GLOBAL CONVERGED SECURITY BOARD

Client Organisation Bundle

Organisational Trustmark - responsibilities, evidence and templates

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

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

Intended for: Enterprise clients (applicants)

Classification: Party bundle - Client

© 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 Client Organisation Bundle. It explains how your organisation applies, what you are accountable for, what evidence the Board expects, what you pay and how findings and appeals work.

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 - Client.

#	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 - Applying, fees and payment
- Section 3 - Preparing evidence
- Section 4 - Review, findings, award and renewal

Annexes (templates)

- C1 Application readiness checklist
- C2 Scope statement
- C3 Evidence portfolio index
- C4 Declaration of interests
- C5 Self-implementation declaration (Route A)
- C6 Findings response form
- C7 Trustmark use undertaking

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

SECTION 1

Your responsibilities and accountabilities

The Client is always the applicant. Whatever route you use, your organisation owns its security programme, its evidence and its operations.

- Name an executive sponsor and a CCSO (or acting CCSO) before applying.
- Choose your route: implement yourself (Route A) or engage a GCSB Accredited Consultant or Partner (Routes B/C).
- Submit only evidence you can stand behind; you remain accountable for it even where a partner prepared it.
- Pay GCSB fees directly to GCSB by Stripe; partners never collect, discount or pass on GCSB fees.
- Communicate with GCSB through your own GCSB account so the record is complete and dated.
- Declare any relationship with GCSB reviewers, auditors or Board members.
- Never self-assign a tier or display the mark before award, or after expiry.

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

No guarantee. Neither GCSB nor any partner can guarantee an award, a tier or a date. The tier is set by the Board's score.

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

SECTION 2

Applying, fees and payment

Step	What you do	Result
1	Create and verify your GCSB account at gcsb.uk	Applicant account
2	Complete the self-assessment and Annex C1 readiness checklist	Readiness confirmed
3	Prepare scope statement (C2) and evidence portfolio (C3)	Submission pack
4	Pay the £1,300 application fee by Stripe	Payment verified
5	Submit through your account with declarations (C4, and C5 for Route A)	Application accepted for review

GCSB fees

Item	Fee (GBP)	Notes
Organisational Trustmark application fee	£1,300	Paid by Stripe before the application is accepted.
Award fee - Bronze (score 60-69)	£850	Payable on award.
Award fee - Silver (70-79)	£2,150	Payable on award.
Award fee - Gold (80-89)	£4,300	Payable on award.
Award fee - Platinum (90-100)	£6,900	Payable on award.
Validity	12 months	GCSB-OT certificate number and Public Register entry; renewal required.

Source: gcsb.uk Organisational Trustmark schedule, which prevails over any other figure. Any partner fees are a separate contract between you and the partner and never influence the tier.

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

SECTION 3

Preparing evidence

- Every asset must be dated, owned, hashed (SHA-256) and listed in the portfolio index (Annex C3).
- Each of your procedures references its parent GCSB code and edition, for example GCSB-PRC-IRBC-001 to your IRBC-01.
- Tailoring may add detail; it may not remove or weaken a mandatory step.
- Show operating evidence from the last 12 months, not only written policy. Screenshots alone are not sufficient where system exports exist.

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 - Client.

SECTION 4

Review, findings, award and renewal

After submission, your evidence is examined by the Board (Routes A/B) or by an independent GCSB-Registered External Auditor (Route C). The Board decides in every route. Incomplete submissions are returned within 10 business days with what is missing.

Findings and appeals

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
5 Appeal	Client disputes the decision	GCSB complaints and appeals procedure; reviewed by people not involved	Per gcsb.uk/legal/complaints

On award

- Pay the award fee for the tier awarded.
- Receive your GCSB-OT certificate number, certificate and Public Register entry.
- Display the mark only as set out in Annex C7, for 12 months.
- Start renewal evidence in month 11; an optional partner health check is your choice.

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

Client templates

ANNEX C1

Application readiness checklist

Executive sponsor named	
CCSO or acting CCSO named	
Route chosen (A / B / C)	
Partner name and accreditation no. (if any)	
Scope agreed internally	
Self-assessment completed (date)	
All 10 standards traced	
Operating evidence within 12 months	
Fees budgeted	

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

ANNEX C2

Scope statement

Legal entity name	
Registered address and country	
Sites in scope	
Systems and cloud environments in scope	
Approximate users	
Exclusions and reasons	
Interfaces with third parties	
Applicable regulations (e.g. NIS2, DORA)	
Primary contact	

Name and position	Signature	Date

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

ANNEX C3

Evidence portfolio index

Doc ID	Title	Parent GCSB code	Owner	Date	SHA-256 hash

Add rows as needed. Material changes after submission require a new index and declaration.

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

ANNEX C4

Declaration of interests

Any relationship with GCSB Board members or reviewers	
Any relationship with the assigned auditor (Route C)	
Any prior engagement of the auditor by the Client (36 months)	
Other matters the Board should know	

Name and position	Signature	Date

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

ANNEX C5

Self-implementation declaration (Route A)

Organisation	
Statement: we implemented the framework ourselves using published GCSB documents	
Internal reviewer of readiness	
Portfolio index reference and hash	
Remote walk-through availability	

Name and position	Signature	Date

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

ANNEX C6

Findings response form

Application reference	
Finding number and clause	
Response: accepted / clarification requested	
Clarification or corrective action	
New evidence references and hashes	
Target date	

Name and position	Signature	Date

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

ANNEX C7

Trustmark use undertaking

Certificate number (GCSB-OT-...)	
Tier awarded	
Valid to	
Undertaking: use the mark only for the scope awarded, only while valid, linking to the Public Register entry, without alteration	
Undertaking: withdraw the mark on expiry, suspension or withdrawal	

Name and position	Signature	Date

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