CONVERGED SECURITY | RESEARCH COMPANIONS

PUBLIC SAMPLE EDITION

Converged Incident Response and Continuity

Shared Decisions, Safe Recovery and Evidence

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Converged Incident Response and Continuity
Shared Decisions, Safe Recovery and Evidence
Public sample edition | Version 1.0 | 11 November 2026

Author: Prof. Dr. Vladimir Bunic
Owner and distributor: Global Converged Security Board

A secondary practical/reference companion to the primary article identified in the research bibliography, read alongside the issued GCSB standards, mandatory procedures and advisory playbooks.

Eight explanatory readings and three fictional reflection exercises develop questions of evidence, authority and practical judgement. Exact reading crosswalks connect the commentary to issued standards, mandatory procedures and advisory playbooks. This is not a course study guide, a complete training sequence or a research article.

Research method and limits. Conceptual architecture synthesis and standards/dependency mapping; proposed benefits require organisation-specific testing.

Publication chronology. The primary article's registered online publication date is 30 September 2026. The CSF standards cited here were issued 13 October 2026; procedures and playbooks followed on 19 October 2026. This companion was prepared for publication on 11 November 2026. Its crosswalk is a later educational comparison, not evidence that the article used these issued editions.

Copyright and reader information

Copyright © 2026 Global Converged Security Board.
All rights reserved.

Except as permitted by applicable law, reproduction, redistribution or adaptation of this companion requires prior written permission. Source articles retain their separate licences; the companion’s rights notice does not change them.

Applicable law and adopted issued standards govern requirements. Mandatory procedures implement parent requirements; playbooks are advisory. Implementation milestones use the starting event stated by the relevant parent standard. Record organisational adoption and certification commencement separately; the Main Standard uses documented adoption for a new adopter. Article publication, source issue and book publication dates do not start an organisation's implementation period.

All exercises are fictional. Use no personal or confidential workplace data and make no live operational changes. Full worked solutions, complete training scenarios and instructor guidance are excluded.

The companion itself has not been peer reviewed and is not a GCSB Journal article. Source articles retain their original authorship, institutional attribution and licences. No ISBN is assigned. Cover imagery is AI-generated illustration.

Suggested citation. Bunic, V. (2026). Converged Incident Response and Continuity: Shared Decisions, Safe Recovery and Evidence. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24129169

Contents

One event, several operational consequences	**4**
Authority and evidence during containment	**5**
Continuity is a service-level question	**6**
Testing the connection between plans	**7**
The CSF lens: incident type is not severity	**8**
Three classifications, three different questions	**9**
Restoration integrity and the weakest dependency	**10**
Exercises that produce usable learning evidence	**11**
Sample exercise 1: Containment versus safe operations	**12**
Sample exercise 2: A technically successful restore	**13**
Sample exercise 3: Two plans, incompatible assumptions	**14**
Research bibliography and evidence	**15**
Reading crosswalk: explanations	**16**
Reading crosswalk: sample exercises	**17**
Issued-source bibliography	**18**
Issued-source bibliography (continued)	**19**

One event, several operational consequences

The primary article proposes a unified incident response and business continuity architecture across IT, OT and physical security. Its contribution is the connection between response coordination and continuity dependencies, rather than a claim that every incident has one technical remedy.

An incident can begin with a compromised account and become a physical access problem, an operational disruption and a personal-data concern. Teams need a common explanation of the event while preserving their specialist expertise and decision boundaries.

Shared situational awareness means describing what is known, what is uncertain and how each observation affects the service. It does not mean granting everyone unrestricted access to every log, camera record or personnel file.

Original companion example: a building-management outage affects cooling, which threatens a server room, while electronic access logs are unavailable. Recovery cannot be reduced to rebooting an application; safe premises and authorised access also matter.

Reading bridge. GCSB-GDL-IRBC-001, Play 1, Define incident categories, severity and authority. Classification supports coordination; the companion does not introduce new severity thresholds.

Authority and evidence during containment

Containment decisions can protect one domain while harming another. Disconnecting a network segment may constrain an attacker but also interrupt an operational dependency. The right decision depends on safety, authority and evidence, not a universally applicable first action.

Before selecting an intervention, distinguish who recommends, who authorises, who performs it and who verifies the result. Escalation is especially important when a local action has consequences for another team or service.

The article discusses Zero Trust enforcement and integrated analytics. Neither is a substitute for authorised incident command. Analytics can inform judgement, while access controls constrain pathways; both require tested assumptions and operational safeguards.

Evidence discipline records observations, times, decisions and changes. A convenient reconstruction made after recovery may conceal uncertainty or make an unverified hypothesis appear established. Preserve original observations where lawful and safe.

Reading bridge. GCSB-GDL-IRBC-001, Play 2, Build the response plan and playbooks. Read the issued source for operational details; this companion contains no executable containment sequence.

Continuity is a service-level question

Business continuity concerns the minimum viable service, its resources and acceptable disruption. A restored database does not establish continuity if staff cannot access the site, suppliers cannot deliver or a safety-critical dependency remains unavailable.

The article connects recovery planning across domains. A dependency map can reveal ordering constraints: restoring one function may require identity services, power, physical access or a supplier interface to be ready first.

Recovery time and recovery point objectives have different meanings. One concerns the targeted time to restore a function; the other concerns the point to which data must be recovered. Their operational interpretation requires business impact, adopted standards and verified technical capability.

A manual alternative can create its own privacy, safety or integrity risks. It should be examined as an operating arrangement, not treated as inherently safe because it avoids the failed technology.

Reading bridge. GCSB-GDL-IRBC-001, Play 3, Establish business continuity. The companion sets no universal recovery target and does not reproduce the source’s fictional timings.

Testing the connection between plans

A response plan and a continuity plan can each look complete while contradicting each other. One may call for isolation of a service that the other assumes will remain available. Joint testing reveals such mismatches before an incident.

Tests need a clear question and observable evidence. Reaching a contact demonstrates contactability; it does not demonstrate decision authority. Restoring a file demonstrates a technical capability; it does not demonstrate full service recovery.

The article is a conceptual proposal, not proof of a quantified improvement. Local validation should examine outcomes and unintended consequences, including the effect on people, physical operation and personal-data handling.

Learning is visible when a finding changes an arrangement and the change is verified. Repeating the same exercise without addressing prior findings may produce activity statistics but weak readiness evidence.

Reading bridge. GCSB-GDL-IRBC-001, Play 4, Train, exercise and test. These are reading prompts, not a complete instructor exercise programme.

The CSF lens: incident type is not severity

GCSB-ST-CSF-001 v2.0 integrates cybersecurity, physical security and operational technology security within one scoped risk approach. Its clause 4 separates hybrid, systemic and cascading descriptions from severity and regulatory reporting deadlines. Personnel, identity, suppliers and privacy cut across the three domains.

A single incident can cross several domains and propagate through several services. Coordination needs a shared account of the event, not an assumption that every team has the same authority or access to every record.

Main Standard clauses 6.6 and 6.11.5 connect unified response, decision authority, continuity and multi-domain recovery testing. GCSB-PRC-CSF-001 Step 7 translates those duties into protocols, escalation records, continuity plans and recovery test results.

GCSB-GDL-CSF-001 Plays 3-4 offer advisory ways to connect control implementation and continuing oversight. The article's unified architecture is a conceptual contribution; the issued standard and procedure, rather than this companion, determine adopted obligations.

Three classifications, three different questions

GCSB-ST-CSF-IRBC-001 clauses 4 and 6.1-6.2 distinguish incident type, severity and decision-making authority. Type asks how the event crosses or propagates between domains. Severity asks about impact and urgency. Authority asks who may decide and act.

GCSB-PRC-IRBC-001 Steps 3-4 connect classification to coordinated response, escalation triggers, reliable notification and continuity activation. An operational escalation does not replace a legal notification; the applicable reporting owner and legal facts remain necessary.

GCSB-GDL-IRBC-001 Play 1 supports discussion of categories and authority. Readers can challenge a report that says only 'hybrid incident' by asking what consequence is known, which command level is engaged and what uncertainties remain.

The exercise on logistics containment intentionally stops at decision questions. Nothing here authorises disconnecting a live system or deferring urgent safety action while governance bodies convene. Cross-domain intervention requires the adopter's lawful authority and safety-qualified arrangements.

Restoration integrity and the weakest dependency

A restore can succeed technically while the service remains unavailable. GCSB-ST-CSF-IRBC-001 clause 6.3 and GCSB-ST-CSF-RMA-001 clause 6.4 link business impact, dependencies, alternative arrangements and validated recovery.

GCSB-PRC-IRBC-001 Step 5 requires coordinated recovery planning, supply-chain continuity and cascade containment. Its RTO/RPO tier values are indicative starting references confirmed or adjusted by the adopter, not universal guarantees or new targets set by this companion.

Identity, physical access and monitoring can each be recovery dependencies. GCSB-ST-CSF-TIA-001 clause 6.7 covers authorised response, fallback and failure of shared services. Restoration should examine safe operation, trusted access and data integrity, not merely a green application screen.

GCSB-GDL-IRBC-001 Play 3 helps connect service requirements to continuity. A reader's evidence request might ask which service outcome was observed and which dependency remained untested. That is a critical-reading task, not a complete recovery runbook.

Exercises that produce usable learning evidence

GCSB-ST-CSF-IRBC-001 clauses 6.4 and 6.6 connect role competence, exercises, significant-incident review and continual improvement. A test is informative when its objective, observations, limitations and resulting changes are traceable.

GCSB-PRC-IRBC-001 Steps 7 and 9 identify exercise reports and post-incident analysis. GCSB-GDL-IRBC-001 Plays 4-5 discuss testing and maintaining evidence. These sources remain the operational references; the three short fictional prompts here are not a complete training programme.

An incompatible-plan test should challenge an assumption such as whether a supplier gateway remains available during containment. Attendance, a successful call and restored data are different observations and support different conclusions.

Improvement requires a justified link from finding to change and verification. A change in document wording may be necessary, but evidence of changed coordination or recovery must come from a suitable test. No quantified effectiveness benefit is inferred from the primary article's conceptual method.

Sample exercise 1: Containment versus safe operations

Fictional situation. A logistics control network is suspected of compromise. Cyber staff propose isolation; operations report that a loading-bay safety dependency uses the same segment.

Reflection prompts. Which facts and authorities must be clarified before a live intervention? How should uncertainty about the shared dependency be recorded?

Your output. A decision-question list, not a shutdown instruction or attack simulation.

Further reading. GCSB-GDL-IRBC-001, Plays 1 and 2. No worked response is provided.

Sample exercise 2: A technically successful restore

Fictional situation. A customer system restores successfully, but staff cannot reach the building and the identity service still fails. The report declares recovery complete.

Reflection prompts. What service outcome has and has not been demonstrated? Which dependency evidence is missing? How might a fallback introduce additional risks?

Your output. A brief challenge to the recovery claim, with explicit evidence limits.

Further reading. GCSB-GDL-IRBC-001, Play 3. No recovery target is invented.

Sample exercise 3: Two plans, incompatible assumptions

Fictional situation. The response plan isolates a supplier gateway during incidents. The continuity plan relies on that gateway for emergency dispatch. Neither team has reviewed the other’s assumption.

Reflection prompts. What question should a joint test answer? What observation would demonstrate a genuine coordination improvement rather than a completed meeting?

Your output. A test objective and evidence request; no complete exercise sequence.

Further reading. GCSB-GDL-IRBC-001, Play 4. No answer key is included.

Research bibliography and evidence

Primary article. Bunic, V. (2026). A UNIFIED CYBER-PHYSICAL INCIDENT RESPONSE AND BUSINESS CONTINUITY ARCHITECTURE FOR MANAGING HYBRID, SYSTEMIC, AND CASCADING RISKS ACROSS IT, OT, AND PHYSICAL SECURITY DOMAINS. International Journal of Science and Research Archive, 20(3), 032-043. https://doi.org/10.30574/ijsra.2026.20.3.1674

Article history. Received 17 July 2026; revised 30 August 2026; accepted 2 September 2026. Online publication: 30 September 2026 (Crossref published-online field; not DOI creation or deposit date).

Source identity. Vladimir Bunic; Converged Security Institute (CSI), Barcelona, Spain.. Publisher article | Original article PDF. Sources checked 11 November 2026.

Declared journal review policy. Read the publisher policy. Public policy describes the journal’s stated process, not an independent audit of the article’s confidential reports.

Scope of this companion. Conceptual architecture synthesis and standards/dependency mapping; proposed benefits require organisation-specific testing. No quantitative benefit, causal effect or universal compliance outcome is inferred.

Source rights. Publisher page and original PDF state CC BY 4.0. No original article text, figures or tables are reproduced. New companion commentary retains its separate reserved-rights notice.

Related primary families. IRBC, TIA, RMA, DPP. The following bibliography links the full issued framework; only the indicated families are central to this volume.

Reading crosswalk: explanations

Standards v2.0 set adopted requirements; procedures v1.0 set mandatory steps; playbooks v1.0 offer advisory methods. The following is an interpretive reading crosswalk, not an operational checklist or a new requirement.

One event, several operational consequences
GCSB-ST-CSF-IRBC-001 §6.1 | GCSB-PRC-IRBC-001 Step 3 | GCSB-GDL-IRBC-001 Play 1
Explain the common event while preserving domain roles.

Authority and evidence during containment
GCSB-ST-CSF-IRBC-001 §6.2 | GCSB-PRC-IRBC-001 Step 4 | GCSB-GDL-IRBC-001 Play 2
Examine containment authority and evidence before action.

Continuity is a service-level question
GCSB-ST-CSF-IRBC-001 §6.3 | GCSB-PRC-IRBC-001 Step 5 | GCSB-GDL-IRBC-001 Play 3
Distinguish technical restoration from service recovery.

Testing the connection between plans
GCSB-ST-CSF-IRBC-001 §6.4 and 6.6 | GCSB-PRC-IRBC-001 Step 7 and 9 | GCSB-GDL-IRBC-001 Play 4
Ask what a joint test actually demonstrates.

Reading crosswalk: sample exercises

Standards v2.0 set adopted requirements; procedures v1.0 set mandatory steps; playbooks v1.0 offer advisory methods. The following is an interpretive reading crosswalk, not an operational checklist or a new requirement.

Sample exercise 1: Containment versus safe operations
GCSB-ST-CSF-TIA-001 §6.7 | GCSB-PRC-TIA-001 Step 8 | GCSB-GDL-TIA-001 Play 4
Question shared-service safety and authorised fallback.

Sample exercise 2: A technically successful restore
GCSB-ST-CSF-IRBC-001 §6.3 | GCSB-PRC-IRBC-001 Step 5 | GCSB-GDL-IRBC-001 Play 3
Identify recovery assumptions not established by a restore.

Sample exercise 3: Two plans, incompatible assumptions
GCSB-ST-CSF-IRBC-001 §6.4 and 6.6 | GCSB-PRC-IRBC-001 Step 7 and 9 | GCSB-GDL-IRBC-001 Play 4
Frame a bounded test objective without an answer key.

Issued-source bibliography

Primary standards and CCSO Policy: v2.0, issued 13 October 2026. Mandatory procedures and advisory playbooks: v1.0, issued 19 October 2026. Verify the current controlled edition and applicable provisions before use.

GCSB-CSF-STRAT | Converged Security Framework: Strategic Standards for Unified Risk Management and Organisational Resilience
Read issued primary source | GCSB-PRC-STRAT-001 | GCSB-GDL-STRAT-001

GCSB-ST-CSF-001 | Converged Security Framework Main Standard
Read issued primary source | GCSB-PRC-CSF-001 | GCSB-GDL-CSF-001

GCSB-ST-CSF-TRA-001 | Training and Awareness
Read issued primary source | GCSB-PRC-TRA-001 | GCSB-GDL-TRA-001

GCSB-ST-CSF-GLA-001 | Governance and Leadership Framework
Read issued primary source | GCSB-PRC-GLA-001 | GCSB-GDL-GLA-001

GCSB-ST-CSF-TIA-001 | Technology Integration and Architecture
Read issued primary source | GCSB-PRC-TIA-001 | GCSB-GDL-TIA-001

Issued-source bibliography (continued)

Primary standards and CCSO Policy: v2.0, issued 13 October 2026. Mandatory procedures and advisory playbooks: v1.0, issued 19 October 2026. Verify the current controlled edition and applicable provisions before use.

GCSB-ST-CSF-IRBC-001 | Incident Response and Business Continuity Framework
Read issued primary source | GCSB-PRC-IRBC-001 | GCSB-GDL-IRBC-001

GCSB-ST-CSF-IAM-001 | Identity and Access Management Standard
Read issued primary source | GCSB-PRC-IAM-001 | GCSB-GDL-IAM-001

GCSB-ST-CSF-DPP-001 | Data Protection and Privacy Standard
Read issued primary source | GCSB-PRC-DPP-001 | GCSB-GDL-DPP-001

GCSB-ST-CSF-RMA-001 | Converged Security Risk Management and Assessment Standard
Read issued primary source | GCSB-PRC-RMA-001 | GCSB-GDL-RMA-001

GCSB-POL-CSF-CCSO-001 | Chief Converged Security Officer (CCSO) Policy
Read issued primary source | GCSB-PRC-CCSO-001 | GCSB-GDL-CCSO-001

RESEARCH COMPANIONS | PUBLIC SAMPLE

Converged Incident Response and Continuity

Shared Decisions, Safe Recovery and Evidence

From research ideas to better questions: eight explanatory readings, three fictional exercises and exact issued-source crosswalks. A separate educational companion, not a standard or peer-reviewed research article.

Prof. Dr. Vladimir Bunic
Global Converged Security Board
Owner and distributor | All rights reserved