Cyber Essentials Plus Assessment Report

Assessment of: Myknowledgemap Limited

Assessed by (Certification Body): Precursor Security

Assessed By (Assessor Name): Euan Czerepaniak

Assessed By (Lead Assessor name): Euan Czerepaniak

Date of assessment visit: 2026-03-05

Date of Report: 6/3/2026

Cyber Essentials Plus certification can only be issued by a licensed Certification Body.

You can confirm the authenticity of this report by contacting IASME Consortium

+44 (0)3300 882752

1. About this report

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard.

Cyber Essentials requires organisations to have a number of technical and procedural controls in place to improve their information security in order to mitigate common internet-borne cyber attacks. Cyber Essentials Plus is a series of tests that provide a further level of assurance that these technical controls have been successfully implemented within an organisation.

This report is a record of the Cyber Essentials Plus audit of Myknowledgemap Limited against the Cyber Essentials standard that has been carried out by Euan Czerepaniak of the Certifying Body Precursor Security.

Cyber Essentials provides assurance that a number of key information security controls are in place within an organisation. For further assurance, the IASME information security standard provides a broader set of controls that enable good information security governance across an organisation.

1.1 Summary of findings

The internal scans brought back minimal vulnerabilities with a CVSS of 7.0 and above which were promptly remediated, the client keeps on top of all updates and stands by the 14 day patching windows. A pass has been awarded.

The assessment concluded that the configuration of the organisations external network and workstations were setup to a secure standard which adhered to the Cyber Essentials requirements.

Malware Protection solutions were in place on all assessed devices, and up to date, and cloud solutions were each configured with appropriate authentication solutions.

Web based downloads were also protected against.

When reviewing the patch levels for the assessed end user devices, only a few patches were identified during the auditing on the sampled hosts. Overall a good audit to which the client should be awarded the cyber essentials certification

The assessor has concluded that Myknowledgemap Limited has passed the required tests and should be awarded the Cyber Essentials Plus certification.

The Certificate Number is 865dbba6-e9a6-4cb4-b123-d1ee83424978 and can be found at https://registry.blockmarktech.com/certificates/865dbba6-e9a6-4cb4-b123-d1ee83424978/

The second certificate number is ca56c00d-8838-4fdb-bba1-162ef55f6ec5 and can be found at https://registry.blockmarktech.com/certificates/ca56c00d-8838-4fdb-bba1-162ef55f6ec5/

If a test has not been passed successfully, the assessor has provided feedback within the relevant section.

Evidence of activities

In carrying out the audit, the assessor will have carried out a number of technical tests and have seen documentary evidence. This evidence forms a basis for the assessor's recommendations and where appropriate has been included in this report.

Scope of CE+ Audit

The following networks and locations were considered in the scope of this assessment:

For the external, the following IP address/domain was provided: 52.147.54.49, myknowledgemap.drayddns.com, 188.65.100.234, 188.65.100.235, 188.65.100.236, 188.65.100.237, 188.65.100.238

For the internal, local hostnames were used for authenticated scans. Network 192.168.1.x, 192.168.2.x

Any areas that were excluded from the audit are listed below:

No items were excluded from the assessment

Remote Vulnerability Assessment

The purpose of this test is to test whether an Internet-based opportunist attacker can hack into the applicant's system with typical low-skill methods.

Each external IP address that is in scope has been scanned to identify any services that are open to the internet. All open services are tested to confirm that they have met the requirements of Cyber Essentials.

Remediations for Remote Vulnerability Assessment
N/A

Internal Testing

A suitable set of devices that was selected at random by the assessor that is representative of 100% of the applicant infrastructure.

A summary of the breakdown of this sample is as follows:

Full client estate listed as follows:
18 x Windows 11 Pro 25H2
6 x Windows 11 Pro 24H2
Hypervisor: HP Proliant DL160 running Windows Server 2019 Standard (Hyper-V),
Hosting:
  Domain Controller 1: Windows Server 2019 Standard,
  Domain Controller 2: Windows Server 2019 Standard,
  VPN Server: Windows Server 2022 Standard
1 x iPhone 13 (iOS 26)
1 x iPhone 14 (iOS 26)
1 x Samsung S25 (Android 16)
1 x Samsung Galaxy S22 (Android 16)
1 x Pixel 9 Pro XL (Android 16)
1 x Pixel 9a (Android 16)

Sample selected:
3
Windows 11 Pro 25H2
3
Windows 11 Pro 24H2 - ALL NOW UPGRADED TO 25H2 SO sampling covered
1
Hypervisor: HP Proliant DL160 running Windows Server 2019 Standard (HyperV),
2
Hosted - Windows Server 2019 Standard
1
Hosted - Windows Server 2022 Standard
2
IOS 26 - now only 1 as consolidated
2
Android 16

Authenticated vulnerability scan of devices

The purpose of this test is to identify missing vulnerability fixes within the defined CE+ test scope that could be exploited within the bounds of the CE threat model. Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism prescribed by the vendor to fix a known vulnerability.

This test was awarded PASS by the assessor.

The following vulnerabilities were discovered that scored 7 or higher on CVSS v3 and had a security update available that had been released

by the vendor 14 or more days ago:

MS Office
Dell Support assist
MS Unquoted service paths
.NET/ASP.NET
Firefox
Dell updates
Visual studio
7ZIP
Jetbrains
NodeJS
SQL server unsupported

The assessor has confirmed that these issues have been remediated and the required update applied during the remediation period.

Remediations for Authenticated Vulnerability Scan
After notifying the client, they promptly resolved the highlighted issues and provided full evidence this had been completed, which was then verified. Audit week

Check Malware Protection

This test checks the sampled devices to confirm that all devices in scope benefit from a basic level of malware protection.

All devices and virtual desktop environments should either be using anti malware software or application allow listing.

This test was awarded PASS by the assessor.

All sampled devices have been tested and the assessor who has confirmed that they benefit from a basic level of malware protection.

For all devices using anti-malware software it has been confirmed that the software is functional and is being updated in line with vendor recommendations.

For devices using application allow listing, the assessor has confirmed that the application allow list is configured correctly.

Remediations for Malware Protection Check
N/A

Remediations for Anti-Malware Software
N/A

Remediations for Allow-Listing
N/A

Check Multi-Factor Authentication (MFA) Configuration

All cloud services must be configured to authenticate using MFA. This test is in place to confirm that all cloud services that have been declared in the scope with MFA available are authenticating using MFA.

The assessor has checked the user of each sampled device against every cloud service that they use.

At least one administrator account and one standard user account has been checked for each cloud service.

This test was awarded PASS by the assessor

All users for sampled devices were observed authenticating to cloud services which they use as an organisational service and confirmed that they were authenticating using MFA.

At least one administrator and one standard user for each cloud service was tested.

Remediations for MFA Configuration
N/A

Check Account Separation

This test is conducted to ensure that account separation is in place and that standard users can not conduct administrator tasks.

Elevating privileges is not an acceptable alternative to using separate accounts.

This test was awarded PASS by the assessor

The assessor has confirmed that all users of the sampled devices had standard user accounts and could not carry out an administrative task without entering credentials of a separate admin account.

Remediations for Account Separation
N/A

Applicant Answers

	Applicant Answers	Assessor Score
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant
A1.1 Organisation Name? What is your organisation's name? The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150 including spaces. Where an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations. For example: The Stationery Group, incorporating The Paper Mill and The Pen House It is also possible to list on a certificate where organisations are trading as other names. For example: The Paper Mill trading as The Pen House.	Myknowledgemap Limited	Compliant

A1.2 Organisation Type What type of organisation are you? "LTD" – Limited Company (Ltd or PLC) "LLP" – Limited Liability Partnership (LLP) "CIC" – Community Interest Company (CIC) "COP" – Cooperative "MTL" – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society) "CHA" – Registered Charity "GOV" – Government Agency or Public Body "SOL" – Sole Trader "PRT" – Other Partnership "SOC" – Other Club/ Society "OTH" – Other Organisation	LTD - Limited Company (Ltd or PLC)	Compliant
A1.3 Organisation Number What is your organisation's registration number? Please enter the registered number only with **no spaces or other punctuation**. Letters (a-z) are allowed, but you need at least one digit (0-9). There is a 20 character limit for your answer. If you are applying for certification for more than one registered company, **please still enter only one organisation number**. If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none". If you are registered in a country that does not issue a company number, please enter a unique identifier like a DUNS number.	03954387	Compliant
A1.4 Organisation Address What is your organisation's address? Please provide the legal registered address for your organisation.	UK Custom Fields: Address Line 1: King House Address Line 2: 12 King Street Town/City: York County: North Yorkshire Postcode: YO1 9WP Country: United Kingdom	Compliant

A1.5 Organisation Occupation What is your main business? Please summarise the main occupation of your organisation.	IT Custom Fields: Applicant Notes: Information and communication	Compliant
A1.6 Website Address What is your website address? Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer.	https://www.myknowledgemap.com	Compliant
A1.7 Renewal or First Time Application Is this application a renewal of an existing certification or is it the first time you have applied for certification? If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".	Renewal	Compliant
A1.8 Reasons for Certification What are the two main reasons for applying for certification? Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.	Required for Commercial Contract Custom Fields: Secondary Reason: To Give Confidence to Our Customers	Compliant
A1.8.1 Commercial Contract Organisation Who is the commercial contracting organisation? Please provide the name of the contracting organisation.	The Open University	Compliant

A1.9 CE Requirements Document Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document? Document is available on the NCSC Cyber Essentials website and should be read before completing this question set. Cyber Essentials Requirements for IT Infrastructure v3.2	Yes	Compliant
A1.10 Cyber Breach Can IASME and their expert partners contact you if you experience a cyber breach? We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.	Yes	Compliant
A1.11 Contact Permission Can IASME contact you for research purposes? Both IASME and the UK government occasionally need to ask questions about the process and/or benefits of the Cyber Essentials scheme for research purposes. If you agree to this we will contact you via the email address you registered with, you are free to not respond if we do contact you.	No	Compliant

A2.1 Assessment Scope Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to opt in to the included insurance. Your whole organisation includes all divisions, people and devices which access your organisation's data and services. About Scope Subset Scoping Guidance	Yes	Compliant
A2.3 Geographical Location Please describe the geographical locations of your business which are in the scope of this assessment. You should provide either a broad description (e.g. All UK offices) or simply list the locations in scope (e.g. Manchester and Glasgow retail stores).	Our only office in York.	Compliant

A2.4 End User Devices Please list the quantities and operating systems for your laptops, desktops and virtual desktops within the scope of this assessment. **Please Note: You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for you to list the model of the device.** **Devices that are connecting to cloud services must be included.** **A scope that does not include end user devices is not acceptable.** You need to provide a summary of all laptops, computers, virtual desktops and their operating systems that are used for accessing organisational data or services and have access to the internet. For example, “We have 25 DELL laptops running Windows 10 Professional version 22H2 and 10 MacBook laptops running MacOS Ventura"". Please note, the edition and feature version of your Windows operating systems are required. This applies to both your corporate and user owned devices (BYOD). You do not need to provide serial numbers, MAC addresses or further technical information. **Extended Security Update schemes** For any end-of-life operating system that has an extended security update program, you must maintain the required subscription. If you are using Windows 10 beyond the 14th October 2025 you must be signed up to the Microsoft Extended Security Update program in order to remain compliant. Further guidance: Operating System Support Guidance to BYOD	We have 24 Dell laptops running 18 x Windows 11 Pro 25H2 6 x Windows 11 Pro 24H2	Compliant

A2.4.1 Thin Client Devices Please list the quantity of thin clients within the scope of this assessment. Please include make and operating systems. Please provide a summary of all the thin clients in scope that are connecting to organisational data or services (definitions of which are in the 'Cyber Essentials Requirements for IT Infrastructure' document linked in question A1.9). Thin clients are commonly used to connect to a Virtual Desktop Solution. Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients to be supported and receiving security updates. Cyber Essentials Requirements for IT Infrastructure v3.2	No thin clients in use in our organisation.	Compliant
A2.5 Server Devices Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system. Please list the quantity of all servers within the scope of this assessment. For example: 2 x VMware ESXI 6.7 hosting 8 virtual Windows 2016 servers; 1 x MS Server 2019; 1 x Red Hat Enterprise Linux 8.3	Hypervisor: HP Proliant DL160 running Windows Server 2019 Standard (Hyper-V), Hosting: Domain Controller 1: Windows Server 2019 Standard, Domain Controller 2: Windows Server 2019 Standard, VPN Server: Windows Server 2022 Standard	Compliant

A2.6 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. Please Note: You must include make and operating system versions for all devices. All user devices within the scope of the certification only require the make and operating system to be listed. Devices that are connecting to cloud services must be included. A scope that does not include end user devices is not acceptable. Guidance to BYOD Operating System Support	1 x iPhone 13 (iOS 26) 1 x iPhone 14 (iOS 26) 1 x Samsung S25 (Android 16) 1 x Samsung Galaxy S22 (Android 16) 1 x Pixel 9 Pro XL (Android 16) 1 x Pixel 9a (Android 16)	Compliant
A2.7 Networks Please provide a list of networks that will be in scope for this assessment. You should include details of each network used in your organisation including its name, location and its purpose (e.g. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information.	York Office network, Home workers to York office via VPN.	Compliant
A2.7.1 Home or remote workers How many staff are home or remote workers? Any employee that has been given permission to work remotely (for any period of time at the time of the assessment) needs to be classed as a home/remote worker for Cyber Essentials. For further guidance see the Home and remote working section in the Cyber Essentials Requirements for IT Infrastructure document. Cyber Essentials Requirements for IT Infrastructure v3.2	25 Staff members.	Compliant

A2.8 Network Equipment Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You must include make and model of each device listed. You should include all equipment that controls the flow of data to and from the internet. This will be your routers and firewalls. You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic. If you have home and/or remote workers they will be relying on software firewalls, please describe in the notes field. You are not required to list any IP addresses, MAC addresses or serial numbers.	1x DreyTek Vigor 2962.	Compliant
A2.9 Cloud Services Please list all of the cloud services that are in use by your organisation and provided by a third party. **Please note that cloud services cannot be excluded from the scope of Cyber Essentials.** You need to include details of all of your cloud services. This includes all types of services - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Definitions of the different types of cloud services are provided in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2	Zendesk, Sendgrid, Mailgun, Microsoft Azure, Clickup, Clockify, ElasticSearch, Microsoft Office 365, Cloudinary, Intruder, Statuscake, Crowdstrike, Claude.	Compliant
A2.10 Responsible Person Please provide the name and role of the person who is responsible for managing your IT systems in the scope of this assessment. This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.	Sully Khalifa Custom Fields: Responsible Person Role: IT Services Manager	Compliant

A3.1 Head Office Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m? This question relates to the eligibility of your organisation for the included cyber insurance.	Yes	Compliant
A3.2 Cyber Insurance If you have answered "yes" to the last question then your organisation is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here. There is no additional cost for the insurance. You can see more about it at https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/	Opt-Out	Compliant
A4.1 Boundary Firewall Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers and the internet? You must have firewalls in place between your office network and the internet. **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). Further guidance: Firewalls	Yes	Compliant

A4.1.1 Off Network Firewalls Do you have software firewalls enabled on all of your computers, laptops and servers? Your software firewall needs to be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. Guidance on how to check your software firewall can be found here: About Firewalls **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). **CE Requirement:** Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots. If your organisation doesn't control the network to which a device connects, you must configure a software firewall on the device.	Yes	Compliant
A4.2 Firewall Default Password When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices? The default administrator password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (e.g. BT Business Hub, Draytek Vigor 2865ac). When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed. **CE Requirement:** Change default administrative passwords to a strong and unique password – or disable remote administrative access entirely. Further guidance: About Routers	Yes	Compliant

A4.2.1 Firewall Password Change Process Please describe the process for changing your firewall password. Home routers not supplied by your organisation are not included in this requirement. You need to understand how the password on your firewall(s) is changed. Please provide a brief description of how this is achieved.	Login into the firewall portal Go to system maintenance Administrator Password Enter the old password Enter new password confirm new password click ""OK"" Test the login using the new password save the newly created password in a password manager. pass the new password to the CTO to save securely	Compliant

A4.3 Firewall Password Configuration How is your firewall password configured? Please select the options being used: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length C. A password minimum length of 12 characters and no maximum length D. Passwordless system is being used as an alternative to user name and password, please describe E. None of the above, please describe Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement:** 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 • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Further guidance : Bulletproof your passwords	0: C. A password minimum length of 12 characters and no maximum length	Compliant

A4.4 Firewall Password Issue Do you change your firewall password when you know or suspect it has been compromised? Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs. When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance: Compromised Accounts	Yes	Compliant
A4.5 Firewall Management Process Do you have a process to manage your firewall? At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks.	Yes	Compliant
A4.6 Firewall Review Process Have you reviewed your firewall rules in the last 12 months? Please describe your review process. If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done?). **CE Requirement:** Remove or disable inbound firewall rules quickly when they are no longer needed.	A quarterly review of all IT Services systems is scheduled by the IT Services Team, and Firewall rules and external services are included in this. If a service is determined to no longer be needed, its reviewed with the board and then a company wide announcement is made, to ensure the service is no longer in use. The service is removed by the IT Services team, and then validating it has been removed and all firewall rules removed is placed on the agenda of the next IT Services Team meeting.	Compliant

A4.7 Firewall Inbound Connections Is your firewall configured to allow unauthenticated inbound connections? By default, most firewalls block all services inside the network from being accessed from the internet, but you need to check your firewall settings. **CE Requirement:** Block unauthenticated inbound connections by default.	No	Compliant
A4.8 Allowed Connections Please describe how you approve and document your allowed inbound connections. The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly. At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. **CE Requirement:** Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.	All requests for inbound firewall rules require a documented business case detailing the justification, service to be exposed, ports/protocols, source restrictions, and duration. Requests undergo technical review and risk assessment by the IT Services team before being submitted for board-level approval by an authorised person. Once approved, rules are implemented via Terraform (Infrastructure as Code) ensuring version control and audit trails. All approved rules are recorded in a central Firewall Rule Register and reviewed annually, with associated risks reassessed regularly. The process applies to all inbound access including Azure NSGs, Windows Firewall rules, database firewalls, and blob storage firewall configurations.	Compliant

A4.9 Firewall Remote Configuration Are your boundary firewalls configured to allow access to their configuration settings over the internet? Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question. **CE Requirement:** 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 • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Guidance on VPNs	No	Compliant

A5.1 Remove Unused Software Have you removed or disabled software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieve this. You must remove or disable applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use. To view installed applications: Windows: Right-click on Start > Apps and Features macOS: Open Finder > Applications Linux: Open your software package manager (apt, rpm, yum) **CE Requirement:** You must regularly remove or disable unnecessary software (including applications, system utilities and network services). Further guidance : Removing unnecessary software	Yes As part of the procedure of setting up new PCs, we have a setup checklist, which includes a section on ensuring unneeded pre-installed software is removed.	Compliant
A5.2 Remove Unrequired User Accounts Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business? You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services. To view user accounts: Windows: Right-click on Start > Computer Management > Users macOS: System Settings > Users and Groups Linux: "cat/etc/passwd" **CE Requirement:** You must regularly remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).	Yes	Compliant

A5.3 Change Default Password Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials? A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345". **CE Requirement:** You must regularly change any default or guessable account passwords. Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • 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	Yes	Compliant
A5.4 Internally hosted External Services Do you run or host external services that provide access to data (that shouldn't be made public) to users across the internet? Your business might run software that allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application such as a SaaS or PaaS cloud service that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible. **CE Requirement:** Ensure users are authenticated before allowing them access to organisational data or services.	Yes	Compliant

A5.5 External services Authentication If yes to question A5.4, which authentication option do you use? A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A minimum password length of 12 characters and no maximum length D. Passwordless, please describe E. None of the above, please describe Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about 'Password-based authentication' in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • 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	0: C. A minimum password length of 12 characters and no maximum length	Compliant

A5.6 External services password change process Describe the process in place for changing passwords on your external services when you believe they have been compromised. Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should know how to change the password if this occurs. **CE Requirement**: You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.	We ensure after any purchase that the serial number is registered with the manufacture, and we sign up for any security alerts offered, to notify if any services could be compromised. For users, our IT and Security Policy informs users to change their password if they feel it is compromised, we also use external services like HaveIBeenPwned and external password managers to help track possible issues.	Compliant

A5.7 External services brute-force protection When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks? A. Throttling the rate of attempts B. Locking accounts after 10 unsuccessful attempts C. None of the above, please describe The external service that you provide must be set to slow down or stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access. **CE Requirement:** You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following: • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes • locking devices after more than 10 unsuccessful attempts • When the vendor doesn't allow you to configure the above, use the vendor's default setting.	0: B. Locking accounts after 10 unsuccessful attempts	Compliant

A5.8 Auto-run Disabled Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation? This is a setting on your device which automatically runs software on external media or downloaded from the internet. It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option, you can answer yes to this question. **CE Requirement:** Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded).	Yes	Compliant
A5.9 Device Unlocking When a device requires a user to have the device in hand, do you set a locking mechanism on your devices to access the software and services installed? Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services. **CE Requirement:** Ensure appropriate device locking controls for users that are physically present.	Yes	Compliant

A5.10 Device Unlocking Method Which method do you use to unlock the devices? Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further information. Cyber Essentials Requirements for IT Infrastructure v3.2 The use of a PIN with a length of at least six characters can only be used where the credentials are just to unlock a device and does not provide access to organisational data and services without further authentication. **CE Requirement:** If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services. You must protect your chosen authentication method against brute-force attacks. When it's possible to configure, you should apply one of the following: • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes • locking devices after more than 10 unsuccessful attempts • When the vendor doesn't allow you to configure the above, use the vendor's default setting.	All mobiles in scope have a 6 digit pin which is solely used for device access. Laptops and computers require the use of the users full password, which is a minimum of 12 characters with no maximum.	Compliant

A6.1 Supported Operating System Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes? If you have included firewall or router devices in your scope, the firmware of these devices is considered to be an operating system and needs to meet this requirement. Older operating systems that are out of regular support could be any of the following examples: Windows 7/XP/Vista/ Server 2003, macOS Mojave, iOS 12, iOS 13, Android 8 and Ubuntu Linux 17.10. This is not an extensive list and you should always check with the vendor to confirm if an operating system is still supported It is important you keep track of your operating systems and understand when they have gone end of life (EOL). Most major vendors will have published EOL dates for their operating systems and firmware. **CE Requirement**: You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported. Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability. **Extended Security Update schemes** For any end-of-life operating system that has an extended security update program, you must maintain the required subscription. If you are using Windows 10 beyond the 14th October 2025 you must be signed up to the Microsoft Extended Security Update program in order to remain compliant. Further guidance: Operating System Support Navigating the pitfalls of legacy software	Yes	Compliant

A6.2 Supported software Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems? All software used by your organisation must be supported by a supplier who provides regular security updates and vulnerability fixes. Unsupported software must be removed from your devices. This includes frameworks and extensions. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Yes	Compliant
A6.2.1 Internet Browsers Please list your internet browser(s). The version is required. Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support. For example: Chrome Version 124, Safari Version 15. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	General staff have: Edge 144 Chrome Version 144 Our testers also have: Firefox 147	Compliant
A6.2.2 Malware Protection Please list your malware protection software The version is required. Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: Sophos Endpoint Protection V10, Microsoft Defender, Bitdefender Internet Security 2023. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	ESET Endpoint Security 12.1.2057.3	Compliant

A6.2.3 Email Applications Please list your email applications installed on end user devices and server. The version is required. Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: MS Exchange 2016, Outlook 2019. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Microsoft® Outlook® for Microsoft 365 MSO (Version 2512 Build 16.0.19530.20038) 64-bit. (This is the current channel)	Compliant
A6.2.4 Office Applications Please list all office applications that are used to create organisational data. The version is required. Please list all office applications and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: MS 365, Libre Office, Google Workspace, Office 2016. **CE Requirement**: You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Microsoft® Word for Microsoft 365 MSO (Version 2512 Build 16.0.19530.20038) 64-bit Microsoft® Excel® for Microsoft 365 MSO (Version 2512 Build 16.0.19530.20038) 64-bit. (This is the current channel)	Compliant
A6.3 Software Licensing Are any of the in-scope software or cloud services unlicensed or unsupported? All software must be licensed. It is acceptable to use free and open-source software as long as you comply with any licensing requirements. Please be aware that for some operating systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates. **CE Requirement:** All software on in-scope devices must be licensed and supported.	No	Compliant

A6.4 Security Updates - Operating System Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release? You must install all high and critical security updates and vulnerability fixes within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement. This requirement includes the firmware on your firewalls and routers. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release. It's important that updates are applied as soon as possible. 14 days is considered 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.	Yes	Compliant
A6.4.1 Auto-Updates - Operating System Are all updates applied for operating systems by enabling auto updates? Most devices have the option to enable auto updates. This must be enabled on any device where possible. **CE Requirement**: All software on in-scope devices must have automatic updates enabled where possible.	Yes	Compliant

A6.4.2 Manual Updates - Operating System Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes of all operating systems and firmware on firewalls and routers are applied within 14 days of release? It is not always possible to apply auto updates, this is often the case when you have critical systems or servers and you need to be in control of the updating process. Please describe how any updates are applied when auto updates are not configured. If you only use auto updates, please confirm this in the notes field for this question. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Where possible, all devices have auto updates enabled. In the case where a device could not have auto updates enabled, for example due to a testers machine being isolated from the network, we use Spiceworks Inventory tracking, with agents installed on user machines to track the versions of software installed, and ensure compliance with this. When an update is released for this group of machines, Spiceworks notifies the IT Services Team, and a ticket is raised to update that machine, to keep within the 14 days limit.	Compliant

A6.5 Security Updates - Applications Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release? You must install any such updates and vulnerability fixes within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Yes	Compliant
A6.5.1 Auto-updates- Applications Are all updates applied on your applications by enabling auto updates? Most devices have the option to enable auto updates. Auto updates should be enabled where possible. **CE Requirement:** All software on in-scope devices must have automatic updates enabled where possible.	Yes	Compliant

A6.5.2 Manual Updates - Applications Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes of all applications are applied within 14 days of release? It is not always possible to apply auto updates, this is often the case when you have critical systems or applications and you need to be in control of the updating process. Please describe how any updates and vulnerability fixes are applied when auto updates are not configured. If you only use auto updates, please confirm this in the notes field for this question. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Where tools support it, automatic updates are enabled, to keep them up to date. Specific tools that do not support automatic update are listed, and the users that require this software installed are manually informed of updates and requested to install them. This will be updated within 14 days if this is the case. We use Spiceworks Inventory tracking, with agents installed on user machines to track the versions of software installed, and ensure compliance with this, plus manually signing up to any notifications offered by the software provider.	Compliant
A6.6 Unsupported Software Removal Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates or vulnerability fixes for security problems? You must remove older software from your devices when it is no longer supported by the manufacturer. Such software might include older versions of web browsers, operating systems, and all application software. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet.	Yes	Compliant

A6.7 Unsupported Software Segregation Where you have a business need to use unsupported software, have you moved the devices and software out of scope of this assessment? Please explain how you achieve this. Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set with no internet access. If the out-of-scope sub-set remains connected to the internet, you will not be able to achieve whole company certification and an excluding statement will be required in question A2.2. 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. Where no unsupported software is used across your whole organisation, please declare this here. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet. Further guidance: Subset Scoping Guidance	While there are no machines currently in this state, where this is required, for example when our testers need to validate issues against specific legacy versions of software, then this is done as a virtual machine with no internet access available. If this machine needed to access specific network resources, then the machine would be placed on a VLAN with a firewall between it and any network resources it required. It would also be audited and removed when the requirement for it no longer existed.	Compliant
A7.1 User Account Creation Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process. You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	We have a formal process where the IT Team is notified of all new staff members, and informed of their role, required permissions and start date. As part of this, a hardware review is done to see if they will require new hardware including laptop/PC and mobile phones. This is then confirmed with their manager. Their credentials are created prior to their start date, to allow their hardware to be provisioned for them, however their accounts have a start date set, to disable logins before their start date. There is a formal induction process that happens on their start date, that includes providing them with the credentials.	Compliant

A7.2 Unique Credentials Are all your user and administrative accounts accessed by entering unique credentials? You must ensure that no devices, applications or cloud services can be accessed without entering unique access credentials. Accounts must not be shared. **CE Requirement:** Authenticate users with unique credentials before granting access to applications or devices.	Yes	Compliant
A7.3 Leaver Accounts How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation? When an individual leaves your organisation, you need to stop them accessing any of your systems. **CE Requirement:** Remove or disable user accounts when no longer required.	The IT Team are informed of departures beforehand, and an expiry date is added to the account prior to the departure date, ensuring that their account is automatically disabled. Once the individual has left the company, there is a process to clear down their hardware to prepare it for re-use within the company. This includes fully deleting the disabled account.	Compliant
A7.4 User Privileges Do you ensure that staff only have the access privileges that they need to do their current job? How do you do this? When a staff member changes job role you may also need to change their permissions to only access the files, folders and applications that they need to do their day-to-day work. For Cyber Essentials we require that the principle of least privilege be applied. **CE Requirement**: Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services.	There is a formal process with the IT Team and the users manager that happens before a user changes job role that includes reviewing the new permissions their role will require, and granting or removing them as needed.	Compliant

A7.5 Administrator Approval Do you have a formal process for giving someone access to systems at an “administrator” level and can you describe this process? You must have a process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	Yes we have a formal process. This is managed by the IT Security team, but does not require approval by anyone out side of this team. if another member of staff requires admin access, it is accessed what level of admin it is that they need and what period of time they need the admin access for. When that agreed upon time has passed the rights are then revoked.	Compliant
A7.6 Use of Administrator Accounts How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)? You must use a separate administrator account from the standard user account, when carrying out administrative tasks such as installing software. Using administrator accounts all day long exposes the device to compromise by malware. Cloud service administration must be carried out using separate accounts. Further guidance : User Access - Just Enough or Just In Time **CE Requirement:** Your organisation must 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).	Our IT and Security policies and training cover only using the administrative account for administrative tasks. Every user has two separate accounts, a standard account is for doing daily non-admin tasks such as accessing the internet, emails office 365. An admin account that is required for administrative tasks such as installing software and executing files.	Compliant

A7.7 Managing Administrator Account Usage How does your organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email? This question relates to the activities carried out when an administrator account is in use. You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. Software and update downloads should be performed as a standard user and then installed as an administrator. You may not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff. **CE Requirement:** Your organisation must 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).	Our IT and Security policies and training cover only using the administrative account for administrative tasks. We ensure that administrator accounts have no access to emails and can only be used to carry out administrative tasks. Whereas standard accounts are used for day-to-day tasks such as accessing the internet, and emails.	Compliant
A7.8 Administrator Account Tracking Do you formally track which users have administrator accounts in your organisation? You must track all people that have been granted administrator accounts. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	Yes	Compliant
A7.9 Administrator Access Review Do you review who should have administrative access on a regular basis? You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed. **CE Requirement:** Your organisation must remove or disable special access privileges when no longer required (when a member of staff changes role, for example).	Yes	Compliant

A7.10 Brute Force Attack Protection Where you have systems that require passwords (or where passwords are a backup for a passwordless system), how are they protected from brute-force attacks? A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Passwords are protected against brute-force password guessing by implementing at least one of: • multi-factor authentication • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt – you shouldn't allow more than 10 guesses in 5 minutes • locking devices after no more than 10 unsuccessful attempts	MFA is enabled on our accounts, and accounts will be locked out after 10 failed password attempts, enforced by group policy, and Azure Active Directory policy.	Compliant

A7.11 Password Quality Which technical controls are used to manage the quality of your passwords within your organisation? Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • 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.	MFA is enabled on our accounts, and our password policy is set to a minimum password length of at least 12 and no maximum.	Compliant

A7.12 Password Creation Advice Please explain how you encourage people to use unique and strong passwords. You need to support those that have access to your organisational data and services by informing them of how they should pick a strong and unique password. Further information can be found in the Password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Support users to choose unique passwords for their work accounts by: • educating people about avoiding common 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 by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using 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	Our password policy documentation covers picking a strong and unique password. Our company policy requires all users to create unique and strong passwords, and we actively encourage staff to do so. Staff are supported through training and guidance from the IT team, as well as clear direction in the staff handbook. We provide ongoing education to help staff understand the importance of strong, unique passwords in protecting company systems.	Compliant

A7.13 Password Compromise Policy Do you have a process for when you believe the passwords or accounts have been compromised? You must have an established process that details how to change passwords promptly if you believe or suspect a password or account has been compromised. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance : Compromised accounts	Yes	Compliant
A7.14 Cloud Service MFA Do all of your cloud services have multi-factor authentication (MFA) available as part of the service? Where your systems and cloud services support multi-factor authentication (MFA), for example, a text message, a one-time access code, notification from an authentication app, then you must enable this for all users and administrators. For more information see the NCSC's guidance on MFA at Multi-factor authentication for your corporate online services Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured. A lot of cloud services use another cloud service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA. Further guidance : Applying MFA to access cloud services Securing Your Cloud Services	Yes	Compliant

A7.16 Administrator MFA Has MFA been applied to **all** administrators of your cloud services? It is required that all administrator accounts on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	Yes	Compliant
A7.17 User MFA Has MFA been applied to **all** users of your cloud services? All users of your cloud services must use MFA in conjunction with a password of at least 8 characters. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	Yes	Compliant

A8.1 Malware Protection Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either: A - Having anti-malware software installed and/or B - Limiting installation of applications by application allow listing - for example, using an app store and a list of approved applications, using a Mobile Device Management (MDM) solution or C - None of the above, please describe Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B. • Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers, laptop computers • Option B - option for all in-scope devices • Option C - none of the above, explanation notes will be required. **CE Requirement**: You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the options listed below. • Anti-malware software (option for in-scope devices running Windows or MacOS including servers, desktop computers, laptop computers) • Application allow listing (option for all in-scope devices). Only approved applications, restricted by code signing, are allowed to execute on devices.	0: A - anti-malware software, 1: B - limiting installation of applications by application allow listing from an approved app store	Compliant

A8.2 Anti-malware Updates If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection? This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-malware software. You can use any commonly used anti-malware product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • be updated in line with vendor recommendations • prevent malware from running • prevent the execution of malicious code	Yes	Compliant
A8.3 Scanning Web Pages If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites? Your anti-malware software or internet browser should be configured to prevent access to known malicious websites. On Windows 11, MS Defender SmartScreen can provide this functionality. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • prevent connections to malicious websites over the internet.	Yes	Compliant

A8.4 Application Signing If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications? Some operating systems which include Windows, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications. **CE Requirement**: Only approved applications, restricted by code signing, are allowed to execute on devices.	Yes	Compliant
A8.5 Approved Application List If Option B has been selected: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you maintain this list of approved applications? You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use Mobile Device Management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, processes and training of staff. **CE Requirement:** • 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	Yes	Compliant
All Answers Approved Have all the answers provided in this assessment been approved at Board level or equivalent? An appropriate person will be asked to validate your answers when you submit your questions.	Yes	Compliant

0.1 Assessment Scope Have you verified that the scope for this CE+ assessment is the same as the scope for the applicant's CE verified self assessment (VSA)?	Yes	Compliant
0.2 Networks and Locations in Scope Provide a brief summary of the networks and locations in scope for this CE+ assessment.	For the external, the following IP address/domain was provided: 52.147.54.49, myknowledgemap.drayddns.com, 188.65.100.234, 188.65.100.235, 188.65.100.236, 188.65.100.237, 188.65.100.238 For the internal, local hostnames were used for authenticated scans. Network 192.168.1.x, 192.168.2.x	Compliant
0.3 Excluded Items If you have chosen to exclude any items, please provide a summary. For example: "Company Website is excluded because it is located with the cloud hosting provider, and as such not required, as per the Cyber Essentials Plus scoping requirements". If anything is excluded from the verified self assessment (VSA) in this CE+ assessment, then the VSA will need to be assessed again or the issue remediated within the prescribed 30 day window.	No items were excluded from the assessment	Compliant
0.4 Organisation Name What is the name of the applicant? Please provide the organisation's full name, to match that provided for their CE verified self assessment.	Myknowledgemap Limited	Compliant

0.6 CE VSA Date What date did the client pass their verified self assessment (VSA)? Provide the date that the client passed their verified self assessment. Cyber Essentials Plus must be completed within 90 days of the date of certifying for Cyber Essentials. The 30 day remediation period is inclusive of the 90 days. The CE+ assessment should be completed as close as possible to the date of the Cyber Essentials verified self assessment certification date, and sufficient time must be allowed for the remediation period within the 90 days. Extensions will only be granted in extreme circumstances. This does not include Christmas, Easter or other publicly notified holidays, the dates of which are static or known in advance.	2026-01-29	Compliant
0.7 CE+ Certification Date On what date/s was the CE+ assessment carried out? Please enter the date that the CE+ testing was carried out.	2026-03-05	Compliant
0.8 Scope Description What is the scope description that should appear on the CE+ certificate? The CE+ Scope must match the CE verified self assessment scope. This must be the same scope description as the organisation's CE verified self assessment certificate. If the scope is the whole organisation please enter "Whole organisation".	Whole organisation	Compliant
0.9 CE+ Test Platform Which CE+ Testing platform have you used, to run the email audit tests?	scan.cyberessentials.site	Compliant
0.10 Audit Location Was the CE+ audit carried out remotely or onsite?	Remotely	Compliant
0.11 Scanning Tool Which vulnerability scanning tool was used for the external and internal audit? Was it supplied by the Certification Body or the applicant?	Tenable Nessus Nessus Professional Supplied by Certification Body	Compliant

1.1.1 Scan Recommended Ports Have you scanned all external IP addresses for the client on all TCP and UDP ports?	Yes	Compliant
1.1.1.2 External Addresses Have you checked all external addresses against the networks and network devices in the CE VSA? You must check against the answers given in Section 2 of the VSA. Please list the quantity of external IPs tested. Where it is unclear how many external IP addresses were tested, the quantity should be clarified with the applicant.	Yes - 2	Compliant
1.1.2 Identify Critical and High Risk Vulnerabilities Did you identify any vulnerabilities that were scored 7 or higher on CVSS v3? The CVSS v3 score is taken from the base score, and temporal scoring should not be taken into account.	No	Compliant
1.1.3 Other Vulnerabilities For each Internet-accessible service you discover you must use the flow diagram in the Cyber Essentials Plus Test Specification document. Did the flow chart highlight any vulnerabilities to be identified as a fail?	No	Compliant
1.1.4 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant
2.1.1 Sample Device Identification Has a suitable sample of all end user devices, servers and IaaS instances been identified, in line with Cyber Essentials Plus scheme guidance? The sample must be selected by the CE+ assessor not the applicant. The sample must be 100% representative of the applicant's infrastructure.	Yes	Compliant

2.1.2 Details of Sampling You must provide a brief summary of your device sampling decision. Sample calculation data must be retained by the certifying body for the lifetime of the certificate.	Full client estate listed as follows: 18 x Windows 11 Pro 25H2 6 x Windows 11 Pro 24H2 Hypervisor: HP Proliant DL160 running Windows Server 2019 Standard (Hyper-V), Hosting: Domain Controller 1: Windows Server 2019 Standard, Domain Controller 2: Windows Server 2019 Standard, VPN Server: Windows Server 2022 Standard 1 x iPhone 13 (iOS 26) 1 x iPhone 14 (iOS 26) 1 x Samsung S25 (Android 16) 1 x Samsung Galaxy S22 (Android 16) 1 x Pixel 9 Pro XL (Android 16) 1 x Pixel 9a (Android 16) Sample selected: 3 Windows 11 Pro 25H2 3 Windows 11 Pro 24H2 - ALL NOW UPGRADED TO 25H2 SO sampling covered 1 Hypervisor: HP Proliant DL160 running Windows Server 2019 Standard (HyperV), 2 Hosted - Windows Server 2019 Standard 1 Hosted - Windows Server 2022 Standard 2 IOS 26 - now only 1 as consolidated 2 Android 16	Compliant
2.1.3 Authenticated Vulnerability Scan Has a full authenticated vulnerability scan been conducted on all devices in your sample?	Yes	Compliant
2.1.4 Internal Vulnerability Scores Did you identify any vulnerabilities for the tested devices that were scored 7 or higher against CVSS v3 scoring? The CVSS v3 score is taken from the base score, and temporal scoring should not be taken into account.	Yes	Compliant Assessor Notes: PASS - Now fixed

2.1.4.1 Internal Vulnerability Assessment Do any of the vulnerabilities identified in the internal vulnerability scan relate to issues for which a vulnerability fix has been made available by the software vendor (and was released more than 14 days ago)? Only vulnerabilities for which the vendor has released a vulnerability fix, and the client has failed to install the fix will cause a fail for this test. If you identify a high risk or critical vulnerability for which a vulnerability HAS NOT been released, you should answer NO to this question (which will result in a PASS for the client).	Yes	Compliant
2.1.4.2 List of Vulnerabilities Identified Please list the vulnerabilities for which a vulnerability fix has been released. When vulnerabilities have been identified, a summary list must be provided.	MS Office Dell Support assist MS Unquoted service paths .NET/ASP.NET Firefox Dell updates Visual studio 7ZIP Jetbrains NodeJS SQL server unsupported	Compliant
2.1.4.3 Applicant Addressed Vulnerabilities Has the applicant applied the vulnerability fixes to address the identified vulnerabilities? Please provide notes on what happened. If there are vulnerabilities identified, the client must remediate the vulnerabilities and the identified service must be retested by the CE+ assessor within the 30 day remediation window.	Yes	Compliant Assessor Notes: After notifying the client, they promptly resolved the highlighted issues and provided full evidence this had been completed, which was then verified.
2.1.5 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	After notifying the client, they promptly resolved the highlighted issues and provided full evidence this had been completed, which was then verified. Audit week	Compliant

3.1.1 Sample Confirmation Has a suitable sample of all end user devices, servers and IaaS instances that provide a user-interactive desktop been identified in line with Cyber Essentials Plus scheme guidance? You must use the same devices as picked in the sample for the authenticated vulnerability scan. VDI Servers, Virtual desktop servers, DaaS servers must be tested. All other servers do not need to be tested.	Yes	Compliant
3.1.2 Malware Protection Method For all end user devices in the sample, have you identified which method of preventing malware is in use? Please select every method that is in use at this organisation. The methods of preventing malware available are: A - having anti-malware software installed or B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications)	0: A - having anti-malware software installed, 1: B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications)	Compliant
3.1.3 Email Domains Which email domain/s have been tested? List the email domains.	@myknowledgemap.com	Compliant
3.1.4 Email Addresses How many individual email addresses have been tested? List the quantity per email domain tested.	5 x	Compliant
3.1.5 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant
3.2.1 Anti-Malware Software Installed For all devices in the sample relying on A - anti-malware software, is antivirus software installed on all end user devices or virtual desktop environments?	Yes	Compliant

3.2.2 Anti-Malware Software Testing For all devices in the sample relying on A - anti-malware software, determine whether the test files will work for the testing purpose. Test files must be used to test all anti malware software that uses signature based scanning. Determine whether the test files should be triggered using the software installed and then answer one of the following options: A - Test files work on all sampled devices B - Test files do not work on any device within the sample set C - Test files work on some of the devices in the sample set	A - Test files work on all sampled devices	Compliant
3.2.3 Email Delivery Test For all end user devices in your sample using anti malware software that should defend against the test files, have you tested email delivery by sending a test email with no attachments and verified the receipt of the email?	Yes	Compliant
3.2.4 Email Test Files Have you sent a suitable set of test files by email to each device in the sample (this should include "malware" test files and "executable" test files)? You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "exectuable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.	Yes	Compliant
3.2.5 All Attachments Blocked Were all of the email attachments containing malware blocked by all of the end user devices in your sample? You should answer No if you were able to open any of the malware attachments.	Yes	Compliant

3.2.6 Test Files - Email - Binary Files Test Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the email attachments containing executable (non-malware) files? You should answer no if you were able to open an executable attachment without a warning or opportunity to cancel.	Yes	Compliant
3.2.7 Test Files - Web Delivery For all devices in your sample using anti malware software that should defend against the test files, have you attempted to open both "executable" and "malware" test files using a web browser? You must use a standard user account for this test (not an administrator account). You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "exectuable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.	Yes	Compliant
3.2.8 Test Files - Web - Malware Blocked Test Files - Web - Malware Blocked Were all of the downloads containing malware blocked by all of the end user devices in your sample? If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.	Yes	Compliant
3.2.9 Test Files - Web - Malware Warning Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the downloads containing executable (non-malware) files? If the browser prompts the user to decide whether to "run" or "save as" then this is classed as a pass for this test.	Yes	Compliant

3.2.12 Anti-Malware Software Updated For all devices in your sample using anti malware software, have you confirmed that the software has been updated in accordance with the vendor's configuration instructions?	Yes	Compliant
3.2.13 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant
3.3.1 Application Allow List Testing For all devices in the sample relying on B - certificate based application allow listing, have you confirmed that the list of trusted root certificates are provided by the operating system manufacturer?	Yes	Compliant
3.3.3 Unsigned Executables For all devices in the sample relying on B - certificate-based application allow listing, has it been confirmed that an unsigned executable and executables with a certificate that does not chain to a trusted certificate will not run on the end user device?	Yes	Compliant
3.3.4 Code Signing For all devices in the sample relying on B - certificate-based application allow listing, have you confirmed that operating system policy settings are in place to ensure that code signing applies to all of the applicable file formats to the relevant device?	Yes	Compliant
3.3.5 All Devices Protected Are you satisfied that every device in your sample is protected from malware using one of the methods described in Q3.1.2? If NO, please add notes to explain why.	Yes	Compliant
3.3.6 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant

4.1.1 Cloud Sample Identification Provide a list of all cloud services used by the applicant that provides an authentication service. A list of all cloud services tested must be provided. Any cloud service that has been declared in the verified self assessment as not providing MFA does not need to be tested. Where a cloud service authenticates through another cloud service, only the authentication service needs to be tested in the sample. (For example if an organisation authenticates 10 x cloud services via Azure SSO, only the Azure would need to be tested).	Zendesk, Sendgrid, Mailgun, Microsoft Azure, Clickup, Clockify, ElasticSearch, Microsoft Office 365, Cloudinary, Intruder, Statuscake, Crowdstrike, Claude.	Compliant
4.1.2 Check MFA configuration of sampled users Were all users challenged with an MFA prompt prior to a successful login using an incognito browser or untrusted device? Notes required -result must be recorded for each cloud service tested. Observe the users trying to log in with their standard user accounts to each cloud service that they use. This test is carried out against the user accounts belonging to the user that would use each sampled device to carry out their daily tasks. If the user is also an administrator for that service, ask them to login with their administrator account using the same method. Answer No if an MFA prompt wasn't provided and the user successfully logged into the cloud service.	Yes	Compliant

4.1.3 Confirmation that all cloud services have been checked Have all cloud services as listed in the verified self-assessment been checked to confirm that MFA has been applied? All cloud services listed in the verified self-assessment that have not been declared as 'not providing MFA in A7.15' must have their authentication method checked. All authentication methods must have been checked with one Administrator and one standard user. If any of the cloud services were not checked as part of the sample an additional administrator and / or user must be checked. Where an organisation does not have any standard users, please provide notes to detail this. Where an organisation does not have any standard users, please provide notes to detail this.	Yes	Compliant
4.1.4 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant
5.1.1 Confirm Standard User Account Details Has every user account on the sampled devices confirmed to you they are logged in with a Standard User account? This test is carried out on all sampled end user devices and/or desktop environments with the account/s that the standard user/s that would normally use that device would use for their daily tasks. You should check the name associated with each account to confirm the sample is true and representative.	Yes	Compliant
5.1.1.1 Quantity of Accounts Provide the quantity of accounts tested per sampled device.	2	Compliant
5.1.2 Confirm Account Separation For all end user devices and the accounts, when observing a standard user attempting to run a process, were they asked to enter administrator credentials? If the user was not prompted for an additional login to a separate administrator account, answer No and describe what happened.	Yes	Compliant

5.1.3 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	N/A	Compliant
6.1.1 Executive Summary Provide a summary of your findings here – ideally one or two paragraphs to give a flavour of the report. Briefly mention locations and scope. You should also highlight any notable anomalies and action points, pointing the reader to the appropriate section of the report for more information.	The internal scans brought back minimal vulnerabilities with a CVSS of 7.0 and above which were promptly remediated, the client keeps on top of all updates and stands by the 14 day patching windows. A pass has been awarded. The assessment concluded that the configuration of the organisations external network and workstations were setup to a secure standard which adhered to the Cyber Essentials requirements. Malware Protection solutions were in place on all assessed devices, and up to date, and cloud solutions were each configured with appropriate authentication solutions. Web based downloads were also protected against. When reviewing the patch levels for the assessed end user devices, only a few patches were identified during the auditing on the sampled hosts. Overall a good audit to which the client should be awarded the cyber essentials certification	Compliant
6.1.2 Lead Assessor Details A Lead Assessor must review and sign off the findings of this assessment and confirmed that they agree with them. Please provide the name of the Lead Assessor for this assessment. If you are a Lead Assessor, please enter your own name (you will not require a second person to sign off the assessment). A Lead Assessor is an assessor that holds one of the qualifications in List A of the Assessor Requirements document. A Lead Assessor must review and agree with the findings of any CE+ assessments issued by a CB. If the person carrying out the assessment is already a Lead Assessor, you will not require a second person to sign off the assessment.	Euan Czerepaniak	Compliant