ebook

The changes to Cyber Essentials and what they mean for businesses

FLOW
the smart choice

security

FLOW
the smart choice

Contents

What is Cyber Essentials?

A government-backed scheme to increase the baseline security levels of companies and organisations. At the simplest level, the standard ensures that companies are taking basic steps to increase the overall security of their business-critical systems.

There are two levels Cyber Essentials Standard (CES) and Cyber Essentials Plus (CEP). CES is a self-assessment where a series of questions are asked and the applicant must answer. CEP is the audited version of this where specific items are tested in various ways.

The National Cyber Security Centre (NCSC) evaluate the needs and basic measures companies and organisations can take to improve security. This information is filtered down to IASME which have the role of being the sole Cyber Essentials Partner to maintain standards and oversee the running of the scheme on a day-to-day basis. By being a point of contact for certification bodies (CBs) who carry out the assessment process. Certification bodies assess companies and organisations to a set of criteria issued to them by IASME.

Details of Cyber Essential

Details of Cyber Essentials Plus

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

What has changed in 2022?

The question set “Beacon” released April 2021, and more recently “Evendine” released 24th of January 2022 heralded the largest changes to the scheme since its inception. Changes to the boundary of scope have highlighted what the scheme aims to secure now that many companies and organisations have altered the way they work i.e. cloud-based or hybrid environments.

Based on the latest information supplied relating to the Evendine questions set we have recorded the changes, what this means for businesses and what they can do to prepare.

Requirements of Cyber Essentials - NCSC
Details of the changes - IASME

Note

Our SaaS based managed service built on Palo Alto's Prisma Cloud, for Cloud Security Posture Management (CSPM) is a cloud agnostic service that provides broad-based support for all contemporary cloud technologies.

It enables organisations to manage their cloud debt by staying on top of misconfigurations, potential vulnerabilities, threats and compliance violations, all within a single integrated platform.

See the value of a CSPM managed service

cloud

Change 1: All cloud services are in scope

This relates to any cloud services under configuration responsibility of the applicant upon which any organisational data or services are held or processed. The applicant is responsible to ensure they are configured with all the Cyber Essentials controls being met. The following definitions have been made; Infrastructure as a Service (Iaas), Platform as a Service (PaaS) and Software as a Service (SaaS).

What can be done to prepare?

Begin to create an inventory of the services utilised identifying the cloud service type and audit existing security measures and controls implemented so far. Who implements the controls will vary from service to service (IaaS, PaaS and SaaS). Here are the 5 key controls to consider

- Firewalls
- Secure Configuration
- User Access Controls
- Malware Protection
- Security Update Management.

Change 2: Home workers

Anyone working from home for any amount of time is now classified as a “home worker”. Any devices used by these staff members to access organisational data will result in those devices falling within the scope and needing to comply with requirements set out.

Home (e.g. broadband) routers used to provide internet access that are supplied by an Internet Service Provider (ISP) will not fall within the scope. The boundary shifts to the host-based software firewall on that given device i.e. Laptop or Desktop.

What can be done to prepare?

Ensure that all devices used to access company information have their software firewalls enabled and are generally compliant with Cyber Essentials and Cyber Essentials Plus requirements.

Change 3: Multifactor authentication

Multifactor authentication needs to be used to provide additional protection to administrator accounts used to connect to cloud services like O365. The password element of the multi-factor authentication approach must have a password length of at least 8 characters, with no maximum length restrictions.

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

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

This will also eventually encompass all accounts, including standard users but this is not due to be a requirement until 2023.

What can be done to prepare?

Enable MFA as an option wherever and whenever possible.

Change 4: Updates to password-based authentication requirement

Changes have been made here to further improve this area to protect against Brute-Force style attacks.

When using passwords, one of the following protections should be used to protect against brute-force password guessing:

- Using multi-factor authentication
- Limiting the rate of unsuccessful or guessed attempts.
- Locking accounts after no more than 10 unsuccessful attempts

Technical controls are used to manage the quality of passwords. This will include one of the following:

- Using multi-factor authentication in conjunction with a password of at least 8 characters, with no maximum length restrictions.
- 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

Change 5: Thin clients

For companies and organisations utilising a thin client estate/set-up to access servers facilitating virtual desktop environments. These have now clearly been brought into scope with explicit mentioning within assessor guidance.

What can be done to prepare?

Ensure these devices comply with all Cyber Essentials and Cyber Essential Plus controls.

Example

In an “in scope” Cisco device authenticated through RADIUS linked to Active Directory; where previously a single shared account “CiscoAdmin” may have been used by Cisco’s global TAC for support or troubleshooting by their task force; requirements are now for EVERY ENGINEER involved in accessing the devices to have their OWN SEPARATE admin accounts e.g. MShaheedAdmin, JDelacroixAdmin, etc. multiplied by number of engineers. This extends also to any other vendor accounts of this type and any MSP support accounts must be treated in the same way. Single “shared” accounts with forensic attribution monitored by surrounding system as has been prevalent globally to date are NOT compliant for the purposes of Cyber Essentials. There must be separate, personal accounts. This has been confirmed by the authorative sources at IASME.

Change 6: Account separation

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).

This also extends to shared administrative accounts for support purposes the company providing 3rd party support needs to facilitate separate named accounts for any individual conducting work on an applicant company or organisation.

What can be done to prepare?

Admin accounts should be standalone that would require you to login/enter a set of credentials to conduct an administrative task. Creating separate named admin accounts will be enough to meet this requirement.

Change 7: Device unlocking requirements

Biometrics or a minimum password/pin length of 6 characters must be used to unlock a device where applicable.

What can be done to prepare?

An added layer of security to implement biometric authentication i.e. fingerprint or face detection and pin/password of at least 6 characters should be provided.

Note

The previous dispensation for e.g. “Local” attack vectors or “Low complexity” attacks, allowing them to be re-calculated against temporal or environmental scoring; has been removed.

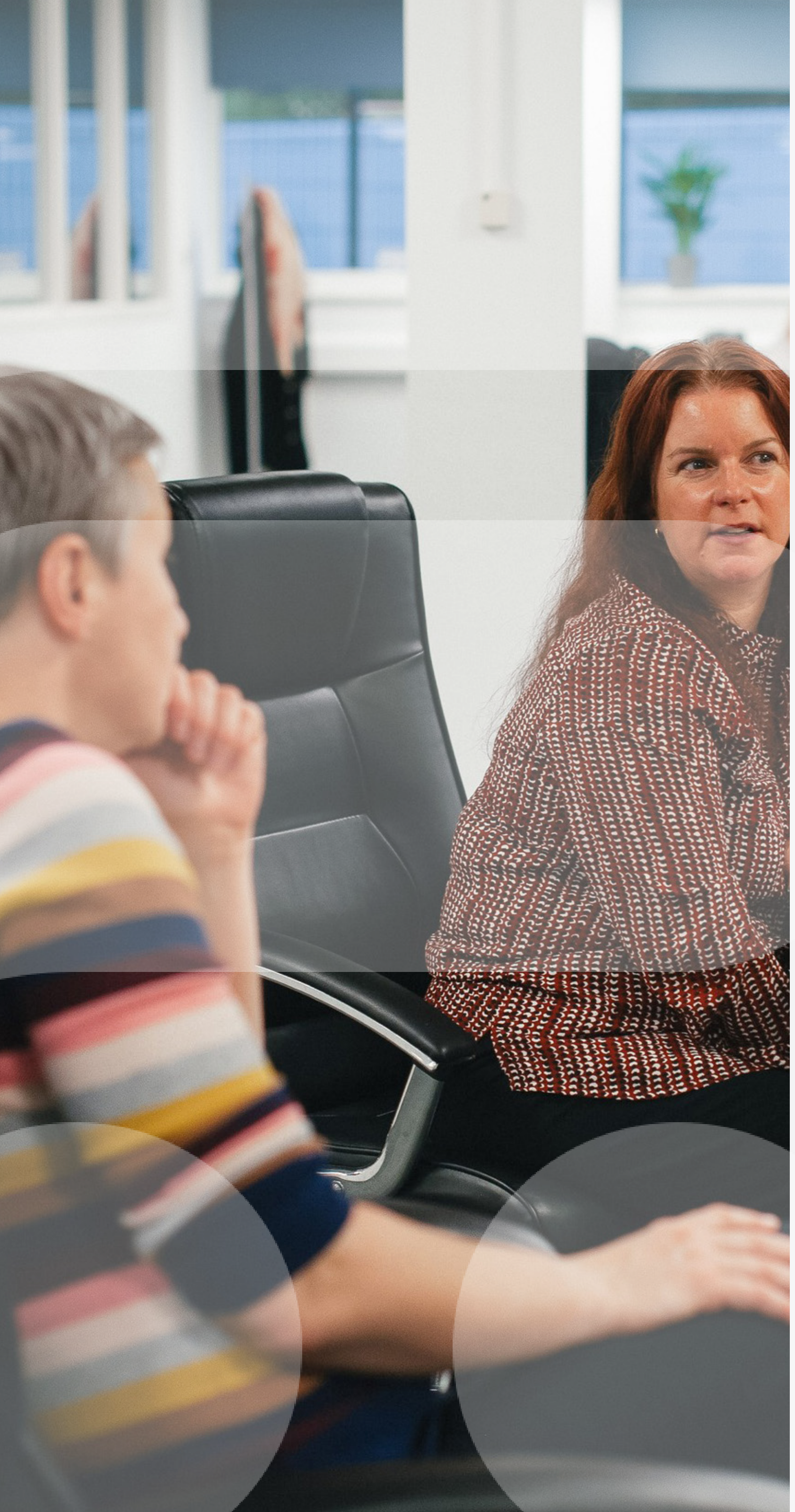
Change 8: All ‘critical’ and ‘high’ vulnerabilities and unsupported applications

All security-related updates must be applied within a 14-day patch window. These are updates for “Critical” and “High” vulnerabilities in accordance with the CVSS v3 marking scheme. None may be present if there is a patch/mitigation available.

Unsupported software removed from scope will be marked for compliance from January 2023. Its continued presence will result in an automatic failure. Often treated with the “compensating control” mitigation which will also no longer be an option as of now.

What can be done to prepare?

- Ensure all software is licensed and supported
- Remove any unsupported software or remove the devices hosting them from scope by using a defined ‘sub-set’ that prevents all traffic to/from the internet.
- Have automatic updates enabled where possible.
- Apply updates, including any manual configuration changes required to make the update effective, within 14 days of an update being released, where;
    - The update fixes vulnerabilities described by the vendor as ‘critical’ or ‘high risk’.
    - The update addresses vulnerabilities with a CVSS v3 score of 7 or above.
    - There are no details of the level of vulnerabilities the update fixes provided by the vendor.



Change 9: All servers are now in scope

All server types (specifically only those that are in-scope of Cyber Essentials as per NCSC and IASME scoping documents) including virtual servers on a "sub-set" of an assessment where the scope has been defined as "whole organisation" are now in scope. This also means that for any company carrying out Cyber Essentials Plus these devices will also be subject to testing.

What can be done to prepare?

Ensure these devices comply with all Cyber Essentials and Cyber Essential Plus controls.

Change 10: Changes to the self-assessment

Along with a general change of wording for existing questions plus some new inclusions. There have been some changes to ensure devices within scope are supported by their respective vendors. This requires more evidence than previously to be provided by the applicant. For example A2.6 will now require device make and model of all Laptops/Desktops/Tables that may be in scope.

This is to allow the assessor to determine whether the device can support the security updated firmware versions. It is NOT a requirement to provide the actual firmware details but application, web browser, AV and O/S version details ARE now required.

What can be done to prepare?

Collect the make model and software version details for all mobile, workstation and server devices in advance of starting to fill out the CE questionnaire. It is advised that the burden of evidence on the applicant side has increased exponentially in the case of e.g. global enterprises that may never have had this information so plan as far ahead as this requirement may need.

This also has an impact on the time it takes to mark self-assessments in that markings that would previously have taken around an hour may now take a day or more. Please ensure you leave adequate time from initial submission for marking before any deadlines approach.

How Flow can support you

CNS, part of the Flow group, are one of the largest cyber certification bodies in the UK. We can provide you with the support and expertise you need to handle these changes and achieve the Governance Certifications.

With skilled network penetration testers, we can advise on solutions or implementations to address any points of failure, to ensure compliance and optimal security.

The smart choice

Flow provide efficient and secure solutions to organisations allowing them to do business in confidence, with seamless transition and without fear of a cyber-security attack.

Our expertise

datacentre

networks

cloud

security

T: (0) 1442 927 996
info@flowtransform.com
flowtransform.com