CONVERGED SECURITY | RESEARCH COMPANIONS

PUBLIC SAMPLE EDITION

Governing Converged Infrastructure Risk

Dependencies, Decision Rights and Assurance

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Governing Converged Infrastructure Risk
Dependencies, Decision Rights and Assurance
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. Qualitative conceptual study using literature, documented incidents, thematic analysis and regulatory triangulation; not a controlled effectiveness trial.

Publication chronology. The primary article's registered online publication date is 29 June 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). Governing Converged Infrastructure Risk: Dependencies, Decision Rights and Assurance. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24129167

Contents

From isolated hazards to dependency pathways 4

Structural, operational and assurance layers 5

Regulatory context without checklist substitution 6

Assurance under uncertainty 7

The CSF lens: a scoped, accountable service 8

Ownership is more than a register entry 9

Decision rights, challenge and continuity of oversight 10

Evidence cadence without compliance theatre 11

Sample exercise 1: A shared dependency with no owner 12

Sample exercise 2: A green compliance report 13

Sample exercise 3: An action closed twice 14

Research bibliography and evidence 15

Reading crosswalk: explanations 16

Reading crosswalk: sample exercises 17

Issued-source bibliography 18

Issued-source bibliography (continued) 19

From isolated hazards to dependency pathways

A service can depend on assets owned by several teams. A transport operator may need electricity, signalling, communications, building access and trusted staff coordination at the same time. Reviewing each asset separately can miss the route by which a local failure becomes a service-level disruption.

The primary article identifies five convergence patterns: cyber-physical interdependencies, operational-cyber propagation, human-factor amplification, regulatory-risk misalignment and organisational fragmentation. These are analytical lenses, not mutually exclusive incident labels or a mandatory scoring scale.

A useful dependency discussion distinguishes the initiating event, enabling conditions, affected functions and consequences. Two systems on the same network are not automatically equally critical; their effect on service delivery and safe operation matters.

Original companion example: a station can retain functioning ticket servers while losing safe passenger flow because the door-control and public-address services share a failed local power supply. Asset availability and service continuity are different questions.

Reading bridge. GCSB-GDL-RMA-001, Play 2, Identify and register risks: describe cause, event and consequence with accountable ownership. This advisory practice helps express pathways without importing the playbook’s worked examples.

Structural, operational and assurance layers

The article proposes a hybrid governance model with structural, operational and assurance layers. Read the layers as complementary questions: who has authority; how work is coordinated; and how leaders know the arrangements operate as intended.

A structural decision names accountable owners and reserved decisions. Operational coordination makes escalation, handover and dependencies visible across teams. Assurance compares claimed arrangements with evidence from tests, incidents, exceptions and review.

A committee alone does not resolve accountability. A collective discussion still needs a person authorised to accept a risk or fund a treatment. Similarly, a named owner without access to resources or escalation routes can become an accountability label with little practical effect.

An evidence request should expose the link between a decision and its result. For example, an approved dependency treatment should be connected to an operating control and a review of what changed, not only to the approval minute.

Reading bridge. GCSB-GDL-RMA-001, Play 6, Integrate risk into decisions: connect significant business decisions to relevant risk evidence. The companion adds interpretation, not an additional compulsory governance layer.

Regulatory context without checklist substitution

The article considers NIS2, CER, GDPR, DORA and the Cyber Resilience Act as part of its EU governance discussion. They address different entities, activities, risks and legal instruments; they do not all apply automatically to every infrastructure operator.

An organisation should distinguish the relevant entity, activity, jurisdiction, implementation stage and responsible authority before translating a regulatory reference into an operational obligation. A shared incident may engage several regimes while retaining separate decision and notification routes.

Common evidence can support multiple purposes, but a single dashboard does not prove compliance with all regimes. A record suitable for security oversight may need different handling before being used for a personal-data decision or supplied to an authority.

For readers outside the EU, the analytical dependency model may still be useful. Its legal discussion should not be treated as a statement of local law. Qualified advice and current official texts govern legal applicability.

Reading bridge. GCSB-GDL-RMA-001, Play 1, Establish the risk method: clarify scales, appetite and authority before assessment. The research’s regulatory triangulation remains contextual analysis, not legal advice.

Assurance under uncertainty

Conceptual research can organise a difficult problem without demonstrating that the proposed arrangement works equally well in every sector. Readers should separate the plausibility of a governance design from evidence of its effectiveness in a particular organisation.

Ask what evidence would challenge the design: a handover that fails, an unresolved dependency, contradictory risk assessments, or a recurring incident after an action was marked closed. These observations are more informative than merely counting completed documents.

An assurance discussion should state its scope and uncertainty. A sample of one site may reveal a material weakness, but it cannot establish that every site is ready. Stronger conclusions require a justified sample and defensible test conditions.

A practical learning loop links observation, decision, action and verification. If the evidence changes, the risk explanation and decision may need to change too. This is disciplined revision, not a weakness to hide.

Reading bridge. GCSB-GDL-RMA-001, Play 5, Monitor, review and report: reviews should affect priorities and decisions. No performance percentage or new deadline is prescribed by this companion.

The CSF lens: a scoped, accountable service

The Converged Security Framework Main Standard, GCSB-ST-CSF-001 v2.0, integrates cybersecurity, physical security and operational technology security. Personnel, information, identity, suppliers and privacy are cross-cutting concerns, not extra domains that replace this three-domain structure.

Its clause 4 distinguishes hybrid threats crossing physical and digital vulnerabilities, systemic interconnections and cascading sequential failures. A dependency can support all three descriptions. None is automatically a severity tier, an incident command level or a legal reporting clock.

Read the research article's structural, operational and assurance layers as a way of questioning this scoped service. They are not additional CSF offices. Main Standard clauses 2.2-2.4 require documented organisational interfaces and legal applicability; clause 6.1 establishes executive accountability and cross-functional governance.

GCSB-PRC-CSF-001 Steps 1-2 connect adoption and scope to an accountable structure. GCSB-GDL-CSF-001 Play 1 offers advisory implementation ideas. A formal adoption record matters because reading the book or naming a committee does not confer recognition or establish implementation.

Ownership is more than a register entry

A dependency map explains how failure travels; a risk register explains what an authorised person will do about it. GCSB-ST-CSF-RMA-001 clauses 6.1-6.2 connect objectives, criteria, scenario, uncertainty, residual exposure and accountable ownership. A risk owner and an action owner may be different people.

GCSB-PRC-RMA-001 Steps 2 and 6 make that relationship observable through an entry, evaluation, treatment decision, resources, validation and residual-risk decision. An organisational chart alone cannot establish that the named person has the authority or resources to resolve the exposure.

A practical evidence chain links the service objective to a dependency, a treatment decision, an operating control and a verification result. The companion's transport example can be examined through that chain without choosing a score, accepting risk or prescribing a technical treatment.

GCSB-GDL-RMA-001 Plays 2 and 4 explain registration and treatment. Their methods are advisory; the parent requirements and mandatory procedure govern. Evidence of completed work should not be confused with evidence that the service dependency is controlled.

Decision rights, challenge and continuity of oversight

The research model gains practical meaning when authority is recorded. GCSB-ST-CSF-GLA-001 clauses 6.1-6.3 distinguish board oversight, CCSO authority and cross-functional coordination. Delegation should make clear which matters are reserved and what happens when a decision exceeds local authority.

Committee agreement is not automatically a risk acceptance. A minute should identify the decision, evidence considered, authorised decision-maker and follow-up. GCSB-GDL-GLA-001 Plays 2 and 4 help readers examine structure and oversight without adding another approval body.

Governance continuity also matters. Clause 6.9 addresses succession and continuity; a dependency on one unavailable executive can be a service risk. Clause 6.10 protects governance information, so assurance access remains purposeful and bounded rather than a blanket entitlement.

The useful challenge is whether the structure can make and review a contested cross-domain decision. A committee that exchanges updates but leaves a material exposure unresolved offers coordination activity, not demonstrated governance effectiveness.

Evidence cadence without compliance theatre

The Main Standard gives recurring oversight a defined basis: clause 6.8.3 requires monthly committee meetings; clauses 6.2.3 and 6.11.2 specify quarterly threat analysis and compliance reporting; clause 6.11.7 specifies semi-annual gap analysis. These are issued requirements, not new book recommendations.

GCSB-PRC-CSF-001 Step 10 identifies reporting records, metric definitions and tracked remediation. GCSB-GDL-CSF-001 Plays 4 and 6 discuss the operating rhythm and evidence-backed completion. The content of a review should change when the risk picture changes; redating an unchanged report is weak evidence.

GCSB-ST-CSF-RMA-001 clause 6.6 requires defined measurements rather than unexplained percentages. Ask which population, period, evidence source and exclusions support a green status, and whether the result actually supports the stated conclusion.

Clause 7 of the Main Standard distinguishes the 12-month suite baseline from the 18-month track limited to Governance, Technology and Training requirements. An extended domain track does not postpone the Main Standard's obligations. This book offers interpretation, not a substitute implementation calendar.

Sample exercise 1: A shared dependency with no owner

Fictional situation. A regional transport interchange has separate cyber, facilities and operations registers. Each team assumes another owns backup power for the shared communications room. A routine maintenance outage reveals that passenger communications and station access depend on the same supply.

Reflection prompts. Describe a credible cause-event-consequence pathway. Identify the decision that crosses departmental authority. What evidence would distinguish ownership, coordination and assurance?

Your output. A short dependency sketch and three unanswered governance questions. Do not assign a numeric score or invent a treatment deadline.

Further reading. GCSB-GDL-RMA-001, Play 2. No model answer is included.

Sample exercise 2: A green compliance report

Fictional situation. A board report marks five regulatory programmes green because their policy documents are signed. An operational review finds that the programmes use different incident classifications and incompatible reporting records.

Reflection prompts. What does the green status actually demonstrate? Which shared evidence might improve coordination without erasing different legal requirements? Which applicability questions require specialist advice?

Your output. Three questions for the handling executives and a statement of the report’s evidence limits.

Further reading. GCSB-GDL-RMA-001, Play 6. No legal conclusion or worked solution is supplied.

Sample exercise 3: An action closed twice

Fictional situation. Two successive reviews identify the same supplier handover failure. The action was closed after a new contact list was issued, but no handover was tested.

Reflection prompts. Separate completion of a document from effectiveness of the arrangement. What would a proportionate verification activity need to observe? What uncertainty would remain?

Your output. A one-paragraph assurance challenge and a list of evidence to request.

Further reading. GCSB-GDL-RMA-001, Play 5. No answer key or complete training scenario is included.

Research bibliography and evidence

Primary article. Bunic, V. (2026). Risk Convergence in Critical Infrastructure Governance in the European Union: A Qualitative Framework for Integrated Multi Domain Risk Oversight. International Journal of Public Administration, Management and Economic Development, 11(1), 34-46. https://doi.org/10.60026/ijpamed.v11i1.261

Article history. Published by the journal on 29 June 2026; received/revised/accepted dates are not supplied on the article page. Online publication: 29 June 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. Qualitative conceptual study using literature, documented incidents, thematic analysis and regulatory triangulation; not a controlled effectiveness trial. 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. RMA, GLA, STRAT. 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.

From isolated hazards to dependency pathways
GCSB-ST-CSF-RMA-001 §6.2 | GCSB-PRC-RMA-001 Step 2 | GCSB-GDL-RMA-001 Play 2
Trace a service dependency into an owned scenario, keeping uncertainty visible.

Structural, operational and assurance layers
GCSB-ST-CSF-GLA-001 §6.1-6.3 | GCSB-PRC-GLA-001 Step 2 | GCSB-GDL-GLA-001 Play 2
Distinguish board oversight, executive authority and coordination.

Regulatory context without checklist substitution
GCSB-ST-CSF-001 §2.4 and 6.3 | GCSB-PRC-CSF-001 Step 5 | GCSB-GDL-CSF-001 Play 3
Separate legal applicability from the reuse of common security evidence.

Assurance under uncertainty
GCSB-ST-CSF-RMA-001 §6.6 | GCSB-PRC-RMA-001 Step 7 | GCSB-GDL-RMA-001 Play 5
Test the basis of assurance claims and defined metrics.

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: A shared dependency with no owner
GCSB-ST-CSF-RMA-001 §6.1-6.2 | GCSB-PRC-RMA-001 Step 2 | GCSB-GDL-RMA-001 Play 2
Question missing ownership without assigning risk acceptance.

Sample exercise 2: A green compliance report
GCSB-ST-CSF-001 §6.11 | GCSB-PRC-CSF-001 Step 10 | GCSB-GDL-CSF-001 Play 4
Challenge a green report against its evidence and scope.

Sample exercise 3: An action closed twice
GCSB-ST-CSF-RMA-001 §6.5-6.6 | GCSB-PRC-RMA-001 Step 6-7 | GCSB-GDL-RMA-001 Play 4
Distinguish a completed action from a verified operating result.

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

Governing Converged Infrastructure Risk

Dependencies, Decision Rights and Assurance

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