Protect your organisation against cybercrime

What is Cyber Essentials? Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against common cyber threats.

Why is it important? Cybercrime is a worldwide issue that affects all organisations, of all sizes and in all sectors. It is vital all organisations focus on basic cyber hygiene, to ensure they are better protected from the most common cyber threats. The Cyber Essentials Scheme has been developed as part of the UK's National Cyber Security Programme and in close consultation with industry.

Whats involved in Cyber Essentials?

The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the Scheme, in order to defend against the most common and unsophisticated forms of cyber-attack.

There are two levels of certification that can be achieved.

Level 1 Cyber Essentials

Requires the organisation, with help from a practitioner, to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.

Level 2 Cyber Essentials Plus

This covers the same requirements as Cyber Essentials but tests of the systems are carried out by an external certifying body, using a range of tools and techniques.

What are the benefits of the Cyber Essentials accreditation?

- Reduces your chance of a cyber attack by 65%
- An accredited recognition that your organisation complies with best practice in IT security
- You get £20K cyber insurance included with your certification (if your turnover is under £20m)
- Provides reassurance for you & your key stakeholders that IT security is properly provisioned
- Cyber Essentials is increasingly becoming a pre-requisite when bidding for new business.

ramsac
the secure choice

The 5 Cyber Essentials key controls

Cyber Essentials defines a set of five key security controls, which, when properly implemented, will better protect organisations, small and large, from attacks using software and techniques which are freely available on the open internet.

1. **Boundary firewalls and internet gateways**
   Good set up of devices designed to prevent unauthorised access to or from private networks.

2. **Secure configuration**
   Systems are configured in the most secure way.

3. **Access control**
   Only those who should have access to systems have access, and at the appropriate level.

4. **Malware protection**
   Virus and malware protection is installed and up-to-date.

5. **Patch management**
   The latest support version of applications is used and all neccesary patches have been applied.

How does Cyber Essentials Plus differ from Cyber Essentials Basic?

While the Basic accreditation helps establish your recommended security baselines, it is not verified by a certifying body, whereas the Plus accreditation is and ensures that your written and technical policies are functioning effectively in practice.

CYBER ESSENTIALS PLUS

How can ramsac help you achieve Cyber Essentials and Cyber Essentials Plus?

ramsac's trained Cyber Essentials specialists conduct a gap analysis to assess your network and IT practices against the Cyber Essentials standard. We provide a gap report, review the findings with you, and agree on actions and any necessary project work to prepare for external certification. Once ready, we refer you to a suitable third-party certifier.

For Cyber Essentials Plus, we guide you through the entire process, coordinating with the certifying body and creating a tailored schedule. We conduct a pre-assessment to ensure readiness, support you during the external assessment, and keep you updated throughout. Once all criteria are met, we'll handle the certification process for you.

Find out more

For more information on Cyber Essentials Plus and how you can get your organisation certified please contact ramsac on Tel: **01483 412 040** email: **info@ramsac.com**

ramsac
the secure choice