

Converged Security Risk Management and Assessment Standard

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-RMA-001
Title	Converged Security Risk Management and Assessment 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-rma-001-risk-management

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. Numbered risk management requirements
- 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 Intended use

This standard connects cross-domain risk identification, analysis, evaluation, treatment and monitoring with the Main Standard's security framework, Strategic direction and Governance accountability. It is intended for adopter governing bodies, CCSOs, enterprise risk teams, cybersecurity, physical security and OT owners, identity administrators, privacy and legal advisers, business continuity personnel and assurance functions.

1.2 Issuer and adopter

GCSB issues standards. The adopting organisation implements them within its actual scope and lawful authority. An adopter's board, CCSO, Enterprise Risk Management Committee, Board Risk Committee, IAM committee and SOC are

not GCSB offices. The issuer's Governance Charter does not automatically set an adopter's quorum, employment terms or incident command arrangements.

GCSB is not a training, consulting or audit provider. Adoption does not itself confer statutory powers, ISO certification, GCSB accreditation, a credential, a Trustmark Award or a product endorsement. Assessment and recognition require their own separate authorised schemes and independent decisions.

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 and evidenced risk decisions across cybersecurity, physical security and operational technology security, including hybrid, systemic and cascading exposures, through scoped objectives and demonstrable evidence.

2.2 Scope

The adopter shall document entities, services, facilities, systems, data, personnel, third parties and security domains within scope, material interfaces and the justification for exclusions. An absent OT estate shall be explained rather than invented. Dependencies outside direct control shall still be assessed, with controls limited by applicable law, actual authority and agreements.

Joint ventures and suppliers shall not be deemed wholly controlled merely because they interface with organisational systems. Risk sharing, assessment rights, information exchange and incident cooperation shall be documented through lawful arrangements. No unlimited right to audit another organisation is created by this standard.

2.3 Applicable obligations

The adopter shall identify binding legal, regulatory, contractual and scheme duties by entity, jurisdiction, sector and activity. UK GDPR and EU GDPR, NIS2 national implementation, DORA, phased CRA/AI Act provisions, eIDAS, PCI DSS and voluntary ISO/NIST references shall be distinguished. An aggregate compliance score does not authorise non-compliance with binding law.

A voluntary standard cannot waive law, give an unidentified regulator powers or constitute an executed contract.

3. Normative references and related documents

3.1 Controlled reference approach

Normative references shall be identified by exact title, edition, applicable provisions and availability. A list of names is not blanket incorporation. Associated guidance, where issued by GCSB, shall not be represented as published or approved without evidence.

Reference	Role
GCSB-ST-CSF-001	Master scope, baseline requirements and exception authority
GCSB-CSF-STRAT	Organisational direction
GCSB-ST-CSF-GLA-001	Adopter oversight, delegation and reporting
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	Operational, privacy, response and competence interfaces
ISO 31000:2018	Risk management guidance
ISO/IEC 27001:2022 and ISO 22301:2019	ISMS and BCMS requirements alignment where applicable
NIST SP 800-30, SP 800-53 and SP 800-63	Risk assessment, control and identity guidance as applicable
CVSS as cited	Technical vulnerability-severity input, distinct from enterprise risk
IEC 62443, ISO/IEC 19794 and Common Criteria as cited	Specialist industrial, biometric and evaluation references
MITRE ATT&CK, STIX/TAXII, YARA and OpenIOC as cited	Threat mapping or exchange methods

No certification or universal recovery target is implied by these references. The adopter shall verify the applicable edition, parts and provisions before relying on any external reference.

3.2 Legal and technical reference control

The adopter shall maintain a legal applicability register separately identifying legislation, implementing measures, regulator guidance, voluntary standards and contracts. Technical references shall distinguish authentication from authorisation protocols and biometric data formats from security-effectiveness guarantees. No universal external notification clock, statutory budget or processing-capacity minimum is created by this standard.

4. Terms and abbreviations

Term	Meaning
Converged security	Coordinated cybersecurity, physical security and OT security within documented scope

Risk	Effect of uncertainty on objectives, assessed with the relevant threats, exposures, controls, likelihood and consequences
Risk owner	Adopter role accountable for a specified risk and authorised decisions within documented delegation
Risk appetite / criteria	Approved boundaries and criteria used to evaluate exposures and treatment decisions
Residual risk	Exposure remaining after controls/treatments, assessed with their actual effectiveness and limitations
Hybrid / systemic / cascading	Cross-domain exploitation, interconnected broad disruption and propagating failure types; not severity tiers
Severity	Assessed impact and urgency against documented criteria, separate from incident type or escalation level
CCSO	Chief Converged Security Officer or equivalent cross-domain executive role under the Main Standard
RTO / RPO	Scoped recovery-time / recovery-point objectives derived from business impact and approved requirements
Integration coverage	Measured coverage of a specified eligible population with documented acceptance criteria
Accuracy / false-positive rate	Distinct model/test measures requiring population, labels, calculation, thresholds and validation evidence
CVSS	Vulnerability-severity scoring input, not a standalone measure of organisational risk
Exception	Authorised, recorded deviation from a standard requirement within lawful bounds; not a legal exemption

5. Roles, responsibilities and governance

5.1 Issuer control

Standards are developed and reviewed by the Certification and Standards Committee and approved by the Governing Council under its Charter. Standards are published at gcsb.uk.

5.2 Adopter accountability

The governing body shall approve risk appetite and reserved material decisions, oversee the strategy and receive risk reports. The CCSO shall coordinate cross-domain risk processes under executive delegation, reporting to the chief executive or equivalent with regular direct board communication.

Domain specialists and business risk owners shall assess and treat scoped exposures. Safety, privacy, legal and operational responsibilities remain with their competent owners; the CCSO's coordination does not grant unlimited

powers over all entities or processing. Assurance shall be separated from ownership of the controls reviewed. Data protection officer advice and monitoring shall not be equated with determining all purposes and means of processing.

5.3 Committee interface

The adopter shall document the coordination committee, IAM committee, Enterprise Risk Management Committee and Board Risk Committee relationships, decisions, escalation and reserved authority, including the Main Standard's exception approval route.

6. Numbered risk management requirements

6.1 Risk context, criteria and ownership

6.1.1 The adopter shall maintain documented risk objectives, scope, criteria and ownership, connected to organisational strategy and approved risk appetite. Criteria shall address safety, continuity, financial, confidentiality, integrity, privacy, physical and applicable legal consequences.

6.1.2 Each material risk shall have an accountable owner and recorded evaluation, treatment decision, responsible action owners, status and escalation route. Risk decisions shall remain within delegated authority; statutory responsibilities shall not be displaced by a dashboard or model.

6.2 Unified risk register and dependencies

6.2.1 The adopter shall maintain a unified register covering scoped cybersecurity, physical and OT risks and relevant identity, supplier, environmental and business dependencies. Each entry shall identify scenario, affected objectives/assets/services, threats, exposures, existing controls, likelihood/impact method, uncertainty, residual exposure, owner, treatment and review evidence.

6.2.2 The adopter shall document hybrid, systemic and cascading pathways, shared failure points and material dependencies across security domains. Quantitative correlation shall not be represented as causal proof without justified analysis.

6.3 Assessment and threat analysis

6.3.1 Risk assessments shall be conducted at least annually using a documented method aligned with ISO 31000 principles as applicable. Reassessment shall be event-driven and shall address material change, incidents, new dependencies and control failure.

6.3.2 Threat landscape analysis shall be performed quarterly and shall cover the relevant scoped domains and identity/supplier threats. Intelligence shall be assessed for provenance, timeliness, relevance, reliability, lawful use and coverage.

6.3.3 Assessment methods shall distinguish technical vulnerability severity from enterprise risk. CVSS may inform technical prioritisation, but treatment shall also consider asset criticality, exploitation, business/safety consequences, controls and uncertainty.

6.4 Business impact and recovery interface

6.4.1 The adopter shall maintain business impact analyses for material scoped services and dependencies, including IT/OT integration, physical access, identity/federation failures, suppliers and shared security-platform outages.

6.4.2 Recovery priorities, recovery time objectives, recovery point objectives and alternative operating/authentication arrangements shall be documented, approved against business impact and tested. Specific recovery-time and recovery-point values are indicative and shall be confirmed by the adopter in its own procedures, aligned with its business impact analysis, unless a binding law or regulatory requirement sets them.

6.4.3 Dependency and cascade containment strategies shall be documented and validated at least annually. Exercises shall validate restoration integrity, operational safety and failure of shared coordination or identity services.

6.5 Treatment and coordinated control implementation

6.5.1 The adopter shall document coordinated treatment plans across affected domains, with risk owner, chosen response, control purpose, accountable implementation owner, resources, target completion, validation and residual-risk decision. Avoidance, reduction, sharing and retention shall be evaluated within actual authority and applicable law.

6.5.2 Treatments shall connect to applicable Technology, Identity, Data Protection and Incident Response requirements. Defence in depth, segmentation, access lifecycle, privileged access, backup, physical protection and incident playbooks shall be scoped to the exposure and dependencies. Controls shall be vendor-neutral and, where relevant, safety-qualified; no specific vendor product is mandated.

6.5.3 Live OT safety and authorised change procedures shall be addressed before any control affecting operational technology is implemented.

6.6 Monitoring, integration and measurement

6.6.1 The adopter shall maintain coordinated monitoring and risk-to-incident information exchange across scoped domains, including defined operating arrangements and safe fallback.

6.6.2 Every coverage, availability, accuracy, latency and compliance indicator shall have a defined eligible population, numerator/denominator, calculation, measurement window, evidence source, exclusions, target, owner and escalation. Coverage claims shall distinguish cybersecurity sources, all security domains, integrated platforms, organisational assets and IAM implementation, and the adopter shall define and document the applicable target for each.

6.6.3 A percentage measure shall not authorise an unmet binding duty or exclusion of critical uncovered dependencies.

6.7 Analytics and model assurance

6.7.1 Where models support risk decisions, the adopter shall document purpose, data provenance, assumptions, scope, limitations, validation, uncertainty and accountable human decision authority. Training/test separation, out-of-sample performance, drift and material changes shall be evaluated where applicable.

6.7.2 Automated containment, identity revocation and operational changes shall be bounded by authorised playbooks, safety, privacy and continuity safeguards and recorded for review. A prediction or correlation alone shall not confer authority to make a material risk-acceptance or legal decision.

6.7.3 Any retained performance or accuracy measure for analytics shall have a defensible validation method and scoped applicability, not a mathematical guarantee from iteration count alone.

6.8 Identity, privacy and supplier risk

6.8.1 The adopter shall assess privileged access, lifecycle failures, federation trust, authentication disruption, credential compromise and identity-data dependencies. Controls shall include lawful access governance, audit evidence, compromise handling and recovery interfaces aligned with GCSB-ST-CSF-IAM-001.

6.8.2 Privacy assessment shall identify actual controller/processor responsibilities, lawful bases, applicable special-category conditions, necessity, rights, retention and transfer requirements. Explicit consent shall not be assumed to be the universal lawful basis for biometric processing; biometric accuracy does not establish lawful processing. For data-subject rights timing, the adopter shall apply the UK statutory period where UK law governs, and within the European Union, the period set by applicable EU and Member State law.

6.8.3 Critical security suppliers shall receive annual risk assessment, with cyber and physical considerations and OT/identity dependencies where relevant. Contracts and operating arrangements shall address authorised information exchange, incident cooperation, assessment rights and remediation. Background checks and external access shall remain lawful and proportionate.

6.9 Incident escalation and continuity

6.9.1 Risk monitoring shall connect to documented incident triggers, response authority, cross-domain coordination, evidence and continuity procedures. Hybrid/systemic/cascading classifications shall be separate from severity, with Level 1 response teams, Level 2 CCSO and Level 3 board-risk engagement.

6.9.2 Activation, detection, response and containment timescales for each escalation level shall be documented by the adopter as indicative values confirmed in its own procedures, with explicit start and stop events, unless a binding law sets a specific clock. Urgent safety or containment action shall not be deferred until a board convenes.

6.9.3 External notifications shall follow applicable law and role-specific triggers, recipients, awareness events and deadlines, separately from internal escalation and response.

6.10 Competence and information control

6.10.1 The adopter shall define and evidence competence for risk owners, analysts, specialists, committee personnel and incident teams, with practical assessment and corrective development. Training shall distinguish attendance, completion, pass rate, demonstrated competence and operational effectiveness.

6.10.2 The adopter shall define and document its own completion, pass rate, proficiency and annual update-hour targets for risk competence, consistent with applicable Governance and Main Standard requirements. Adopter training is not automatically professional continuing development credit or entitlement to a GCSB award.

6.10.3 Risk records, models and evidence shall be classified, access-controlled, retained and disposed of under documented purpose and applicable law. Record integrity, versioning, traceability and lawful information exchange shall be maintained. Organisational classification labels do not imply statutory security clearances.

7. Implementation and transition

Full implementation of this standard shall be achieved within 12 months of certification commencement, with a gap assessment of existing systems completed within 6 months of certification commencement.

Phase	Indicative timing	Deliverables
Assessment and planning	Months 1-3	Baseline, risk inventory, authority and scope deliverables
Technology integration	Months 4-8	Risk automation dependencies aligned with GCSB-ST-CSF-TIA-001 rollout
Process integration	Months 6-10	Overlap management and acceptance evidence
Operational monitoring	Months 9-12	Capabilities and completion criteria confirmed
Full deployment	Within 12 months of certification commencement	Evidence of commencement, exceptions and companion readiness
Existing systems assessment	Within 6 months of certification commencement	Compatibility deliverables confirmed

Monthly progress reporting through coordination committees and CCSO oversight shall be maintained. Existing operations shall not be disrupted solely to satisfy a new capability under this standard without an approved transition and change safeguard.

8. Evidence, monitoring and corrective action

The adopter shall maintain proportionate, verifiable evidence of scope, risk register, criteria/ownership, assessments, threat analyses, business impact analysis, dependency/cascade validation, treatment decisions, monitoring, model assurance, training, supplier review, incidents, exceptions and corrective actions.

Reviews shall identify unmet requirements, coverage gaps, ineffective controls, overdue actions, uncertainty and material exposure. Corrections shall have an owner, priority, due date, validation and escalation. Management reporting shall identify assumptions and uncertainty rather than claim complete decision effectiveness, statistical superiority or risk elimination without evidence.

Conformity assessment shall distinguish mandatory requirements from guidance and separately authorised scheme criteria. A readiness score shall not create accreditation, a statutory exemption or permission to ignore an unmet mandatory control. Where illustrative cost, savings or return-on-investment figures are used, they are illustrative examples, not commitments or guarantees.

9. Exceptions, escalation and review

All deviations shall be recorded with business justification, affected requirement, scoped risk/impact, compensating controls, owner, approval, duration, review and remediation. Under suite rule S4, the CCSO may approve temporary

exceptions up to 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. Risk escalation shall not replace this with a generic designated authority or make the 12-month limit an absolute bar.

Exception processing shall be timely and shall not create automatic approval, permit advance deviation without authority or allow a legal breach to be waived. Urgent risk escalation shall be kept separate from administrative completion.

A standard exception cannot waive binding law or confer a scheme entitlement. Changes to risk criteria, models, scope, material treatments or evidence shall be controlled, assessed for safety/privacy/dependency impact, authorised and validated. Emergency operating decisions shall be documented within lawful delegation and reviewed by the competent authority.

Certification and enforcement decisions 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.

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

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.