PENTEST CYBER

Pricing & Service Description

G-Cloud 15 – Cyber Essentials

PENTEST CYBER

PUBLIC

V 1.0

CESG Certified Professional

TIGERSCHEME Providing excellence in penetration testing

OFFENSIVE SECURITY OSCP

CISCO CERTIFIED CCNP ENTERPRISE

CISCO CERTIFIED SPECIALIST

CISCO CERTIFIED CCNA

Assured Service Provider in association with National Cyber Security Centre

Crown Commercial Service Supplier

IASME GOVERNANCE AUDITED GOLD CERTIFIED

GDPR CERTIFIED

QUALITY PRINCIPLES CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

1. Pricing Table

Prices are exclusive of **VAT**.

Service Name	Service Description	Total Rate
Cyber Essentials / Cyber Essentials Plus	Considerations are the number and type of devices in scope on an estate. A typical estate of around 20 users using a single build type of varying software packages, with up to 30 external facing IP addresses exchange services, would be ~£3500.	CE: £990 CE+: £2,500 - £10,000

2. What are Cyber Essentials, Cyber Essentials Plus and IASME?

Cyber Essentials is a UK government endorsed certification that organisations and companies can achieve to demonstrate they meet a baseline level of cyber security. At its simplest, it encourages the implementation of essential measures and controls that are proven to help mitigate real-world cyber-attacks.

There are two levels to Cyber Essentials; the self-assessed version in which the applicant completes a series of questions that get marked by a qualified assessor. Cyber Essentials Plus, ensures the self-assessment content is validated through technical tests carried out on IT assets.

The National Cyber Security Centre (NCSC) oversees the scheme's overall direction. They work closely with their Cyber Essentials partner, IASME, to deliver it to organisations and companies of different shapes and sizes. IASME are also the point of contact for Certification Bodies that provide the scheme to applicants. Certification Bodies, such as Pentest Cyber, ensure the quality of service for the scheme by having in-house personnel with appropriate knowledge, skill, and vetting.

Supporting guidance: https://www.ncsc.gov.uk/cyberessentials/overview

The three options in demonstrating cyber awareness and strategy.

© Pentest Cyber 2026 www.pentestcyber.co.uk

- **Cyber Essentials** - Complete a series of questions through a verified self-assessment that is then marked against a set of criteria defined by NCSC and IASME.

- **Cyber Essentials Plus** - The audited version of Cyber Essentials captures a state of cyber hygiene and assesses vital areas prone to exploitation. Cyber Essentials is a prerequisite to obtaining Cyber Essentials Plus.

- **IASME Governance** - Includes Cyber Essentials with further questions surrounding information assurance, which helps highlight the presence of high-value policies and procedures—widely recognised as a cost-effective alternative to ISO 27001 and GDPR due diligence.

2.1. Core Subject Areas of Testing

- **Firewalls** - Ensure routers and default host-based software firewalls are enabled and properly configured. Assess perimeter defences for base-level cyber hygiene.

- **Secure Configuration** - Secure password-protected accounts with a practical approach to prevent guessing, password spraying and brute force attempts.

- **User Access Controls** - Check appropriate access and permission security by ensuring staff are not using admin accounts to perform daily work while adopting models like least privilege.

- **Malware Protection** - Identify weaknesses with execution policies and adhere to best practices for anti-malware, software approval lists and application sandboxing. Prevent and limit the attack surfaces for malware and propagation.

- **Update Management** - Capture a benchmark of vulnerability exposure and identify the effectiveness of patch management. Counter vulnerability releases by software updates and mitigation within an appropriate base defence window.

© Pentest Cyber 2026 www.pentestcyber.co.uk

3. How often should I pursue these certifications?

It is advised to carry out CE / Plus / IASME Governance annually to ensure minor changes that build up over time are audited, patching solutions continue to function, and vulnerabilities are identified and measured versus the continuous evolvement of the threat landscape.

Mandating bodies such as MoD, Education, and Health require annual frequency for Cyber Essentials and Cyber Essentials Plus. Insurance policies require continuous compliance (such as Cyber Insurance) and arguably should be maintained to prove due diligence under the Data Protection Act.

4. Are your testers suitably certified?

Pentest Cyber are appropriately qualified to provide Cyber Essentials services, offering clearance to a high government standard while being OSCP, Tiger Scheme, Cisco CCNP, NCSC CCP IA-Auditor, SIRA qualified and are Cyber Essentials, Cyber Essentials Plus, and IASME Auditors.

5. How much does Cyber Essentials / Plus Cost?

We only offer our accreditation services as a fully managed bundle, designed from our vast experience of what is necessary to achieve these, garnered from the programme's inception to the present day (inc. the many and ongoing annual changes).

Around 95% of clients fall into the scope of our managed CE service, which is £990 + VAT and our managed CE+ service, which is £4000 + VAT. Our business model focuses on helping organizations raise the minimum defences required as efficiently as possible and, as a by-product, meeting the minimum standard required for accreditation. We offer unlimited resubmissions at the CE stage, removing the prevalent and unjust "maximum revenue through maximum failures" business model.

Our base Cyber Essentials Plus bundle allows for a remote service covering up to 5 different build types and 30 externally facing IP addresses. Large estates or those with additional needs (e.g., 2+ "Class B" external

© Pentest Cyber 2026 www.pentestcyber.co.uk

addresses) will price on a case-by-case basis.

Pentest Cyber's existing clientele consists of one person micro organizations to global enterprises of 10,000+ users in various sectors.

We pride ourselves on transparency, clearly defining the boundary of the managed service. These include the number of consultancy days, audit days and any required retesting. Any "hidden extras" such as setup fees are included within the service bundle and fixed while tailored to your specific needs (with 95% of organizations being eligible for the same "standard bundle" of services).

*Prices and terms are subject to change if IASME/NCSC deadlines such as the 6-month life of the question set are exceeded or in response to changes to other aspects of the Cyber Essentials programme parameters.

6. What is included in the report for these?

Pentest Cyber provides a full testing report for Cyber Essentials Plus, which covers the following items:

- **Executive Summary** – A non-technical summary of issues for management and executives.
- **Evidence of Activities** – A summary of activities carried out to achieve the assessment.
- **Project Scope** – An area defining the agreed scope
- **Detailed technical write-up** – The anatomy of found issues for each testing area, severity, and references.
- **Risk level** – Overall risk to listed issues aligned with CVSSv3
- **Recommendations** – Pragmatic recommendations and references to remedy the cause.

© Pentest Cyber 2026 www.pentestcyber.co.uk

7. How do we work compared to other providers?

Pentest Cyber personnel are highly experienced in the delivery and remedial consultation of Cyber Essentials and Plus; one staff member has issued over 1000 certifications alone, and collectively over 3,500 (01/01/2022).

Our business model focuses on helping organizations raise the minimum defences required as efficiently as possible and, as a by-product, meeting the minimum standard required for accreditation. We offer unlimited resubmissions at the CE stage, removing the prevalent and unjust "maximum revenue through maximum failures" business model.

Pentest Cyber positions itself as a sole security service, positioning ourselves as independent auditors, preventing the use of our knowledge as a lever to on-sell systems and services.

We only offer our accreditation services as a fully managed bundle, designed from our vast experience of what is necessary to achieve these, garnered from the programme's inception to the present day (inc. the many and ongoing annual changes).

With our vast array of collective knowledge, we can engage with your technical team to advise on practical, real-world options for remediation.

© Pentest Cyber 2026 www.pentestcyber.co.uk

8. About Pentest Cyber

Pentest Cyber, a world-class resource for cyber assurance and remote penetration testing services. We specialise in subject areas such as Cyber Essentials, web application, cloud, and infrastructure testing.

Pentest Cyber deploys a vast array of professional tools, techniques, and bespoke methodologies to every engagement. UK personnel are appropriately vetted "to a high government standard" and qualified to national and international certification pathways (OSWE, OSCP, CSTL, CCNP, CCP IA Auditor, CCP SIRA).

We operate under UK law and comply with all relevant legislation. We require proof of ownership and explicit permission to undertake tasks to ensure compliance with applicable law.

Pentest Cyber operates in all sectors, including those requiring strict international security protocols. We operate remotely, use pseudonyms, and secure communication protocols as standard to protect our personnel and clients.

Pentest Cyber methodology and code of conduct align with leading international standards, consistently upholding quality through progressive elaboration, formal peer review, and sign off.

Delivered using best practice policies and procedures, carried out by highly qualified and vetted individuals with knowledge and skills of the prevailing threat landscape; covered by a rigorous code of conduct.

If you need an intuitive, autonomous test team "vetted to a high government standard" who understand CABs, ISO 27001, ITIL, "follow the sun", DCPP or the many other industry acronyms indicating specific security needs; then look no further.

© Pentest Cyber 2026 www.pentestcyber.co.uk

9. Security Accreditations and Affiliations

Cyber Essentials is the UK Government standard for cyber security. The protections you need to have in place for Cyber Essentials Plus are the same, but this time the verification of our cyber security is carried out via a technical audit.

The audited IASME Governance standard is IASME's highest level of certification and is an excellent alternative to ISO 27001 for small and medium-sized organisations.

IASME GDPR Certified demonstrates that we have considered the General Data protection regulation (GDPR) and acted accordingly to standard.

The Quality Principles standard is an IASME certification and is an excellent alternative to ISO 9001 for small and medium-sized organisations.

© Pentest Cyber 2026 www.pentestcyber.co.uk

An OSCP has demonstrated the ability to use persistence, creativity, and perceptiveness to identify vulnerabilities and execute organised attacks under tight time constraints. OSCP holders have also shown they can think outside the box while managing time and resources.

Tiger Scheme provides a way in which skills and experience can be formally recognised and is more than a statement of previous work or a reference. Skills assessments leading to certification are rigorous and are based on academic standards.

The CCP assured service has been developed by the NCSC in consultation with government, industry, and academia to address the growing need for specialists in the cyber security profession and sets the standard for UK cyber security professionals.

© Pentest Cyber 2026 www.pentestcyber.co.uk