Cyber Essentials Audit & Microsoft Secure Score Evaluation

Introduction – Cyber Essentials

The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level "commodity threat". It lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organisations should have in place.

Properly implementing the Cyber Essentials scheme and leveraging the Microsoft stack effectively will protect against the vast majority of common internet threats.*

In 2015, the average cost of breaches to large businesses that had them was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme.**

**(UK) National cyber security strategy 2016-2021*
***2016 Government Cyber Health Check and Cyber Security Breaches Survey*

Cyber Essentials / Cyber Essentials Plus

Cyber Essentials (level one) follows a self-assessment questionnaire (SAQ). Through the completion of this the candidate organisation demonstrate how they have achieved compliance with the 5 technical control areas. The SAQ is submitted to a certification body who review the submission against the standard.

Cyber Essentials Plus (level two) offers a higher level of assurance to the candidate organisation. The protections you need to have in place are the same, in addition to satisfactory completion of the SAQ additional validated vulnerability testing is carried out in line with the standard.

Introduction - Microsoft Secure Score Evaluation

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken

Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 security centre, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Secure Score Evaluation

Report on the current state of the organization's security posture.
Improve their security posture by providing discoverability, visibility, guidance, and control.
Compare with benchmarks and establish key performance indicators (KPIs).
Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

Introduction – ADM Computing

ADM is an IT services and support provider. We have been established since 1984 and are a Microsoft Gold Partner with over 250 technical Microsoft certifications, Sophos Platinum Partner and WatchGuard Gold Partner as well as holding other leading vendor accreditations. ADM are ISO/IEC: 27001, ISO:9001, ISO:14001 and Cyber Essentials Plus accredited.

ADM have an in-house Cyber Security team, including two certified Advanced Cyber Essentials Practitioners. This plus our compliance with Cyber Essentials Plus means that ADM are well placed to assist businesses and organisations in the process of gaining compliance with Cyber Essentials.

ADM's Cyber Security practice have developed security audits for businesses. These audits will test the candidate organisation's infrastructure within the scope intended for the certification. This will follow the requirements for Cyber Essentials – the UK minimum standard for business in Cyber Security.

Project approach

ADM Computing take an audit & recommendation / remediation / certification three phase approach to Cyber Essentials. This approach considers the requirements for completion of the official questionnaire (undertaken by ADM, assessed by the Certification Body). Our approach can be summarised as follows:

Cyber Essentials self-assessment questionnaire

- Phase one - Audit & Secure Score Evaluation
    - Pre-audit conference call
    - Onsite audit
    - Remote collation of audit data
    - Compilation of questionnaire and remediation report
- Phase one - Recommendation - reports will be provided that include:
    - Summary of all actions that are needed to attain compliance
    - Supplementary reports covering IT estate, such as user accounts, registered devices, admin users, deployed software (and versions)
    - Separate report detailing Secure Score Evaluation and recommendations.
- Phase two – Remediation
    - Advice on remediation requirements where needed
    - Remediation works undertaken by candidate organisation or other third party
    - ADM can give additional resource to assist with remediation if required (at additional cost dependent on requirements)
- Phase three – CE Certification
    - ADM to review remediation actions and complete questionnaire with updated evidence
    - Sign-off of questionnaire by candidate organisation and submission to certification body by ADM

Annual renewal (CE only)

An annual renewal is required, ADM can discuss the requirements for this once the initial certificate is awarded.

Additional notes

- ADM will require full access to the servers and infrastructure of the candidate organisation.
- The candidate organisation will need to supply copy of IT policies including user management and system change management (exact requirements will be discussed during the audit)
- ADM will require access to your Microsoft 365 tenant for the purpose of producing the Microsoft Secure Score Evaluation.

Project Scope

This Cyber Essentials engagement is based on a scoped certification as follows:

- Engagement scope
  - Cyber Essentials (level one)
  - The single specified candidate organisation, its staff, corporate managed desktops / laptops and security infrastructure
  - Organisation has 50 users or less
  - Single Microsoft Active Directory and/or Microsoft Azure Active Directory
  - Systems containing critical / sensitive business data
  - Microsoft 365 tenant

- Out of scope
  - All other areas of the candidate organisation beyond the in-scope outlined above
  - Cyber Essentials Plus (level two) - subject to additional scoping and quotation
  - Implementation of Secure Score recommendations.