



# Security questionnaires and tenders: what buyers ask, and how to answer

Buyers ask about the same controls in different words. A supplier that keeps the record behind each answer, and states its gaps with a date, answers faster and is believed.



|                |                                          |
|----------------|------------------------------------------|
| Entity         | Black Shard Pty Ltd · ABN 66 696 910 773 |
| Document ID    | BS-RPT-05                                |
| Classification | Public                                   |
| Version        | 1.0                                      |
| Published      | 26 October 2026                          |
| Figures        | Tools read 26 Oct 2026                   |

## Executive summary

---

Our security questionnaire translator sorts each question into one of 56 control families. It flags 8 of the 56 as asking for an artefact that most small and mid-sized suppliers do not hold.

We group the 56 families into 10 themes, the way a tender response is usually organised. Infrastructure, devices and email: 11 control families, none of them scarce. Assurance and testing: 4 control families, 3 of them scarce.

Our cyber insurance readiness check asks 22 questions in 9 groups, grouped the way proposal and renewal forms group theirs.

Most questions are answered from records a well-run firm already keeps: a policy export, a backup restore record, a list of administrators, a certificate of currency. The questions that hurt are the few that ask for an artefact the supplier does not hold, and the answers that hurt most are the ones that imply it does.

- Keep one evidence pack with the record behind every common answer, and update it when a control changes.
- Answer each question with what is in place, the exceptions, and the date they close.
- For a scarce artefact, say plainly that you do not hold it, and offer the evidence you do.

## Method

---

Our security questionnaire translator reads a pasted questionnaire line by line and sorts each question into a control family from a fixed dictionary, most specific first. For each family it states what the question is reaching for, the record that answers it and a truthful partial answer, and it flags the families that ask for an artefact most small suppliers do not hold. It runs in the browser: nothing entered into it is sent to us.

We counted the families and the flags in the tool's source on 26 October 2026. We group the 56 families into 10 themes, the way a tender response is usually organised. The themes are ours; the families and the flags are the tool's.

Our cyber insurance readiness check asks 22 questions in 9 groups, grouped the way proposal and renewal forms group theirs. We counted its groups and questions from its source on the same day.

No customer data is in any figure. The counts describe the tools, never what anyone typed into them.

# What questionnaires ask about

## WHAT SECURITY QUESTIONNAIRES ASK ABOUT



56 control families in 10 themes; the cyan part of each bar is the families that ask for an artefact most small suppliers do not hold. Source: Our security questionnaire translator, read 26 October 2026.

Infrastructure, devices and email: 11 control families, none of them scarce. Governance, risk and people: 9 control families, 1 of them scarce. Data handling, privacy and AI: 7 control families, 1 of them scarce.

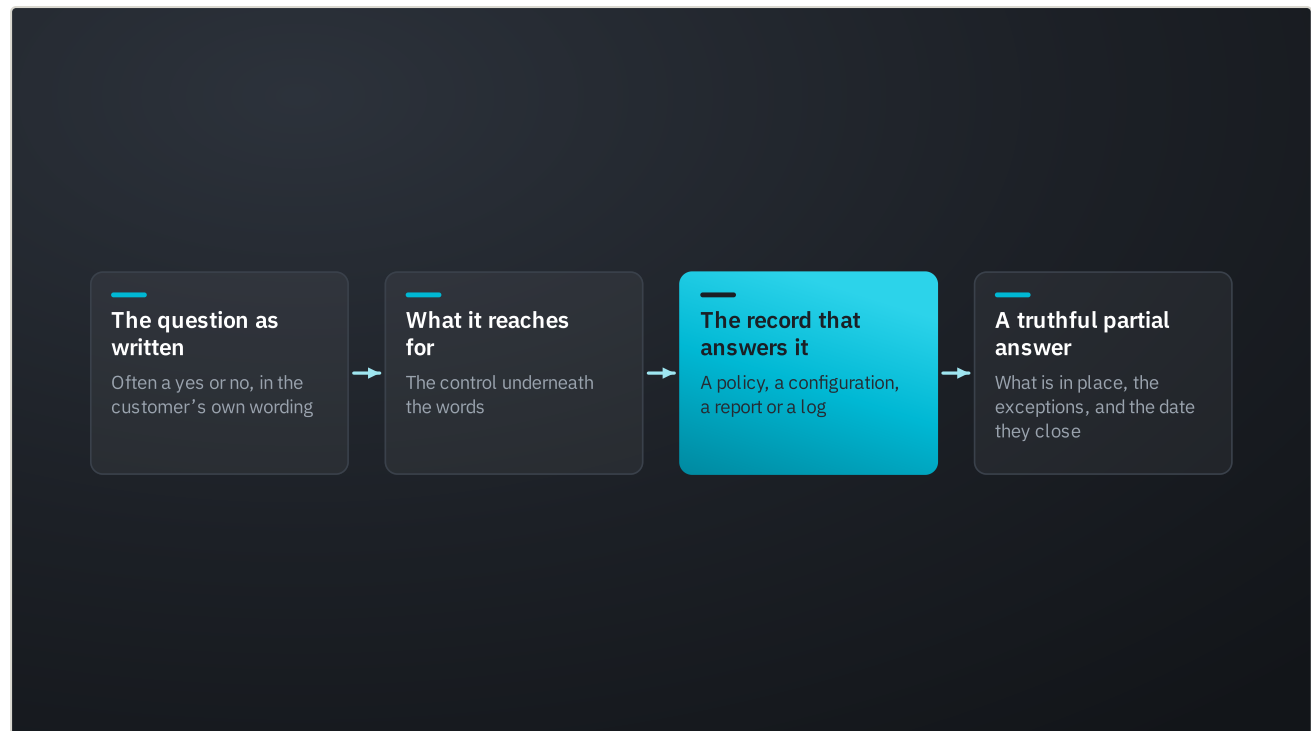
Secure development: 6 control families, 1 of them scarce. Identity and access: 5 control families, none of them scarce. Assurance and testing: 4 control families, 3 of them scarce.

Encryption and keys: 4 control families, 1 of them scarce. Monitoring and incident response: 4 control families, 1 of them scarce. Continuity and availability: 3 control families, none of them scarce. Suppliers and hosting: 3 control families, none of them scarce.

The breadth is the burden. A questionnaire of a few hundred lines touches most of the dictionary, and a supplier that answers each line from memory writes a different answer to the same question every time. The families repeat across buyers, so one set of records answers most of them.

# The answer pattern

## THE ANSWER PATTERN



Every family in the translator is answered the same way: name what the question reaches for, hand over the record, and state the gap with its date. Source: Our security questionnaire translator, read 26 October 2026.

Every family in the translator is answered the same way. Name what the question is reaching for under its wording. Hand over the record that shows it. Where the control is partly in place, say what is covered, what is not, and when the rest will be.

## Multi-factor authentication

The question asks whether a stolen password on its own gets someone in, including into administrator accounts and the services you sign into. The record is the enforcement policy, the systems it covers and every account excluded from it. An exception list stated up front reads better than a yes that has to be walked back later.

## Backup and restore

The question asks whether backups exist, how far back they reach and whether a restore has ever been done. The restore test carries the weight: give the date of the last one, and say plainly if backups have never been restored.

## Logging and monitoring

The question asks whether you could reconstruct what happened, and whether anything is watching in the meantime. Give the log sources, the retention period you can produce and who receives the alerts. A short retention stated honestly holds up better than an implied year you cannot show.

## Security incident response

The question asks whether there is a plan, whether anyone owns it, and whether it has been used or rehearsed. A short plan that names who decides and who calls the customer is a real plan. Say when it was last exercised,

including if it has not been yet.

## Data location and cross-border access

The question asks which country the data sits in and who outside Australia could reach it. Give the hosting regions first, then the access paths, including overseas support staff of the providers you use.

## Sub-processors

The question asks who else touches the buyer's data and how you assure them. List the infrastructure provider, the email and support tools and anything that processes customer content. The one left off the list is the one that surfaces later.

# The scarce artefacts

It flags 8 of the 56 as asking for an artefact that most small and mid-sized suppliers do not hold.

| THE FAMILY                                   | WHAT THE BUYER WANTS                                           | THE TRUTHFUL ANSWER                                                                                                              |
|----------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Certifications and independent attestations  | A current certificate or an attestation report, with its scope | Name what you hold, with its scope and dates. If you hold nothing, say so and offer the control descriptions and their evidence. |
| Audit rights and on-site assessment          | An unrestricted right to inspect you on site                   | Offer an annual questionnaire response with evidence supplied under confidentiality, and the clause you can support.             |
| Penetration testing                          | A dated report from an independent tester                      | Give the date, the scope and where the findings stand. A vulnerability scan is named as a scan.                                  |
| Third-party components and bill of materials | A generated software bill of materials                         | State the dependency scanning and alerting you run, and whether a bill of materials can be produced on request.                  |
| Cryptographic key management                 | Hardware-backed key custody                                    | Name the managed key service you use and its access controls.                                                                    |
| Continuous monitoring and out of hours cover | A staffed team watching every hour                             | Say what is watched, what wakes a person, and what waits until morning.                                                          |
| Data loss prevention                         | A licensed programme with tuned policies                       | Describe the sharing restrictions, forwarding rules and egress controls you actually run.                                        |
| Threat intelligence and threat modelling     | A funded intelligence function                                 | Name the advisories you follow and a threat model you have written.                                                              |

The pattern across the eight is the same: the buyer names the enterprise artefact, and a small supplier answers with the control it runs and the evidence for it. Buyers mark a missing artefact down. They mark an implied one down further, and remember it.

# What a cyber insurance proposal form asks

## WHAT A CYBER INSURANCE PROPOSAL FORM ASKS



22 questions in 9 groups; identity, backups, email and endpoints carry the most. Source: Our cyber insurance readiness check, read 26 October 2026.

Our cyber insurance readiness check asks 22 questions in 9 groups, grouped the way proposal and renewal forms group theirs. Identity and multi-factor coverage, backups and restoration, email filtering and impersonation, and endpoint protection and detection carry 3 questions each; remote access, privileged accounts, patching internet-facing systems, supplier access and incident response readiness carry 2 each.

The groups track how claims arise: a mailbox taken over, ransomware through remote access, a payment redirected by a forged email. Underwriters ask the same things a security questionnaire asks, in plainer words, and the answers on a proposal form become representations the policy relies on. An answer that overstates a control can cost the claim.

The groups with the most questions are the controls that decide the cost of an incident: whether multi-factor authentication covers every mailbox and service, whether backups survive an administrator compromise, whether payment changes are verified by phone, and whether endpoint alerts reach someone outside business hours.

## Tenders

Government and council tenders ask the same questions inside a larger response, with evidence attached and the answers scored. We bid into federal and state agencies. Tender responses built from our own records: certificates, insurance and the work we have delivered.

Pre-qualification removes a share of the work: a supplier already on an arrangement has answered the eligibility questions once. Ready for Queensland councils, NSW Government and Victorian Government buyers: Local Buy LB308, NSW SCM0020 and a Victorian Fair Jobs Code certificate.

What wins is the evidence pack behind the response: the certificate on its register, the assessment read from live systems, the insurance certificates, the incident response plan, and a referee who can speak to delivered work.

## What to do

1. Build an evidence pack: the security policy, the multi-factor enforcement export, the backup restore record, the administrator list, the incident response plan, the insurance certificates and any certificate or assessment you hold.
2. Write one master answer for each control family, from the pack, and reuse it in every questionnaire.
3. State each gap with the date it closes, and keep the dates.
4. For a scarce artefact, answer with the control you run and its evidence, and never imply the artefact.
5. Answer the insurance proposal form from the same pack, because the insurer will read it again after a claim.
6. Review the pack when a control changes, and at least once a year.
7. Run a questionnaire you have received through our translator before you answer it, to see which families it falls into and which ask for something you do not hold.

Our free tools run in the browser with nothing sent to us: the security questionnaire translator, the cyber insurance readiness check, the Essential Eight check and the penetration test scope builder.

## Our record

Black Shard builds and defends the systems Australian organisations run on. We answer security questionnaires and tenders from the same evidence pack we recommend, and it holds these records.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027, on the CyberCert register.
- Essential Eight Maturity Level 3, assessed September 2026.
- Pre-qualified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Our CISO is an Exemplar Global Certified Lead Auditor for ISO/IEC 27001:2022.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 1 January 2026.

24/7 incident line: 1800 370 270. The evidence behind each line goes out on request to [info@blackshard.com.au](mailto:info@blackshard.com.au).

## Sources

---

- Black Shard security questionnaire translator: <https://blackshard.com.au/tools/security-questionnaire-translator>
- Black Shard cyber insurance readiness check: <https://blackshard.com.au/tools/cyber-insurance-readiness-check>