

CYBER ESSENTIALS

Your Guide to How Cyber Essentials has Changed (and why it is more essential than ever in defending your business)


Jon Towers

Director, Grant McGregor Ltd




Table of Contents

What is Cyber Essentials?	04
The Five Technical Controls	05
What is Cyber Essentials Plus?	06
Why should my organisation consider Cyber Essentials?	08
How has Cyber Essentials changed?	10
What does this mean in practice?	12
The impact on Certification Bodies	14
The importance of recertification	16
How Grant McGregor can help	18
What to do next	20



Cyber Essentials has proved to be a popular and successful scheme. I believe that success has been partly down to its simplicity; take a set of technical controls that we know will make it difficult for adversaries to exploit basic Internet vulnerabilities, help organisations to implement them, and verify that they have done so.



UK National Cyber Security Centre (NCSC)

What is Cyber Essentials?

The Cyber Essentials scheme was launched by the UK Government in June 2014 following Government concern that UK organisations were not doing enough to protect themselves from cyber threats, even the most common and unsophisticated cyberattacks.



The National Cyber Security Centre, a part of GCHQ, owns the Cyber Essentials scheme - operating it as part of its mission to *"make the UK one of the safest places to live and do business online"*.

Cyber Essentials has been designed to help UK businesses protect themselves against cyberattacks and put cyber security within reach of the vast majority of UK organisations.

Cyber Essentials is based on five technical controls which organisations should implement as part of their cyber security strategies. These are: **access control, secure configuration, software updates, malware protection, firewalls and routers.**

The format was developed after research showed that the majority of breaches happen because organisations have a weakness in one or more of these five key areas.

Cyber Essentials is completed through self-assessment, although organisations can enlist the help of a Certification Body to help them through the self-assessment process.

The self-assessment must be independently verified by a Certification Body.

Speak to our friendly team today about your cyber security requirements

The Five Technical Controls



ACCESS CONTROL

This looks at the management of access to administrator accounts and the controls over who has access to your data and services. Grant McGregor always recommends working to the principle of “least privilege”.



SECURE CONFIGURATION

This concerns the need to review the settings for your devices and software (here again, you should be choosing the most secure). In addition, you should have processes in place for changing passwords and removing unused accounts and software.



SOFTWARE UPDATES

By keeping your devices and applications up to date, you protect against vulnerabilities. All too often this is overlooked by organisations, yet it is simple to get right and will protect you from a great number of common cyber threats.



MALWARE PROTECTION

You must protect your organisation from viruses and other malware by using properly configured anti-malware software and only allowing trusted applications.



FIREWALLS & ROUTERS

You should create a “buffer zone” between your IT network and other external networks so that incoming traffic can be analysed to find out whether or not it should be allowed onto your network. And don't forget to place Firewalls onto your EUD!

What is Cyber Essentials Plus?

Cyber Essentials Plus is the step after you become Cyber Essentials Certified. Similar to Cyber Essentials, it is based on the same five technical controls as Cyber Essentials and requires organisations to be audited against their CE self-assessment submission.

Where Cyber Essentials Plus differs is that it requires a technical audit of the systems that are in the scope of assessment.

This assessment must be completed by an accredited Cyber Essentials Plus Assessor.

The assessor will review and appraise a representative set of user devices, all Internet gateways and all servers accessible to Internet users. Typically, the assessor will select a random sample of systems, usually equivalent to around ten percent of the total devices/systems used.

It is this extra physical appraisal that gives the Cyber Essentials Plus certification a greater level of assurance than the Cyber Essentials certification.

However, **either is well worth having**: the Cyber Essentials certification not only helps to focus your organisation on the important issue of cyber security, it also demonstrates your commitment to good cyber security to potential customers, partners, regulatory bodies and other stakeholders.



UK small businesses hit by
10,000
cyber attacks a day



In the UK
2/3
of **SMEs** were victim to an
attack

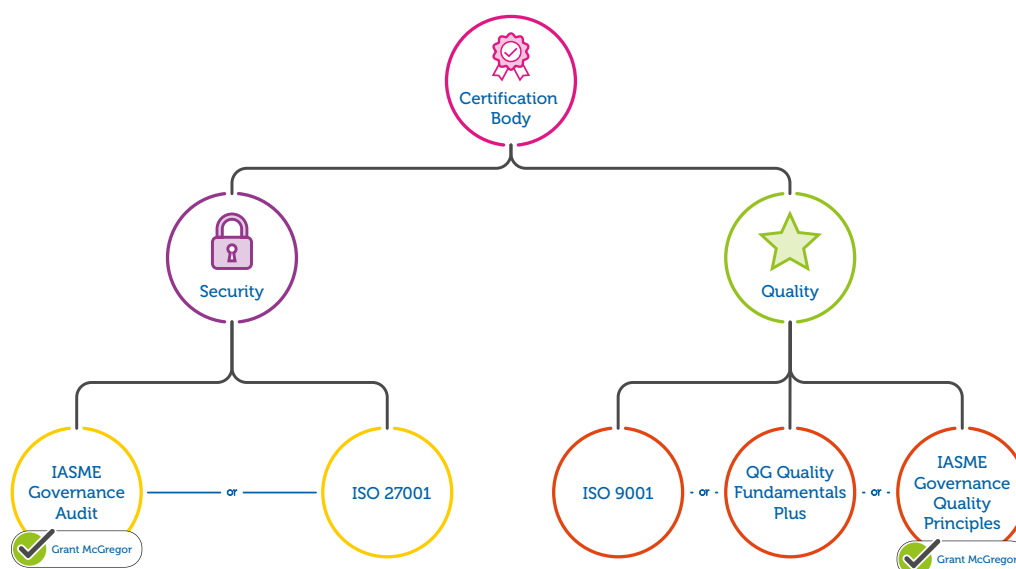
HOW DO I FIND A CERTIFICATION BODY?

Grant McGregor is an official Certification Body for the Cyber Essentials scheme and we partner with an accredited Assessors to conduct Cyber Essentials Plus. We have qualified Cyber Essentials and IASME/GDPR assessors in-house. Our assessors can be on hand to answer questions and assist with support and advice throughout the whole of your certification journey.

You can find a full list of Certification Bodies on the IASME's [website](#).

How certification bodies qualify

Certification Bodies must achieve both the Security and Quality elements to qualify.



IMET Alloys

We wanted to obtain Cyber Essentials to confirm we had robust information security systems in place.

By gaining Cyber Essentials certification we are able to demonstrate our commitment to security for our business partners. It also gives us a differential when negotiating new contracts.

Grant McGregor provided consultancy on the requirements of Cyber Essentials. Their guidance on planning a stages approach to the project was invaluable.

Why should **my organisation** consider Cyber Essentials?

There are several reasons why every organisation can benefit from achieving Cyber Essentials certification.



Enhanced security

Going for a Cyber Essentials certification helps to focus business attention and resources on the importance of good cyber security.

Importantly, by addressing the five key technical controls, most organisations will reduce the likelihood of success and the potential impact of any phishing attacks, malware, ransomware, password guessing, or network attacks attempted against them.

Simple and cost effective

As we've mentioned, the five technical controls that form the pillars of the Cyber Essentials schemes were developed in response to research that showed that the majority of breaches happen because organisations have a weakness in one or more of the five key areas.

The self-assessment is comprehensive enough to make a real difference in these five key areas, but simple enough to be attainable and realistic for the vast majority of businesses and organisations. This makes Cyber Essentials a really good, practical choice to help you boost your organisation's ability to avert and limit a cyber attack.



Gain and retain business

An increasing number of public, private and third-sector contracts are mandating Cyber Essentials certification for their suppliers. For UK Ministry of Defence contracts, Cyber Essentials is required throughout the entire supply chain.



Speak to our friendly team today about your cyber security requirements

Protecting your business from cyber security threats couldn't be simpler

 **Take the next step**

Demonstrate your commitment to cyber security

The Information Commissioner's Office (ICO) recognises the Cyber Essentials scheme and its ability to provide certain assurances and help protect personal data within an organisation's IT system.

Under GDPR, you have a responsibility to protect the personal data you hold. Cyber Essentials is a very good way to demonstrate that you are taking this responsibility seriously and have put the appropriate measures in place.

ICO, the body to which data breaches must be reported under GDPR, has stated that having a Cyber Essentials certificate issued within the last year is something it will take into account in the event of a data breach. This means that a current Cyber Essentials certification offers you some protection from the hefty penalties and fines associated with a data breach under GDPR.

Furthermore, Cyber Essentials is encouraged by other regulators, such as the Financial Conduct Authority which has stated that Cyber Essentials can improve your security.

04



05



Small firms benefit from Cyber Liability insurance

Achieving a verified self-assessed Cyber Essentials certification qualifies some small and mid-size businesses for Cyber Liability insurance cover. For Certified Organisations that have a turnover of less than £20 million, this cover is included as part of the scheme.

How has Cyber Essentials **changed**?

In 2019, NCSC announced it would be changing the way the Cyber Essentials and Cyber Essentials Plus schemes are operated, managed and quality-assured.

For the five years since Cyber Essentials was launched in 2014, the scheme had been administered through five Accreditation Bodies: APMG, Crest, IRM, QG Management and the IASME Consortium.

Following a review of the delivery of the scheme, NCSC decided to make changes to ensure that the assessor and advisor standards are the same wherever you are in the UK and whatever your choice of Certification Body and whichever Accreditation Body they operate under.

Instead of operating the scheme through five accreditation bodies, NCSC took the decision that the scheme would be operated via a single partner.

Having been one of five accreditation bodies, in October 2019 IASME became the sole partner for the revised scheme. Since April 1, 2020, IASME has been solely responsible for the administration and management of the Cyber Essentials and Cyber Essentials Plus schemes.



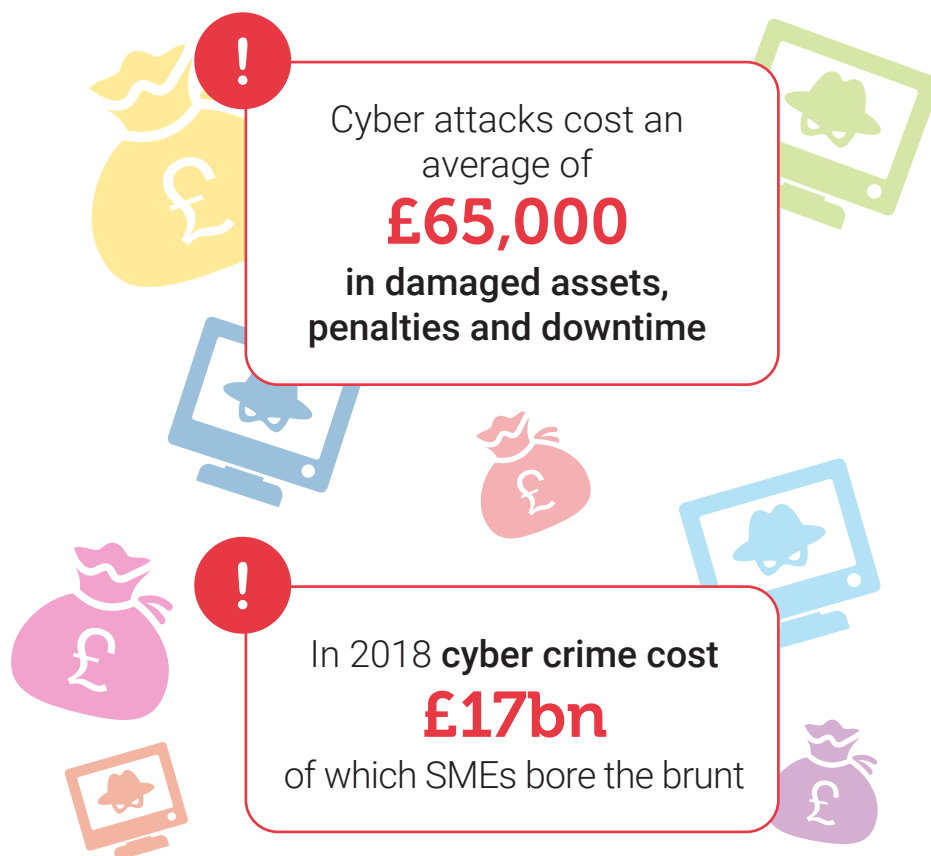
Speak to our friendly team today about your cyber security requirements

Who are IASME?



IASME was founded on the principle that basic cyber security is an essential requirement for the supply chains of all organisations.

In addition to the Cyber Essentials scheme, IASME also operates the IASME Governance standard. This was developed over several years during a government-funded project to create a cyber security standard akin to ISO 27001 but which is more achievable and affordable for small companies. The IASME Governance assessment includes a Cyber Essentials assessment and a review of GDPR requirements and is available either as self-assessment or on-site audit.



What does this mean in practice?

The new operating model will be in place for at least the next 5 years.

For organisations that are new to Cyber Essentials, this change will not impact you: you are still free to select your own choice of Certification Body to help you attain certification.

For organisations that previously achieved certification via IASME, you should notice very little difference in the way the scheme is administered. Most existing Certification Bodies, including ourselves, are continuing to operate as Certification Bodies under the new operating model. So the Grant McGregor Team and our assessors remain at your disposal to guide you through the recertification process and with any other cyber security related issues.



For organisations that previously achieved certification via a Certification Body aligned with one of the old Accreditation Bodies, you may notice some changes to the process next time around. This may include:

- While some of the questions in the self-assessment will require yes/no answers, others may require additional information. This is to enable the assessor to ensure you have the appropriate technical controls in place.
- You will not be required to upload any documentation such as policies or procedures; you need only upload the signed declaration to confirm that the answers you have given are true.
- An IT system and its related security can change significantly over the course of a year. For this reason, rather than rely on a repeat of the previous year's answers, an IASME assessment will require you to enter your answers afresh each year.
- The fixed cost for assessment submission to Cyber Essentials basic certification is £300+VAT. (but note that professional Certification Bodies or consultants will charge you additional fees for their services and/or additional support).

It is also worth noting:

- All staff-owned devices will need to be included in the scope of assessment if they access business data, including email.
- Any servers that are connected to Internet will need to be included within the scope of assessment.
- All home- and remote-worker networks are now also within the scope of the assessment.

Speak to our friendly team today about your cyber security requirements



As well as establishing how we are going to work together, the team at the NCSC has been focussed on developing the new standards that are required to ensure all Certification Bodies and assessors are carrying out their roles in a consistent way.

Working with a single partner has allowed us to define and implement a minimum standard of competence for everyone involved in the scheme, something we haven't been able to do previously.

We have also been supporting IASME with the development of their assessment platform and specifying the standard that any external Certification Body platform will need to meet to connect."

UK National Cyber Security Centre (NCSC)



The impact on Certification Bodies

Certification Bodies – especially those which operated under an Accreditation Body that wasn't IASME – will experience the brunt of the change.

The NCSC reports: "IASME already had 175 Certification Bodies across the UK with 312 assessors. We're pleased to say that these will all be continuing with the scheme.

In addition, since October, IASME have trained an additional 65 Certification Bodies and 194 assessors transferring in from the outgoing Accreditation Bodies as well as training 46 completely new Certification Bodies and 84 assessors from scratch.

This means by the April 1, 2020, we will have more than 280 Certification Bodies and 670 assessors across the UK and Crown Dependencies."

Grant McGregor has undertaken all the necessary training and quality assurance to provide Cyber Essentials support services to our customers.

Amongst our staff, we have fully certified assessors and a wealth of experience guiding organisations through their Cyber Essentials and Cyber Essentials Plus certification processes.

Are you ready to protect your business with this vital cyber security scheme?



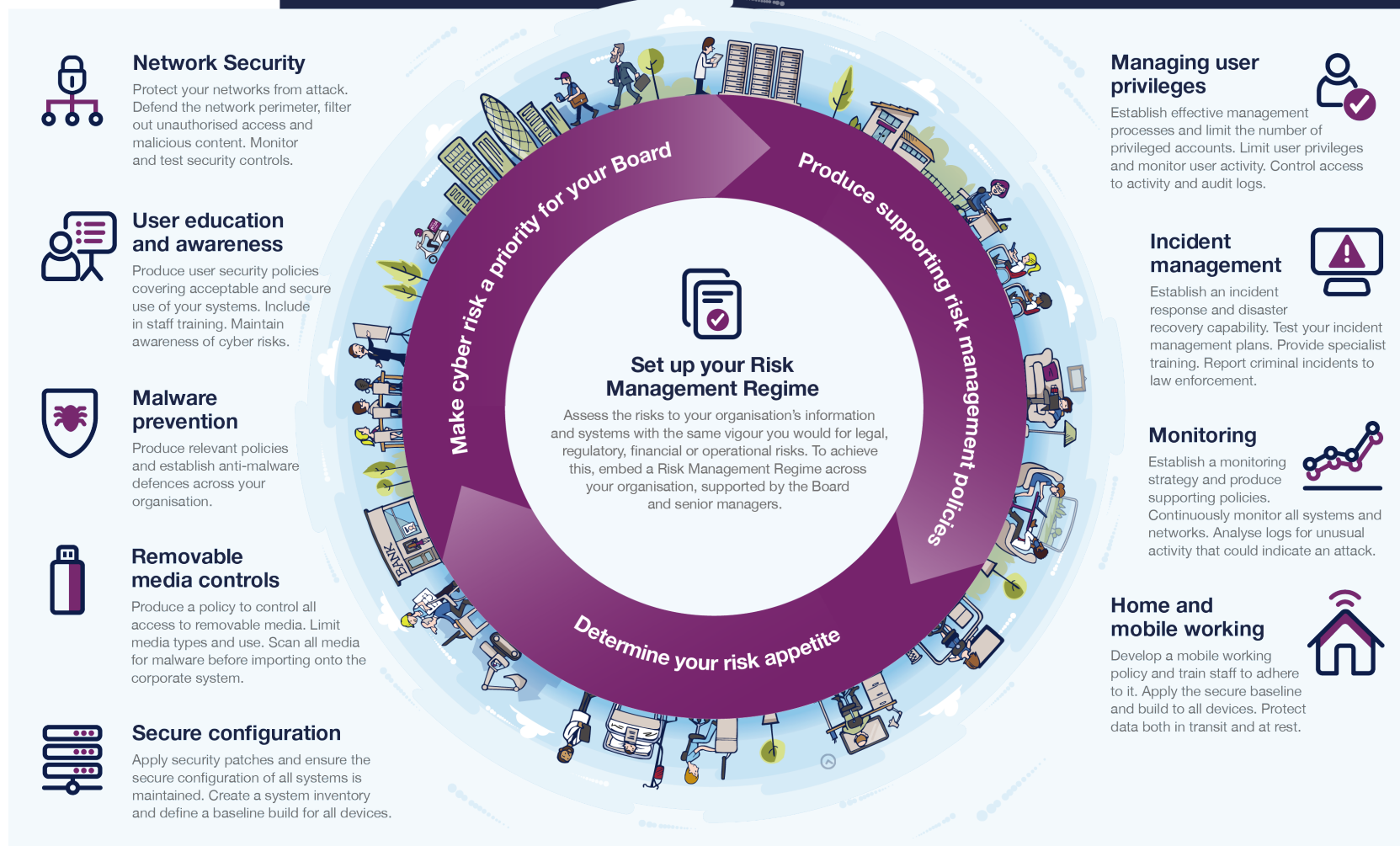
Take the next step

Speak to our friendly team today about your cyber security requirements



10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



The importance of recertification

If you have achieved Cyber Essentials certification already, it's definitely worth renewing your it.

01 There's a financial incentive too: the Cyber Liability insurance cover which is awarded to all UK SMEs (under a £20m turnover) when they achieve Cyber Essentials lasts for a full year and continues providing an organisation recertifies to Cyber Essentials.

02 You will be listed as Cyber Essentials certified on the Government website for one year from the date of your certification. You will continue to be listed so long as you recertify.

03 You'll need your Cyber Essentials certificate to be issued within the last year if it is to be taken into account by ICO in the case of a data breach.

04 An up-to-date certificate reassures your current and potential clients that you take cyber security and data processing seriously.



We were being asked more often, particularly in Contract submissions, what our IT standards and securities were.

Grant McGregor guided us through the process with relative ease. It highlighted some areas where on reflection our hardware/software/policies needed improvement and having undertaken these changes we feel we are much more secure as an organisation.

It undoubtedly gives us a competitive edge when bidding for new work. It has certainly ruled out some competition in a recent 6 figure bid, which we won. It also gives our customers (largely NHS and Universities) assurance that their data exchange with us is as secure as it possibly can be.

If you have certified once, it should be relatively simple for you to recertify – unless you have had major infrastructure changes or your software has gone out of support.

Even in such a scenario, the Grant McGregor team is always on hand to support you throughout your Cyber Essentials or Cyber Essentials Plus certification process, as well as other cyber-security and IT related concerns.

Speak to our friendly team today about your cyber security requirements



What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect**. The following **security controls**, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey



User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?



Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.



Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.



Malware Protection

Can block malicious emails and prevent malware being downloaded from websites.



Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.



Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach



Breach



Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.



Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.



Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.



Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.



User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.



User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.



Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

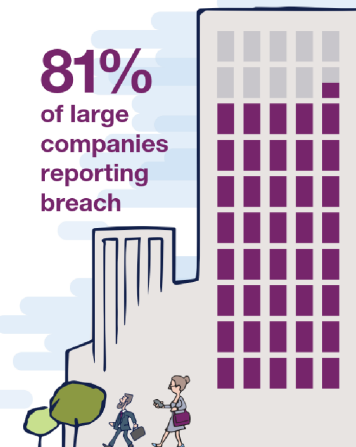


Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

81%
of large
companies
reporting
breach



How Grant McGregor can help

Grant McGregor became an accredited IASME Certification Body for Cyber Essentials (CE) and Cyber Essentials Plus back in 2016.

We have a strong and long-standing relationship with the National Cyber Security Centre's (NCSC) sole Accreditation Body, IASME, and we are an early-adopter of the scheme in Scotland as a key member of the Scottish Business Resilience Centre.

Since 2016, we have helped nearly 100 different businesses and organisations to certify for Cyber Essentials / Plus, including:

- Government bodies such as the Scottish Public Pensions Agency and the Office for the Scottish Charity Regulator;
- Housing Associations and Charities, and;
- businesses large and small including Accountants, Legal Practices, Manufacturers and many more.

Our Cyber Team has huge depth of experience around the five main controls that are central to the Cyber Essentials / Plus schemes. We have developed a very effective set of tools, techniques and technologies to help our clients to save time and money when addressing or improving the way they handle these five aspects. Again, this means that we won't just tell you what's wrong or non-compliant for you, we'll be able to help you to improve the day-to-day processes or adopt robust policies to improve your cyber compliance and readiness.

Many people ask us; "how long will it take for us to pass?" Whilst there's no firm guarantee of a pass, experience tells us that certification often takes us less than a month for a company that is ready to go. Of course, this very much depends how much time

Our fully qualified in-house Cyber Assessors are all seasoned IT Professionals who live and breathe IT daily in the service work we do for hundreds of other companies supporting their systems, staff and security. As they are not simply 'compliance consultants', our Assessors don't simply tell you what needs to be done but they can often guide you on how to do it.

Grant McGregor also works closely with some other carefully-selected and experienced Certification Bodies to provide additional, external support that can provide useful objectivity or additional expertise where required.

and focus you are ready to put into it but that's where we can help. If you already have a good handle on all of your IT 'assets' including systems, devices, applications and people then you're probably in a good place to get started. If you know you need support with capturing detail about any or all of these, then we're ready to help.

We've adopted some clever tools and technology that can seriously speed-up and simplify the information-gathering process for Cyber Essentials / Plus and quickly find the gaps to concentrate on. Used longer-term, our ingenious tools can help your organisation to remain CE and CE Plus compliant over time and not just achieve a 'point in time' pass. It depends why you're gaining the certification in the first place – just for compliance-sake or to improve your overall protection against cyber crime and business disruption – but we can help you to maintain your guard to defend your business against 80% of the most common forms of attack or breach.

Finally, a word of caution. As the scheme has evolved under NCSC and IASME, all CE Certification Bodies (CB) have had to demonstrate the quality and robustness of their own policies, processes and systems. All CE Assessors have had to requalify to rigorous, new standards and not all have evolved and done so. Now all IASME CBs must hold the equivalent of ISO27001 for Quality Management and ISO 9001 for Information Security Management. Grant McGregor has achieved these standards and this is no mean feat yet not all apparent 'Certification Bodies' or 'Cyber Consultants' have done so and IASME are working to stop this kind of false advertising.

So, when choosing a partner to help you to certify, think about why you are doing this... Is it because you have to e.g. for a tender or to remain a member of a professional body? Perhaps it's because you wish to demonstrate to all of your stakeholders that you take information security seriously? Or you know that such cyber crime is rapidly rising and recognise that you want to defend your business against disruption and the obvious dangers of falling victim to a cyber-criminal.

We're ready to help. If you're ready to start, take a look at the next step...

Our qualified assessors



David Lawrence

Co-Founder and Director &
Cyber Essentials Assessor
IASME Assessor
GDPR Assessor



Paul Sinclair

IT Service Manager &
Cyber Essentials Assessor
IASME Assessor
GDPR Assessor



Doug Davey

IT Infrastructure Manager &
Cyber Essentials Assessor
IASME Assessor
GDPR Assessor

What to do next

We've developed a twelve point checklist to help you understand your readiness to get **Cyber Essentials Certified**.

The simple checklist identifies the most common areas that you should be concentrating on to meet the needs of the five Cyber Essentials Controls. Once you've completed it, **send it back to us for a free Cyber Essentials Pre-Assessment (worth £199)**.

GRAB YOUR FREE COPY TODAY

or visit <https://grmc.it/cyber-essentials-checklist>

Our twelve point checklist will give you a quick insight into which areas of your business may leave you vulnerable to a cyberattack - offering access to your sensitive company data

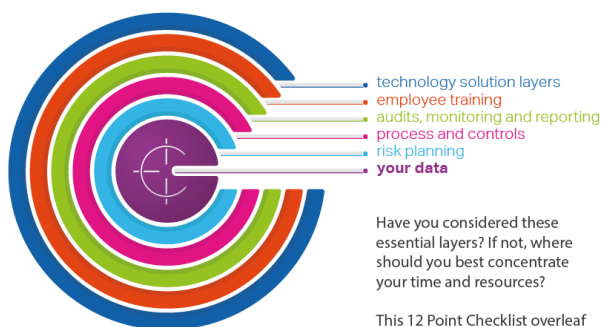
Your data is vulnerable to attack - and there's plenty of evidence that no company is too big or too small to be a target. The personal and corporate data you hold on your systems is worth money to cybercriminals - whilst also being the lifeblood of your business.

Your peers are already taking steps to make sure they're ahead of the threat. What more could you be doing to keep your business competitive and secure?

Cybercrime is fast growing. Can you be sure you are suitably protected?

Cybercrime is not your fault but it is your responsibility to protect both your own and your customers' data.

The 5 Vital Layers Securing Your Data from Cyber Criminals



Speak to our friendly team today about your cyber security requirements

grantmcgregor

technology · people

Grant McGregor Ltd is a professional IT Support Services company serving a variety of businesses and organisations large and small in Edinburgh, Glasgow, across central Scotland and around different parts of the UK.

Our specialties are systems auditing & planning (IT consulting), network improvement projects, ongoing network/computer support, maintenance and development. We also provide technologies to help you to protect and secure your data, to be more productive in everyday life and to comply with an increasingly regulated world.

Our key strength is our people - all of us take pride in not only delivering the results you want and expect, but also by being trustworthy, knowledgeable, systematic, accountable, but above all friendly and easy to work with.

To find out more about us, visit us on the web www.grantmcgregor.co.uk or better still, visit us in person!



IKM were finding that increasingly as part of our tender process companies were being asked to be Cyber Essentials certified and not having the certification excluded us from applying for these tenders.

Assisted by Grant McGregor, the application and auditing process was fairly straightforward as there were many processes already in place, but it was also an ideal opportunity to review our current systems and policies.

We are looking to capitalise on our investment in the certification and shall now look to projects that were previously out of our scope.



