# CYBER ESSENTIALS

CYBER ESSENTIALS

IASME CONSORTIUM

Registered Partner

www.ccnlimited.com

# IMPROVE SECURITY

An IASME-licensed Cyber Essentials certification body will independently verify your security status.





**The Cyber Essentials scheme is a world-leading, cost-effective assurance mechanism for organisations of all sizes to help demonstrate to customers and other stakeholders that the most important basic cyber security controls have been implemented.**

Cyber Essentials offers a sound foundation of basic cyber hygiene measures that all types of organisation can implement and build upon. The UK government believes that implementing the scheme's five basic controls can significantly reduce an organisation's vulnerability to the most common cyber attacks.

The Cyber Essentials scheme was designed in consultation with small and medium-sized enterprises (SMEs) to ensure it is light-touch and achievable (including certification) at low cost. As there are two options, Cyber Essentials and Cyber Essentials Plus, organisations have flexibility in the level of assurance they wish to gain and how much they want to spend to achieve that level. However, certification is just a 'snapshot' of an organisation's cyber security practices. To maintain that security, the organisation must regularly conduct risk assessments and review its existing controls, updating and patching them as new threats arise.

Cyber Essentials offers the right balance between providing assurance of an organisation's commitment to implementing cyber security while keeping the approach simple and the costs low. However, the scheme is not designed for protecting the organisation from more advanced, targeted attacks; to address those threats, organisations will need to implement additional measures as part of their security strategy, such as those outlined in ISO 27001, the international standard for information security management.

**"Around 80% of cyber attacks could be prevented"**



## Background

In 2012, the UK government launched '10 steps to cyber security'. In 2013, it published 'Small businesses: what you need to know about cyber security', to help organisations figure out whether they were truly managing their cyber risks, and encourage boards and senior executives to take ownership of those risks and account for them in the organisation's overall risk management programme.

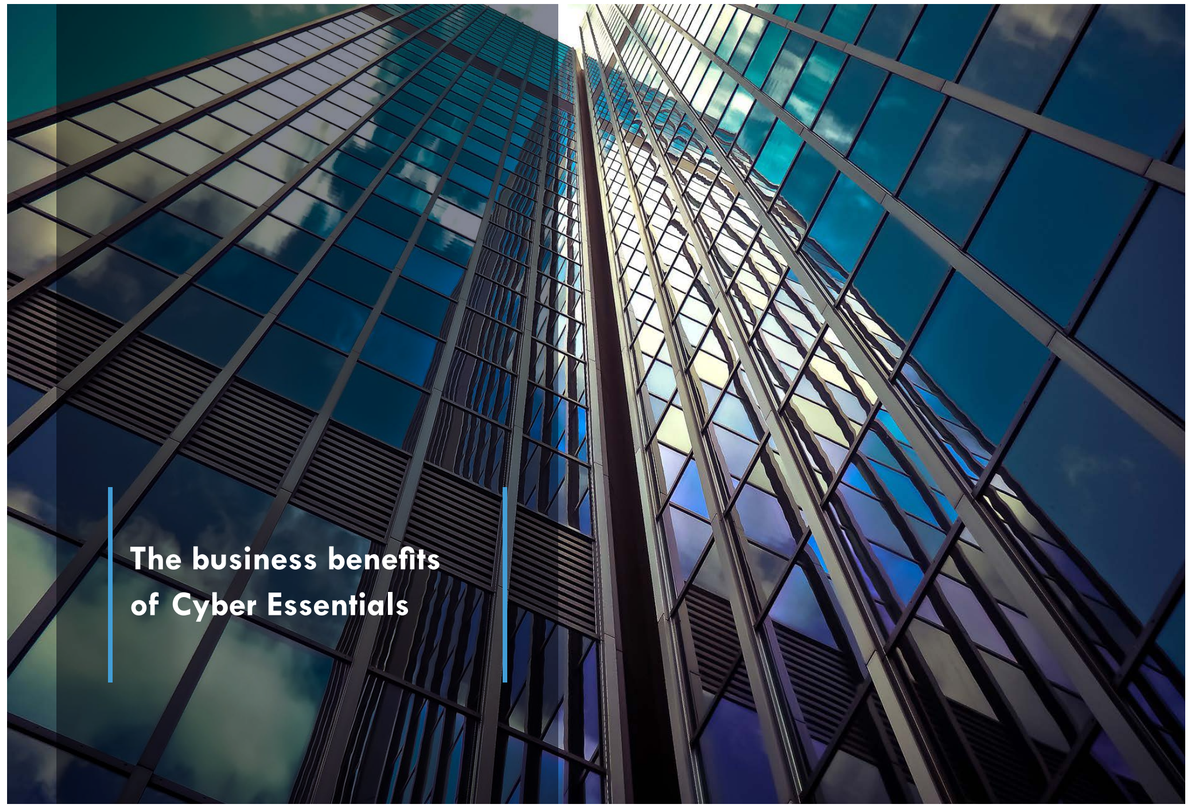
However, although more organisations were adopting stronger security measures, the government found that a number of them were not applying certain security controls, leaving them vulnerable to threats – including older and less sophisticated threats.

Cyber Essentials was developed to plug this gap with a straightforward approach to core cyber security principles. The scheme was formalised in November 2013.

## Why should you achieve Cyber Essentials certification?

CYBER ESSENTIALS

Keep reading



# The business benefits of Cyber Essentials





## The benefits of achieving Cyber Essentials certification

According to the UK government, "Around 80% of cyber attacks could be prevented" with just five basic security controls.

Even without achieving certification, the scheme's controls provide a basic level of protection that can ward off the vast majority of cyber attacks, allowing you to focus on your core business objectives.

Properly implementing the controls has the additional advantage of driving business efficiency throughout the organisation, saving money and improving productivity.

However, achieving certification brings extra benefits. For instance, it can reduce insurance premiums; a 2015 government publication, 'UK cyber security: the role of insurance in managing and mitigating the risk', found that most insurers believe that "Cyber Essentials would provide a valuable signal of reduced risk when underwriting cyber insurance for SMEs, allowing them to use a reduced question set and informing their decisions to underwrite", and that "participating insurers operating in the SME insurance sector have agreed to build reference to the Cyber Essentials standard into their cyber insurance applications, and will look to simplify the application where accreditation has been achieved by the applicant."

### Protected against around 80% of cyber attacks

Implementing the five controls correctly will help you protect your organisation.

### Demonstrate security and help secure the supply chain

Achieving Cyber Essentials certification will help you demonstrate your commitment to protecting any data you hold, including that of your customers and suppliers.

### Increase chances of securing business

Cyber Essentials certification will help boost your reputation and give you a better chance of winning contracts.

### Drive business efficiency

You will be able to focus on your core business objectives while knowing that you are protected from the most common cyber attacks.

### Work with the UK government and MOD

Cyber Essentials will give you the opportunity to work with the UK government, while Cyber Essentials Plus will also give you the opportunity to work with the Ministry of Defence (MOD).

### Potentially reduce cyber insurance premiums

Cyber insurance agencies look more favourably on organisations that have achieved Cyber Essentials certification.

# The five controls and certification process



## What are the five controls?

The Cyber Essentials controls are an excellent starting point for protecting your organisation from the more common and freely available hacking tools. They cover the following key areas:

### Choose the most secure settings for your devices and software

Web server and application server configurations play a key role in cyber security. Failure to properly configure your servers can lead to a wide variety of security problems.

Computers and network devices should be configured to minimise the number of inherent vulnerabilities and provide only the services required to fulfil their intended function. This will help prevent unauthorised actions and ensure that each device publicly discloses only the minimum information about itself.

A scan can reveal opportunities for exploitation through insecure configuration.

### Use a firewall to secure your Internet connection

Firewalls are designed to prevent unauthorised access to or from private networks, but both hardware and software need to be properly set up to be fully effective.

Boundary firewalls and Internet gateways determine who has permission to access your system from the Internet and allow you to control where your users can go. Antivirus software may help protect the system against unwanted programs, but a firewall helps keep attackers or external threats from getting access to your system in the first place. To adjust the security provided, much like any other control function, you can make changes to the firewall 'rules'.

### Control who has access to your data and services

Even though it is tempting, for convenience's sake, to give many users administrator rights, it is important to minimise access to your data and services to reduce the risk of a criminal hacker being presented with open access to your information. Obtaining administrator rights is a key objective for criminal hackers, as this allows them to gain unauthorised access to applications and other sensitive data.

User accounts, particularly those with special access privileges, should be assigned only to authorised individuals, managed effectively, and provide the minimum level of access to applications, computers and networks.

### Keep your devices and software up to date

Any software is prone to technical vulnerabilities and, once discovered and shared publicly, cyber criminals rapidly exploit them if they are not properly patched or updated.

Regularly updating software and operating systems will help fix any known weaknesses. Doing this as quickly as possible is crucial to mitigating the risk of a criminal hacker exploiting them first.

### Malware protection

It is important to protect your organisation from malicious software (or 'malware'), which will seek to access files on your system.

Malware can wreak havoc by stealing confidential information, damaging files or, in the case of 'ransomware', locking files and preventing access unless you pay a ransom.

Protecting against a broad range of malware (including computer viruses, worms, spyware, botnet software and ransomware) and including options for virus removal will protect your computers, your important documents and your privacy.

## How we certify organisations to the Cyber Essentials and Cyber Essentials Plus schemes

Although non-IASME certification options exist, none of them offer the same level of independent verification and stakeholder assurance that the official option does.

Thousands of organisations have certified to the scheme, with many more achieving certification every day, giving them a competitive edge as well as other benefits.

IASME Consortium®

## Certification process

### Cyber Essentials

A self-assessment option that demonstrates you have key controls in place to help protect against a wide variety of common cyber attacks. The certification process has been designed to be lightweight and easy to follow.


**Cyber Essentials**

### Cyber Essentials Plus

A more advanced level of the scheme that includes all steps of a Cyber Essentials application, as well as an external scan, an internal assessment of the five security controls and an internal vulnerability scan on a sample of workstations and mobile devices. Cyber Essentials Plus is a requirement for organisations looking to work with the MOD.


**Cyber Essentials Plus**



## Certification process stages

### Scope

Certification can apply to an organisation's full enterprise IT or just to a subset. Either way, the scope needs to be clearly defined before the certification process can get underway.

You must define the boundary of the scope in terms of the function managing it, the network boundary and the physical location. The requirements apply to all devices and software that:

- Accept incoming network connections from untrusted Internet-connected hosts;
- Establish user-initiated outbound connections to devices via the Internet; and
- Control the flow of data between any of the above devices and the Internet.

Any organisation-owned mobile and remote devices, and user-owned devices that access organisational data or services are in scope.

Wireless devices (including wireless access points) are also in scope if they can communicate with other devices via the Internet. Cloud services are also within scope if it is practicable to apply the Cyber Essentials requirements to them.

Commercial web applications created by development companies (rather than in-house developers) that are publicly accessible over the Internet are also in scope.

### CCN Pre-Assessment Security Audit

As part of the certification process and scope, CCN will carry out a detailed pre-assessment security audit on your network which will include a review of your staff awareness methodology and internal security processes.
On completion of the assessment, you will be advised on any changes to the network setup that may be required, along with any internal processes you may wish to implement prior to proceeding with the SAQ.

### SAQ

Once the organisation has determined its scope, the next step to certification is to complete a self-assessment questionnaire (SAQ). This comprises 70 questions across 8 sections (including the 5 control areas); all sections must be passed.

We will assess your responses and the scope you have defined. Assuming these are acceptable, we will award you Cyber Essentials certification. Organisations seeking Cyber Essentials Plus certification will then continue to the following stages.

### Further assessment – Cyber Essentials Plus

This comprises a series of internal vulnerability tests of the system(s) in scope.

The internal scan checks patch levels and system configuration, while a security and anti-malware test ensures the organisation's systems are resistant to malicious email attachments and web-downloadable binaries. Despite being internal tests, these can sometimes be performed remotely.

Once the internal tests have been completed, an external vulnerability scan must be performed against the in-scope public-facing infrastructure. The external scan checks the patch levels and system configuration.

## Certification process stages continued

### Further assessment continued

The internal and external tests must be passed within one month of each other. To help ensure this, we conduct the internal tests first, as it is easier to arrange the remote external scan.

The tests aim to verify the SAQ and identify vulnerabilities within the organisation's Internet-facing infrastructure that could be exploited by attackers with a low level of skill.

Test reports

- After completing the tests, we will issue a report stating the outcomes and explaining what actions, if any, should be taken to mitigate any further risks or vulnerabilities. Our reports aim to give you meaningful information about the risks to your organisation and activities.

### Certification

Once the scans have been successfully completed and approved, the certificates and Cyber Essentials and Cyber Essentials Plus badges will then become available to download, shortly followed by the test report.

## Key information

- All technical tests and the application sign-off must be completed within a 14-day window, as the tests are seen as a 'snapshot' due to the constant evolution of threats.
- All applications must be completed within six months of starting the application process.
- Cyber Essentials and Cyber Essentials Plus certificates are valid for one year. All certificates issued under the previous scheme before 30 June 2020 will be valid until 30 June 2021.
- Each Cyber Essentials Plus external vulnerability scan applies to up to 16 IP addresses as standard. Further IP addresses can be tested for an additional cost.
- Each Cyber Essentials Plus application includes device testing for up to ten sample devices as standard.





## The 'sixth control' for effective cyber security

The five controls covered in Cyber Essentials are a great starting point to becoming cyber secure, but they don't protect you against one of the top threats – your employees.

People are the first and last line of defence against cyber security threats. Out of all UK organisations that suffered an attack or breach in the past 12 months, more than 80% were targeted by phishing.* To not fall victim, staff need to be well-rehearsed in questioning the contents of their inbox, spotting phishing emails and immediately reporting them.

Staff awareness e-learning courses deliver an effective defence against phishing attacks by educating your staff efficiently and cost-effectively.

### Train your staff against phishing threats

Our Phishing Staff Awareness E-Learning Course is updated with new scenarios every three months, including the latest examples of real phishing attacks, giving your organisation the best chance of combatting them.

Course contents:

- What is social engineering?
- How to identify social engineering attacks
- What are the consequences of a phishing attack?
- How easy it is to fall victim to a phishing attack
- How are phishing attacks orchestrated?
- How to identify a phishing scam
- Ground rules for avoiding phishing scams

To find out more, email rebecca@ccnlimited.com
or telephone 01738 506070

### Licence

This is a one-year, easily renewable licence.

### Duration

The course takes approximately 45 minutes to complete.

### Course contents

The course covers four areas in depth with engaging content and activities.

### Assessment

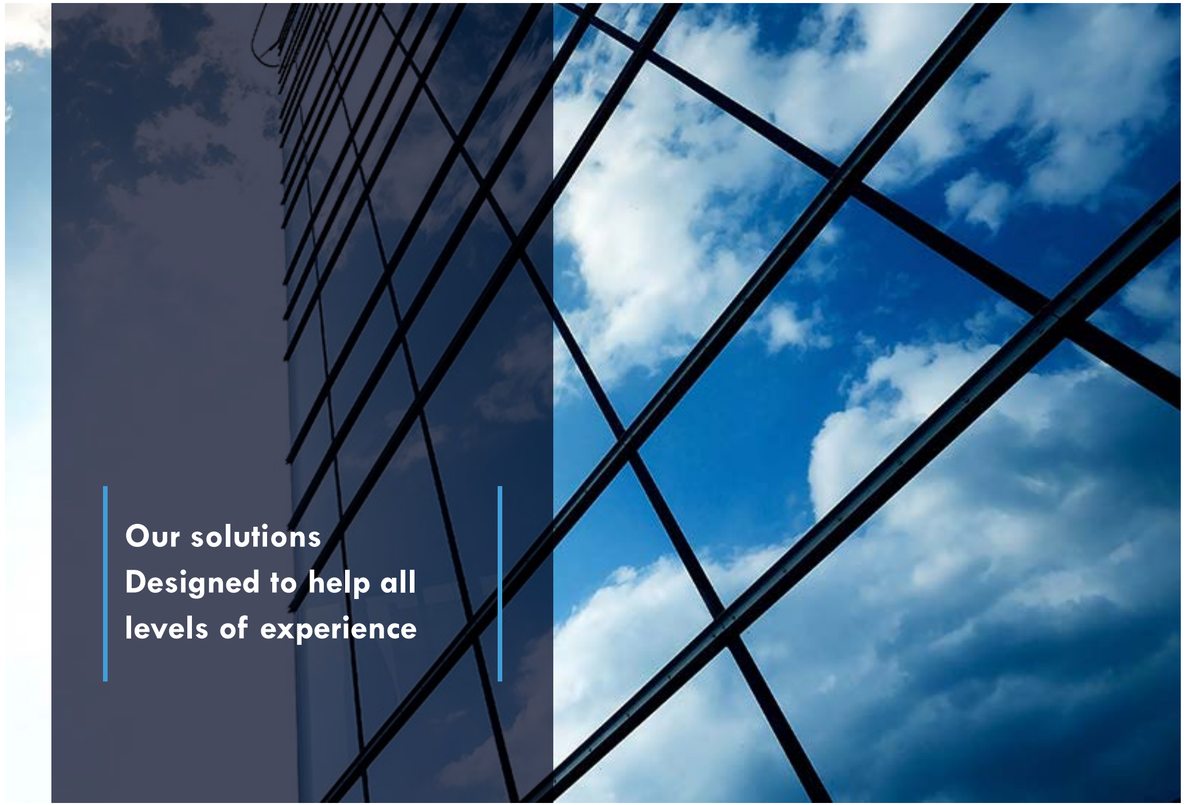
The course assessment comprises 20 randomly selected multiple-choice questions.

### Retake

The course can be retaken as many times as needed until the pass mark has been achieved.

### Audit trail

A certificate is issued to all staff who pass the test that displays their test score. This is trackable in the learning management system, and provides excellent proof of participation should you be audited.








## Cyber Essentials packaged solutions

CCN Limited's fixed-price solutions can help you achieve certification to either Cyber Essentials or Cyber Essentials Plus at a price that suits you.

### Cyber Essentials

| Included | Get A Litle Help | Get A Lot Of Help |
|---|---|---|
| Certification | ✓ | ✓ |
| Precheck | ✓ | ✓ |
| Documentation toolkit | ✓ | ✓ |
| Remote support (2 hrs) | ✓ | |
| On-site consultancy (1 day) | | ✓ |
| On-site assessment | | |

### Cyber Essentials Plus

| Included | Certification | Get A Litle Help | Get A Lot Of Help |
|---|---|---|---|
| Certification | ✓ | ✓ | ✓ |
| Precheck | ✓ | ✓ | ✓ |
| External vulnerability scan | ✓ | ✓ | ✓ |
| Documentation toolkit | | ✓ | ✓ |
| Remote support (2 hrs) | | ✓ | |
| On-site consultancy (1 day) | | | ✓ |
| On-site assessment | ✓ | ✓ | ✓ |

**Documentation toolkit**

Includes all necessary customisable policies and procedures to meet the Cyber Essentials requirements.

**Remote consultancy**

Remote support provides online consultancy to give you expert help on specific issues.

**On-site consultancy**

A cyber security practitioner will provide guidance on completing the SAQ and how to implement the five controls.

**Further assessment**

We will visit your office(s) and thoroughly check whether your IT meets the Cyber Essentials standard.

The assessment involves a scan of your in-scope internal network, focusing on workstations and mobile devices.

This will be followed by an external scan to confirm that the boundary controls are in place and effective.

## Which package should you choose?

IT Governance offers a range of packages to help you implement Cyber Essentials, eliminating the cost of extensive consultancy work, travelling and other expenses. Using a specially formulated combination of tools and resources, our packages will help you manage your project from beginning to end.

### Cyber Essentials*

- You are confident defining the scope of your assessment to encompass the entire organisation; and
- You own and operate your entire IT infrastructure; and
- You are familiar with the five Cyber Essentials controls and know how to implement them.

Or

- You have previously achieved Cyber Essentials certification that you are looking to renew, and your scope has not changed.

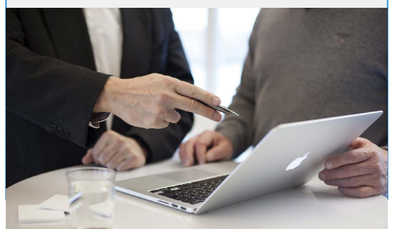
* The certification-only package is only available for Cyber Essentials Plus.

### Cyber Essentials Plus

- You have a more complex or expansive IT infrastructure, which may be Cloud-based or a shared office environment; and
- You are confident you have the skills to define your scope but have some questions about what should be included; and
- You know how to configure your IT to improve security but do not fully understand the five key controls.

### Staff Awareness Training

- You are a highly complex organisation with a range of IT infrastructure; or
- You want to achieve certification for a specific site or subset of your organisation where there are dependencies on other parts of the organisation; or
- You have not previously certified and have little or no knowledge of how to define your scope or implement the five controls.





IT Governance is a leading IASME-licensed certification body, and has awarded thousands of certifications, with many more organisations achieving certification every day.

You can conduct the entire certification process online, without any expert cyber security knowledge.

We provide all tools and resources needed to achieve certification at both levels of the Cyber Essentials scheme.

We deliver all the technical tests and assessments, conducted by our experienced, qualified testers. We do not outsource any of the services required to achieve certification.

We've issued more than 5,000 certificates and we've been a certification body for the past 5 years

We have six packaged solutions available to support organisations with varying levels of experience through the Cyber Essentials or Cyber Essentials Plus certification process.

Having led ISO 27001 implementations since the inception of the Standard, we have the knowledge and insight to help you take the next steps beyond Cyber Essentials.

Our **Cyber Essentials** clients include:

action for children

AIRBUS DEFENCE & SPACE

vodafone

NHS Professionals

LOCKHEED MARTIN





## Why CCN chose IT Governance

- IT Governance is a global leader in information and cyber security management systems expertise.
- We are an IASME-licensed certification body and have been verified as meeting the high standards mandated by the IASME Consortium.
- Our expertise in standards and regulations such as the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, the General Data Protection Regulation (GDPR) and ISO 9001 means we can offer an integrated approach to compliance.
- We provide independent and unbiased advice – we are not affiliated with any software or hardware solution.
- We are an International Board for IT Governance Qualifications (IBITGQ) Accredited Training Organisation (ATO), and an official publisher of the IBITGQ study guides and courseware.
- Our cost-effective and customised advisory services provide a tailored route to achieving improved cyber security, scalable to your budget and needs.

CYBER ESSENTIALS PLUS

IASME Consortium®

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

ACCREDITED IBITGQ Certifying Competence TRAINING ORGANISATION

ISO 27001 CERTIFICATION EUROPE

BS 10012 CERTIFICATION EUROPE

ISO 9001 CERTIFICATION EUROPE

ISO 27001 CERTIFICATION EUROPE

**Computer Cable Networks Limited**

Algo Business Centre
Glenearn Road
Perth, PH2 0NJ

**t:** 01738 506070
**e:** support@ccnlimited.com
**w:** www.ccnlimited.com