



SECURITY & RESILIENCE

Cybersecurity essentials

for growing businesses

Review access, devices, recovery, suppliers and incident readiness. Establish who owns each control and verify that it works for the services your business depends on.

THE WORK

Trace one important business service through its accounts, devices, data and suppliers. Check the controls at those connections.

THE RESULT

A short, evidence-backed improvement plan with clear responsibility, recovery requirements and a decision on unresolved exposure.

INSIDE THIS GUIDE

02 Map the critical service

04 Reduce exposure

06 Prepare for disruption

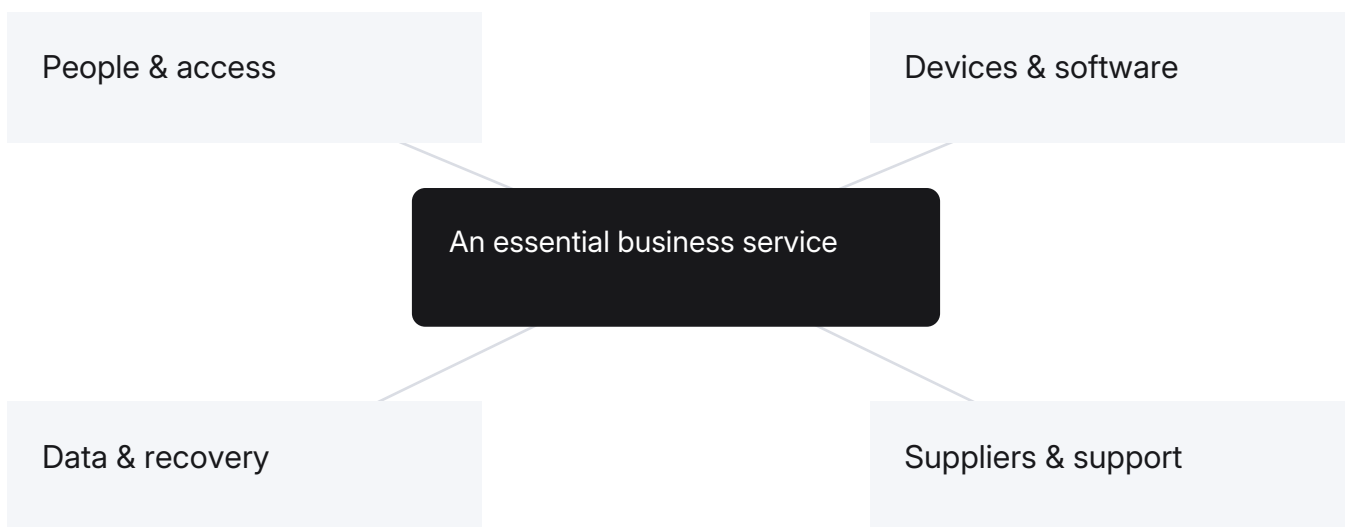
03 Control access

05 Prove recovery

07–08 Prioritise and record

Map service dependencies

A security review becomes manageable when it starts with a business service and follows the dependencies that make it work.



Choose a service, then trace it

Choose a service whose interruption would stop revenue, delivery or essential administration. Name the business owner and describe the outcome people need, such as accepting an order or accessing a scheduled appointment.

Walk through the service with someone who performs the work. Record the applications, administrator accounts, devices, integrations and external support it relies on. Include less visible dependencies: a shared mailbox, an API credential or the person who can recover an account.

Turn assumptions into checks

For each dependency, ask who owns it, who can change it, how failure becomes visible and how it can be recovered. Check the configuration or an operating record; a policy alone does not show that a control is active.

Keep the scope narrow enough to verify. Expand to another service after the first has an owner, a dependency list and a credible recovery route. Escalate any dependency that nobody can administer or restore.

02 / IDENTITY

Access management

An account should have a known owner, a necessary purpose and a reliable way to revoke its access.

01

Enforce strong sign-in

Require multifactor authentication for email, remote access, sensitive applications and administrative accounts. Prefer phishing-resistant methods where supported. Check enforcement on every sign-in route, including legacy clients and administrator recovery.

Completion check

Review the enforcement policy and sign in with a test account. Confirm an excluded route cannot bypass the requirement.

02

Separate administration

Give people ordinary accounts for daily work and named privileged access for administration. Remove unnecessary privileges and use time-limited elevation where the platform supports it. Store emergency access securely with a controlled recovery process.

Completion check

Identify who can grant administrator access, retrieve emergency credentials and see an alert when those credentials are used.

03

Close the leaving path

Treat departures and role changes as a connected task: disable identity access, revoke sessions, remove application accounts, transfer ownership and rotate shared secrets when required. Independent applications may survive central sign-out.

Completion check

Use the latest completed departure record to reconcile the identity directory with applications, devices and shared credentials.

04

Own non-human access

Give integrations and service accounts an owner and a stated purpose. Limit their permissions to the required operation. Record where credentials are stored, what depends on them and how rotation can be completed without an outage.

Completion check

Select an active integration and identify its permissions, last review, recovery contact and safe revocation route.

03 / DEVICES & SOFTWARE

Device and software protection

A software inventory is useful only when it connects an exposed asset to someone who can act.

Keep an actionable inventory

List the devices, cloud services and internet-facing applications used by the service. Record the owner, supported software version, management status and exposure. Include devices used remotely and systems administered by a supplier.

Reconcile the list with management consoles, cloud billing and sign-in records. Investigate unfamiliar assets and accounts. Remove a retired asset only after its access, data and dependent integrations have been addressed.

Limit the paths into the service

Review remote administration, public storage, open network services and default accounts. Disable what the service does not need. Protect administration behind controlled access and verify that public-facing changes match the intended design.

Prioritise updates by consequence

Set update urgency using active exploitation, external exposure, available privileges and the importance of the affected service. A severe issue on an exposed sign-in system needs a different response from a low-impact issue on an isolated test device.

Assign an owner to deploy and verify the update. When an update cannot proceed, document the reason, reduce exposure where possible and set a review date. A permanent exception without a compensating control is an unresolved risk.

Connect alerts to a response

Confirm that endpoint and service alerts reach a monitored destination. Name who reviews them and what happens when the primary contact is unavailable. Test the route with a safe platform-generated event; an unread alert does not provide protection.

Close the loop

A completed action needs evidence: the asset now reports the expected version, the exposed route is closed, or the alert reached a person who acknowledged it. Record the evidence with the task.

04 / RECOVERY

Test recovery

A successful backup job shows that a copy was created. Recovery is proven when the business can use the restored service.

01

Define

Name the service, recovery owner and acceptable interruption.

02

Restore

Recover into a controlled environment using the documented route.

03

Validate

Check data, access, configuration and connected services.

04

Operate

Complete a real business task and record the elapsed time.

Set the requirements together

Ask the business owner how long the service can be unavailable and how much recent work can be lost. Record these as recovery requirements, then compare them with what the test achieves. Desired recovery time is not measured recovery time.

Include application configuration, keys, access permissions and integration settings in the plan. Data alone may not rebuild an operational service. Check retention against accidental deletion as well as a broad system failure.

Protect the recovery route

Use recovery copies whose deletion or modification is restricted separately from everyday administration. Depending on the system, this may involve offline or immutable copies and separate credentials. Check that the people and credentials needed for recovery remain available during an identity outage.

Replication can reproduce corruption or deletion; it should not be assumed to provide a recoverable history. Test the actual restoration method and record any dependency that was missing or required undocumented knowledge.

A useful recovery result

Record what was restored, the recovery point, elapsed time, missing dependencies and the business task completed. Turn every failed step into an owned action and repeat the failed part after correction.

05 / SUPPLIERS & RESPONSE

Supplier and incident readiness

The first response should establish ownership, preserve useful information and keep decisions coordinated.

Clarify the supplier boundary

For each critical supplier, identify who manages access, updates, backups, monitoring and incident notification. Check the service agreement against the tasks your team assumes the supplier performs. Record any gap as an assigned responsibility.

Keep a usable support route and escalation contact outside the affected service. Verify who may authorise an urgent change and who can retrieve the account details needed to open a support request.

Coordinate before changing systems

The incident lead should confirm the scope, involve the relevant technical owner and decide immediate containment. Preserve logs and useful evidence before routine cleanup overwrites them. Record decisions, owners and times in one controlled incident record.

Give reports a clear destination

Publish a simple internal route for suspicious messages, missing devices, unexpected access and service disruption. Name the incident lead and a deputy. Provide an approved alternative if ordinary email or chat is unavailable.

The person reporting should record the time, affected system, observed behaviour and any action already taken. They should avoid investigating through an account or device that may be compromised.

Plan communication and recovery

Agree who communicates with staff, customers and suppliers and who reviews sensitive statements. Assess notification obligations with the appropriate legal or privacy owner for the situation. Restore service through the documented recovery process and confirm business operation before closing the incident.

Employee awareness

Ask staff to verify unusual requests, changed payment details and requests for credentials through a known, independent contact route. Do not use contact details supplied in the suspicious message. Make the reporting route easy to find and rehearse it with the team.

06 / PRIORITIES

Security priorities

Priorities should reflect the consequence of failure and the strength of the evidence, rather than the length of a checklist.

01

Address a live route to harm

Escalate suspected compromise through the incident process. Prioritise exposed administrative access, a known exploitable weakness on a critical service, or sensitive information available beyond its intended audience.

State the immediate containment action and who can approve it. Preserve necessary evidence while technical owners reduce the exposure.

02

Remove a single point of failure

Look for a service that only one person can administer, a recovery process that depends on unavailable credentials, or a backup that cannot be restored.

Assign a second authorised route or prove restoration. A written procedure is incomplete until another authorised person can follow it.

03

Convert gaps into accepted work

Write each improvement as an observable change. Include the affected service, owner, due date and evidence required for closure. Use a test, configuration record or demonstrated recovery instead of a vague statement such as "security improved".

04

Make exceptions expire

An accepted exception needs a business owner, reason, consequence, compensating action and review date. Revisit it when the service, supplier, threat or data use changes.

If the consequence cannot be understood or the control cannot be verified, keep the gap visible. Uncertainty should not be recorded as completion.

07 / ACTION RECORD

Security action record

Use one record for a specific gap. Describe the business consequence and the evidence that will demonstrate closure. Keep sensitive credentials and incident evidence in their controlled systems.

Service or dependency

Accountable owner

Observed gap and business consequence

Name what was checked, what failed and which work could be affected.

Agreed action and completion evidence

State the observable change and how a reviewer will verify it.

Delivery date

Reviewer

Exception or dependency requiring a decision

Record the approving owner, temporary protection and review date where an exception is needed.

Verification result

Verified on