Who can get in?

Practical checks 1 to 5. Continue normal protection and recovery work alongside this review.

Business / critical service	Review owner / date

Each row: choose a result on the left; record evidence, the remaining question, or the N/A reason on the right.

01 / Know the routes in

List public services, cloud accounts, supplier portals, remote-support software, and cellular maintenance connections.

Evidence: Asset/service list reconciled with provider records and firewall/router configuration.

Not reviewed	

02 / Restrict equipment management

Identify which management interfaces need access and who should reach them. Agree a protected, restricted maintenance route.

Evidence: Approved connection diagram or rules, plus the equipment owner's sign-off.

Not reviewed	

03 / Verify support and updates

Check the running build and support status. Give exposed security flaws a prompt, owned remediation plan.

Evidence: Version/build evidence, applicable vendor guidance, and a verified update or temporary restriction.

Not reviewed	

04 / Name every access owner

Identify user, supplier, and service accounts. Remove unnecessary access through a controlled change; check dependencies first.

Evidence: Account inventory, approval, privilege scope, and a receipt for any revocation.

Not reviewed	

05 / Secure defaults and passwords

Change vendor default credentials, use unique passwords, and manage built-in accounts. Never write passwords on this sheet.

Evidence: Configuration review and the named owner of the protected credential store.

Not reviewed	

Who can get in?

Practical checks 6 to 10. Continue normal protection and recovery work alongside this review.

Use the same business service as page 1. Unknown answers need a named follow-up. Do not record passwords, keys, personal details, or raw logs.

Each row: choose a result on the left; record evidence, the remaining question, or the N/A reason on the right.

06 / Check the actual sign-in route

Verify multi-factor authentication for remote access, exposed applications, and administrators where supported. Check alternate routes too.

Evidence: Route-specific policy and an agreed sign-in test. Prefer phishing-resistant options where supported.

Not reviewed	

07 / Keep everyday protections running

Keep operating systems, applications, and endpoint protection supported and updated during this review.

Evidence: Representative update/protection status and a named person handling exceptions.

Not reviewed	

08 / Make suspicious messages reportable

Use supported email/browser software. Show staff how to report suspicious messages and requests without approving them.

Evidence: Supported-client record, reporting route, and a harmless reporting exercise.

Not reviewed	

09 / Keep the evidence and assign alerts

Verify important sign-in/admin records are collected. Name who receives alerts, responds, and covers absence.

Evidence: An agreed test record and alert received by its owner; documented coverage or gaps.

Not reviewed	

10 / Prove a route back to work

Protect a recovery copy, its access, and dependencies. Rehearse one critical service safely and record the result.

Evidence: Completed recovery worksheet with elapsed time, usable-data age, and open actions.

Not reviewed	

Trace one route. Close one gap.

Start with existing records. Agree any test or change with the service and equipment owners.

Account / access route

Who needs it and for what work?

Systems / permissions it can reach

Approval / expiry / dependency reference

Restriction or removal to agree

Change owner / safe window

OWN THE NEXT ACTION

Action and expected result

Action owner / due date

Next review / trigger for earlier review

Verification method, evidence, and result

Known suspicious access needs evidence preservation and the incident process. Do not scan or change live equipment without authorization. Confirm dependencies before removing an unexplained account or connection.

SOURCE POINTERS / RELATED GUIDANCE

CIS Controls v8.1: 1.1, 2.1/2.2, 4.2/4.6/4.7, 5.1/5.2, 6.1-6.5, 7.3/7.4, 8.1-8.3, 9.1, 10.1, 11.1-11.5, 14.2/14.6, 17.1. References support parts of these prompts; completing this sheet does not establish compliance. Recovery foundations 11.1-11.4 are IG1; sampled testing 11.5 is IG2/3. NIST SP 1300 and CSF 2.0 support concurrent protection, detection, response, and recovery.

CIS safeguard details: cisecurity.org/controls/cis-controls-navigator

NIST small-business guide: csrc.nist.gov/pubs/sp/1300/final