

REVIEW AND ASSURANCE

What to prepare for a security programme review

Prepare the scope, people and evidence for a security programme review that leads to useful business decisions.

By Haroon Mahmood

A security programme review should leave you able to make decisions: what needs attention, what can wait, and where your team needs help. The preparation is about giving the reviewer a clear view of the business and the way security actually works.

Bring the imperfect inventory, the overdue actions and the procedure that everyone follows but nobody has written down. Each helps explain where you are starting. A polished document pack can wait.

In a previous in-house role, I established an organisation's first dedicated security function, including its risk register, policies, governance and control assurance approach. That work involved turning the findings of reviews and independent testing into actions that business and technology owners could deliver. It shapes the questions I ask: what matters here, how do you know it is protected, and who can act when it is not?

Start with the decision you need to make

Write down why you want the review now. "Understand our security posture" is a reasonable starting point, but it leaves a lot open. Be more specific:

- We are signing larger customers and need a credible improvement plan.
- Our IT team has inherited several systems and needs help deciding what to fix first.
- We have bought security tools but are unsure whether the important risks are covered.
- Leadership wants to know what additional capacity or investment is justified.

Agree who will receive the findings and who can approve action. Put the decision meeting in the diary before interviews begin. Otherwise, the review can finish just as the people needed to use it become unavailable.

Draw a boundary around the work

Name the business activities, systems, locations and suppliers included. Describe important exclusions and dependencies, especially where another company runs part of the service. For a hosted customer platform, this might include your application, identity provider, cloud configuration, support processes and recovery arrangements. A provider's own infrastructure might be outside your direct control, while your reliance on it remains relevant.

The NCSC's introductory risk guidance recommends defining the assessment boundary, its connections and external dependencies. That gives everyone a shared understanding of what the review can cover. [Read the NCSC's scoping guidance](#).

Agree the reference framework and the depth of review too. NIST CSF 2.0's Current and Target Profiles offer a way to describe the outcomes you achieve today and the outcomes you want to prioritise. The target should reflect your business, obligations and risks. [NIST's profile guide explains the approach](#).

Make clear whether the engagement includes interviews, document review, demonstrations or technical testing. A programme review does not automatically include penetration testing, certification or a detailed assessment of every system.

Gather a small, useful evidence pack

Start with existing material. The table below is a practical starting point; agree what is relevant with your reviewer.

Area	Useful material	What it helps establish
Business priorities	Critical services, important commitments, planned changes	Where disruption or information loss would matter most
Technology and data	System list, simple architecture diagram, significant data flows	What is being protected and where dependencies sit
Ownership and decisions	Named service owners, security responsibilities, committee decisions	Who runs controls and who can accept risk
Known concerns	Risk register, previous findings, incidents, open exceptions	What the business already knows and what remains unresolved
Control operation	Recent access reviews, patch records, recovery tests, monitoring examples	Whether important controls work in practice

Area	Useful material	What it helps establish
Policies and procedures	Current approved documents and the instructions teams use	Whether expectations are clear and workable
Suppliers and resources	Critical supplier list, assurance records, delivery plans and team capacity	Where responsibility and delivery depend on others

For each item, record its owner, date, scope and location. If an inventory is incomplete, say which areas are missing. If a test failed, include the failure and the follow-up. Those details help the reviewer judge confidence in the evidence.

An empty field is a useful question. Filling it with an assumption hides the question.

Show how work happens

Arrange short conversations with people who run the business as well as those responsible for security. Depending on scope, that may include IT, engineering, HR, procurement, finance and a service owner. Give them the review purpose and likely topics in advance.

Ask people to bring an example: a recent leaver, a supplier onboarding decision, a change to a critical system or a recovery test. Follow the work from the initial request to its completion. This reveals handovers, approvals and workarounds that a policy alone may not explain.

Illustrative example: a business has a procedure requiring access to be removed when someone leaves. A useful review follows a selection of recent departures from the HR notification through the identity platform to separately managed applications. It checks what happened, when, and how completion was confirmed. A closed service ticket is one part of that evidence.

Agree how samples will be selected. Include exceptions and different teams where they matter. A small sample can reveal weaknesses; it cannot establish that every transaction or system is sound. Record what was sampled, the period covered and any reason the result may not represent the wider business.

Share evidence with care

Agree an access-controlled workspace and named recipients before sending material. Prefer the minimum evidence needed to answer the question. A redacted record or supervised demonstration may be enough; passwords, secret keys and complete customer datasets usually are not needed for a programme review.

Set expectations for downloading, onward sharing, retention and deletion. Keep sensitive findings available only to those who need them. Where redaction removes important context, explain the limitation and agree another way to validate the point.

Also agree how a serious discovery will be escalated during the review. An indication of compromise or an urgent exposure needs an immediate conversation with the responsible people.

Agree what a useful report contains

Ask for findings that connect the evidence to a business consequence, explain uncertainty and identify the decision or action needed. Recommendations should acknowledge existing work, dependencies and delivery capacity.

The report should separate confirmed weaknesses from areas that could not be assessed. It should also state its scope, methods and limitations. Assurance needs refreshing as systems and circumstances change; the NCSC describes many assurance activities as a snapshot and recommends maintaining confidence throughout a service's life. [Read its guidance on maintaining assurance](#).

Leave time for factual corrections before the report is finalised, then agree who owns the next steps.

Your preparation note

Copy these prompts into a page and complete them with the sponsor:

- **Purpose:** The decision this review needs to support is...
- **Scope:** These services, systems and teams are included...
- **Boundaries:** These exclusions and dependencies matter...
- **People:** The sponsor, coordinator and control owners are...
- **Evidence:** Existing material is held here; these gaps are known...
- **Handling:** Access, retention and urgent escalation are agreed as follows...
- **Outcome:** We will review the findings and assign action on...

That is enough to begin a productive scoping conversation.

Kurosec's [security programme review](#) helps you understand your position and identify practical priorities. [Contact us](#) to discuss what you need the review to answer.

Further reading

- [NIST SP 1301: Creating and Using Organizational Profiles](#) - a structured approach to current and target outcomes.
- [NCSC: How to gain and maintain assurance](#) - confidence in controls over time.