CONVERGED SECURITY | COMPANION BOOKS

CSP | PUBLIC SAMPLE EDITION

Converged Security Professional

Enterprise Governance, Risk and Applied Practice

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Converged Security Professional
Enterprise Governance, Risk and Applied Practice
Public sample edition | First published edition, version 1.0
11 November 2026

Author: Prof. Dr. Vladimir Bunic

Global Converged Security Board
Owner and distributor

Overview. An enterprise exploration of governance, cross-organisational dependencies and readiness, with selected perspectives from issued GCSB playbooks.

A secondary practical/reference companion comprising four readings and three independent reflection exercises. Complete training sequences and worked solutions are not part of this publication.

Keywords. Converged Security; governance; enterprise risk; identity; business continuity; assurance.

Copyright and reader information

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

Except as permitted by applicable law, reproduction, redistribution, adaptation or transmission requires prior written permission from the copyright holder. Public availability does not grant an open reuse licence.

Owner and distributor: Global Converged Security Board.
Author: Prof. Dr. Vladimir Bunic.
Course delivery and training: Converged Security Institute (CSP).

Applicable law and adopted issued standards govern requirements; mandatory procedures implement parent provisions; playbooks are advisory. This educational publication is not a standard, formal assessment or Journal research article and confers no qualification or organisational conformity.

Exercises use fictional situations. Apply no live changes and disclose no personal or confidential workplace data. Operational decisions require appropriate authority, verified evidence and applicable legal and safety advice.

Playbook passages are selected paraphrases attributed by identifier, play title and edition. Referenced publications retain their own rights and status; references imply no endorsement. Cover imagery is AI-generated illustration.

Suggested citation. Bunic, V. (2026). Converged Security Professional: Enterprise Governance, Risk and Applied Practice. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24128340
Published 11 November 2026. No peer-review status is claimed.

Contents

A companion for enterprise judgement **4**

Governance across organisational boundaries **5**

Dependencies, privacy and identity **6**

Continuity, change and demonstrated capability **7**

Sample exercise 1: Shared service, separate authority **8**

Sample exercise 2: Shared identity disruption **9**

Sample exercise 3: A readiness claim **10**

Issued-source bibliography **11**

Issued-source bibliography (continued) **12**

A companion for enterprise judgement

Enterprise Converged Security brings governance, risk, privacy, identity, technology and continuity into coordinated decisions. Coordination is valuable because services cross organisational boundaries; it is limited because accountability and lawful authority remain with the responsible entities.

Beyond a combined dashboard. A shared view may help organisations coordinate, but it cannot grant one party unrestricted control of another's services, evidence or personal data. Agreements, delegated authority and actual processing roles still matter.

Published-playbook perspective. Give each document a distinct purpose, owner and review date. The published play recommends retiring or merging duplicate and contradictory documents so readers can find the current controlled source. GCSB-GDL-GLA-001, Play 3: Establish the policy hierarchy (v1.0).

Primary reading. Main GCSB-ST-CSF-001, Strategic GCSB-CSF-STRAT and Governance GCSB-ST-CSF-GLA-001; the CCSO policy addresses an adopter office, not an automatic personal credential.

Governance across organisational boundaries

A governance model connects decisions to accountable owners, delegated authority and reserved matters. A committee name or organisational chart alone does not show who may accept a material risk, approve a change or commit another party's resources.

Coordination versus control. A joint service can involve several legal entities and suppliers. Shared reporting does not transfer their statutory duties. Interface arrangements should make decision rights, information sharing and incident cooperation understandable within the actual agreements.

Assurance and ownership. The party operating a control and the party reviewing its evidence have different functions. Independence must be considered when assigning review responsibilities; a status report is not by itself an independent assurance decision.

Evidence-led reporting. Leadership needs material consequences, uncertainty, responsible owners and decisions, not only activity counts. Evidence should connect to the relevant requirement and be suitable for the decision being asked of the reader.

Published-playbook perspective. Leadership needs findings that can reach the governing body without being filtered by the control owner. The published play connects independent challenge, conflicts records and finding-closure evidence.
GCSB-GDL-GLA-001, Play 4: Operate oversight and assurance (v1.0).

Primary reading. GLA and GCSB-POL-CSF-CCSO-001; PRC-GLA/PRC-CCSO and advisory GDL-GLA/GDL-CCSO.

Dependencies, privacy and identity

Shared identity services, suppliers and monitoring platforms can create common failure points. Analyse how an event might propagate between services while separating a plausible dependency from a proven causal pathway.

Enterprise risk. Technical vulnerability information is one input. Treatment decisions also depend on affected objectives, safety, existing controls, uncertainty, ownership and delegated authority. A risk-sharing agreement does not erase residual exposure.

Processing-specific accountability. Data protection roles should be determined for each activity. Sharing incident evidence can involve personal data, contractual limits and different jurisdictions. Security usefulness does not establish permission to disclose everything.

Identity evidence. Account privileges, federation, lifecycle events and logs must be assessed together with purpose, retention and access. An authenticated identity and an approved right to perform a particular action are distinct.

Published-playbook perspective. Connect business cases, changes and supplier decisions to relevant register entries. The published play challenges token statements such as “no significant risks” and feeds incident learning back into the register. GCSB-GDL-RMA-001, Play 6: Integrate risk into decisions (v1.0).

Primary reading. RMA, DPP and IAM; matching procedures/playbooks. Include DPP 6.4-6.5 for technical safeguards and IAM 6.8 for privacy, retention, transfers and breach assessment involving identity evidence.

Continuity, change and demonstrated capability

A disruption can demand coordinated decisions from incident leaders, service owners, facilities specialists, privacy advisers and suppliers. Their responsibilities cannot be collapsed into a single technical restoration task.

Safe recovery. Availability, integrity, permissions and operational safety all influence whether a service is ready to return. Recovery objectives need business-impact and dependency evidence; indicative tiers do not override binding duties or the adopter's approved criteria.

Change and integration. Architecture and supplier decisions affect trust boundaries, interfaces and evidence. Vendor-neutral descriptions of required outcomes are more useful than assuming that a product label establishes conformity.

Competence. Attendance and knowledge are different from demonstrated task performance. Readiness depends on responsible owners, evidence of capability and suitable reassessment. A roadmap or training record alone cannot confer a qualification.

Published-playbook perspective. Use process-level business impact, dependencies and tested alternatives to evaluate continuity. The published play distinguishes an aspirational target from demonstrated restore and fallback capability.
GCSB-GDL-IRBC-001, Play 3: Establish business continuity (v1.0).

Primary reading. IRBC, TIA, TRA, Main and Strategic; their mandatory procedures and advisory playbooks. The complete sources govern adoption timing and acceptance requirements.

Sample exercise 1: Shared service, separate authority

Fictional scenario. Two organisations share a reception facility and a contracted security service. A proposed steering group would approve access changes for both. No documented delegation or agreement describing that power has been supplied.

Reflection prompts. What can a coordinating group discuss without claiming approval authority? Which decisions require each organisation's accountable owner? What information would establish the intended delegation and boundaries?

Your note. Write a short briefing identifying the unresolved authority questions. Do not invent contractual rights or appoint a decision-maker on the organisations' behalf.

Playbook reading. GCSB-GDL-GLA-001, Play 1: Map the current governance reality. Read the published play before responding.

Use fictional organisations and do not include confidential contracts or employer records.

Sample exercise 2: Shared identity disruption

Fictional scenario. A supplier-hosted identity service becomes unavailable. Several partner organisations report different operational effects. The supplier has confirmed an outage but has not identified a cause or recovery time.

Reflection prompts. Which dependencies need to be distinguished? What is known about service impact and what remains uncertain? Which parties own continuity decisions, and what limits apply to sharing identity evidence?

Your note. Prepare five questions for a joint situation discussion. Distinguish facts, service consequences, authority and information-sharing boundaries without constructing a full response playbook.

Playbook reading. GCSB-GDL-IRBC-001, Play 3: Establish business continuity. Read the published play before responding.

This exercise does not authorise live account changes or emergency access.

Sample exercise 3: A readiness claim

Fictional scenario. A programme reports that a security integration is ready because equipment is installed and staff attended an awareness session. No task-performance, service-acceptance or independent review evidence accompanies the report.

Reflection prompts. What does the report establish, and what does it not establish? Which source families address technology, competence and governance? Who must own any acceptance decision?

Your note. Draft a concise request for further evidence. Separate installation, participation, demonstrated capability and authorised acceptance without claiming that any single document proves readiness.

Playbook reading. GCSB-GDL-TRA-001, Play 1: Analyse training needs. Read the published play before responding.

Do not use an actual organisation's unpublished assurance findings for this exercise.

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

CSP | PUBLIC SAMPLE EDITION

Converged Security Professional

From decision rights to shared-service dependencies, this volume examines how organisations coordinate security without surrendering accountability.

Selected issued-playbook perspectives connect each reading to practical application. Three short exercises invite independent reflection; the bibliography provides direct access to the primary sources.

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