CONVERGED SECURITY | COMPANION BOOKS

CSCE | PUBLIC SAMPLE EDITION

Converged Security Cyber Expert

Foundations, Technologies and Applied Practice

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Converged Security Cyber Expert
Foundations, Technologies 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 introductory exploration of connected security systems, risk evidence, privacy and recovery, 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; physical security; cybersecurity; operational technology; risk; privacy.

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 (CSCE).

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 Cyber Expert: Foundations, Technologies and Applied Practice. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24128338
Published 11 November 2026. No peer-review status is claimed.

Contents

A companion to the issued framework 4

Connected systems, distinct responsibilities 5

Risk, uncertainty and evidence 6

Privacy, continuity and accountable recovery 7

Sample exercise 1: A changed access service 8

Sample exercise 2: An incomplete device report 9

Sample exercise 3: Visitor information 10

Issued-source bibliography 11

Issued-source bibliography (continued) 12

A companion to the issued framework

Converged Security examines how physical security, cybersecurity and operational technology affect the same services, people and assets. A digital identity failure can influence a building-access decision; an equipment change can affect monitoring, privacy and safe operation at the same time.

Scope and judgement. Identify the service, relevant entities, systems, people, data and interfaces before selecting controls. Record what is known and what is assumed. A dependency outside direct control does not create authority over another organisation.

Published-playbook perspective. Begin with how decisions are actually made, not only the organisational chart. The published play suggests collecting decision evidence and identifying gaps between formal and informal arrangements.
GCSB-GDL-GLA-001, Play 1: Map the current governance reality (v1.0).

Primary reading. Main Standard GCSB-ST-CSF-001; Strategic Standard GCSB-CSF-STRAT; Governance GCSB-ST-CSF-GLA-001. Matching procedures and advisory playbooks appear in the bibliography.

Connected systems, distinct responsibilities

A security installation is more than its visible equipment. Readers, cameras, controllers, management software, accounts, networks and maintenance arrangements create a chain of dependencies. The useful question is not only whether a device works, but which service depends on it and under whose authority it operates.

Interfaces matter. Management traffic, event reporting and media transport can use different paths and protections. Evidence that one path is protected does not establish protection for every other path. Product capabilities must be distinguished from actual configuration and verified operation.

Identity is not permission. Authentication establishes an identity claim; authorisation determines permitted actions. A valid account need not have unrestricted administrative rights. Access should be assessed by purpose, resource, privilege, duration and accountable approval.

Operational consequences. A change intended to improve security can affect emergency egress, temperature control or service availability. Technology decisions need competent safety and operational input as well as technical evidence.

Published-playbook perspective. Reconcile technology, procurement and facilities sources. The published play highlights connected physical-security systems that may be absent from IT inventories; record ownership, purpose and dependencies rather than treating the equipment list as the whole service.
GCSB-GDL-TIA-001, Play 1: Inventory and map the estate (v1.0).

Primary reading. Technology GCSB-ST-CSF-TIA-001 and Identity GCSB-ST-CSF-IAM-001; related TIA and IAM procedures/playbooks. See IAM 6.8 for privacy and information controls involving identity evidence.

Risk, uncertainty and evidence

A vulnerability describes a weakness; enterprise risk connects a defined scenario to organisational consequences and existing controls. A technical severity rating alone does not establish the likelihood or business impact of a particular service failure.

Describe the pathway. State how an initiating event could affect systems, people or services, including shared dependencies. Hybrid and systemic descriptions concern the pathway; severity concerns consequences and priority. A cascading consequence is not evidence of the initiating cause.

Keep uncertainty visible. Distinguish observations from hypotheses. Record the source and limits of evidence, the assumptions used and the accountable risk owner. A precise-looking score cannot repair unsupported inputs.

Methods and authority. The issued RMA standard calls for a documented method and approved criteria. The course's Likelihood × Impact × Convergence Factor calculation is a teaching model, not a universally mandated GCSB formula. This sample does not reproduce the course calculation set or assessment materials.

Published-playbook perspective. Describe cause, event and consequence instead of an undifferentiated label such as “cyber risk”. The published play combines asset, threat and scenario lenses and attaches an owner and review date to each entry. GCSB-GDL-RMA-001, Play 2: Identify and register risks (v1.0).

Primary reading. Risk GCSB-ST-CSF-RMA-001, especially 6.1-6.3 and 6.5; related PRC-RMA and GDL-RMA.

Privacy, continuity and accountable recovery

Logs and footage may support security while also recording personal data. Purpose, actual processing roles, lawful use, access and retention must be assessed for the activity in question. The presence of a security purpose does not remove privacy obligations.

Roles depend on processing. An organisation can have different roles for different activities. A supplier is not automatically a processor merely because it provides equipment; consider whether it processes personal data on another party's behalf.

Response is wider than restoration. Incident coordination includes operational safety, evidence, authorised decisions and continuity. Technical availability alone does not prove safe recovery or correct permissions.

Recovery objectives. Indicative recovery-time and recovery-point values in the issued framework must be confirmed against business impact, dependencies and binding obligations. They are not blanket targets for every service.

Published-playbook perspective. Map business processes and their information, including footage, visitor records and access logs. The published play connects the inventory to purpose, processing basis, retention and ownership rather than relying on a list of databases.
GCSB-GDL-DPP-001, Play 1: Discover and inventory data (v1.0).

Primary reading. Data Protection GCSB-ST-CSF-DPP-001 and Response/Continuity GCSB-ST-CSF-IRBC-001; matching procedures/playbooks. For technical privacy safeguards, also consult DPP 6.4-6.5.

Sample exercise 1: A changed access service

Fictional scenario. A small office replaces a local access-management application with a supplier-hosted service. Existing doors remain in use. Facilities, IT and reception each hold different information about the change. You have no verified details of emergency behaviour or account privileges.

Reflection prompts. What service and interfaces would you place within scope? Which facts are missing before judging whether the change is safe? Which responsibilities belong to the adopter and which require supplier agreement?

Your note. Write up to 200 words separating observations, assumptions and questions. Identify relevant primary-source families without attempting to certify compliance.

Playbook reading. GCSB-GDL-TIA-001, Play 1: Inventory and map the estate. Read the published play before responding.

Use only fictional information. Do not test live doors, accounts or emergency systems for this exercise.

Sample exercise 2: An incomplete device report

Fictional scenario. A report says that a building controller might be reachable from an external network. The report gives no verified route, permissions, operating context or evidence of exploitation. A manager asks whether the service should be disconnected immediately.

Reflection prompts. Which statements are observations and which are hypotheses? What business and safety context is needed to understand the consequence? Who has authority to approve an operational change?

Your note. List five questions you would ask before making a risk recommendation. Describe the limits of the supplied evidence; do not invent a numerical risk result.

Playbook reading. GCSB-GDL-RMA-001, Play 2: Identify and register risks. Read the published play before responding.

This is a reasoning exercise, not authorisation to scan, access or isolate an operational system.

Sample exercise 3: Visitor information

Fictional scenario. Reception records visitor names and hosts. A proposed dashboard would combine those records with door events. The request describes convenience but gives no defined purpose, retention period or access model.

Reflection prompts. What processing activity is being proposed? Which privacy and access questions must be resolved? What additional information is needed before deciding whether an impact assessment is required?

Your note. Prepare a short question list for the responsible owner. Separate legal-applicability questions from technical-capability questions and avoid assuming that every dataset linkage has the same legal answer.

Playbook reading. GCSB-GDL-DPP-001, Play 1: Discover and inventory data. Read the published play before responding.

Do not enter real visitor records, employee identities or confidential workplace information.

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

CSCE | PUBLIC SAMPLE EDITION

Converged Security Cyber Expert

From connected doors and devices to the evidence behind a risk decision, this volume introduces the foundations of Converged Security.

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