90-day cybersecurity checklist

Assign a person to each task. Check it off when the verification passes.

Business or team _____ **Milestone date** _____ **Accountable lead** _____

Task **Owner role and name**

☐ **Expand phishing-resistant sign-in** **Identity owner** _____

Do. Extend passkey or security key requirements to more eligible accounts. Plan recovery before enforcing changes.

Verify. Check the policy against the account list and record any gaps. Test sign-in and approved recovery with a pilot account.

☐ **Verify network separation** **Network owner** _____

Do. Review guest, staff, admin and backup boundaries. Limit access between them to approved connections.

Verify. On a restricted test service, confirm guest access fails and an approved admin can connect.

☐ **Recover without a major dependency** **Recovery owner** _____

Do. In a test environment, rehearse losing a major dependency, such as your main sign-in provider or a critical supplier.

Verify. Have a business user complete a workflow with the fallback. Compare elapsed time and missing data against targets.

☐ **Resolve overdue security exceptions** **Business owner** _____

Do. Fix overdue exceptions or get an accountable leader to accept the remaining risk for a limited time.

Verify. Keep proof of the fix or a signed risk decision naming temporary safeguards, an owner and the expiry date.

☐ **Run an incident response exercise** **Incident lead** _____

Do. Walk through a ransomware or payment fraud scenario with IT, finance and a business owner.

Verify. Record who escalated and authorized containment. Note which decisions were timely and what the team missed.

☐ **Assign fixes and schedule retests** **Incident lead** _____

Do. Give each failed step an owner and due date. Schedule a retest of the failed steps.

Verify. Check the action log and retest date. Close each gap when the team demonstrates the fix works.

Gaps to close

Action, owner and due date

_____

_____