organisation is subject to additional regulatory requirements (for example NIS2, DORA, PCI DSS or sector-specific regulations), the most restrictive requirement applies. Critical infrastructure operators shall implement any additional training controls required by their sectoral regulations and by the Main Standard.

Exclusions: statutory and sectoral training duties remain the responsibility of the adopting organisation.

3. Normative references

GCSB-ST-CSF-001 Main Standard; 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.

The following are informative external references, cited by title without asserting unverified edition details: ISO 31000 Risk management; ISO/IEC 27001 Information security management systems; ISO 22301 Business continuity management systems; IEC 62443 series on industrial automation and control systems security; the General Data Protection Regulation (GDPR) and UK GDPR; the NIS2 Directive; the Digital Operational Resilience Act (DORA); the Cyber Resilience Act; and the EU AI Act, where applicable to the organisation.

Associated guidance, where issued by GCSB, provides supporting implementation material.

4. Terms, definitions and abbreviations

Cross-functional security training: training that integrates cybersecurity, physical security and operational technology security content for relevant personnel.

Security awareness programme: a programme delivering ongoing security education to all personnel, with role-based content.

Competency: the demonstrated knowledge, skill and practical capability required for a security-related role, established and verified through assessment.

Tabletop exercise: a discussion-based exercise used to validate personnel and organisational response to security scenarios.

Simulation drill: a practical, scenario-based exercise used to validate personnel response capability under realistic conditions.

Hybrid risks, systemic risks and cascading risks: risk categories aligned with the Main Standard (GCSB-ST-CSF-001) and treated, for incident type and severity, consistently with GCSB-ST-CSF-IRBC-001.

CCSO: Chief Converged Security Officer, or the adopter's equivalent accountable executive.

5. Roles, responsibilities and governance

The adopting organisation shall define and document the following roles: board-level oversight; a CCSO or equivalent executive; a training governance committee; training administrators; competency assessors; and human resources or learning function owners. These are roles within the adopting organisation; they are not GCSB offices and carry no GCSB operational authority.

The organisation shall establish a committee responsible for the strategic direction of its technology-related training, with representation from relevant functions including IT security, physical security, operational technology, human resources and executive leadership. This committee shall convene at least quarterly to review training effectiveness, assess emerging competency requirements and oversee budget allocation for training initiatives, consistent with the governance committee cadences set out in GCSB-ST-CSF-GLA-001.

This standard is reviewed by the Certification and Standards Committee and approved by the Governing Council, and is published at gcsb.uk.

6. Requirements

6.1 Cross-functional security training

The organisation shall deploy and maintain cross-functional security training programmes that integrate cybersecurity, physical security and operational technology security training across all personnel within scope, supporting the Main Standard's unified approach to competency development.

6.2 Security awareness programmes

The organisation shall implement and operate security awareness programmes delivering role-based security education to all personnel, covering hybrid threat recognition, cross-domain security incidents and integrated response procedures. The organisation shall define and document its own completion-coverage target for these programmes; a target of the order of 95% of personnel is an illustrative example, not a commitment or guarantee, unless the organisation adopts it as its own documented requirement. Training content and assessment shall comply with applicable data protection law, including GDPR, UK GDPR and relevant sector-specific requirements.

6.3 Specialised personnel training

The organisation shall provide specialised training for personnel in security operations, technical and leadership roles, including incident response, threat analysis, cross-domain security management, and competency relevant to technology platforms covered by GCSB-ST-CSF-TIA-001. Technology platform training shall be vendor-neutral and proportionate to the platforms actually deployed by the organisation; no vendor product is mandated by this standard. Where the organisation sets pass-rate or scoring thresholds for competency assessment (for example a minimum practical assessment score), it shall define, document and apply these consistently, together with the related assessment population and frequency.

6.4 Cross-domain training integration

The organisation shall establish and maintain integration between training programmes across security domains to enable coordinated curricula, shared scenarios and consistent competency assessment, supporting the Main Standard's converged approach to hybrid, systemic and cascading risks.

6.5 Competency framework, assessment and reassessment

The organisation shall implement a competency framework covering all security-related roles, with assessment on appointment and periodic reassessment thereafter. The organisation shall define and document its pass thresholds, assessment frequency and reassessment cadence, and shall align these, so far as practicable, with the competency assessment and annual reassessment requirements of GCSB-ST-CSF-IAM-001. Any annual continuing-education hours or quarterly training-hour targets referenced by the organisation are matters for it to define and document; where used as illustrative examples only, they are not commitments or guarantees.

6.6 Tabletop exercises and simulation drills

The organisation shall conduct tabletop exercises and simulation drills to validate personnel and organisational response to multi-domain security incidents, using scenarios aligned with GCSB-ST-CSF-IRBC-001. Exercises shall address hybrid incidents affecting both physical and digital domains, systemic incidents involving interconnected system failures, and cascading incidents involving sequential, propagating failures. Where operational technology environments are used in drills, the organisation shall apply appropriate safety controls to avoid disruption to live systems. The organisation shall define and document the exercise frequency and the period of threat-scenario material used to inform exercise design.

6.7 Technology-platform training

Training on technology platforms within the scope of GCSB-ST-CSF-TIA-001 shall be vendor-neutral and proportionate to the platforms the organisation actually operates. Where applicable to the organisation's environment, training shall address security information and event management / physical security information management (SIEM/PSIM) platform operation, zero trust architecture principles, and the use of artificial intelligence and machine learning in threat detection, at a level proportionate to each individual's role. The organisation shall not be required to maintain vendor certifications for every deployed platform; where certification maintenance is adopted as an organisational requirement, it shall be proportionate to role and platform criticality.

6.8 Training records, documentation and governance

The organisation shall maintain documentation evidencing the operation of its training programmes, including curricula, competency frameworks, delivery records and assessment outcomes. Personal data within training records shall be processed in accordance with GCSB-ST-CSF-DPP-001. Governance arrangements shall define roles and responsibilities for training administration, competency assessment and continuous improvement, and shall provide for regular review of training content to maintain currency with the threat environment and with applicable technology platforms. Where the organisation sets a target update period following platform changes (for example updating materials within a defined number of days of a significant change), it shall define and document that period.

6.9 Governance oversight of technology training

The organisation's training governance committee, or equivalent body, shall maintain oversight of technology-related training content and its currency, including periodic review of training effectiveness and of emerging competency requirements arising from changes to technology platforms in scope.

6.10 Monitoring, effectiveness measurement and continual improvement

The organisation shall monitor the effectiveness of its training and awareness programmes and apply continual improvement, including review of exercise outcomes, assessment results and identified competency gaps. Any cost, savings or return-on-investment figures associated with training investment are, where referenced by the organisation, illustrative examples only and not commitments or guarantees.

7. Implementation and transition

Full implementation of this standard follows the extended implementation track of 18 months from certification commencement provided for Training and Awareness under the suite implementation provisions, comprising a gap assessment of existing training systems and a baseline competency assessment by month 6, a foundation phase completing by month 6, a development phase completing by month 12, and full capability achieved by month 18. The 12-month baseline controls and 6-month gap assessment set out in the Main Standard continue to apply throughout this track.

8. Evidence, monitoring, assessment and corrective action

Certification assessment under this standard comprises a completeness review, assessment against the requirements of clause 6, documented scoring, a written decision, and, where applicable, a remediation plan and corrective action. Where remediation is required, the organisation shall document a remediation plan and complete it within the timescales it has agreed with GCSB; where the organisation's own procedures set indicative periods (for example a 30-day plan with 90-day completion), these are indicative values for the organisation to confirm in its own procedures. Revocation of certification is subject to a reapplication bar, the length of which the organisation shall confirm in its own procedures unless otherwise fixed by the applicable GCSB certification procedure.

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; until that procedure specifies otherwise, any clocks referenced in an organisation's own procedures remain indicative and the organisation shall confirm them in its own documentation.

This standard 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 before litigation. No compulsory arbitration applies. The statutory rights of regulators and data subjects are unaffected.

9. Exceptions, escalation and review

Deviations from this standard require documented business justification and CCSO approval. The CCSO may approve temporary exceptions for up to 12 months. 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 at least quarterly.

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.