CONVERGED SECURITY | COMPANION BOOKS

CCSO | PUBLIC SAMPLE EDITION

Chief Converged Security Officer

Executive Mandate, Investment and Crisis Oversight

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Chief Converged Security Officer
Executive Mandate, Investment and Crisis Oversight
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 executive companion exploring the CCSO office's mandate, resourcing, independent reporting and contribution to strategic risk decisions and crisis leadership.

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; executive accountability; CCSO mandate; investment; independence; crisis governance.

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 (CCSO).

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. Cover imagery is AI-generated illustration.

Suggested citation. Bunic, V. (2026). Chief Converged Security Officer: Executive Mandate, Investment and Crisis Oversight. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24128653

Contents

A mandate beyond the title **4**

Resourcing and strategic investment **5**

Independent access and candid reporting **6**

Executive crisis leadership and learning **7**

Sample exercise 1: Appointment without capacity **8**

Sample exercise 2: A filtered risk report **9**

Sample exercise 3: An uncertain crisis briefing **10**

Issued-source bibliography **11**

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

A mandate beyond the title

The Chief Converged Security Officer is an executive governance role, not simply a renamed technical manager. Its practical effect depends on a defined scope across physical, cyber and operational technology security, documented authority and access to the appropriate executive and governing-body forums.

Source attribution. GCSB-CSF-STRAT provides the strategic context for unified risk management. The detailed CCSO role is defined in the issued CCSO Policy, supported by the Main Standard and Governance Standard. Cite the document that actually establishes a duty rather than attributing every duty to the strategic text.

Limits matter. Formal security authority does not remove statutory duties, privacy requirements, safety constraints or the accountabilities of other officers. Scope, lawful purpose and relevant consultation remain necessary when exercising a mandate.

Published-playbook perspective. Put the mandate in writing and align it with the governing body's appointment decision. The play distinguishes a genuine authority model from a title whose practical powers remain unchanged.
GCSB-GDL-CCSO-001, Play 1: Define and approve the mandate (v1.0).

Primary reading. GCSB-POL-CSF-CCSO-001; GCSB-ST-CSF-GLA-001; GCSB-ST-CSF-001. GCSB-PRC-CCSO-001 sets the mandatory office-establishment steps.

Resourcing and strategic investment

Accountability must be matched by the capacity to act. Time, staff, competence, budget and continuity arrangements determine whether the CCSO office can operate its mandate. Approving an appointment without addressing these factors may transfer blame without improving security.

Investment as a risk decision. A security proposal should connect the business objective, current exposure, treatment options and evidence of expected benefit. Product capability is not proof of operational value; value depends on adoption, trustworthy information and an accountable operating model.

Enterprise partnership. The CCSO contributes the cross-domain security view to enterprise risk management. Business executives retain ownership of their outcomes. Acquisitions and new services should be examined for inherited dependencies and unresolved risk without assuming the CCSO owns every enterprise risk.

Published-playbook perspective. Match appointment with explicit resourcing and a continuity arrangement, and record conflicts when roles are combined. Its fictional budgets and time allocations are illustrations, not universal requirements. GCSB-GDL-CCSO-001, Play 2: Appoint and resource the office (v1.0).

Primary reading. Issued CCSO Policy; GCSB-ST-CSF-GLA-001; GCSB-CSF-STRAT on strategic alignment and enterprise risk. Apply the corresponding mandatory procedures.

Independent access and candid reporting

Executive reporting should let the governing body understand exposure and make informed decisions. An attractive summary loses its value if inconvenient findings are removed before the people accountable for oversight receive them.

Information for the audience. Operational teams need detailed facts and tasks. Executives need trade-offs and resource decisions. The governing body needs risk relative to appetite, assurance and the consequences of decisions. Each view should reconcile to consistent underlying evidence.

Direct access is an operating safeguard. Record how concerns reach the governing body, including refused resources, serious incidents and disputed exceptions. A written reporting right may be ineffective if its use is informally blocked; independence must be examined in practice.

Published-playbook perspective. Establish reporting and direct-access arrangements in the mandate and standing orders, with escalation triggers understood in advance. The advisory play emphasises reports arriving as submitted rather than passing through a filter.
GCSB-GDL-CCSO-001, Play 3: Establish reporting and independence (v1.0).

Primary reading. Issued CCSO Policy and Governance Standard, together with GCSB-PRC-CCSO-001 and GCSB-PRC-GLA-001. Consult the actual issued provisions for reporting cadence and applicable escalation rules.

Executive crisis leadership and learning

A cross-domain crisis brings operational response, business continuity, safety, legal duties and stakeholder communication together. Executive leadership must support the authorised response and strategic decisions without creating competing command chains.

Separate roles. Incident command coordinates the operational response under approved arrangements. Executive leadership addresses resource trade-offs, business consequences, oversight and authorised communications. The CCSO's actual powers and escalation obligations follow the issued policy and adopted arrangements.

Facts and uncertainty. A briefing should distinguish confirmed facts, working assumptions and missing information, with sources and times. Legal and data-protection specialists assess applicable notification duties; a public example cannot establish which law, trigger or clock applies to a real event.

Published-playbook perspective. The office's day-to-day operating rhythm connects incident coordination, exceptions, risk reporting and training oversight. Written delegation limits help prevent every decision depending on one person. GCSB-GDL-CCSO-001, Play 4: Operate the office day to day (v1.0).

Primary reading. Issued CCSO Policy; GCSB-ST-CSF-IRBC-001; GCSB-ST-CSF-RMA-001; GCSB-ST-CSF-DPP-001. Use their mandatory procedures, with legal and safety input, for real decisions.

Sample exercise 1: Appointment without capacity

Fictional scenario. An engineering group names a CCSO in a board minute. The appointee retains a full operational workload; no budget line or deputy is recorded. A forthcoming automated-facility project requires cross-domain review, but the project sponsor assumes the appointment alone settles governance.

Reflection prompts. Which facts establish appointment and which establish capacity? What evidence would clarify authority, resourcing and continuity? Which decisions belong with the governing body rather than the appointee alone?

Your note. Write up to 200 words identifying missing evidence and questions for an executive discussion. Do not invent a required budget or authorise the project.

Playbook reading. GCSB-GDL-CCSO-001, Play 2: Appoint and resource the office (v1.0).

This is a reflection exercise, not an appointment decision or competence assessment.

Sample exercise 2: A filtered risk report

Fictional scenario. A CCSO report records an unresolved shared-service dependency affecting several sites. An executive asks for the finding to be removed before circulation because it may distract the board from approving expansion. The underlying technical facts have not been challenged.

Reflection prompts. What distinguishes factual correction from suppression? Which adopted documents should establish the reporting route? What evidence would let the governing body understand both the dependency and the expansion decision?

Your note. Write up to 200 words separating facts, decision needs and governance questions. Avoid claiming that every unresolved risk automatically blocks investment.

Playbook reading. GCSB-GDL-CCSO-001, Play 3: Establish reporting and independence (v1.0).

No model board report or full worked response is supplied.

Sample exercise 3: An uncertain crisis briefing

Fictional scenario. A science campus experiences access-service disruption and missing environmental telemetry. Operations reports a local fault; the security team suspects a shared identity issue. No cause is verified. The chief executive needs a briefing while the authorised incident team investigates.

Reflection prompts. Which facts are confirmed and which are hypotheses? What information belongs in an executive briefing rather than a tactical instruction? Which specialists should assess safety, continuity and possible notification duties?

Your note. Write up to 200 words outlining questions and information categories for the briefing. Do not classify the cause as proven, invent a legal deadline or direct live containment.

Playbook reading. GCSB-GDL-CCSO-001, Play 4: Operate the office day to day (v1.0).

Use fictional data only. No response sequence, inject schedule or solution is included.

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

CCSO | PUBLIC SAMPLE EDITION

Chief Converged Security Officer

From an appointment without resources to an uncertain crisis briefing, this volume examines how the CCSO office connects authority, evidence and executive 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