

IT Audit and Health Check

On-site IT audit for a small or mid-sized organisation: network, servers and cloud, devices, backup, accounts and security, with rated findings.

1. Details

Who the work is for and what it covers.

Project

Filled in from the project in SiteSurvey.

Customer

Site *

Site address

Date of audit *

Auditor

What does the audit cover? (tick all that apply)

- ☐ Network and internet
- ☐ Servers and storage
- ☐ PCs, laptops and mobiles
- ☐ Cloud services and email
- ☐ Backup and recovery
- ☐ Accounts and security
- ☐ Comms room and cabling

Number of staff who use IT

Number of sites

Who looks after IT now? (choose one)

- ☐ In-house ☐ An outside IT company ☐ A mix ☐ Nobody in particular

What does the customer say is not working?

2. Network and internet

How the site connects, and what protects it.

Internet connection (choose one)

- ☐ Full fibre
- ☐ Fibre to the cabinet
- ☐ Leased line
- ☐ Mobile (4G or 5G)
- ☐ Satellite
- ☐ Other: _____

Download (Mbps)

Upload (Mbps)

Is there a second connection if the main one fails?

- ☐ Yes ☐ No

Firewall or router make and model

Does it still get security updates from the maker? (choose one)

- ☐ Yes ☐ No ☐ Not known

If applicable: Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported. A firewall that no longer gets updates should be replaced.

Switches (choose one)

- ☐ Managed ☐ Unmanaged ☐ Mixed ☐ Not known

Is guest Wi-Fi kept separate from the main network? (choose one)

- ☐ Yes ☐ No ☐ No guest Wi-Fi

Is there an up to date network diagram?

- ☐ Yes ☐ No

How do staff connect from outside? (choose one)

- ☐ VPN
- ☐ Cloud services only
- ☐ Remote desktop open to the internet
- ☐ No remote access

If applicable: Remote desktop open to the internet is a common way in for attackers. Recommend a VPN or a gateway with multi-factor authentication.

Photos of the cabinet and network equipment (photos: attach, or note the file names)

3. Servers and cloud

Where the data and email live.

Email (choose one)

- ☐ Microsoft 365
- ☐ Google Workspace
- ☐ Exchange server on site
- ☐ From the web host
- ☐ Other: _____

Where are files kept? (choose one)

- ☐ SharePoint or OneDrive
☐ Google Drive
☐ Server or NAS on site
☐ On individual PCs
☐ A mix
☐ Other: _____

Are there servers or storage devices on site?

- ☐ Yes ☐ No

Servers and storage (copy this block for each one; if applicable)

Name *

What it does

Operating system and version

Does it still get security updates? (choose one)

- ☐ Yes ☐ No ☐ Not known

If applicable: Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported.

Year bought

Age (years) (if applicable; worked out automatically in the app)

Warranty or support contract (choose one)

- ☐ In place ☐ Expired ☐ Not known

Free disk space (%)

4. PCs, laptops and mobiles

The devices people work on.

Desktops

Laptops

Company phones and tablets

Devices in total (worked out automatically in the app)

How many run an operating system that no longer gets security updates?

If applicable: Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported.

How are updates installed? (choose one)

- ☐ Automatically, and checked
- ☐ Automatically, nobody checks
- ☐ By hand
- ☐ Not known

Updates. Cyber Essentials requires updates that fix critical or high risk vulnerabilities (a CVSS v3 base score of 7 or above) to be installed within 14 days of release.

Are laptops encrypted? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Anti-malware on every device? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Do staff use administrator accounts for day to day work?

- ☐ Yes ☐ No

If applicable: Cyber Essentials requires separate accounts for administrative work, with no email or web browsing from them.

Is there an up to date list of devices?

- ☐ Yes ☐ No

5. Backup and recovery

Whether the organisation could carry on after losing its data.

Is anything backed up?

- ☐ Yes ☐ No

If applicable: No backup. Put this first in the summary.

What is backed up? (if applicable; tick all that apply)

- ☐ Servers
- ☐ Shared files
- ☐ Email
- ☐ Cloud services such as Microsoft 365
- ☐ Individual PCs
- ☐ Line of business systems
- ☐ Other: _____

How often? (if applicable; choose one)

- ☐ Daily or more ☐ Weekly ☐ Less often ☐ Not known

Is a copy kept off site or in the cloud? (if applicable)

- ☐ Yes ☐ No

Is there a copy that ransomware on the network could not reach? (if applicable)

- ☐ Yes ☐ No

When was a restore last tested? (if applicable)

Days since the last restore test (if applicable; worked out automatically in the app)

Is there a written plan for what to do if systems are lost?

☐ Yes ☐ No

Are servers and network equipment on a UPS?

☐ Yes ☐ No

6. Accounts and security

Who can get in, and how.

Multi-factor authentication on email and cloud services * (choose one)

☐ All users ☐ Administrators only ☐ Some users ☐ Nobody

If applicable: Multi-factor authentication. The Cyber Essentials requirements say to always use it for administrative accounts and for accounts that can be reached from the internet.

Are accounts closed when people leave? (choose one)

☐ Yes, same day ☐ Yes, eventually ☐ No process ☐ Not known

Are any logins shared between people?

☐ Yes ☐ No

How are passwords looked after? (choose one)

☐ Password manager
☐ Each person remembers their own
☐ Written down or in a spreadsheet
☐ Not known

Cyber Essentials (choose one)

☐ Certified ☐ Certified: Cyber Essentials Plus ☐ Lapsed ☐ Never certified

Have staff had security awareness training in the last year?

☐ Yes ☐ No

7. Findings and recommendations

One entry for each thing the customer should act on.

Findings (copy this block for each one)

Area * (choose one)

☐ Network and internet
☐ Servers and storage
☐ Devices
☐ Cloud and email
☐ Backup and recovery
☐ Accounts and security
☐ Comms room and cabling
☐ Licences and contracts
☐ Other: _____

Risk * (choose one)

☐ High ☐ Medium ☐ Low

What did you find? *

What do you recommend?

Who should act on it?

By when?

Photos or screenshots (photos: attach, or note the file names)

Findings (worked out automatically in the app)

High risk findings (worked out automatically in the app)

8. Summary and sign-off

The overall picture, in plain words for the customer.

Overall * (choose one)

☐ Good: minor improvements only ☐ Needs attention ☐ At risk: act now

Summary for the customer

The three things to do first

Auditor name

Auditor signature

Customer name

Customer signature