CYBER MANAGEMENT ALLIANCE

ASSURANCE, NOT AUDIT · NO PASS/FAIL · NO BLAME

Security Policy **Assurance Review**

Your policies, independently evidenced. A line-by-line assurance review of your security policy suite.

- A traceable view of policy strengths, gaps and contradictions
- Clear mapping to the standards and regulatory expectations that matter to you
- A priority-rated, remediation-ready tracker your teams can act on immediately
- A document-led review with almost zero demand on your people or systems

For security, risk, compliance and governance teams — and the executives, boards and committees accountable for policy oversight.

Prepared before · Effective during · Stronger after

PRACTITIONER-LED INDEPENDENT REVIEW

THE CHALLENGE

Policies are your evidence layer. Yet most suites have never been tested as a whole

When a regulator, auditor, insurer, customer or incident investigator asks how you manage cyber risk, your policies are the evidence you point to first. Yet policy suites often drift quietly out of date. Approval fields are blank. Review dates have passed. One document says "must" while another says "should". Roles, exceptions and cross-references no longer agree. Individually these issues can look minor; together they weaken confidence in the entire control environment.

The hardest gaps are usually invisible from inside the organisation. They sit between documents, in governance routes and in wording that no longer reflects current guidance or regulatory expectations. The Security Policy Assurance Review exposes those gaps **before a hostile reader does** — and gives your teams precise, practical wording-level fixes.

WHAT IT IS

Independent assurance, line by line

A Security Policy Assurance Review is an independent, structured evaluation of your information security and IT policy suite against recognised good practice, relevant regulatory expectations and, critically, against itself. The benchmark set is agreed at scoping and may include current NCSC guidance, ISO/IEC 27001:2022, Cyber Essentials, DORA, NIS2, FCA expectations, the NCSC Cyber Assessment Framework and UK data-protection requirements.

It is assurance, not audit. There is no pass/fail verdict and no blame. Strengths are formally credited alongside gaps, giving leaders a fair picture of what already works and what needs attention.
Every observation is anchored to an exact location in your document and, where applicable, to the relevant standard clause or regulatory requirement. Your teams can verify each finding and act on it without interpretation.

The result is a **living findings tracker** for your whole policy suite — priority-rated, remediation-ready and yours to maintain as gaps are closed.

HOW IT WORKS

You send documents. We return evidence.

1 **Scoping conversation**
We agree on the policies in scope, typically 5–15 documents, along with your sector, priorities and the benchmark frameworks that matter to you.

2 **Independent line-by-line review**
Our practitioners review every document against the agreed criteria and against the rest of the suite. They check terminology, governance, cross-references and control consistency.

3 **Findings evidenced and located**
Each observation includes an exact locator, a plain-English explanation, the relevant framework reference where applicable, a High/Medium/Low priority and practical remediation. Strengths are recorded with equal rigour.

4 **Living tracker delivered and walked through**
You receive one review sheet per policy, a summary dashboard and an Open/WIP/Closed/N/A status column. We walk your team through the output so nothing is left ambiguous.

5 **Re-review to evidence progress**
Once remediation is complete, a follow-up or annual review confirms closure and creates a clean, dated assurance trail for boards, auditors and regulators.

WHAT MAKES IT DIFFERENT

Traceable, balanced and almost zero disruption

Exact-location traceability
Every finding points to the relevant section, paragraph or page.

Framework mapped
Relevant observations connect directly to the standards, guidance and regulatory requirements that apply.

Suite-level assurance
Contradictions, broken cross-references and inconsistent governance routes are surfaced across documents.

Remediation focused and balanced
Practical wording-level fixes turn findings into a work plan, while strengths are formally evidenced and credited.

METHODOLOGY

Independent. Rigorous. Evidenced. Actionable.

WHAT YOU RECEIVE

A permanent, defensible policy assurance record

Each Security Policy Assurance Review delivers:

- A per-policy review sheet with every finding traceable to an exact document location
- Standard and regulatory mapping tailored to your organisation
- High/Medium/Low priority ratings so remediation can be sequenced sensibly
- Specific, actionable remediation for every gap
- Strengths formally credited alongside improvement opportunities
- Suite-level consistency findings across terminology, roles, responsibilities and controls
- A summary dashboard showing findings by policy and priority
- A living client-status tracker with Open/WIP/Closed/N/A fields
- A findings walkthrough and optional follow-up assurance review to evidence progress

Every finding is anchored to an **exact location in your document** — so remediation, board reporting and audit responses all point to the same defensible evidence.

Companion assessments

Policies describe intent; capability is a different question. The Technical Resilience Assessment and Operational Resilience Assessment can test whether the resilience your policies describe exists in practice.

SAMPLE OUTPUT

What the review looks like in practice

NEXT STEPS

Ready to put your policies **beyond question?**

A policy suite should do more than exist. It should be current, consistent, defensible and clear enough to guide real decisions.

The Security Policy Assurance Review replaces assumption with evidence. It shows exactly what stands up to scrutiny, where the gaps sit and what to fix first.

Book a scoping call

Request the full review outline

Speak to our policy assurance team

Independent review. Traceable findings. **A living remediation record.**

CYBER MANAGEMENT ALLIANCE

+44 (0) 203 189 1422
info@cm-alliance.com
71-75 Shelton Street, Covent Garden, London, WC2H 9JQ