

Cybersecurity readiness

Six questions to turn uncertainty into a practical first step.

For business and IT leaders: review one business-critical service. For each question, mark Known, Partial, or Unknown and identify the evidence you can show.

01 / Who owns the risk?

Name the accountable business owner, the service, and the impact of a disruption. Evidence: an owner list and agreed recovery priorities.

02 / What needs protecting?

List the systems, sensitive data, vendors, and access paths the service depends on. Evidence: an inventory with owners and dependencies.

03 / Who can get in?

Review MFA coverage, privileged access, and joiner/leaver steps. Evidence: a recent access review and documented exceptions.

04 / What would you notice?

Confirm which identity, endpoint, and cloud events are collected and who reviews alerts. Evidence: a sample alert with a named responder.

05 / What happens during an incident?

Identify who makes decisions, who is contacted, and how work continues. Evidence: a response plan and a record of a tabletop discussion.

06 / Can you restore the service?

Check whether backups are protected and recovery has been tested. Evidence: a restore-test record and documented recovery gaps.

YOUR NEXT STEP

Choose one high-impact unknown. Assign an owner, request the evidence, and set a review date. Bring the results to a discovery conversation to define an assessment scope.

Priority gap: _____ Owner: _____ Review date: _____

Reference: NIST Cybersecurity Framework

Educational worksheet informed by the NIST CSF. It is not an audit, certification, or complete control assessment.