Pricing & Service Description

G-Cloud 13 – IT Health Check

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

G-Cloud clients will receive a 10% discount on the first order. Prices are exclusive of **VAT**.

Service Name	Service Description	Total Rate
IT Health Check	Considerations are the number and type of devices in scope on an estate. A typical estate of around 200 users using a single build type of varying software packages, with in-house domain controllers and exchange services, would be ~£3500.	£2,500 - £10,000

2. What is an IT Health Check?

The Cabinet Office IT Health Check is an excellent means of discerning cyber hygiene within an organization by testing defined samples of the user, network, and public assets; presented within a formal, peer-reviewed report.

Supporting guidance: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance

3. How often should I conduct an IT Health Check?

It is advised to carry out an ITHC at least annually to ensure minor changes that build up over time are audited, patching solutions continue to function, and vulnerabilities are identified due to the continuous evolvement of the threat landscape. Some certifications, such as ISO 27001, require such testing at a set frequency to continue compliance.

Where changes to networks or where new applications are introduced, it is recommended that additional testing is to be conducted. This ensures that these changes are not introducing new vulnerabilities into production environments.

4. Are your testers suitably certified?

Pentest Cyber are appropriately qualified to provide an ITHC assessment, 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 an IT Health Check cost?

The cost of an IT Health Check depends on the specification and outcome set to achieve. Each project requires a technical scope specification to capture the testing boundary and prompt notification of issues that may arise.

Pentest Cyber, by this nature, do not provide a set price for these services to enable confidence and assurance in our delivery. We aim to be competitive, so please contact us to discuss pricing vs competition of similar quality.

6. What is included in an IT Health Check report?

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

- Executive Summary – A non-technical summary of issues for management and executives.
- Project Scope – An area defining the agreed scope
- Detailed technical write-up – The anatomy of found issues, severity, and references.
- Risk level – Overall risk to listed issues aligned with OWASP Top 10 and CVSS.
- Recommendations – Pragmatic recommendations and references to remedy the cause.

7. How do we work compared to other providers?

The three testing areas, external, internal and network assets, cover a broad spectrum to attain a benchmark of cyber hygiene. The scope remit of an ITHC are devices for which the applicant is responsible for patching. Servers or services hosted in a "cloud" environment for which others hold the responsibility (e.g., O365) are not directly in scope.

All ITHC endeavours require a definitive scope agreement to enable confidence and assurance in our delivery. Pentest Cyber has developed a pragmatic and efficient approach by phasing each testing area by priority, assessing public assets, working inward.

8. About Pentest Cyber

Pentest Cyber, a world-class resource for remote penetration testing services. We specialise in subject areas such as 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 (OSCP, QSTM, 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.

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.

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.