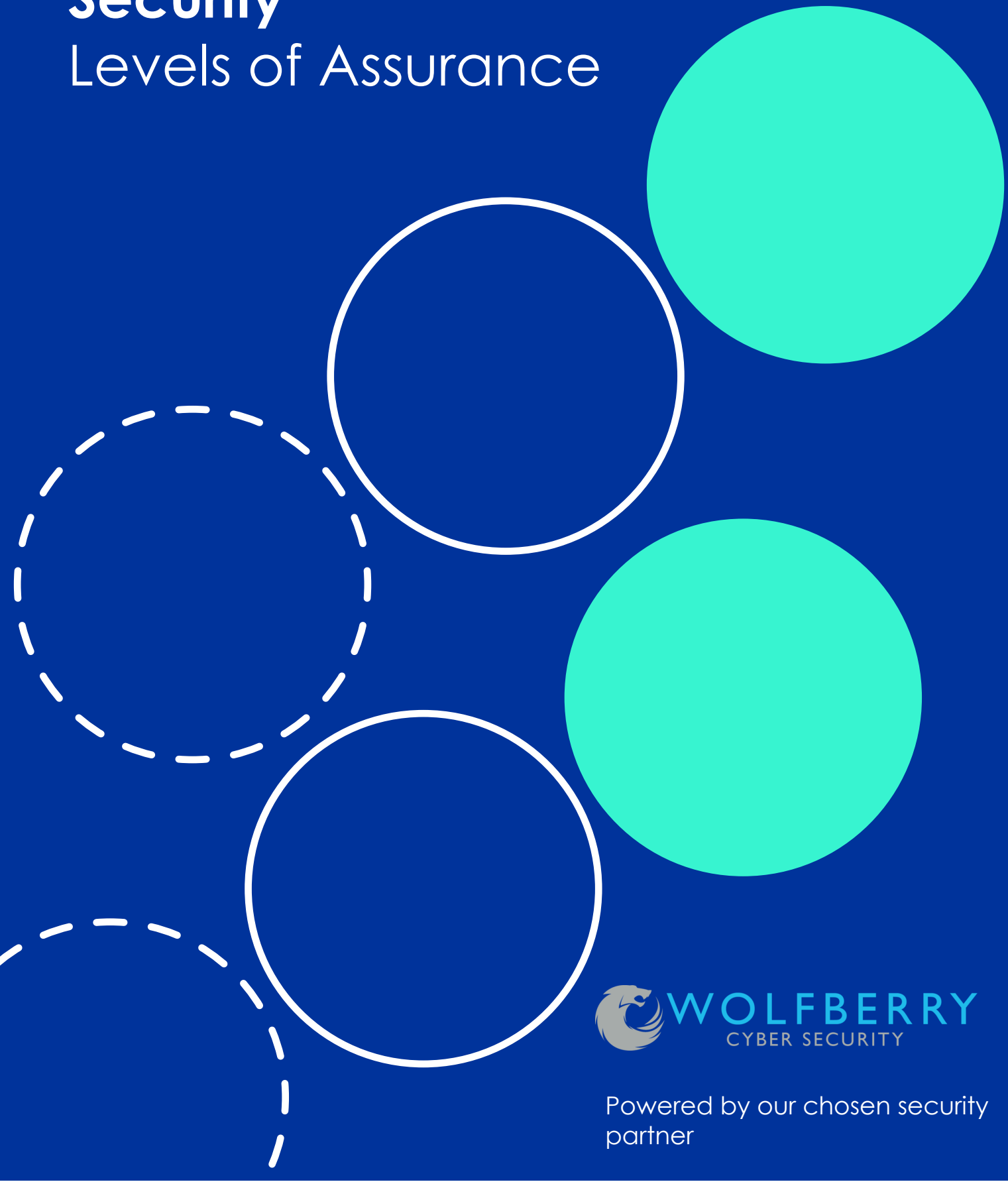
Circle.

Security
Levels of Assurance



WOLFBERRY
CYBER SECURITY

Powered by our chosen security partner

Circle Cyber Security

At Circle, we don't take a 'one size fits all' approach. We work with our customers closely to look at the organisation's needs as well as the end user requirements to ensure that we are always providing the best solution.

As an organisation, we take the security of our customers and users seriously and consistently review our robust security policies and management systems. We also maintain the international standard for a quality management system, ensuring that we provide products and services that meet customer and regulatory requirements and always strive for continuous improvement.

When you work with us, you don't get an IT supplier but partner with your best interest in mind. We look at your organisation as a whole, working with you to find the best solution to match what you need now and to support your future goals. Long and short of it - is this right for you? If not, then we will find the right solution for you.

We pride ourselves on building long-lasting partnerships with organisations. Our Technical Architects and Account Management will form a key part of building a long-term IT strategy and roadmap for you. We ensure that you always have the right solution for your organisation, now and in the future.

Our goal is to provide the right level of protection for any organisation, regardless of size or sector. We take a layered approach to security, with each layer protecting a different part of your infrastructure and services to enhance the overall strength and security posture. Therefore, we offer 3 levels of security, so you can find the one that suits your organisation the best.

How can you protect your organisation?

We understand that organisations need different levels of protection. So, we provide a range of solutions with varying levels of protection and assurance, organised into affordable packages.

Level 1 - Essentials

Achieve the Cyber-Essentials certificate for your organisation with our hassle-free, fully assisted process. This will give you a 30% assurance level with system testing carried our annually. Cyber Essentials is suitable for all organisations, of any size, in any sector.

30%
assurance level

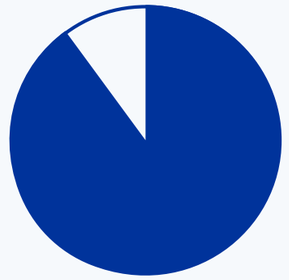
Level 2 - Standard

A subscription service that meets the client's needs, all neatly packaged into a low monthly cost. This includes a complete network scan, website scan, monthly reports, quarterly reviews and awareness support to deliver a 60% assurance level.

60%
assurance level

Level 3 - Premium

Our level 3 support takes the level 2 subscription and adds further benefits to enhance your security posture. Level 3 identifies malware, blocks internet attacks, secures your cloud infrastructure, protects against rogue users and more. So, you can achieve a 90% assurance level.



90%
assurance level

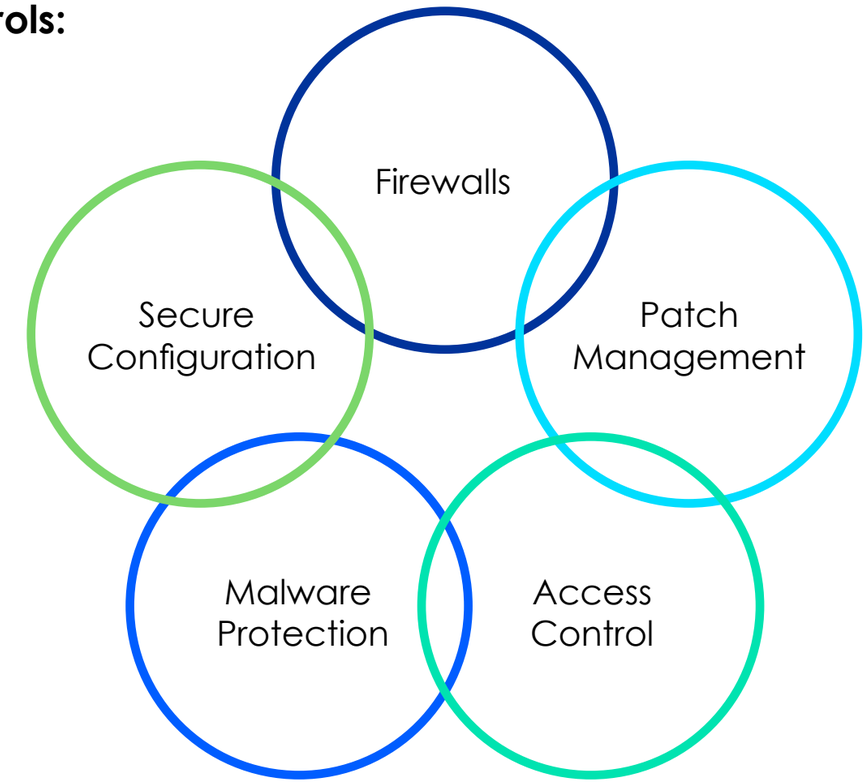
Level 1
Cyber Essentials Plus

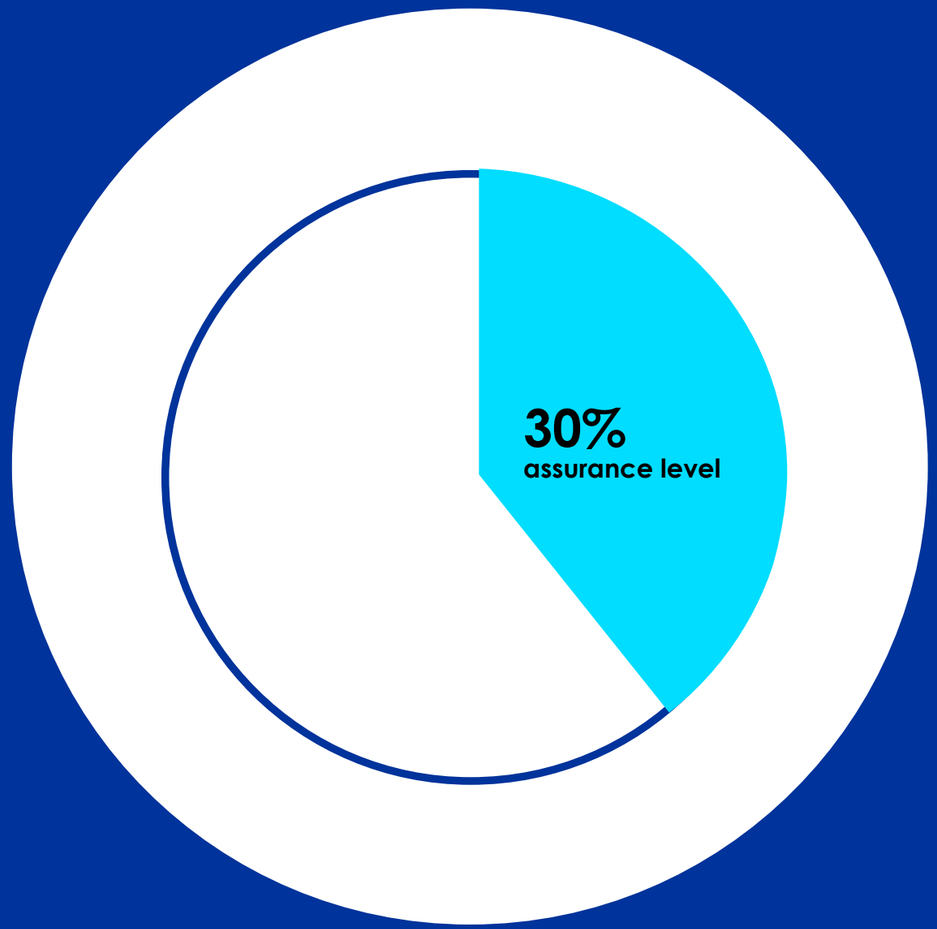
Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

Cyber Essentials Plus is an-onsite security audit of your organisations computer systems and should not be confused with Cyber Essentials standard, which, is simply a self-assessment questionnaire and offers little to no protection to your network. Essentially, 'Cyber Essentials' is you saying you have the security controls in place and 'Plus' is the Certification Body auditing the technical controls to confirm compliance.

Achieving your Cyber Essentials certification with us ensures a hassle free experience. Many organisations worry they will need new hardware/ software to get through CE Standard and Plus, but this is not usually the case. We will guide you through the process and advise you on what you'd actually need to achieve your certification with ease. The technology will test your systems for you, so testing can be done when it's convenient for you. If needed, retesting can be completed immediately without an on-site visit.

Cyber Essentials Plus covers 5 controls:





Why choose level 1?

Level 1 is great as a starting point to show you're taking security seriously, you will only achieve around 30% assurance of protection with this option. The tests are only completed annually, against a sample of your systems and not the entire network, which is reflected in the assurance level. It's no doubt that the Cyber Essentials certification is a fantastic start to a stronger cyber security posture, but it really is only the start of a long journey.

When applying for Cyber Essentials Standard, you can choose to add IASME governance to your application. It's a fantastic companion certification when combined with the Cyber Essentials scheme, covering many of the latter's deficiencies, such as disaster recovery planning and GDPR compliance.

Level 2
Standard

Including all the benefits of level 1, level 2 is a simple subscription service to meet user needs, all neatly packaged into a low monthly cost. As standard, this subscription includes:

Complete Network Scan

While Cyber Essentials Plus only covers approximately 10% of your network, level 2 will scan your complete network every month. Scanning schedules can be provided to suit client needs.

Website scan

Protecting your website is essential whether you have a portal or a simple brochure website. A website hack can lead to reputational damage, or even worse - data loss.

Monthly Reports

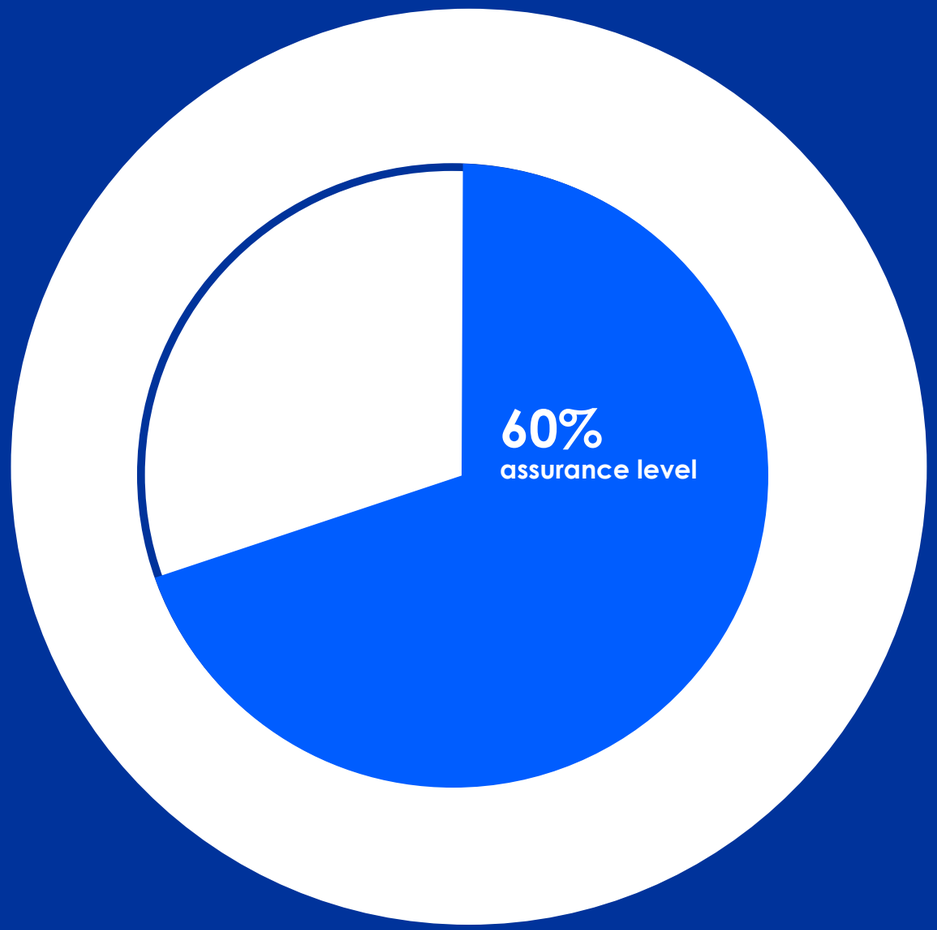
A complete monthly report showing the current status of your company's network, allowing you to spot trends and make the appropriate changes.

Quarterly Reviews

We will liaise with you and your IT provider, share guidance and recommendations to help improve your company's security posture.

Awareness Support

Identifying which users are susceptible to phishing emails is an excellent indicator of the level of threat your organisation faces from the most prevalent form of cyber attack. As part of your subscription, we will run bespoke and relevant simulations to fully test your users. This gives you a true reflection of the effects of phishing to your organisation, unlike templated off-the-shelf phishing simulations. On average, 14% of users click on links during these exercises, demonstrating just how affective these attacks are.



Why choose level 2?

This subscription provides around 60% protection against cyber threats. Unlike Level 1's annual testing against a portion of your network, Level 2 will scan your complete network every month. This gives you a clear understanding of your organisation's security posture, with the added bonus of phishing simulations and quarterly reviews to ensure your IT systems are providing the necessary level of protection.

The IASME self-assessment is included in the cost of a monthly standard Level 2 subscription, if your business needs it.

Level 3 Premium

Our Level 3 support takes the standard Level 2 subscription and adds active threat detection into the mix. With a 24/7 security operations centre (SOC) based in Cardiff, we will monitor and improve your organisation's security posture while preventing, detecting, analysing, and responding to any cybersecurity incidents.

Level 3 offers global visibility; devices are monitored no matter where they are. Once a simple agent is installed, the SOC team actively search for configuration changes and malicious or vulnerable user activity. Level 3 Premium is designed to give you peace of mind while you concentrate on your job, leaving all the hard work to us.

What does Level 3 do?

Identify Malware

An organisation fell victim to ransomware every 14 seconds in 2019. It's predicted by 2021 it will be every 11 SECONDS.

cybersecurityventures.com

Block Internet Attacks

Hackers attack every 39 SECONDS, on average 2,244 times a day.

University of Maryland

Defend Microsoft 365

1.2 million Microsoft accounts were compromised in January 2020 alone.

windowscentral.com

Protect against Rogue Users

Insiders are considered responsible for 28% of cybercrime breaches.

PwC

Secure your Cloud Infrastructure

Through 2022, at least 95% of cloud security failures are predicted to be the customer's fault.

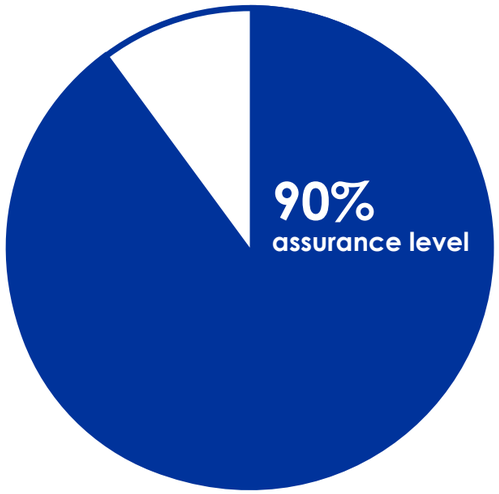
Gartner

Quarterly reviews and monthly reports are also included with a Level 3 subscription. Future services are added at no extra cost.

Other benefits of Level 3 Include...

Annual Penetration Tests

Building upon Level 2's automated external vulnerability scans, the Level 3 subscription includes annual penetration testing of your external estate (such as web applications, websites, firewalls, etc). A penetration test is a manual audit of a target, meaning it's a thorough examination, finding the network vulnerabilities before the hackers do.



Awareness Education Portal (ÆP)

In addition to the phishing simulations provided with Level 2, we are currently developing an awareness education platform. This program will cover awareness training for all levels of staff, educating them on the dos and don'ts of cyber security. Upon completion this will be included in your Level 3 subscription.

The dark web is a rich source of information for cybercriminals; understanding if any of your company's data exists on it is a vital defence.

The cost of IASME Governance Audited is included with a Viper Æ subscription. This is an in-person audit and step up from standard governance qualification.

Why Choose Level 3?

Networks are no longer confined to a single geographical location, and the threat from phishing and internet based attacks means it's never been easier for cyber-criminals to breach your outer defence.

Level 3 protection has been designed to protect your devices no matter where they are, keeping your users and data safe by providing the necessary visibility with today's threat landscape.