Loss Prevention Standards – Cross Classes

Cyber Security:

Cyber Essentials Accreditation

Version: 1.1
Date: 14th February 2024

This document provides guidance on Cyber Essentials, a UK Government-backed scheme designed to help organisations recognise cyber-crime threats and how to assess their ability to protect against them.

AVIVA

Cyber Security Essentials - Accreditation

Introduction

Cyber-attacks and infiltrations aimed at all sizes of business and at individuals, have increased dramatically. Cyber criminals are constantly changing their tactics, making it difficult for organisations to protect their systems and data. Ransomware and phishing attacks have become particularly predominant and remain significant threats. This is due in part to the increase in remote working, as employees access their organisation's network from home and this arrangement creates new vulnerabilities.

The Business Continuity Institute (BCI), in conjunction with the British Standards Institution publish their Horizon Scan Report annually. This report has been an indicator as to what businesses had seen as the biggest impacts on their organisation in the previous 12-months, and what their biggest concerns were for the coming year. The picture that this report provides is one where cyber-attacks were previously a minor issue, but over the last few years they have become a large threat across most organisations. The 2022 Report shows cyber-attacks and data breaches as the threats with the greatest likelihood to happen and the greatest potential impact. This clearly shows the concerns businesses have.

Benefits of Cyber Essentials Accreditation

There can be many reasons to obtain accreditation. With cybercrime becoming a major threat to businesses across the globe, securing your IT and data and keeping your security measures and procedures up to date, will not only be essential for yourself, but could also give you a competitive edge in your market. It also helps to support your reputation and assure your data protection policies.

Having the accreditation:

- Gives you certified cyber security, from a UK Government-backed scheme.
- Provides you with a clear picture of your organisation's cyber security level.
- May assure your customers that you are working.
- Means your organisation may attract new business given that you have cyber security measures in place.

Some customers, going forward, may even require Cyber Essentials certification from their suppliers.

Cyber Essentials Accreditation

Cyber Essentials is a UK Government-backed scheme designed to help recognise the threats and assess an organisation's ability to protect against them.

The scheme will help businesses avoid, or at least minimise, the impact on their business of:

- Phishing attacks
- Malware
- Ransomware
- Password guessing
- Network attacks

Obtaining Cyber Essentials Accreditation

To help businesses protect themselves against cybercrime Aviva recommends the Cyber Essentials Certification, at a minimum, and ideally the Cyber Essentials Plus Certification (see below).

An organisation must first carry out a self-review of their security policies and technical controls, in key areas such as user access controls, anti-virus tools, firewalls, and software updates to show they meet the requirements before they can be certified.

An independent certification body then examines the organisation's self-assessment. If any areas need improving, this must be completed before they can be certified.

The certification must be renewed each year. This includes re-evaluating the controls annually to maintain compliance with the standards. Regular reviews will help ensure the 'defences' in place continue to be effective against evolving threats.

Cyber Essentials Plus

For those organisations who want to improve cyber security further, there is Cyber Essentials Plus Certification. This is the highest level of certification provided by the Cyber Essentials scheme.

An independent Certification Body conducts an onsite audit to verify the implementation of security controls within the organisation's IT setup.

In addition to the self-assessment, Cyber Essentials Plus includes a technical audit to verify the results. An assessor would select a representative sample of devices to audit. They also analyse vulnerability scan results.

The Plus Certification proves an organisation has externally validated protective security measures in place and not just self-attested policies. It provides increased confidence for customers and stakeholders about an organisation's cyber defences.

The certification must be renewed annually just like the standard Cyber Essentials Certification.

How Does Cyber Essentials Work?

Cyber Essentials sets out five controls which can be implemented immediately to strengthen cyber defences:

1. Firewall - use a firewall to secure an internet connection.
2. Settings - choose the most secure settings for devices and software.
3. User Privileges - control who has access to data and services.
4. Protections - protect against viruses and malware.
5. Updates - ensure the latest updates for devices and software are installed, these include security updates.

As cybercrime is becoming quite common and cyber criminals can be anything from an individual… to an organised group or state, with attacks from anywhere in the world, it is essential to protect data and sensitive information for:

- ✓ Your own organisation.
- ✓ Your customer's.
- ✓ Your supplier's.

With Cyber Essentials accreditation, proof and assurance can be provided to business partners, to existing and prospective customers and to any other interested parties, that your organisation is proactively guarding against cyber-attack. The implemented protections facilitate ongoing monitoring, ensuring compliance with the necessary security measures and keeping them current… in the fight against cybercrime.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- ActionFraud

Additional Information

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

14th February 2024

Version 1.1

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.