SoConnect CyberSmart

CYBER ESSENTIALS PLUS PRE-AUDIT CHECKLIST

A checklist you can run through to help prepare your organisation before a Cyber Essentials Plus audit.

Pre-audit checklist to ensure a smooth audit

- Confirm all software (including Adobe, Java, etc) is fully up to date on all devices including servers. (To do this you need to download and install Nessus Professional. They have a 7-day trial version of Nessus Professional for a credentialed patch scan). Please DON'T INSTALL NESSUS MORE THAN 7 DAYS BEFORE THE AUDIT.
- Remove all rarely used software on each device – old browsers such as Firefox are a common issue.
- For devices running macOS please enable file sharing. This option can be found in 'System preferences --> Sharing'. Please note, this only required if you're scanning over a network.
- For the devices running Windows 10, the startup type set to "Manual" for the Windows service “RemoteRegistry". This option is opened by typing “services” in the search bar on Windows 10 home screen.
- For devices running Windows 10, the following registry value also needs to be created. This option is opened by typing "regedit" in the search bar on the Windows 10 home screen.

  1.Hive and key path:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
  2. On System, right click then select New --> DWORD (32-bit) Value / REG_DWORD
  3. Value name: LocalAccountTokenFilterPolicy
  4. Value data: 1 (decimal)
- Ensure all devices including laptops have up to date AV engines and signature files – preferably using an enterprise management dashboard app.
- Ensure all executable attachments are prevented from being delivered to your email provider.
- Ensure the AV plugin for each browser in use has been activated and updated.

CYBER ESSENTIALS PLUS

0333 240 1824

SoConnect CyberSmart

The auditor will ask you to provide the following

- Administrator-level user account access will be required to perform the scan.
- A list of all devices (Firewalls, Servers, PCs, laptops, workstations, tablets and mobile phones) that are in scope with details of their current operating system. Please note, if you're using Windows 10 a registry edit will be required for these devices to allow the scans to run.
- An email account for each device. For example, if you have users using Windows 10, build 1909, 2004 and 20H2, we will require an email account that can be used on each device.
- A consent form will be required prior to starting the onsite test and this will be prepared once the visit dates have been agreed.

The testing process includes the following tests:

- Confirmation of the devices to be tested.
- Scanning of devices to identify vulnerabilities using Nessus Professional scanning software – requires details of the admin credentials for each device.
- Checking the installation and configuration of anti-virus software.

> DOING ALL THE PREPARATION WORK WILL ENSURE A SMOOTHER AUDIT, MINIMAL DISRUPTION TO YOU AND YOUR STAFF, PLUS THE ADDED BONUS OF A HAPPY AUDITOR - WHICH IS ALWAYS A GOOD THING.
>
> GLEN - HEAD OF CYBER AUDIT

CYBER ESSENTIALS PLUS

0333 240 1824