

SUPPLIER ASSURANCE

Reviewing supplier security without drowning in questionnaires

Focus supplier assurance on business dependency, information and access, then turn evidence into a clear decision.

By Haroon Mahmood

A supplier review should help you decide whether to use a service, what needs to change before you do and what you will need to watch afterwards. A long questionnaire is useful only if its answers help with those decisions.

For a smaller business, review time is limited. Spend it where a supplier's mistake, compromise or outage could cause real harm. You can make a sensible start with a short supplier record, a few meaningful questions and someone accountable for the decision.

Understand the service before asking about controls

A supplier's name and annual spend tell you little about its security significance. A modest subscription might hold the records your business needs every morning. An expensive purchase might involve no access to your information or systems.

Create a record for the actual service. Name its business owner, describe what it does, identify the information it handles and record access to your systems or premises. Ask how the business would continue if the service became unavailable or its information could no longer be trusted.

The NCSC's supply-chain principles support this starting point: understand what needs protection, who supplies it and the risks created by that relationship. [NCSC: Understand the risks](#).

Use a small number of review levels

The following is a suggested starting model. Agree your thresholds with the people who own business risk, and record the reasoning behind each classification.

Review level	Typical exposure	Sensible starting approach
Limited	No sensitive information or access to business systems or restricted premises; disruption is manageable.	Confirm the service, access limits and owner. Record why deeper review is unnecessary.

Review level	Typical exposure	Sensible starting approach
Material	Business information or integrations are involved; a failure would disrupt a team or service.	Ask targeted questions, review relevant existing evidence and agree actions for significant gaps.
Critical	Privileged access, highly sensitive information, essential operations or a difficult-to-replace dependency.	Bring together the business owner, technical team and relevant commercial specialists for a deeper review of controls, recovery and contractual arrangements.

A supplier can move between levels as its use changes. A design tool used for public images has a different exposure when it starts holding unreleased product designs and connecting to shared company storage.

These levels are Kurosec's proposed working structure, not a prescribed classification. NCSC guidance also uses tiering examples and explicitly expects organisations to tailor them. [NCSC: Create key components for your approach](#).

Ask for evidence that resolves a question

Start with what the supplier already has: a relevant assurance report, security overview, independent testing summary or explanation from the team operating the service. Identify what those materials answer before sending another form.

Useful questions are tied to your intended use:

- **Access:** Who can reach our information, including supplier administrators, and how is access approved and removed?
- **Incidents:** How would you tell us about an incident affecting our service or information, and who would coordinate with us?
- **Recovery:** What recovery arrangements cover this service, and what recent evidence shows that they work?
- **Other providers:** Which subcontractors or hosting dependencies matter to our service, and how are changes communicated?
- **Exit:** How can we retrieve our information, remove integrations and close access when the relationship ends? What deletion or retention arrangements apply afterwards?

Follow up where an answer is vague. If availability is critical, a statement that backups exist leaves recovery unresolved. Ask for a suitable summary of the latest recovery exercise, what it covered and whether significant issues remain open. Request only the detail needed for the decision, with an appropriate way to handle confidential material.

Read certificates and reports carefully

ISO/IEC 27001 concerns an information security management system. A certificate is useful evidence, but check the named organisation, scope, validity and whether the service you intend to buy falls within it. [ISO: ISO/IEC 27001](#).

A SOC 2 report needs reading too. AICPA's illustrative Type 2 report includes the system description, auditor's report, control tests and their results. Review those sections for relevance to your service, the period covered and issues requiring follow-up; do not stop at the cover page. [AICPA: Illustrative SOC 2 report](#).

Ask what the supplier expects your organisation to configure or operate. For example, secure sign-in features provide little help if your own administrator leaves them disabled. Treat gaps in scope or evidence as questions to resolve, with their significance judged against the service's exposure.

An illustrative scenario: a new payroll service

This is an example of how the approach can work, not a report of a particular client engagement.

A growing business wants to move payroll to a new provider. The subscription is affordable, but the service will hold employee and bank details and support a time-sensitive business process. It therefore needs a deeper review than its purchase price might suggest.

The business owner and reviewer examine the supplier's assurance material, then focus on unanswered questions: administrator access, approval of bank-detail changes, incident contacts, recovery and data export. The review identifies that the customer must configure certain access restrictions itself, and the proposed export arrangements are unclear.

The decision could be to proceed once the access settings are checked and an export has been demonstrated. The record names who will complete each action, who will verify it and who authorises go-live. The business also agrees what it would do if payroll were unavailable at a critical point. Any unresolved material exposure goes to the person authorised to accept it.

Finish with a decision someone can act on

Use a short decision record:

Record	What to capture
Service and owner	Intended use, information, access and dependency.
Review level	Classification and the reason for it.
Evidence reviewed	Source, date, scope and important limitations.
Findings	The gap, its business consequence and proposed response.

Record	What to capture
Decision	Proceed, proceed subject to conditions, defer or decline; name the authorised decision-maker.
Conditions	Action, owner, due date and how completion will be checked.
Follow-up	Next review, change triggers, incident contact and exit arrangements.

Distinguish conditions that must be met before use from improvements permitted afterwards. Decide in advance what happens if an agreed deadline is missed. Work with your commercial or legal adviser to put agreed security commitments into the contract. Revisit the assessment when the service gains sensitive data, wider access, new dependencies or a more important operational role.

For critical services, consider concentration too: several suppliers may rely on the same underlying platform. NIST SP 800-161 integrates supply-chain security with broader organisational risk management, which is useful when individual reviews reveal a shared business dependency. [NIST SP 800-161 Rev. 1, Update 1](#).

Experience behind this approach

In a previous in-house role at a global technology organisation, I established and led the supplier-security programme, including its framework, risk-based assessment approach and delivery processes. I led supplier assessments and worked with Procurement, Legal and business owners to turn findings into decisions, contractual commitments and remediation.

Kurosec can apply that experience through a [security programme development engagement](#): define a proportionate review process, assess priority suppliers and make decisions easier to track. [Contact us](#) to discuss your supplier relationships.

Further reading

- [NCSC supply-chain principles: Understand the risks](#).
- [NCSC: Create key components for your assessment approach](#).
- [ISO's explanation of ISO/IEC 27001](#).
- [AICPA's illustrative SOC 2 report](#) - public overview; the full example requires member access.
- [NIST SP 800-161 Rev. 1, Update 1](#) - detailed supply-chain risk management guidance.