InfoSec GOVERNANCE LTD

A GUIDE TO STARTING YOUR CYBER ESSENTIALS PLUS CERTIFICATION

IASME GOVERNANCE

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

IoT SECURITY ASSURED

Starting your Cyber Essentials Plus Journey

The Cyber Essentials Plus certification involves several tests which are described below.

1. External vulnerability scan of your external IP address(es) and any Infrastructure as a Service (IaaS) systems
2. Authenticated vulnerability scan to check patching on devices, including any IaaS systems
3. Anti-malware software protection verification on all sampled devices
4. Email malware check via email
5. Web browser malware check
6. Multi-factor authentication verification
7. Account separation verification

If you pass all these tests without any failures, you will be granted a Cyber Essentials Plus certification, any failures of the above tests must be resolved within 30 days of the report finding.

Do you meet the requirements for certification?

- ✓ Already achieved the Cyber Essentials Basic certification within the last 3 months
- ✓ Or; aim to have completed Cyber Essentials Plus certification within 3 months of achieving Basic certification
- ✓ Your Plus certification is based upon the same criteria/scope of the basic self-assessment certification.

It is advised that a date is booked as soon as possible after passing the basic self-assessment certification to ensure you have enough time to pass.

Please note that if you are over the 3-month window, you will need to re-take and pass your Cyber Essentials basic certification again at additional cost.

Do you meet the requirements for certification?

- ✓ You allow and will perform any infrastructure related changes to ensure that a credentialed vulnerability scan using local administrator/root privileges can be carried out on all devices.

- ✓ Are you running an anti-malware solution which utilises signature-based scanning, this does not include net generation products such as Crowdstrike. See https://isgovern.com/blog/cyber-essentials-and-crowdstrike-what-you-need-to-know/ for more information.

Review the terms and conditions of the certification and assessment before proceeding with certification, this can be found at: https://isgovern.com/terms-and-conditions-cyber-essentials-plus/

Stage 1: Arranging the audit & supplying information

Once you have checked that you are ready to proceed with Cyber Essentials Plus, you will need to confirm with InfoSec Governance that you would like to go ahead. We will provide a formal quotation for you to review and accept, once agreed the process can start.

If InfoSec Governance did not perform your Cyber Essentials Basic certification, we will require a copy of your self-assessment report and Cyber Essentials basic certification before we can continue with the audit.

Stage 1: Arranging the audit & supplying information

We will require your external IP address information and a point of contact for the audit.

We will also need verification of any external services you manage and update, such as web servers, cloud-based servers, Infrastructure as a Service etc.

Once we have the necessary information, a date will be agreed between both parties and a decision will be made whether the audit is conducted onsite at your office or performed remotely via Microsoft Teams.

Stage 2: Configuring the environment for scanning

As part of the audit, InfoSec Governance will perform a credentialed vulnerability scan of your computers and servers, to check that they are patched and do not have any vulnerabilities above CVSS 7.0.

If an onsite audit is being performed, we will use our own copy of Nessus Professional and our own laptop. However, if this is being performed remotely, we will require you to install our copy of Tenable.io on all sample set devices.

Stage 2: Configuring the environment for scanning

If performing an onsite scan, Nessus requires several infrastructure changes before we can obtain the information we need, please liaise with your IT department as soon as possible to ensure that these are implemented before the audit date.

Configuring Windows environments - https://isgovern.com/blog/how-to-setup-your-windows-environment-for-a-nessus-credentialed-patch-scan/

Configuring MacOS environments - https://isgovern.com/blog/how-to-setup-your-macos-environment-for-a-nessus-credentialed-patch-scan/

Once the changes have been made, it is advised that a test scan is performed to ensure results are as expected. We have an article showing how to do this here: https://isgovern.com/blog/how-to-perform-a-nessus-credentialed-scan-for-cyber-essentials-plus/

Stage 3: Audit day

On the day of the audit an InfoSec Governance Cyber Essentials Assessor will go over the process and what will be expected of the day.

The audit will start with the performing of the credentialed vulnerability scan, once this has been completed, the remaining show and tell tests will be conducted. This will involve checking devices to ensure anti-malware is in place and up to date, devices are patched and up to date, as well as checking mobile devices and performing web browser and email tests.

If at any point there is a failure of the assessment, the assessor will raise the point and talk about how this can be resolved. If it can be resolved during the audit, it will be retested at the same time, otherwise you will have up to 30 days to remediate any changes.

Stage 3: Audit day – External vulnerability scan

We will perform a vulnerability scan against your external infrastructure that is within scope of the assessment. For example, external Gateway IP addresses, managed web servers, Infrastructure as a Service.

This scan will scan all TCP and UDP ports, from 1 – 65535. We will check to ensure that if any web portals are found, that default credentials have been changed.

If you manage any servers, such as your web site or cloud-based servers, these will be included.

Stage 3: Audit day – Authenticated vulnerability scan

We will perform an authenticated vulnerability scan against your internal devices, this will check to make sure that there are no unsupported applications installed as well as ensuring that your computers are up to date and have no security vulnerabilities.

Findings will be based against any vulnerabilities that are classified as CVSS 7.0 or above and are identified as high risk or critical.

Any unsupported or high/critical security vulnerabilities found will result in the failure of the assessment and will be subject to 30 days to remediate and be certified.

Stage 3: Audit day – Verification of anti-malware on devices

We will check your devices to ensure that anti-malware software is installed and in place and is being kept up to date. This included any cloud-based systems which are managed by the business.

The assessor will check to ensure that updates have been applied recently and that the product is up to date. This will also include mobile devices which access business data. This will include checking to make sure devices are up to date and to check that there are no untrusted system/user certificates are in place

Stage 3: Audit day – Malware check via browser download

As part of the audit, we will request users involved in the audit to navigate to a website and download certain file types. This will be performed on each browser installed on their computer.

If the user can download and execute a file within “two-clicks” this will be classified as a failure of the certification.

Note: Prompting the user to open/save will be classified as a pass.

Stage 3: Audit day – Malware check via email delivery

We will email you several files to the users involved within the audit and will check to see what emails they receive.

Once the files have been received, we will record the findings to see if the user can run/execute any attachments.

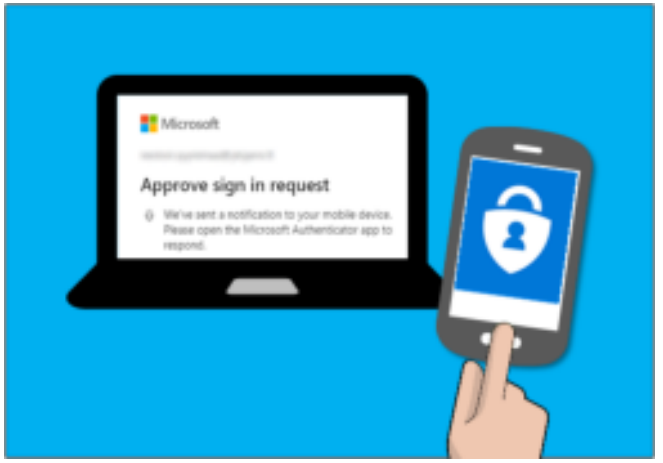
Stage 3: Audit day – Multi-factor authentication validation

The verification of multi-factor authentication being applied on all cloud-based services (such as Microsoft 365, Google Workspace) is implemented for Administrative and user-based accounts.

The auditor must see a multi-factor authentication prompt to show that it is enabled.

This test will be tested against **all** users **within** the sample set of the audit.

- Administrative accounts **must have** MFA enabled from January 2022
- Standard account must have MFA enabled **from** January 2023



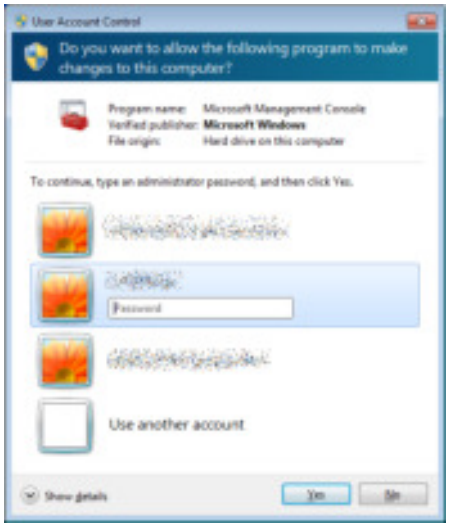
NCSC multi-factor guidance can be found here: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

Stage 3: Audit day – Account separation validation

The verification of account separation for the current running user. This is to ensure that the user is not running as an administrative/root level user.

The auditor will be looking for a prompt to switch to an administrative/root level account to perform an action.

This test will be tested against **all** users **within** the sample set of the audit.



Stage 4: Findings

Once the audit has been completed. You will be provided with a findings report, if you are failing any tests within the assessment, you will be informed of which areas and what needs to be actioned to become compliant.

Any remediation work will need to be completed and verified within 30-days of finding. Failure to achieve this will result in additional costs.

Stage 5: Certification

Congratulations, if the audit and findings came back with no failures and our assessor is happy with the audit, you will be sent a final findings report with your certification.

You will also be sent a branding guidelines document and official logos to use on your marketing material.

Appendix: What to look out for

- Ensure that all devices within the business are up to date, including firmware for remote access devices
- Ensure that all users are running as standard level user accounts
- Ensure that obsolete SSL protocols, such as SSLv2, SSLV3 are disabled across all systems
- Ensure that your cloud-based systems which are being used have multi-factor authentication enabled
- Ensure that your cloud-based systems which are managed by the business have anti-malware protection installed and up to date
- Ensure that browsers installed are patched and up to date
- Ensure that browsers do not allow users to download files without being prompted for an action

Get in touch

InfoSec Governance is an information security company who help businesses protect themselves from cyber based threats.

Contact us today to discuss your requirements and see how we can help you stay safe and secure.

InfoSec Governance Ltd
The Work Place, Heighington Lane, Aycliffe Business Park, Newton Aycliffe, DL5 6AH

Call us : **0330 043 0826**
Email us : **info@isgovern.com**
Visit us : **https://isgovern.com**

IASME GOVERNANCE

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

IoT SECURITY ASSURED

InfoSec Governance
The Work Place, Heighington Lane, Aycliffe Business Park, Newton Aycliffe, DL5 6AH
0330 043 0826 | info@isgovern.com | https://isgovern.com