National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Cyber Essentials: Requirements for IT infrastructure

Version 3
November 2021

Contents

We specify the requirements under five technical control themes:

- firewalls
- secure configuration
- user access control
- malware protection
- security update management

As a Cyber Essentials scheme applicant, you must ensure that your organisation meets all the requirements. You may also be required to supply various forms of evidence before your chosen Certification Body can award certification at the level you seek.

Proceed as follows:

1. Establish the **boundary of scope** for your organisation and **determine what is in scope within this boundary.**
2. Review each of the five **technical control themes** and the **controls they embody as requirements**.
3. Take steps as necessary to **ensure that your organisation meets every requirement**, throughout the scope you have determined.

What's new

- Added a home working requirement and information on how this is to be included in the scope of certifications.
- All cloud services are now in scope, added definitions and a shared responsibility table to assist with this.
- Extended the multi-factor authentication requirement in relation to cloud services.
- Updated the password-based authentication requirement and added a new section on multi-factor authentication. This requirement has also been moved to the 'user access' control.
- Thin clients are now in scope and added to the 'devices' definition.
- Added a new device unlocking requirement to the 'secure configuration' control.

- Added a new statement clarifying the inclusion of end user devices in the scope of certifications.
- Further information on unsupported applications added to the ‘security update management’ control.
- Removed specific ‘email, web, and application servers’ from control definitions and replaced with ‘servers’.
- Updated the bring your own device (BYOD) section.
- Updated the wireless devices section.
- Added a new ‘servers’ definition.
- Added a new ‘sub-set’ definition and information on its impact on the scope.
- Added a new ‘licensed and supported’ definition.

Definitions

- **Software** includes operating systems, commercial off-the-shelf applications, plug-ins, interpreters, scripts, libraries, network software and firmware.
- **Devices** includes all types of hosts, networking equipment, servers, networks, and end user devices such as desktop computers, laptop computers, thin clients, tablets and mobile phones (smartphones) — whether physical or virtual.
- **Applicant** means the organisation seeking certification, or sometimes the individual acting as the main point of contact, depending on context.
- A **corporate VPN** is a Virtual Private Network solution that connects back to the applicants office location or to a virtual/cloud firewall. This must be administered by the applicant organisation so that the firewall controls can be applied.
- **Organisational data** includes any electronic data belonging to the applicant organisation. For example, emails, office documents, database data, financial data.

- **Organisational service** includes any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the applicant organisation. For example: Web applications, Microsoft Office 365, Google Workspace, Mobile Device Management containers, Citrix Desktop, virtual desktop solutions, IP telephony.
- A **sub-set** is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.
- **Servers** are specific devices that provide organisational data or services to other devices as part of the business of the applicant.
- **Licensed and supported software** is software that you have a legal right to use and that a vendor has committed to support by providing regular updates (patches). The vendor must provide the future date when they will stop providing updates. The vendor does not have to be the original creator of the software, but they must have the ability to modify the original software to create updates.

Scope

Overview of the scope

Assessment and certification should cover the whole of the IT infrastructure used to perform the business of the applicant, or if necessary, a well-defined and separately managed sub-set. Either way, the boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. The scope must be agreed between the applicant and the Certification Body before assessment begins.

A sub-set can be used to define what is **in scope** or what is **out of scope** for Cyber Essentials.

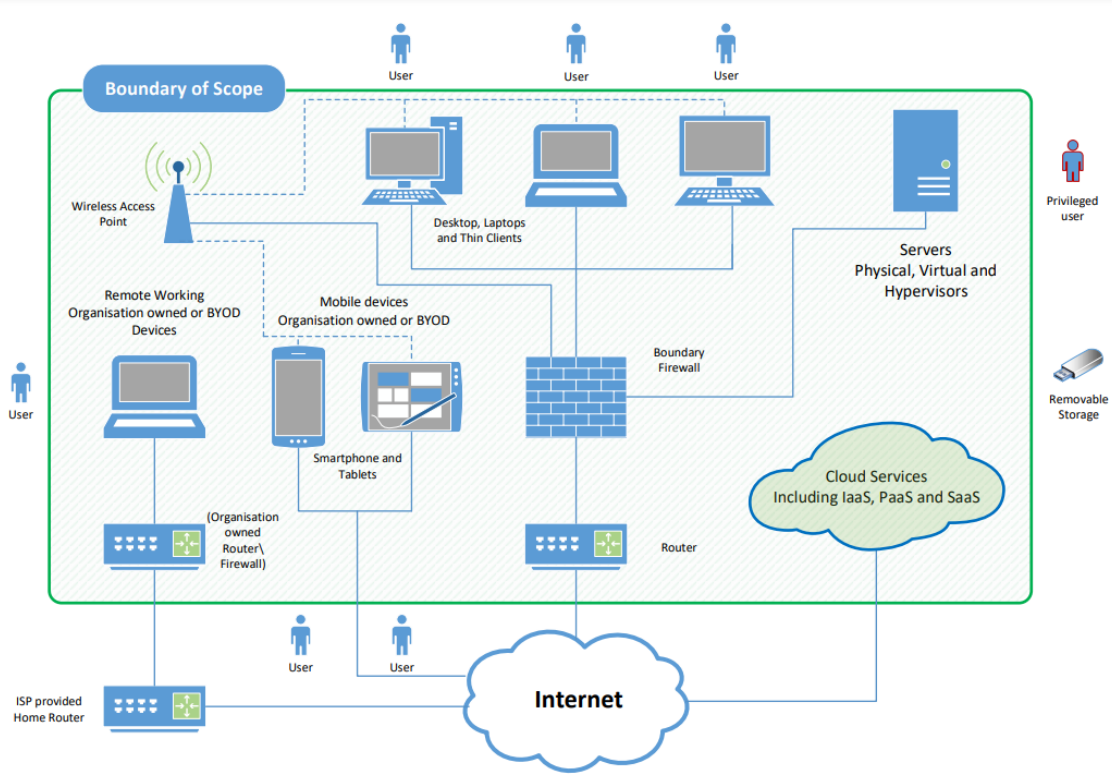
> **Information** Organisations that choose a scope that includes the whole IT infrastructure achieve the best protection and increase customer confidence.

The requirements apply to all the devices and software that are within the boundary of the scope and that meet the any of these conditions:

- can accept incoming network connections from untrusted internet-connected hosts; or
- can establish user-initiated outbound connections to devices via the internet; or
- control the flow of data between any of the above devices and the internet.

A scope that does not include end user devices is not acceptable.

Figure 1: Scope of the requirements for IT infrastructure -



Bring your own device (BYOD)

In addition to mobile or remote devices owned by the organisation, user-owned devices which access organisational data or services (as defined above) are in **scope**. However, all mobile or remote devices used **only** for the purpose of:

- native voice applications
- native text applications
- multi-factor authentication applications

are **out of scope**.

Traditionally, user devices were managed through centralised administration, ensuring consistency across the organisation. In such cases, certification of the security controls is straightforward as there will be a standard build or reference to assess.

BYOD complicates matters, as users are given more freedom to 'customise' their experience making consistent implementation of the controls more challenging. Using the organisational data and services definitions to enforce strong access policies should remove some of this ambiguity.

Home working

The default approach is that all corporate or BYOD home working devices used for applicant business purposes within the home location are **in scope** for Cyber Essentials.

Internet Service Provider (ISP) routers and user provided routers are **out of scope** which means that the Cyber Essentials firewall controls need to be applied on the user devices (e.g. a software firewall).

If a router is supplied to the home worker by the applicant organisation, then that router will be **in scope**.

If the home worker is using a corporate VPN, their internet boundary is on the company firewall or virtual/cloud firewall.

Wireless devices

Wireless devices (including wireless access points) are:

- **in scope** if they can communicate with other devices via the internet
- **not in scope** if it is not possible for an attacker to attack directly from the internet (the Cyber Essentials scheme is not concerned with attacks that can only be launched from within the signal range of the wireless device)
- **not in scope** if they are part of an ISP router within the home location

Externally managed services — cloud

If the applicant's data or services are hosted on cloud services, then these services must be **in scope**.

In cloud services **the applicant is always responsible** for ensuring all the controls are implemented, but some of the controls can be implemented by the cloud service provider. Who implements which control depends on the type of cloud service. We consider three different types of cloud service:

- **Infrastructure as a Service (IaaS)** - the cloud provider delivers virtual servers and network equipment that are configured and managed by the applicant, much like physical equipment would be. Examples of IaaS include Rackspace, Google Compute Engine, or Amazon EC2.
- **Platform as a Service (PaaS)** - the cloud provider delivers and manages the underlying infrastructure, and the applicant provides and manages the applications. Examples of PaaS include Azure Web Apps and Amazon Web Services Lambda.
- **Software as a Service (SaaS)** - the cloud provider delivers applications to the applicant, and the applicant configures the services. The applicant must still take time to ensure the service is configured securely. Examples of SaaS include Microsoft 365, Dropbox, Gmail.

Who implements the controls will vary depending on the design of the cloud service used, but the table below is presented as a guide to who would typically be expected to implement each control:

Requirement	**IaaS**	**PaaS**	**SaaS**
firewalls	both applicant and cloud provider	cloud provider and sometimes also the applicant	cloud provider
secure configuration	both applicant and cloud provider	both applicant and cloud provider	both applicant and cloud provider
user access control	applicant	applicant	applicant
malware protection	both applicant and cloud provider	cloud provider and sometimes also the applicant	cloud provider
security update management	both applicant and cloud provider	both applicant and cloud provider	cloud provider

Where the cloud provider implements a control, the applicant must satisfy themselves that this has been done by the cloud provider committing to implementation within contractual clauses or documents referenced by contract, such as security statements or privacy statements. Cloud providers will often explain how they implement security in documents published in their trust centres, which will include reference to a 'shared responsibility model'.

Externally managed services — other

Where the applicant is using other externally managed services (such as remote administration) it may not be possible for the applicant to meet all the requirements directly. The applicant may **choose** whether or not to include these services within the boundary of scope, according to feasibility.

If included, then the applicant must be able to attest that the requirements that are outside of the applicant's control are being adequately met by the service provider. Existing evidence may be considered (such as that provided through PCI certification of a cloud service, and ISO 27001 certifications that cover an appropriate scope).

Web applications

Commercial web applications created by development companies (rather than in-house developers) and which are publicly accessible from the internet are **in scope** by default. Bespoke and custom components of web applications are **not in scope**. The primary mitigation against vulnerabilities in such applications is robust development and testing in line with commercial best practices, such as the Open Web Application Security Project (OWASP) standards.

Requirements, by technical control theme

Firewalls

Applies to: boundary firewalls, desktop computers, laptop computers, routers, servers, IaaS, PaaS, SaaS.

Objective

Ensure that only safe and necessary network services can be accessed from the internet.

Introduction

All devices run network services, which create some form of communication with other devices and services. By restricting access to these services, you reduce your exposure to attacks. This can be achieved using firewalls and equivalent network devices, or data flow policies in cloud services.

A boundary firewall is a network device which can restrict the inbound and outbound network traffic to services on its network of computers and mobile devices. It can help protect against cyber attacks by implementing restrictions, known as 'firewall rules', which can allow or block traffic according to its source, destination and type of communication protocol.

Alternatively, where an organisation does not control the network a device is connected to, a software firewall must be configured on a device. This works in the same way as a boundary firewall but only protects the single device on which it is configured. This approach can provide for more tailored rules and means that the rules apply to the device wherever it is used. However, this increases the administrative overhead of managing firewall rules.

> **Information** Most desktop and laptop operating systems now come with a software firewall pre-installed, we advise that these are turned on in preference to a third-party firewall application.

Requirements under this technical control theme

Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device).

For all firewalls (or equivalent network devices), the applicant organisation must routinely:

- change any default administrative password to an alternative that is difficult to guess (see password-based authentication) — or disable remote administrative access entirely
- prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need and the interface is protected by one of the following controls:
    - multi-factor authentication (see MFA details below)

    - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach
- block unauthenticated inbound connections by default
- ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation
- remove or disable unnecessary firewall rules quickly, when they are no longer needed
- use a software firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Secure configuration

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, thin clients, IaaS, PaaS, SaaS.

Objective

Ensure that computers and network devices are properly configured to:

- reduce the level of inherent vulnerabilities
- provide only the services required to fulfil their role

Introduction

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:

- an administrative account with a predetermined, publicly known default password or without multi-factor authentication enabled
- pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- pre-installed but unnecessary applications or services

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Requirements under this technical control theme

Computers and network devices

The applicant must be active in its management of computers and network devices. It must routinely:

- remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)
- change any default or guessable account passwords (see password-based authentication)
- remove or disable unnecessary software (including applications, system utilities and network services)
- disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the internet)
- ensure authentication of users before allowing access to organisational data or services
- ensure appropriate device locking controls (see 'device locking', below) for physically present users.

Device unlocking credentials

Where a device requires the physical presence of a user to gain access to the services the device offers (e.g. laptop logon, mobile phone unlock) the user must unlock the device using a credential such as a biometric, password or PIN before gaining access to the services.

Biometric tests, passwords and PINs must be protected against brute-force attack by at least one of:

- 'throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
- locking devices after no more than 10 unsuccessful attempts

Technical controls must be used to manage the quality of credentials. If credentials are solely to unlock a device a minimum password or PIN length of at

least 6 characters must be used. When the device unlocking credentials are used elsewhere, then the full password requirements in 'user access control' must be applied to the credentials.

User access control

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, IaaS, PaaS, SaaS.

Objective

Ensure user accounts:

- are assigned to authorised individuals only
- provide access to only those applications, computers and networks actually required for the user to perform their role

Introduction

Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information. By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. When such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation.

'Administrative accounts' are especially highly privileged, for example. Such accounts typically allow:

- execution of software that has the ability to make significant and security relevant changes to the operating system
- changes to the operating system for some or all users
- creation of new accounts and allocation of their privileges

All types of administrator will have such accounts, including domain administrators and local administrators.

Now consider that if a user opens a malicious URL or email attachment, any associated malware is typically executed with the privilege level of the account that user is currently operating. Clearly, you must take special care over the allocation and use of privileged accounts.

Example

> Jody is logged in with an administrative account. If Jody opens a malicious URL or email attachment, any associated malware is likely to acquire administrative privileges. Unfortunately, this is exactly what happens. Using Jody's administrative privileges, a type of malware known as ransomware encrypts all of the data on the network and then demands a ransom. The ransomware was able to encrypt far more data than would have been possible with standard user privileges, making the problem that much more serious.

Requirements under this technical control theme

The applicant must be in control of its user accounts and the access privileges granted to each user account that has access to the organisation's data and services. Importantly, this includes accounts that third parties use for access, for example for device management or support services. It must also understand how user accounts authenticate and control the strength of that authentication. This means the applicant must:

- have a user account creation and approval process
- authenticate users before granting access to applications or devices, using unique credentials (see password-based authentication)
- remove or disable user accounts when no longer required (when a user leaves the organisation or after a defined period of account inactivity, for example)
- implement MFA, where available. Authentication to cloud services must always use MFA.
- use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Password-based authentication

All user accounts require the user to authenticate.

Where this is done using a password, the following protections should be used:

- Passwords are protected against brute-force password guessing by implementing at least one of:
    - using multi-factor authentication (see below)
    - 'throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
    - locking accounts after no more than 10 unsuccessful attempts

- Technical controls are used to manage the quality of passwords. This will include one of the following:
    - using multi-factor authentication (see below)
    - a minimum password length of at least 12 characters, with no maximum length restrictions
    - a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.

- People are supported to choose unique passwords for their work accounts. This is enabled by:
    - educating people on how to avoid common or discoverable passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.
    - encouraging people to choose longer passwords. This can be done by promoting the use of multiple words (a minimum of three) to create a password, (e.g., 'Three Random Words')

    - providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used.
    - not enforcing regular password expiry
    - not enforcing password complexity requirements

- There is an established process to change passwords promptly if the applicant knows or suspects the password or account has been compromised.

Multi-factor authentication (MFA)

As well as providing extra protection for passwords that are not protected by other technical controls (above), multi-factor authentication should always be used to provide additional protection to administrative accounts, and accounts that are accessible from the internet.

The password element of the multi-factor authentication approach must have a password length of at least 8 characters, with no maximum length restrictions.

There are four types of additional factor that may be considered:

- a managed/enterprise device
- an app on a trusted device
- a physically separate token
- a known or trusted account

Additional factors should be chosen so that they are usable and accessible. This may require user testing to verify if a factor is suitable for the users. For more information see the NCSC's guidance on MFA.

> **Information** SMS is not the most secure type of MFA, but still offers a huge advantage over not using any MFA. Any multi-factor authentication is better than not having it at all. However, if there are alternatives available that will work for your use case, we recommend you use these instead of SMS.

Malware protection

Applies to: Servers, desktop computers, laptop computers, tablets, mobile phones, IaaS, PaaS, SaaS.

Objective

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

Introduction

The execution of software downloaded from the internet can expose a device to malware infection. Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources of malware infection include: malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

If a system is infected with malware, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm from malware by:

- detecting and disabling malware before it causes harm (anti-malware)
- executing only software that you know to be worthy of trust (allow listing)
- executing untrusted software in an environment that controls access to other data (sandboxing)

Example

> Acme Corporation implements code signing alongside a rule that allows only vetted applications from the device application store to execute on devices. Unsigned and unapproved applications will not run on devices. The fact that users can only install trusted (allow listed) applications leads to a reduced risk of malware infection.

Requirements under this technical control theme

The applicant must implement a malware protection mechanism on all devices that are in scope. For each such device, the applicant must use at least one of the three mechanisms listed below:

Anti-malware software

- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.
- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the internet (by means of deny listing, for example) — unless there is a clear, documented business need and the applicant understands and accepts the associated risk.

Application allow listing

- Only approved applications, restricted by code signing, are allowed to execute on devices. The applicant must:
    - actively approve such applications before deploying them to devices
    - maintain a current list of approved applications Users must not be able to install any application that is unsigned or has an invalid signature.

Application sandboxing

- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user. This includes:
    - other sandboxed applications
    - data stores, such as those holding documents and photos
    - sensitive peripherals, such as the camera, microphone and GPS
    - local network access

Security Update management

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, firewalls, routers, IaaS, PaaS, SaaS.

Objective

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

Introduction

Any device that runs software can contain security flaws, known as 'vulnerabilities'.

Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks in organisations with these weaknesses.

Caution

> Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as 'patches' or security updates. These may be made available to customers immediately or on a regular release schedule (perhaps monthly).

Requirements under this technical control theme

The applicant must ensure all in scope software is kept up to date. All software on in scope devices must be:

- licensed and supported
- removed from devices when it becomes un-supported or removed from scope by using a defined "subset" that prevents all traffic to / from the internet
- have automatic updates enabled where possible
- updated, including applying any manual configuration changes required to make the update effective, within 14 days* of an update being released, where:
    - The update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'
    - The update addresses vulnerabilities with a CVSS v3 score of 7 or above

- There are no details of the level of vulnerabilities the update fixes provided by the vendor

For optimum security and ease of implementation it is strongly recommended (but not mandatory) that **all** released updates be applied within 14 days.

*It is important that these updates are applied as soon as possible. 14 days is seen as a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.

Information

> If the vendor uses different terms to describe the severity of vulnerabilities, see the precise definition in the Common Vulnerability Scoring System (CVSS). For the purposes of the Cyber Essentials scheme, 'critical' or 'high risk' vulnerabilities are those with a CVSS3 score of 7 or above or are identified by the vendor as "critical or high risk.

Caution

> Some vendors release security updates for multiple issues with differing severity levels as a single update. If such an update covers any 'critical' or 'high risk' issues then it must be installed within 14 days.

Further Guidance

Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.

Backing up your data is not a technical requirement of Cyber Essentials; however we highly recommend implementing an appropriate backup solution.