Keyfort™
Keyfort for IT Engineering & Cloud Computing Services

Cyber Essentials overview to accreditation

Definition

Cyber Essentials is the product of the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF). It is therefore a government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors. The scheme addresses five key controls that, when implemented correctly, can prevent around 80% of cyber-attacks.
At the point of completing good housekeeping by way of the 5 controls, organisations can then apply and pay for Cyber Essentials accreditation.

5 key controls

1. **Secure configuration**
   By ensuring your computers and network devices are configured properly, you can identify systems or databases that you no longer need or use. You will have the opportunity to reduce your overall storage and bandwidth consumption, as well as reducing the level of inherent security vulnerabilities.
2. **Boundary firewalls and internet gateways**
   Using boundary firewalls to monitor traffic to your server(s) enables you to better understand and manage your bandwidth requirements, potentially allowing you to renegotiate your hosting costs, as well as blocking attackers and external threats.
3. **Access control and administrative privilege management**
   Managing access control and administrative privileges erodes the opportunity for staff to install time-wasting software on to their computers, as well as removing the insider threat.
4. **Patch management**
   Keeping on top of software patching and licensing makes your company more productive, as well as more secure. Patches often improve the performance of the products they apply to, and remove issues that slow down employees, such as crashes and poor performance caused by congested networks.
5. **Malware protection**
   Implementing appropriate malware protection has its obvious security advantages, but an often overlooked hidden benefit is the time and cost savings that result from avoiding devices being out of action.

CYBER ESSENTIALS

Cyber essentials assessment framework also provides these additional outcomes:

- Drive business efficiency
- Save money
- Improve productivity by streamlining processes

Implementation of Cyber Security Control is carried out as a self-assessment questionnaire (SAQ). Honesty is the key here; honesty with yourself and honesty within your team. By highlighting risks in the SAQ and implementing effective steps to mitigate risk, you will be further strengthening your organisation's resilience and defence against cyber-attack. The requirements for passing are that you score overall highly within each particular section/control. Hence it is possible to pass without being 100% on the questionnaire. When filling out the questionnaire, it is recommended that you include as much detail as possible.

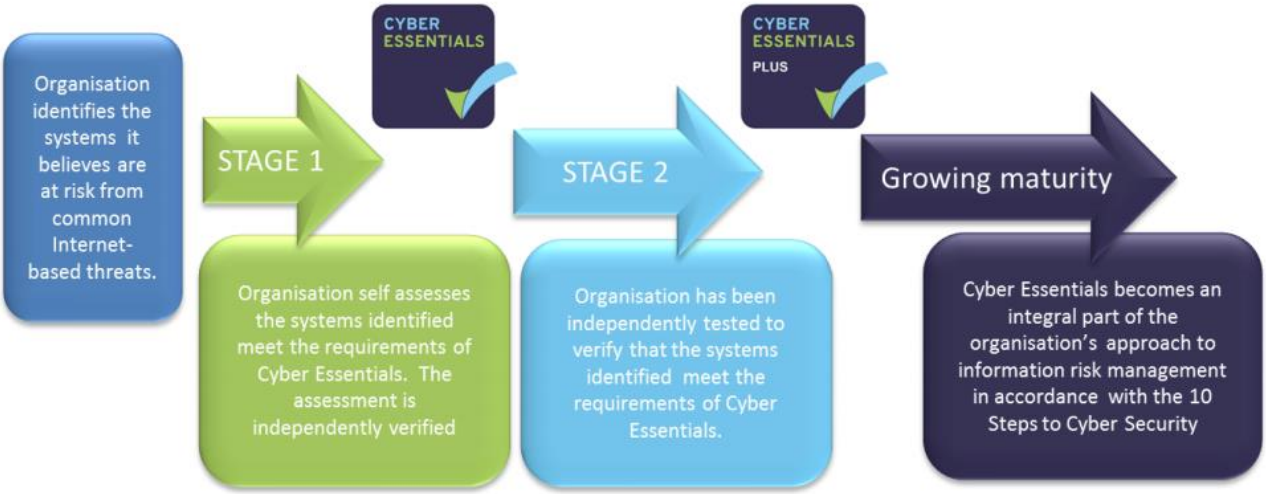
Cyber Essentials Certification

Whether or not you achieve certification status to the scheme, the Cyber Essentials controls provide a level of protection that you need to implement in your organisation to protect it from the vast majority of cyber-attacks, allowing you to focus instead on your core business objectives.

It is important to recognise that certification only provides a snapshot of the cyber security practices of the organisation at the time of assessment, while maintaining a robust cyber security stance requires additional measures such as a sound risk management approach

By using this mechanism organisations of any type and size can use this to demonstrate to customers, investors, insurers and other stakeholders that they have taken essential due diligence precautions to secure their information against the majority of cyber risks.

Having implemented the Cyber Essentials controls the following options are available:



CYBER ESSENTIALS

Types of Accreditation

Cyber Essentials certification is awarded on the basis of a verified self-assessment Questionnaire (SAQ). An organisation undertakes their own assessment of their implementation of the Cyber Essentials control themes via a questionnaire, which is approved by a senior executive such as the CEO. This questionnaire is then verified by an independent Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded. This option offers a basic level of assurance and can be achieved at low cost.
It is recommended to conduct a vulnerability scan to assess cyber security readiness.

Cyber Essentials Plus includes all of the assessments for the Cyber Essentials certification but offers a higher level of assurance through the external testing of the organisation's cyber security approach. Plus accreditation also includes an additional internal scan and an on-site assessment of infrastructure, specifically focusing on workstations and mobile devices.
Given the more resource intensive nature of this process, Cyber Essentials Plus will cost more than the foundation Cyber Essentials certification.

Keyfort™ Cyber Security Services

1. Advice, assistance and guidance to completion of Cyber Essentials SAQ. (Day rate)
2. Vulnerability scanning and reporting (per block of 32 IP addresses).
3. Vulnerability scanning, reporting and engineer on-site risk assessment.
4. Coordination of Cyber Essentials certification via accreditation body. (P.O.A)