GLOBAL CONVERGED SECURITY BOARD

# External Auditor Bundle

Organisational Trustmark - independent evidence examination

Document ref: GCSB-OM-AUD-2026 | Version 1.0 - Board approved final document

Date: 5 November 2026 | Governing law: England and Wales

Intended for: Independent GCSB-Registered External Auditors

Classification: Party bundle - Auditor

© 2026 Global Converged Security Board. All rights reserved. Not for onward distribution beyond the intended party.

HOW TO USE THIS BUNDLE

# Purpose, parties and ground rules

The GCSB Organisational Trustmark is delivered through a set of party bundles. Each bundle contains only what one party needs: its responsibilities, its accountabilities and the templates it completes. All bundles share this opening section so every party works from the same routes, rules and vocabulary.

**This is the External Auditor Bundle.** It covers the independent examination of evidence in Route C: independence, the verification playbook, reporting and your recommendation to the Board.

| Bundle | Intended for | Availability |
|---|---|---|
| Client Organisation Bundle (GCSB-OM-CLI-2026) | Enterprise clients applying for the Trustmark | Issued on request and on application |
| Implementation Partner Bundle (GCSB-OM-IMP-2026) | GCSB Accredited Consultants and Accredited Partners | Issued on accreditation |
| External Auditor Bundle (GCSB-OM-AUD-2026) | Independent GCSB-Registered External Auditors (GCSB-EA) | Issued on appointment |

## What stays public

The award criteria, domains, tier thresholds, fees, validity, the three certification routes and the complaints and appeals procedure are published at gcsb.uk and apply equally to everyone. Nothing in any bundle changes them. How the Board internally moderates and decides is GCSB know-how and is not part of any party bundle.

## The three certification routes

| Route | Who implements | Who examines evidence | Who decides |
|---|---|---|---|
| A - Self-implementation | The Client itself, using the published standards, procedures, playbooks and self-assessment | GCSB Board certification review | GCSB Board |
| B - Two-party (current) | GCSB Accredited Consultant or Accredited Partner | GCSB Board certification review | GCSB Board |
| C - Three-party (target) | GCSB Accredited Consultant or Accredited Partner | Independent GCSB-Registered External Auditor (GCSB-EA) | GCSB Board |

**Separation rule.** GCSB never acts as implementation partner, in any route: a certification body may not build what it certifies (ISO/IEC 17065 and 17021-1 principle). Whoever examines evidence never implements for the same client. Consultants implement, auditors examine, the Board decides. Where no partner is available, the Client uses Route A and may obtain training from CSI or support from an existing GCSB Accredited Partner.

**Integrity safeguard.** No route changes, relaxes or shortcuts any criterion, domain weight, tier threshold, fee or validity rule. Clients move to Route C once an eligible, conflict-free GCSB-EA is available for their region, unless already in review.

## Framework references

All codes follow the currently published GCSB Converged Security Framework (CSF) suite at gcsb.uk/csf. Proposed revisions are not referenced until the Board publishes them. Standards and procedures are mandatory; playbooks are advisory.

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

| # | Standard (mandatory) | Procedure (mandatory steps) | Playbook (advisory) |
|---|---|---|---|
| 1 | GCSB-CSF-STRAT - Strategic Standard | GCSB-PRC-STRAT-001 | Strategic playbook |
| 2 | GCSB-ST-CSF-001 - Main Standard | GCSB-PRC-CSF-001 | Main implementation playbook |
| 3 | GCSB-ST-CSF-GLA-001 - Governance & Leadership | GCSB-PRC-GLA-001 | Governance playbook |
| 4 | GCSB-ST-CSF-RMA-001 - Risk Management & Assessment | GCSB-PRC-RMA-001 | Risk playbook |
| 5 | GCSB-ST-CSF-TIA-001 - Technology Integration & Architecture | GCSB-PRC-TIA-001 | Technology playbook |
| 6 | GCSB-ST-CSF-IAM-001 - Identity & Access Management | GCSB-PRC-IAM-001 | Identity playbook |
| 7 | GCSB-ST-CSF-DPP-001 - Data Protection & Privacy | GCSB-PRC-DPP-001 | Privacy playbook |
| 8 | GCSB-ST-CSF-IRBC-001 - Incident Response & Business Continuity | GCSB-PRC-IRBC-001 | Response playbook |
| 9 | GCSB-ST-CSF-TRA-001 - Training & Awareness | GCSB-PRC-TRA-001 | Training playbook |
| 10 | GCSB-POL-CSF-CCSO-001 - CCSO Policy | GCSB-PRC-CCSO-001 | CCSO office playbook |

## In this bundle

- Section 1 - Your responsibilities and accountabilities
- Section 2 - Independence and conduct
- Section 3 - Verification playbook
- Section 4 - Reporting and timelines

## Annexes (templates)

- A1 Assignment acceptance and independence declaration
- A2 Confidentiality undertaking
- A3 Review plan
- A4 Domain findings log
- A5 Evidence sample verification record
- A6 Findings letter
- A7 Evidence report and recommendation

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

SECTION 1

# Your responsibilities and accountabilities

- Examine and verify the Client's evidence against the published criteria and domains.
- Score each domain with evidence references and issue findings citing clause and gap.
- Send the Board a signed evidence report and recommendation. You recommend; you never award.
- Report only to the Board; never tell the Client the outcome first.
- Keep accreditation conditions, confidentiality and records for the review period.

## Who does what

| Activity | Client | Partner | Auditor | GCSB Board |
|---|---|---|---|---|
| Implement controls and procedures | Accountable | Responsible (Routes B/C) | Never | Never |
| Own evidence and operations | Accountable | Supports | - | - |
| Pay GCSB fees | Responsible | Never collects | - | Receives |
| Examine evidence | - | Never | Responsible (Route C) | Responsible (Routes A/B) |
| Recommend outcome | - | - | Responsible (Route C) | - |
| Decide award and tier | - | - | Never | Accountable |
| Public Register entry | - | - | - | Accountable |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

SECTION 2

# Independence and conduct

| Rule | Requirement |
|---|---|
| Independence window | No training, consulting, implementation or employment with the Client or its Partner for 36 months before and 24 months after the review. |
| Never implement | You may never act as implementation partner for a client you examine. |
| Declare | Complete Annex A1 before accepting; declare any new interest immediately. |
| Evidence only | Base findings only on evidence presented and verified, never on assurances. |
| No inducements | Accept no gifts, success fees or rewards linked to any outcome. |

**Breach.** An undeclared conflict voids the review and may lead to withdrawal of accreditation.

SECTION 3

# Verification playbook

| Concept | Definition | How it is checked |
|---|---|---|
| Data immutability | Evidence cannot be altered undetected | SHA-256 per file; recompute a sample |
| Log preservation | Logs kept with time sync for the review period | Retention settings, NTP source, unbroken sampled sequence |
| Code inheritance | Client documents reference parent GCSB code and edition | Trace table complete; no clause unmapped |
| Operating evidence | Controls run in practice | Dated records within the last 12 months |

## Evidence checklist

| Standard | A passing asset looks like |
|---|---|
| STRAT - Strategic | Board-approved converged security strategy with scope, objectives and dated review. |
| CSF-001 - Main | Single programme charter covering physical, cyber and operational security; scope boundary document. |
| GLA - Governance | Board minutes showing oversight; CCSO appointment; committee terms; KPI reports for two quarters. |
| RMA - Risk | One unified risk register (physical + cyber + OT) with owners, treatment plans and last annual assessment. |
| TIA - Technology | Architecture record showing SIEM/PSIM integration; interoperability tests; zero-trust roadmap status. |
| IAM - Identity | Joiner-mover-leaver records linking badge and system access; MFA coverage; privileged-access reviews. |
| DPP - Privacy | Data inventory, lawful bases, DPIAs for CCTV/biometrics, retention schedule, breach log. |
| IRBC - Response | Joint physical-cyber incident plan; continuity plan with RTO/RPO; exercise report from the last 12 months. |
| TRA - Training | Cross-functional training records, competency checks, tabletop sign-offs. |
| CCSO - Leadership | CCSO office terms, authority, reporting line, change-control log. |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

SECTION 4

# Reporting and timelines

- Receive the portfolio from the Client's GCSB account, never directly from the Partner.
- Verify hashes, completeness and the trace table; then score each domain against the published weights with evidence references.
- Hold a closing meeting with the Client covering findings only, not the recommendation.
- Send findings and the signed report (A7) to the Board within 15 business days of the closing meeting.

## Findings and remediation

| Stage | Trigger | Action | Time limit |
|---|---|---|---|
| 1 Finding | Evidence insufficient or missing | Written finding citing clause and gap | - |
| 2 Clarification | Client disagrees or needs detail | Client replies in writing; one clarification call | 10 business days |
| 3 Remediation | Finding accepted | Client (with Partner if engaged) submits new evidence | 15 business days; one extension of 15 on request |
| 4 Re-review | New evidence received | Affected domains only are re-scored | 10 business days |

The Board checks your report, may sample evidence again, and decides. Appeals are handled by people not involved in the review.

**Disclaimer.** This bundle is a template for information and planning. It is not legal, financial or regulatory advice; parties should take their own advice before signing any agreement. The GCSB Organisational Trustmark is awarded only by the Global Converged Security Board on evidence it has reviewed, under its published criteria; no Implementation Partner, consultant or auditor may promise, guarantee or sell an award. GCSB does not provide training, consulting or audit services. Where this bundle differs from gcsb.uk, gcsb.uk prevails. Governed by the laws of England and Wales. © 2026 Global Converged Security Board. All rights reserved.

ANNEXES

# Auditor templates

ANNEX A1

## Assignment acceptance and independence declaration

| | |
|---|---|
| **Auditor name and GCSB-EA number** | |
| **Client and application reference** | |
| **Partner (if any)** | |
| **Any tie with Client or Partner in past 36 months (must be none)** | |
| **Other interests** | |
| **Undertaking: no engagement for 24 months after** | |

| Name and position | Signature | Date |
|---|---|---|
| | | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

ANNEX A2

# Confidentiality undertaking

| | |
|---|---|
| **Assignment** | |
| **Information covered** | |
| **Storage and transfer method** | |
| **Retention and destruction date** | |
| **Undertaking: use only for this review** | |

| Name and position | Signature | Date |
|---|---|---|
| | | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

ANNEX A3

# Review plan

| | |
|---|---|
| **Scope as submitted** | |
| **Domains and sampling approach** | |
| **Interviews planned** | |
| **Remote or site walk-throughs** | |
| **Schedule** | |
| **Closing meeting date** | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

ANNEX A4

## Domain findings log

| Domain / standard | Evidence refs | Score | Finding (clause and gap) | Severity |
|---|---|---|---|---|
| STRAT - Strategic | | | | |
| CSF-001 - Main | | | | |
| GLA - Governance | | | | |
| RMA - Risk | | | | |
| TIA - Technology | | | | |
| IAM - Identity | | | | |
| DPP - Privacy | | | | |
| IRBC - Response | | | | |
| TRA - Training | | | | |
| CCSO - Leadership | | | | |

ANNEX A5

## Evidence sample verification record

| Doc ID | Stated hash | Recomputed hash | Match | Notes |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

ANNEX A6

# Findings letter

| | |
|---|---|
| **Application reference** | |
| **Findings (number, clause, gap)** | |
| **Evidence required** | |
| **Response deadline (10 business days)** | |
| **Remediation window (15 business days)** | |

| Name and position | Signature | Date |
|---|---|---|
| | | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.

ANNEX A7

# Evidence report and recommendation to the Board

| | |
|---|---|
| **Application reference** | |
| **Summary of scope and exclusions** | |
| **Domain scores with evidence references** | |
| **Open and closed findings** | |
| **Recommendation (award at tier / decline / further evidence)** | |
| **Statement: recommendation only; the Board decides** | |

| Name and position | Signature | Date |
|---|---|---|
| | | |

© 2026 Global Converged Security Board. All rights reserved. Party bundle - Auditor.