PRE-CYBER ESSENTIALS CHECKLIST

CYBER ESSENTIALS PLUS

CYBER ESSENTIALS

atg
IT for business

Steve McGowan - Head of Risk & Compliance

Pre Cyber Essentials Checklist

If you're not looking to have your certification managed and automated by ATG preferring the self assessment route, here's a helpful checklist before you get started.

Choose the most secure settings for your devices and software

☐ Know what 'configuration' means
☐ Find the Settings of your device and try to turn off a function that you don't need
☐ Find the Settings of a piece of software you regularly use and try to turn off an unused function
☐ Read the NCSC guidance on passwords
☐ Make sure you're still happy with your passwords
☐ Read up about two-factor authentication

Control who has access to your data and services

☐ Read up on accounts and permissions
☐ Understand the concept of 'least privilege'
☐ Know who has administrative privileges on your machine
☐ Know what counts as an administrative task
☐ Set up a minimal user account on one of your devices

Protect yourself from viruses and other malware

☐ Know what malware is and how it can get onto your devices
☐ Identify three ways to protect against malware
☐ Read up about anti-virus applications
☐ Install an anti-virus application on one of your devices and test for viruses
☐ Research secure places to buy apps, such as Google Play and Apple App Store
☐ Understand what a 'sandbox' is

Protect yourself from viruses and other malware

☐ Know what 'patching' is
☐ Verify that the operating systems on all of your devices are set to 'Automatic Update'
☐ Try to set a piece of software that you regularly use to 'Automatic update'
☐ List all the software you have which is no longer supported

Self Certification

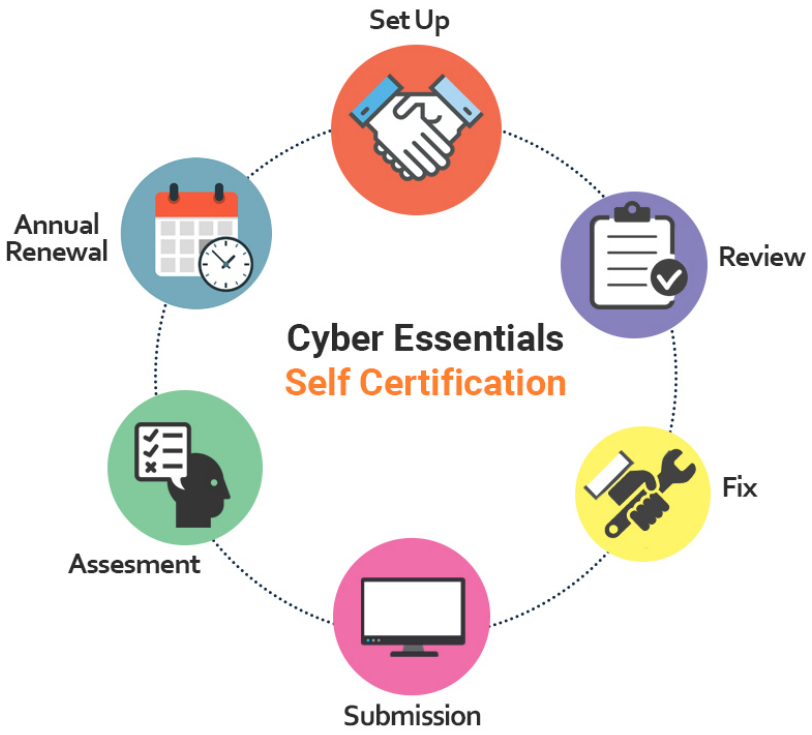
If you're looking to self assess for Cyber Essentials here's how you do that

1 Let us know a bit about your organisation and we'll set you up with an account on our Cyber Essentials Self Service portal.

2 You review your organisation against the standard. This will involve reviewing all elements of your technology with your team and/or IT provider.

3 After reviewing and creating a plan of action you'll need to correct and fix areas that are non compliant or require attention. This will include creating any documentation.

4 Return to your self service portal and submit your answers, adding as much detail as appropriate, including any documentation for review by an assessor.



5 An assessor will review your answers and mark with a pass/fail as appropriate.

6 If you have passed the assessment a certificate will be issued to you for you to use and demonstrate that you have been certified to Cyber Essentials standard.

7 You will have to re-certify annually and follow the same process.

What happens if we fail the assessment?

If you fail we allow you two working days to examine the feedback from the assessor and change any simple issues with your infrastructure and policies. You can then update your answers and the assessor will have another look without any extra charges. However, if you still fail after these two days you will have to reapply and pay the assessment fee again.

How do we certify to Cyber Essentials Plus?

Cyber Essentials Plus involves a technical audit of the systems that are in-scope for Cyber Essentials. This includes a representative set of user devices, all internet gateways and all servers with services accessible to unauthenticated internet users. The assessor will test a suitable random sample of these systems (typically around 10 per cent) and then make a decision whether further testing is required.

You will need to complete your Cyber Essentials PLUS audit within 3 months of your last Cyber Essentials basic certification. Both of these can also be completed at the same time.

Cyber Essentials The Easy Way

We created a managed service to take the headache away from Cyber Essentials.

Not only the certificate, but with our managed service you'll receive regular reports to let you know that your in compliance, and when renewal comes round in 11 months, we'll simply reissue your certificate without any major investment or project required.

Here's the process for us to manage your Cyber Essentials:

1 Complete our sign up form: Its a few questions so we can get your account set up.

2 Call with assessor: we'll gain some more information about your company.

3 We'll install our simple agent on to all your devices.

4 We'll review your infrastructure, using our technology to understand any weaknesses in your systems.

5 We'll advise on any areas that need to be addressed step by step, we'll also be on hand to answer any questions. This will include providing you with any policies required.

6 We issue your certificate, you can then let your suppliers, clients and partners know that data is safe with you with your official Cyber Essential certificate.

7 Data security is an ongoing process. That's why all our offerings include one year of ongoing cyber essentials support, cyber insurance and regular security briefings.

8 Annually we'll reissue your certificate, with no major project as we'll know on a day to day basis that you're compliant.

Please note: If you have systems which are out of date including SBS 2003 and Windows XP you will not be able to certify without replacing or taking them out of scope.

Pros and Cons

Self Assessment

Pros	Cons
▸ Lowest External Expense	▸ Moment in time for compliance, you don't know if you are still protected / compliant ▸ Renewal project every 12 months. ▸ Time consuming planning project for internal staff, or additional costs from IT provider ▸ Documentation required to be created.

Automated / Managed

Pros	Cons
▸ Quick install and only a few questions to be answered over the phone. ▸ If you require any areas to be addressed which are out of compliance we can guide you through the steps required. ▸ Continuous compliance; have confidence that every endpoint is always compliant. ▸ Simple renewal; new certificate is issued annually without the need for major project. ▸ Required documentation included. ▸ Simple, short, easy to understand reports sent to you monthly. ▸ Guaranteed Pass*	▸ Higher expense

* Changes may be required to systems if systems are end of life or no longer supported/receiving updates

Pricing

Self Assessment

Pricing for self submission is £300+VAT per submission. Please note if you are entering multiple submissions for different offices, there will be a submission fee for each of the offices. Re-submissions within 48 hours are included. Other costs to consider are time of your IT staff or additional costs from your IT provider. You may also need to have additional policies created.

Managed Cyber Essentials Compliance

If you're looking for ongoing, managed, Cyber Essentials that's quickly issued and with little impact on your team, our managed service is for you.

Investment varies based on users, the below table details this:

Users	Investment (Per Calendar Month)
0-25 Users	£99.00
26-40 Users	£139.00
41-60 Users	£189.00
61-80 Users	£239.00
80+	Price on Application

What's Included?

- Endpoint scanning across all machines including checks for:
  OS updates, Patches, Antivirus, Firewalls, User rights, Secure configs & more.
- Fully supported submission of answers
- Required Documentation
- Rapid digital issue of Cyber Essentials certification
- Continuous monitoring of devices with monthly security reports

Final Thoughts :
Cyber Security is More Than a Certificate.

In this guide we have covered the top cyber risks and how Cyber Essentials technical controls can help your business. But the certification isn't the be all and end all. There's more to it than that.

The first thing any business should do is look at the risks to you. What's happening in your industry might not relate to you, look for guidance, but make 'risk' a board room discussion and allocate budget accordingly at every step. Because if you Google "Cyber Security Risks.." you're never going to allow your staff to turn on a computer ever again!

"One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks."

Take a look at the systems and processes you use. This isn't just ensuring your firewall is stopping attacks. Very rarely do systems get hacked by a "hacker" trying to penetrate your systems from externally. It's difficult and time-consuming. It's much easier to get one of your users to just tell them a username and password. Likewise, can your reception computer be accessed when not manned? Can the screen be seen from a window? Follow the data in a business and see what risks you might have. Someone leaving with a laptop? Is it encrypted if they leave it on the train? Do you know how they got the files home? Personal Dropbox maybe?

> *"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted; none of these measures address the weakest link in the security chain."*
>
> Kevin Mitnik - "The World's Most Famous Hacker"

That leads me to culture. If you want to have a secure business, technical controls as discussed in this guide are important, but to succeed you need a culture shift. When it comes to cyber security, users are the weakest link and strongest line of defence. Don't create a blame culture. Users get a bad reputation when it comes to cybersecurity, but with social engineering attacks getting better all the time, it's tough out there.

Train users to spot the signs of an attack. More obvious elements are a faked email, but the person ringing on a Friday afternoon, stressed and just asking the person on the end of the phone to confirm a few details? That's a bit more difficult to spot. People want to help, it's in their nature, but criminals know this and will play on it.

Final Thoughts :
Cyber Security is More Than a Certificate.

Use policies and procedures to support users, not to vilify them. A client wants to change some bank details? Have a simple to use a process that can be followed and shared with the person requesting. That way everyone is on the same page, and bring your processes into training. Likewise, have users understand risk. Rather than just saying "you can't do this", have a discussion around "here's a risk, this is what could happen, this is the effect it could have on the organisation, so that's why we can't allow it". If a junior member of staff uses Dropbox to work on a piece of work at home, they weren't thinking about the risks of transferring data outside of the EU, to a non-company owned asset, potentially conflicting your privacy notice. They just wanted to work hard and get the task done. Something goes wrong? Someone makes a mistake? Review the situation and see how it can be improved in the future for all staff.

Finally, technical controls, staff training and policies and procedures are imperative. But ensure that these are constantly being reviewed against the latest risk to you. Being safe from cybercrime isn't an annual, quarterly, monthly task it's daily, if not by the minute.

ATG Supporting Services

At ATG we've been partnering with small and medium businesses for the last 30 years to make technology work for them. Here's a few ways

Award Winning Support

You need support that's always going to be there when you need them but also reduce the amount that you need to contact them, We work 24/7 to keep your staff productive. If they do need us; you go straight through to a qualified engineer to solve the issue.

Find out more.

Disaster Recovery

With increasing incidents of cyber-attacks and user error leading to systems or data being unavailable, having a true business class disaster recovery solution is a necessity. Can your backup have you back running fully within seconds?

Find out more.

Cloud Technologies

Cloud is a buzz word thrown around, but it should support your business to increase productivity and reduce costs. We use technologies such as Microsoft 365 to do that.

Find out more

Risk & Compliance

With the ever growing risks and compliance requirements, you need a partner who is going to be able to take a strategic approach to protecting your business without scare tactics and techno jargon!

Find out more

Managed Cyber Security

We offer a variety of managed security services to protect your business and users. All for an affordable monthly fee.

Find out more.

Cyber Awareness Training & Testing

Training is great, your staff are the last and first line of defence, but how do you know training works?
You test them.

Find Out More

Get in Touch

If you have any questions please feel free to contact the team or I using the details below

If you would like to order your Cyber Essentials service please visit the web link and your account will be created by the team.

Steve McGowan

Head of Risk & Compliance
steve.mcgowan@atg-it.co.uk
01527 570535

Let us contact you.