

IT Security Audit Checklist

Security audit built around the five Cyber Essentials controls, plus backups, physical security and incident readiness, 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 is in scope?

For example the whole organisation, one office, or one network.

Number of users in scope

Number of devices in scope

How this checklist is built. Pages 2 to 6 follow the five technical controls of Cyber Essentials, the minimum standard of cyber security the UK government recommends for organisations of all sizes: firewalls, secure configuration, security update management, user access control and malware protection. This is a readiness check, not a Cyber Essentials assessment or certificate.

2. Firewalls

Every device in scope should sit behind a firewall.

Is every device protected by a firewall, at the network edge or on the device? * (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Has the default administrator password on every firewall and router been changed? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Can the firewall admin page be reached from the internet? (choose one)

☐ No

☐ Yes, protected by multi-factor authentication or a trusted address list

☐ Yes, with a password only

☐ Not known

If applicable: Cyber Essentials only allows this where there is a documented business need and the interface is protected by multi-factor authentication or an IP allow list. Close it off or add one of the two.

Is every inbound rule approved, documented and still needed? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Is a software firewall switched on for laptops used on other networks, such as home or public Wi-Fi?

(choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Notes

3. Secure configuration

Devices and software set up to give attackers less to work with.

Have unused and guest accounts been removed or disabled? * (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Have default and guessable passwords been changed? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Has software that is not needed been removed or disabled? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Is auto-run switched off, so files do not run without the user agreeing? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Do devices need a PIN, password or biometric to unlock? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Where a device unlocks with a PIN or password, Cyber Essentials requires protection against guessing: no more than 10 guesses in 5 minutes, or locking after no more than 10 failed attempts.

Notes

4. Security update management

Supported software, updated quickly.

Is all software licensed and still supported by its maker? * (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

What is unsupported, and on which devices? (if applicable)

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

Are automatic updates switched on where they can be? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Are critical and high risk updates installed within 14 days? (choose one)

☐ Yes ☐ Partly ☐ No ☐ 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.

What evidence did you see?

For example the update report from the management tool.

5. User access control

Accounts for the right people, with no more access than they need.

Is there a process to approve new accounts? * (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Does everyone sign in with their own account? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Are accounts removed or disabled when someone leaves or changes role? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Are administrator accounts separate, and not used for email or browsing? (choose one)

☐ Yes ☐ Partly ☐ No ☐ Not known

Multi-factor authentication (choose one)

- ☐ All users
- ☐ Administrators and internet-facing accounts
- ☐ 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.

Where a password is used, which protection is in place? (choose one)

- ☐ Multi-factor authentication
- ☐ At least 12 characters
- ☐ At least 8 characters with common passwords blocked
- ☐ None of these

If applicable: Cyber Essentials asks for one of the three: multi-factor authentication, a minimum length of at least 12 characters, or at least 8 characters with a deny list that blocks common passwords.

Notes

6. Malware protection

Stopping malicious software from running.

How are devices protected? * (choose one)

- ☐ Anti-malware software
☐ Only approved applications can run
☐ A mix of both
☐ No protection

Is anti-malware kept up to date in line with the maker's recommendations? (if applicable; choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Does it stop connections to malicious websites? (if applicable; choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Is every device in scope covered, including phones and tablets? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Notes

7. Backups, premises and incidents

Outside the five controls, but part of any security audit.

Is important data backed up? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Has a restore been tested in the last year? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Are servers and network equipment locked away? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Do screens lock when left? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Are visitors signed in and accompanied? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Do staff know how to report a security incident, and to whom? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

Personal data breaches. The ICO says a notifiable breach must be reported to it without undue delay, and not later than 72 hours after becoming aware of it. Staff need to know who to tell straight away.

Have staff had security awareness training in the last year? (choose one)

- ☐ Yes ☐ Partly ☐ No ☐ Not known

8. Findings and recommendations

One entry for each thing the customer should act on.

Findings (copy this block for each one)

Area * (choose one)

- ☐ Firewalls
- ☐ Secure configuration
- ☐ Security updates
- ☐ User access control
- ☐ Malware protection
- ☐ Backups
- ☐ Physical security
- ☐ Incident readiness
- ☐ 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)

9. 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