

Incident Response and Business Continuity Framework

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

Document control

Field	Value
Identifier	GCSB-ST-CSF-IRBC-001
Title	Incident Response and Business Continuity 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-irbc-001-incident-response

Contents

- 1. Foreword 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 and intended use

This standard sets out a uniform approach to incident response and business continuity across cyber, physical and operational-technology (OT) domains. It forms part of the Converged Security Framework (CSF) suite and is consistent with the Main Standard (GCSB-ST-CSF-001). Adoption of this standard does not itself confer statutory authority, accreditation, qualification or a Trustmark Award; certification is a separate process under the GCSB certification procedure. GCSB is the issuer and certification body for this standard; it is not a training, consulting or audit provider.

2. Purpose, scope, applicability and exclusions

Purpose. To establish coordinated incident response and business continuity capabilities across cyber, physical and operational-technology domains, consistent with the Main Standard.

Scope. This standard applies to organisations seeking GCSB Trustmark certification for incident response and business continuity capabilities, including entities under their direct managerial control. For joint ventures or partnerships without majority control, this standard applies only where the organisation accesses, processes or manages the relevant incident response systems, data or business continuity facilities.

In scope: incident response systems and infrastructure across IT, OT and physical security domains; business continuity platforms and recovery capabilities; cross-domain integration platforms supporting unified incident response; cloud and hybrid environments supporting integrated incident response operations; third-party and supply chain incident response arrangements; escalation systems and decision-making authorities; recovery time and recovery point objective implementations; and crisis management and communication systems supporting unified response.

Exclusions. Sector-specific legal duties remain with the adopter. Where the NIS2 Directive, DORA, the UK and EU GDPR or other sectoral rules impose stricter requirements, the stricter rule applies. This standard does not itself discharge any statutory reporting duty.

3. Normative references

GCSB-ST-CSF-001 Main Standard; GCSB-ST-CSF-TIA-001 Technology Integration and Architecture; GCSB-ST-CSF-TRA-001 Training and Awareness; GCSB-ST-CSF-RMA-001 Risk Management; GCSB-ST-CSF-DPP-001 Data Protection and Privacy.

Informative external references (the adopter shall confirm the applicable edition before relying on it): ISO 31000 Risk management; ISO/IEC 27001 Information security management systems; ISO 22301 Business continuity management systems; NIST SP 800-61 Computer Security Incident Handling Guide; NIST SP 800-34 Contingency Planning Guide; NFPA 1600 Standard on Continuity, Emergency, and Crisis Management; EN 50131 Intrusion detection systems; EN 50518 Alarm receiving and monitoring centres; EN 62676 Video surveillance systems; EN 60839-11-1 Electronic access control systems; the UK and EU General Data Protection Regulation (GDPR); the NIS2 Directive; the Digital Operational Resilience Act (DORA); the Cyber Resilience Act (CRA); the EU AI Act; and the Digital Services Act (DSA), each applied to the extent it is in force for the adopter.

Associated guidance, where issued by GCSB, provides supporting material and is not itself a certification requirement.

4. Terms, definitions and abbreviations

Hybrid Risks: threats that exploit vulnerabilities across both physical and digital domains simultaneously, requiring coordinated response across multiple security disciplines.

Systemic Risks: interconnected system failures that can cascade across multiple operational areas, potentially causing organisation-wide disruption through network effects and dependencies.

Cascading Risks: sequential failures triggered by an initial incident that propagate through organisational dependencies, creating amplified impact beyond the original scope.

Hybrid, Systemic and Cascading Risks describe how an incident propagates, not its severity tier; the adopter shall maintain a separate severity model, with defined impact thresholds, for classifying incidents by severity (Class 1 Hybrid, Class 2 Systemic, Class 3 Cascading being incident types to which that severity model is applied).

Cross-domain Integration: the technical and operational interoperability between cybersecurity, physical security and operational technology incident response systems, enabling unified monitoring, analysis and response.

Unified Incident Response: coordinated response protocols covering cyber incidents, physical security breaches and operational technology disruptions, with integrated command and control.

Automatic Escalation: systematic notification and decision-making procedures that activate based on predefined incident severity and impact thresholds across security domains.

Chief Converged Security Officer (CCSO): executive role with authority over cybersecurity, physical security and operational technology security functions, accountable for unified risk management across all security domains.

Zero Trust Architecture: a security model requiring continuous verification of all users, devices and network connections, regardless of location or prior authentication status.

IT/OT Convergence: the integration of information technology and operational technology systems, creating risk vectors that require specialised security controls and governance.

5. Roles, responsibilities and governance

Board-level oversight shall be established for converged incident response and business continuity, with designated accountability for unified risk management across all security domains.

A Chief Converged Security Officer (CCSO), or equivalent executive, shall be appointed with authority over cybersecurity, physical security and operational technology security functions, including incident response coordination across all security domains.

A cross-functional governance committee shall meet monthly with representatives from IT security, physical security, OT security, risk management, compliance and business operations.

Unified command and control shall operate during incidents, with standardised communication protocols and clear authority delegation. Designated regulatory-reporting owners shall be identified.

Unified key performance indicators shall be established and monitored across all security domains, with dashboards and alerting for performance degradation.

These are adopter roles and bodies, not GCSB offices. This document is reviewed by the Certification and Standards Committee and approved by the Governing Council. GCSB acts as issuer and certification body only.

6. Requirements

6.1 Unified incident response

The adopter shall deploy and maintain unified incident response protocols that integrate cyber incident response, physical security breach response and operational technology disruption response, with coordinated cross-functional response teams covering cybersecurity, physical security, operational technology and business continuity specialists, and with clearly defined roles and responsibilities.

The adopter shall implement a standardised incident classification system capable of categorising Hybrid, Systemic and Cascading incident types, mapped to the severity-tier model required by clause 4.

The adopter shall establish and maintain cross-domain integration between incident response systems, consistent with GCSB-ST-CSF-TIA-001, to enable real-time situational awareness and coordinated response. Technology used to meet

this requirement shall be vendor-neutral and proportionate to the adopter's risk profile; no specific product shall be treated as mandatory.

Zero Trust Architecture principles shall be applied across incident response operations, with continuous verification of users, devices and network connections during incidents, consistent with GCSB-ST-CSF-TIA-001.

Where the adopter uses artificial intelligence or machine learning capabilities for predictive threat analysis or automated incident response coordination, these shall be proportionate, governed and consistent with GCSB-ST-CSF-TIA-001.

6.2 Escalation and decision-making authority

The adopter shall deploy and maintain notification arrangements that alert designated response teams promptly upon detection of a security incident in any domain.

The adopter shall define escalation levels and decision-making authorities, for example response-team level, CCSO or equivalent executive level, board-level risk committee level, and regulator notification, with the reliability of the notification arrangements evidenced and maintained; the adopter shall set and document its own target reliability and response-time figures as indicative values to be confirmed and evidenced in its own procedures, except where law sets a specific figure.

Escalation shall occur automatically where an incident affects multiple security domains simultaneously, compromises critical infrastructure systems, or shows cascading-failure potential.

Notifications to regulatory authorities shall comply with applicable law, including the NIS2 Directive, DORA and GDPR obligations where applicable to the adopter; for personal data breaches, UK GDPR notification timing follows the UK statutory rule, and for the EU the notification shall be made within the period set by applicable EU and Member State law.

Escalation shall be integrated with business continuity activation for incidents affecting critical business processes.

6.3 Business continuity planning and recovery

The adopter shall maintain business continuity plans addressing scenarios affecting multiple security domains simultaneously, including the simultaneous compromise of cybersecurity, physical security and operational technology systems.

The adopter shall define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical business process by criticality tier. The following indicative tiers, drawn from the source standard, are a starting reference which the adopter shall confirm, adjust and document in its own business continuity procedures, reconciled with any recovery clocks set under GCSB-ST-CSF-RMA-001 and GCSB-ST-CSF-IAM-001:

Process tier	Indicative RTO	Indicative RPO
Critical	4 hours	1 hour
Essential	24 hours	4 hours
Important	72 hours	24 hours
Support	1 week	48 hours

The business continuity capability shall provide integrated recovery procedures, including coordinated activation linking incident response and business continuity teams, alternative operating arrangements, and supply chain continuity arrangements.

The adopter shall develop cascading-failure prevention and mitigation measures, including dependency mapping, identification of cascade triggers, and containment procedures for each identified cascade pathway.

The adopter shall implement hybrid-threat response procedures addressing simultaneous physical and digital domain exploitation, and shall specifically address IT/OT convergence risks with safety-qualified controls for operational technology.

6.4 Training and awareness

Training and awareness shall be aligned with GCSB-ST-CSF-TRA-001. The adopter shall provide cross-functional training for all personnel covering cybersecurity, physical security and operational technology incident awareness and response; specialised training for incident response personnel on converged threat scenarios and hybrid attack vectors; regular tabletop exercises and simulation drills testing response to multi-domain incidents, with lessons learned incorporated into procedures; defined competency requirements for incident response roles; business continuity training for all personnel covering role-specific procedures and communication protocols; and executive training covering crisis management, strategic decision-making during incidents, and regulatory reporting obligations. Training completion targets and competency levels shall be set by the adopter consistent with GCSB-ST-CSF-TRA-001.

6.5 Compliance integration

The adopter shall align its incident response and business continuity management with ISO 31000, ISO/IEC 27001 and ISO 22301 as applicable, and shall map applicable sector-specific regulatory requirements, including the NIS2 Directive and DORA where relevant.

GDPR requirements shall be integrated into incident response procedures, including protocols for breach notification and any cross-border data transfer implications.

The adopter shall maintain an internal audit programme to verify compliance with this standard's incident response and business continuity requirements.

6.6 Monitoring and continual improvement

The adopter shall maintain dashboards providing visibility into incident response and business continuity performance, with alerting for performance degradation across any security domain.

The adopter shall define and operate reporting cadences appropriate to its governance structure, for example periodic compliance reporting, periodic gap analysis, and an annual resilience assessment including recovery-time testing for multi-domain scenarios, reconciled with the cadences used elsewhere in the CSF suite.

Post-incident analysis shall be conducted for all significant incidents, with lessons learned documented and incorporated into procedures and training.

7. Implementation and transition

Full implementation is required within 12 months of certification commencement, with an assessment of existing incident response and business continuity systems completed within 6 months of certification commencement. This standard does not sit on the 18-month extended implementation track. No interim or compensating control removes a legal duty that otherwise applies to the adopter.

8. Evidence, monitoring, assessment and corrective action

Certification assessment comprises application completeness review, desktop and, where applicable, on-site verification, documented scoring, a written decision, and conditional certification with remediation where applicable.

Appeals against certification and enforcement decisions lie 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 across the CSF suite; any specific day-counts referenced during development of this standard are indicative until that procedure is issued.

Any dispute arising from this standard 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

Deviations from this standard require documented business justification and CCSO approval. The CCSO may approve temporary exceptions for up to 12 months. Longer exceptions require approval by the Board Risk Committee on the recommendation of the Enterprise Risk Management Committee. All exceptions are reviewed quarterly, with remediation progress, a risk assessment and compensating controls documented for each exception.

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.

