

An intro to: Cyber Essentials Certifications

Part of our Digital
Foundations programme



What we'll be covering today

- ✓ What is it?
- ✓ Why might you need it?
- ✓ Which certification is for me?
- ✓ How do you go about getting it?
- ✓ Demystifying some of the language
- ✓ Some tools to help assess where you are (hands on)
- ✓ Other useful resources





What is it?

- ✓ Government backed scheme helping organisations guard against the most common cyber threats and demonstrate their commitment to cyber security

<https://www.cyberessentials.ncsc.gov.uk>

- ✓ Renewable annually (and updated periodically)

- ✓ Delivery partner – IASME Consortium

<https://iasme.co.uk/cyber-essentials/>

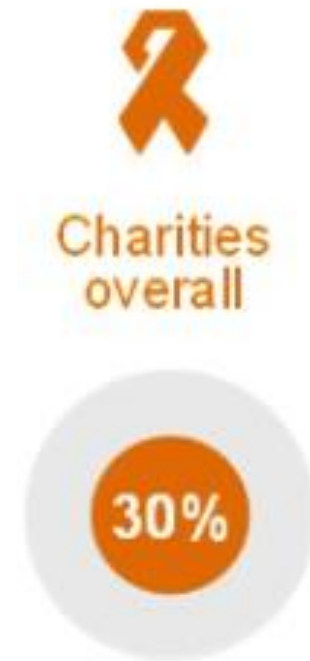


Some context about Cyber Attacks

Question:

In the annual DCMS survey 2022, what percentage of charities reported having a cyber security breach in the last 12 months?

26% 30% 62% 76%



Cyber Security Breaches Survey 2022

Updated 11 July 2022

Which of the following breaches or attacks has your organisation identified in the last 12 months?	Businesses	Charities
Phishing attacks	83%	87%
Other impersonating organisation in emails or online	27%	26%
Viruses, spyware or malware (excluding ransomware)	12%	11%
Denial of service attacks	10%	2%
Hacking or attempted hacking of online bank accounts	8%	6%
Takeover of organisation's or users' accounts	8%	6%
Ransomware	4%	4%
Unauthorised accessing of files or networks by outsiders	2%	2%



Data protection – GDPR principles

1. Process lawfully, fairly and in a transparent manner
2. Collect for specified, explicit and legitimate purposes
3. Only keep what is adequate, relevant and limited to what is necessary
4. Store accurate information and keep up to date
5. Retain only for as long as necessary
6. Process in an appropriate manner to maintain security



Requirement scenarios

1. Accreditations e.g. Lexcel – Legal Practice Quality Mark (Law Society)
2. Funding – referenced / encouraged in central & local government commissioning / funding guidance and NHS Data Security & Protection Toolkit (Information Governance compliance)
3. Cyber Insurance



Feedback from a local Mind

✓ Cyber Essentials Basic

- Initially quite a challenge, as the self-assessment questionnaire used a large amount of technical terminology
- Good opportunity to brush up on the latest terminology and ensure we were using the correct IT security practices
- Great for highlighting key areas of IT security in use and any that may not be hitting the mark and need improving
- Needed invaluable assistance from the Superhighways Team during the year
- Certification was a requirement for Cyber Insurance from our insurance provider



Feedback from a local Mind

✓ **Cyber Essentials Plus:**


- Uses the original self-assessment portion and combines it with an external assessment
- The external assessment portion was assisted by National Mind's IT support partner
- Self-assessment portion included many of the same questions with some updates due to extra requirements for CE Plus.
- Greatest challenge was organising the testing of various staff and trustee devices, based on the operating system – some required follow-up tests if any program was not fully updated
- CE Plus was recommended to us by National Mind





Cyber Essentials levels

- ✓ **Cyber Essentials** – an online self assessment verified by a qualified independent assessor
 - ✓ Includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation & have less than £20m annual turnover (terms apply)



Pricing Structure		
Micro Organisations	0-9 Employees	£300 +VAT
Small Organisations	10-49 Employees	£400 +VAT
Medium Organisations	50-249 Employees	£450 +VAT
Large Organisations	250+ Employees	£500 +VAT





Cyber Essentials levels

- ✓ **Cyber Essentials Plus** – self assessment plus a hands on technical verification audit (price on application from accredited suppliers – see IASME website as before)
- ✓ Check to see if you can access support via the [Funded Cyber Essentials Programme](#) – for eligible organisations including charities

Requirements documentation



National Cyber
Security Centre
a part of GCHQ



Cyber Essentials:
Requirements for IT
infrastructure v3.1

[Download
here](#)



What you should do first?

1. Establish the **boundary of scope** for your organisation, and then determine what is in scope within this boundary
2. Review each of the **five technical control themes** and the controls they embody as requirements
3. Take the necessary steps to ensure that your organisation meets every requirement it needs for the scope you have determined



What's in scope

1. Bring your own Device (BYOD)
2. Home working
3. Wireless devices
4. Cloud services
5. Accounts used by 3rd parties
6. Devices used by 3rd parties
7. Web Applications

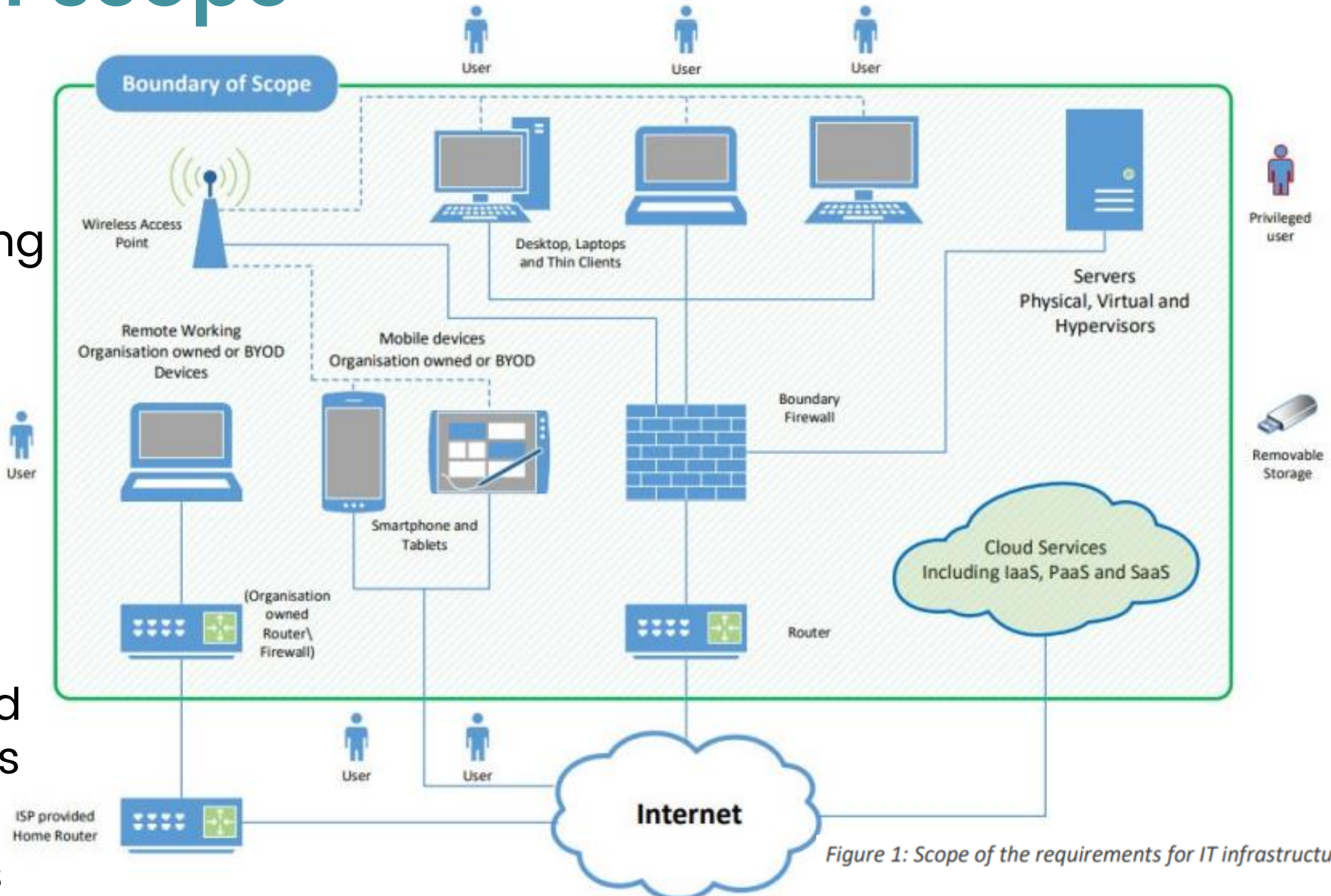


Figure 1: Scope of the requirements for IT infrastructure

Five technical control themes



Firewalls



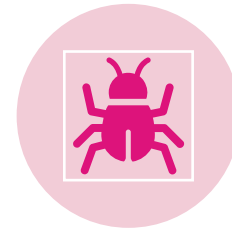
Secure
configuration



Security
update
management



User access
control



Malware
protection



Readiness tool



**From painters
to pet groomers...**

...a simple tool
to help you prepare
your business for
Cyber Essentials.

Government of Wales

 In association with
National Cyber
Security Centre

 **CYBER
ESSENTIALS**

[Go to the
Readiness
tool](#)



NCSC Active Cyber Defence tools

The NCSC provides a range of free cyber security tools and services to charities as part of the Active Cyber Defence (ACD) programme.

✓ Mail Check

Helps organisations assess their email security compliance and adopt secure email standards which prevent criminals from spoofing your email domains

<https://www.ncsc.gov.uk/information/mailcheck>

✓ Web Check

Web Check helps you find and fix common security vulnerabilities in the websites that you manage.

<https://www.ncsc.gov.uk/information/web-check>



NCSC Active Cyber Defence tools

✓ **Early Warning**

Early Warning helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds.

<https://www.ncsc.gov.uk/information/early-warning-service>

✓ **Exercise in a box**

Toolkit of realistic scenarios that helps organisations practise and refine their response to cyber security incidents in a safe and private environment.

<https://www.ncsc.gov.uk/information/exercise-in-a-box>

✓ **Instant Security Checkers**

Instant check and feedback: Email Security Check, IP & Web Address Check and Web Browser check.

<https://basiccheck.service.ncsc.gov.uk>



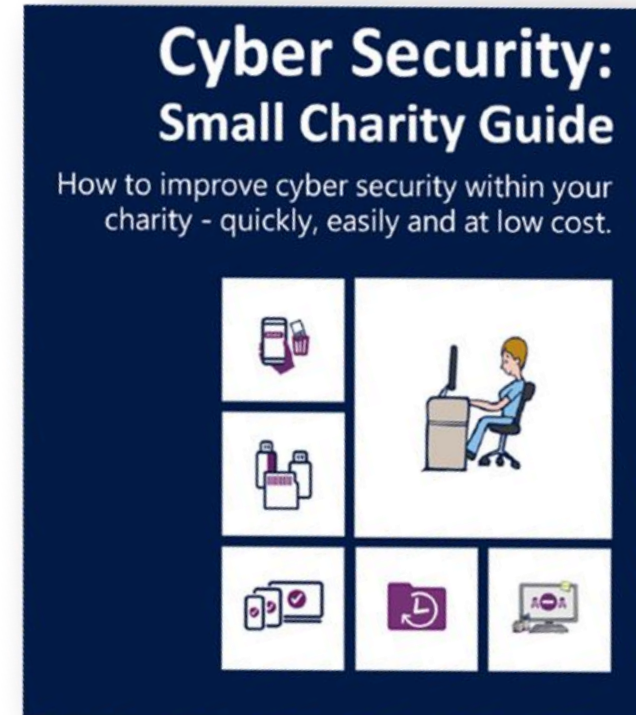
Other useful resources

The National Cyber Security Centre's
5 quick, simple, free or low cost steps

1. Backing up your data
2. Protecting against malware
3. Securing your mobile devices
4. Password best practice
5. Avoid phishing attacks

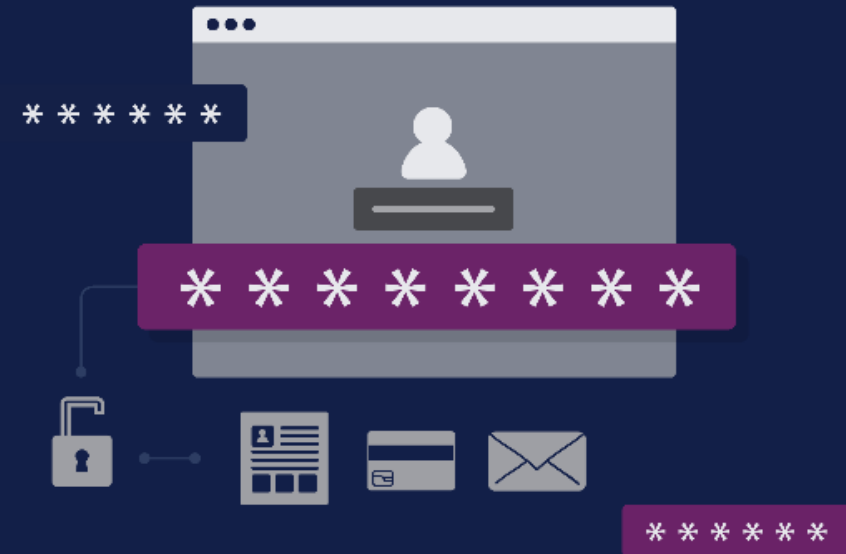
[Download the full guide](#)

[Download the infographic](#)



NCSC training

Creating strong passwords



[Visit intro & full series](#)



Digital Foundations programme

There are many ways we can help small community organisations make sound choices about the digital tools and technology they use.



Communications made easy

Raise your profile using digital tools to engage supporters and fund your future

[Read more »](#)



Digital basics

Work and collaborate online using free and affordable digital tools and technology

[Read more »](#)



Websites for communities

Put your website at the heart of your charity or community organisation's story

[Read more »](#)

[Find out more about the Digital Foundations programme](#)



About Superhighways

Providing tech support to small local charities in London for over 20 years

- ✓ Support
- ✓ Training
- ✓ Consultancy
- ✓ Digital inclusion
- ✓ Datawise London
- ✓ See all services
- ✓ E-news sign up





Thank you for listening

KATE WHITE

COLIN CREGAN

info@superhighways.org.uk

@SuperhighwaysUK

#DigitalFoundations