brigantia

Cyber Essentials Plus - Certification audit

Outlining the process for the Cyber Essentials Plus

Cyber Essentials Plus Process

CYBER ESSENTIALS CERTIFIED PLUS

What is Cyber Essentials Plus?

Cyber Essentials Plus is an audited version of the Cyber Essentials basic, which is a self-assessed online questionnaire. The Plus consists of:

- Audits all controls of Cyber Essentials basic.
- An onsite or remote audit (depends on company size & complexity).
- External vulnerability scan.

Getting a Cyber Essentials Plus Quote

Each quote is bespoke to the company. This is based on company size, complexity and internal mark-up. It's quick and easy to get a quote from us, just contact your Brigantia Account Manager. We will then reach out to you to arrange the audit date.

Pre-Audit

We have created a checklist which should be thoroughly looked through before the date of the audit. By following the document it hugely increases your chances of successful certification. You can find the checklist and other documents here:

https://www.brigantia.com/cyber-essentials-plus-audit-preparation

Prior to Audit

Your audit will be booked by your Account Manager at Brigantia and you will receive a google invite with a 'hangout link' from your auditor, to confirm the date and an email containing this document, the assessment checklist and the consent form. You will need to ensure a dedicated point of contact is available for the audit.

The next steps are as follows:

1. Complete the consent form and send back to your Account Manager
2. Review the pre-audit checklist and action requirements
3. Your auditor will be in touch prior to the assessment to check that this has been completed and will confirm scope and required detvices for sampling.
4. You will then be provided access to a shared google drive for your organisation containing the Qualys agents and installation guide.
5. We recommend installing Qualys agents at least 3 days prior to your audit date.

Day of the Audit

You will need to join your assessor on the 'google hangout' link on the calendar invite. Your auditor will then go through the following:

During the Audit

There are several steps to a Cyber Essentials Plus audit, regardless of being done remotely or onsite. The steps of the audit are:

External Vulnerability Assessment

1. The assessor will confirm your external IP addresses highlighted in consent form and perform a vulnerability scan. The scan is looking for any known vulnerabilities present, open ports in both the TCP and UDP range and what services are being advertised to the internet.
2. Any score of 6.9+ CVSS or higher must be resolved to pass (usually close port or update service).

Contact Brigantia

Internal Vulnerability Assessment

This will be the assessment on the end user device sample list that your auditor will confirm with you prior to audit. All sample end user devices must be available on the day of the audit.

A sample of devices are selected to be included in the assessment - the sample size is determined by how many variants you have of each Operating System in use (e.g. Win 10 Pro Version 20H2, 21H1, 21H2, MacOS Catalina, Big Sur, Monterey). The sample selected needs to ensure that all versions are selected, but will only be a max of 5 for each version.

During this stage we will require you to share the screen of these devices via the google hangout link.

End users may need to be present for the audit if you are unable to remotely access their devices to complete the screen share.

The auditor will complete the following with the assistance of the dedicated point of contact for the audit.

1. **Send fake viruses and inbound malicious emails to the sample of devices selected to be in scope for the assessment from both the web (e.g. Chrome) and native mail add.**
2. **Check the latest patching for in-scope machines. Any out of date patches to operating systems and software must be updated (subject to critical and high CVSSv3 score and date of release).**
3. **Review sufficient malware protection is in place for all machines.**
4. **Do a review of any in scope mobile devices eg Phones and Tablets to confirm they meet the Cyber Essentials requirements. This will include:**
    - **Checking the Operating System is supported**
    - **Ensure device is not jailbroken**

If anything from the Cyber Essentials Plus needs actioning, the auditor will liaise with the most relevant technical person within the company and the dedicated point of contact for the audit.

Post-Audit Audit Passed

Now the audit is complete the auditor needs to write up the full report which depending on if any remediations are needed, can take 1 - 3 working days.

After the report is finished, the auditor will issue your official Cyber Essentials Certificate and send the report, certificate and badges over to you.

Audit Failed

If there are any failure points during the Cyber Essentials Plus Audit, you will be given the opportunity to remediate these on the day and we will retest. If you are unable to complete remediation on the day, we can retest within 30 days of the original audit date as long as this is still within the 90 day window from Cyber Essentials Certification.

The auditor will retest the failing point and once passed will issue the report and certificates within 1-3 working days as above.

Access to certificates

Access to the certificate and report will be in the CyberSmart dashboard under the relevant years Cyber Essentials Plus alongside the Cyber Essentials Plus certified badges.