

Example security review readout

Illustrative example for a fictional business. This is not a client report or a certification assessment.

A small professional services business wants to prioritise security improvements before taking on larger customer commitments.

Review scope: Document review and three conversations with the business sponsor, IT lead and operations lead, covering access, recovery and critical suppliers.

Leadership view: Confirm ownership of these controls and check the missing evidence before relying on them for new customer commitments.

Findings and proposed response

What the review found	What to do and how to check
01 Leaver access ownership is unclear First priority The procedure does not name who confirms access removal from separately managed applications. Why it matters: Access may remain after a departure; current access has not been verified.	Check recent leavers now; agree notification, removal and confirmation responsibilities. Proposed owner: IT lead with HR and application owners Completion check: Reconcile a sample of leavers against application access and record exceptions.
02 Recovery evidence is incomplete Next priority Backup records are available, but the supplied test record does not demonstrate restoration of the customer workspace. Why it matters: Recovery time and completeness remain uncertain.	Agree acceptable disruption and arrange a controlled restoration test. Proposed owner: IT lead with the service owner Completion check: Record scope, elapsed time, data checks and unresolved issues.
03 Critical suppliers need named owners Plan alongside recovery The supplier list has renewal dates but no accountable business owners or review triggers. Why it matters: Important dependencies and changes may receive no security follow-up.	Name owners and prioritise reviews by information, access and business dependency. Proposed owner: Operations lead with service owners Completion check: Check priority records for an owner, decision, actions and next review.

Illustrative plan for the next 90 days

By day 30: Check leaver exposure, assign owners and agree recovery needs.

By day 60: Test recovery and review the most important suppliers.

By day 90: Check completion evidence and revisit unresolved risk.

Illustrative sequencing only. Agree dates against exposure, dependencies and capacity; urgent issues need immediate action.

Decisions needed

Confirm the proposed owners and make delivery time available. Agree acceptable disruption and resources for the recovery test. Name the executive who can approve any remaining risk.

Limits of the example

Limited to supplied documents and conversations; no technical testing or comprehensive control validation. No remediation is claimed complete. Priorities and proposed roles need confirmation against the actual business.