

Business IT health checklist

01 / Accounts and access

Start with people and access: who can sign in, who owns each account and who approves changes.

Company: _____ Reviewed by: _____ Date: _____

Tick one status per item. Confirmed requires evidence. Use unknown if you have not checked.

01. Important accounts have MFA enabled

Check business email, administrator accounts and remote access. Confirm the settings and registered methods rather than assuming MFA is enabled.

Next step: Plan MFA rollout with IT support, a small pilot group and an account recovery procedure.

HIGH PRIORITY

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

02. Each employee has an individual business account

Compare employee and active account lists. Check whether people share a password for email or a business application.

Next step: Separate user accounts and grant access to shared resources through approved groups or delegation.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

03. Former employees' access has been reviewed and revoked

Review email, VPN, cloud applications, shared folders and active sessions. Record who approved business data handover.

Next step: Have an authorised administrator block unneeded access and preserve data according to company decisions before deleting accounts.

HIGH PRIORITY

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

04. Administrator access is separate from everyday work

Check who has administrator rights on computers and business systems, and whether their role requires those rights.

Next step: Agree on separate administrator accounts and reduced privileges, with business application testing.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

05. The company controls its domain, licences and account recovery

Record the domain owner, subscription administrator and authorised recovery contact. Check renewal dates and secure access storage.

Next step: Clarify ownership and permissions. Keep passwords, backup codes and keys in a protected system outside this checklist.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

Notes / evidence / responsible person:

A starting point for a review, not a security certification. Do not record passwords, keys or confidential data.

Business IT health checklist

02 / Backup and recovery

A completed backup message does not prove the business can resume work. Look for evidence of the latest copy and a restore test.

Company: _____ Reviewed by: _____ Date: _____

Tick one status per item. Confirmed requires evidence. Use unknown if you have not checked.

06. Backup covers the data the business needs to operate
List business documents, databases, NAS/server and cloud data. For each group, identify the backup system and responsible person.
Next step: Close backup coverage gaps. Do not treat file synchronisation or RAID as a replacement for a separate backup.

☐ Confirmed

☐ Needs action

☐ Unknown

☐ N/A

HIGH PRIORITY

07. The latest successful backup and failures have been checked
Review the date, scope and report of the latest successful job. Check who receives an alert when a backup fails.
Next step: Assign someone to monitor failures and check that the backup schedule matches acceptable data loss.

☐ Confirmed

☐ Needs action

☐ Unknown

☐ N/A

HIGH PRIORITY

08. A trial restore has been successfully verified
Look for a test date, selected data, results and confirmation that the recovered file or application opens. Record recovery time only if measured.
Next step: Arrange a controlled test in a separate location or test environment without overwriting production data.

☐ Confirmed

☐ Needs action

☐ Unknown

☐ N/A

HIGH PRIORITY

09. A backup copy is protected from problems in the primary system
Check whether a failure, fire or compromised user account could destroy both originals and all copies. Review a separate location and an offline or immutable copy.
Next step: Agree with IT support on a suitable separate copy, access protection and a way to test its recovery.

☐ Confirmed

☐ Needs action

☐ Unknown

☐ N/A

HIGH PRIORITY

10. The business has agreed acceptable downtime and data loss
For critical processes, record acceptable outage duration and loss of recent data. Identify who authorises recovery.
Next step: Align backup and recovery procedures with those objectives. Record the gap between the target and tested result.

☐ Confirmed

☐ Needs action

☐ Unknown

☐ N/A

ROUTINE

Notes / evidence / responsible person:

A starting point for a review, not a security certification. Do not record passwords, keys or confidential data.

Business IT health checklist

03 / Computers and software

An inventory and regular checks help plan equipment replacement and updates before work is interrupted.

Company: _____ Reviewed by: _____ Date: _____

Tick one status per item. Confirmed requires evidence. Use unknown if you have not checked.

11. There is an up-to-date computer and equipment inventory

For each device, record the user, role, purchase year, warranty and recurring problems. Include servers, NAS and network equipment.

Next step: Assign someone to update the inventory when equipment is purchased, assigned, repaired or retired.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

12. Systems and applications are supported and have an update plan

Check versions, vendor support status and recent updates. Record devices that need a specific migration plan.

Next step: Plan supported versions and updates, with backups and critical application testing. Document exceptions.

HIGH PRIORITY

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

13. Device protection is active and alerts are reviewed

Review protection status, updates and recent alerts. For portable computers, also check disk encryption and authorised access to recovery keys.

Next step: Resolve inactive protection and assign responsibility for alerts. Store recovery keys securely outside the checklist.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

14. Licences and business subscriptions are documented

Compare active users, assigned licences, installed software and renewal dates. Check that purchases are recorded for the company.

Next step: Remove unnecessary costs and plan renewals or plan changes based on actual use.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

15. There is a plan for failure of a critical computer or application

Record who relies on each critical device, available replacements and access to business data. Identify recurring problems.

Next step: Plan spares or replacements based on business impact and downtime cost, supported by an annual IT budget.

ROUTINE

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

Notes / evidence / responsible person:

A starting point for a review, not a security certification. Do not record passwords, keys or confidential data.

Business IT health checklist

04 / Network and support organisation

Check real working conditions: connection stability, separated access and a clear way to report problems.

Company: _____ Reviewed by: _____ Date: _____

Tick one status per item. Confirmed requires evidence. Use unknown if you have not checked.

16. Internet and WiFi have been checked at workstations

Record where and when interruptions occur and their symptoms. Test business applications and video calls; one speed test does not establish stability.

Next step: Have IT support check the connection, coverage and network equipment, comparing results under the same conditions.

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

ROUTINE

17. Guest access is separated from business resources

Check whether a guest device can reach internal folders, servers, NAS or network management. A different WiFi name alone does not prove isolation.

Next step: Agree on isolation and access rules, then verify that approved business functions still work.

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

ROUTINE

18. Remote access and network equipment have controlled access

With the administrator, review authorised users, remote access methods, updates and exposed services. Do not enter public IP addresses or passwords in this checklist.

Next step: Limit access to business needs and arrange protection and updates in an agreed maintenance window.

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

HIGH PRIORITY

19. There is a contact and procedure for a critical service outage

Record IT support and internet provider contacts, working hours and escalation arrangements. Review UPS and power outage plans where needed.

Next step: Agree on the call sequence and temporary working arrangements. Leave UPS or shutdown testing to the responsible person.

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

ROUTINE

20. Open issues have an owner, due date and follow-up check

Review recent tickets, recurring failures and the three main risks. For each open issue, record an owner and the agreed next step.

Next step: Include checks in regular maintenance and repeat this checklist after significant business changes.

☐ Confirmed ☐ Needs action ☐ Unknown ☐ N/A

ROUTINE

Next action / owner / due date / verification:

A starting point for a review, not a security certification. Do not record passwords, keys or confidential data.