

Cyber Security

Penetration Testing and Continuous Security Testing and Assurance

A KPMG Service for G-Cloud 15



KPMG – About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.



330+ professionals

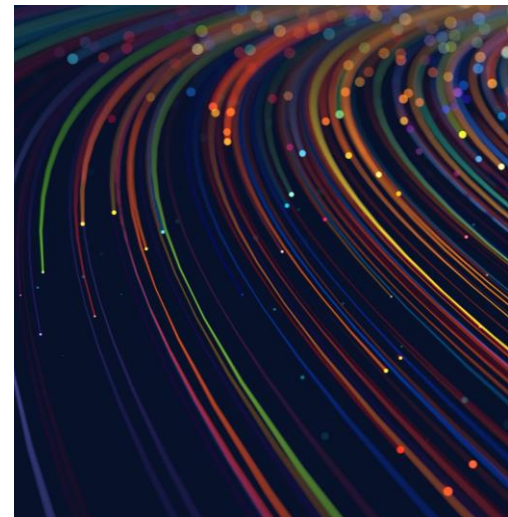
15 office locations

Part of a global team of
6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

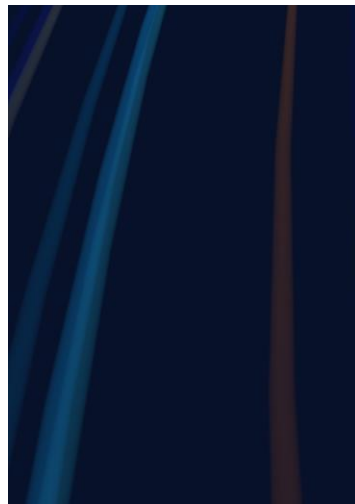
Cyber strategy 	Cyber and enterprise resilience 
Cyber tech transformation 	Cyber defence services 
Cyber risk 	Privacy compliance 
Identity and access management 	Cyber incident response 



Our Cyber team is complemented by our Connected Technology team.

We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.



Cyber Security Penetration Testing and Continuous Security Testing and Assurance



Service Description:

KPMG offer a full range of tailored penetration testing services including vulnerability assessments, infrastructure and web application testing. We provide an independent, objective security assessment for your systems, highlighting risks from external and internal threats. These assessments allow technical risks to be identified enabling mitigating controls to be implemented.



What are the benefits of KPMG Cyber Security Penetration Testing Service?

- Allow you to focus on fixing the most important issues
- Improve security on future-deployed systems
- Maintain your security accreditation
- Know how much information could be used by attackers
- Improved insight into emerging issues and solutions to ever-increasing threats
- Gain trust in the physical aspects of your IT security



Our service features

- Infrastructure Penetration Testing
- Citrix Environment Penetration
- Cyber Response and Malware Analysis
- Source Code Review
- Application Security Testing
- Wireless Security Assessment
- Device Testing
- IT Health Check
- Training and Awareness
- Social Engineering attack

Our Approach

Overview

A mature information security management system should include the need for regular security testing from a technical and configuration perspective, and also from a procedural and user awareness perspective through simulated phishing and social engineering attacks.

KPMG's CDS (Cyber Security Defence Services) team will help you comply with regulatory requirements. In addition to standard assessments, our team has helped public sector organisations create a bespoke range of tests to help them fully understand their weaknesses and risks. Key questions to consider:

- Are my internet-facing infrastructures and web applications secured?
- How do I make it harder for attackers to penetrate my defences to access sensitive corporate and customer information?
- How can I know that my systems are resilient to the latest security issues?
- How can I check the physical security of our operations, as well as our IT systems?
- In the event of a breach, are our logging and monitoring.

Introducing our Penetration testing services.

Our penetration testing service scenarios include:

- White, grey and black box testing: Through defined methodologies which cover the attack paths taken by real-world hackers, we can perform infrastructure and web application penetration testing across all technology types.
- Open source data reconnaissance: How much information is leaked about your organisation which can be used by attackers in further attacks against your systems?
- Social engineering: We can simulate scenarios such as emailing Trojans to specific email accounts to investigate whether perimeter defences can be breached via such mechanisms and persistent back-door access planted in your organisation.
- Physical security: Many organisations rely on the physical security of their building to a greater extent than their firewalls, yet do not test the physical security controls in place.
- Resilience testing: If you have a requirement to operate 24x7, you may have invested in resilient hardware and software, yet may not have tested how well the configuration works.
- Performance testing: In conjunction with our testing group we can provide a performance profile for your hardware to establish if it meets your requirements. We can also perform application stress testing to ensure it can handle the anticipated load.

Potential benefits to you:

- An independent and objective assessment of the security of your IT systems.
- A clear statement of the security risks and priorities to allow you to focus on fixing the most important issues.
- Tracking of your organisation's common IT security technical shortfalls and failings, so that any common issues in your development and deployment processes can be identified and remedied to facilitate improved security on future-deployed systems.



Penetration Testing
Cyber Security
Incident Response



Assured Service provider (CAS)
CHECK Penetration Tester
Commercial Product Assurance
CTAS Provider



CBEST

Why KPMG

We believe cyber security should be about what you can do not what you can't

Why KPMG?



Accredited

KPMG in the UK is accredited by the United Kingdom Accreditation Service (UKAS) to perform ISO27001 certification audits globally.



Independent

Our technical strategies and recommendations are based solely on what is fit and appropriate for your business.



Collaborative

KPMG's I-4 forum brings together over 50 of the world's leading organisations to discuss emerging issues and the solutions which work in an ever-increasing threat landscape.



Trusted

KPMG member firms have a long list of certifications, permits and accreditations to work on engagements for the world's leading organisations.



Global to local

KPMG is a global network of independent member firms with over 189,000 professionals in 152 countries.

We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide.



Award winning

KPMG in the UK shines in independent recognition: We were a leader in the 'Forrester Wave™: Global Cybersecurity Consulting Providers, Q2 2019' report.



How we can help turn risk to advantage

Emulating hacker actions

- Our penetration testing services provide you with an independent and objective security assessment of your IT systems, clearly highlighting the security risks to corporate and customer data from both external and internal threats. Only by emulating real life threat agents, such as disgruntled employees, external hackers and cyber attackers, can the true technical risks present in IT systems be identified. Following identification, the necessary mitigating controls can be implemented.
- Our team have performed a variety of scenario based tests against global financial institutions, retail giants and international media companies. These have included posing as cleaning staff in order to gain access to company buildings, setting up fake wireless access points to capture employee credentials and simulating a rogue employee in order to test incident response teams.

Service Details

Pricing overview, including volume discounts or data extraction costs

Consulting Prices are as per the G Cloud 14 rate structure.

Projects can be charged using either Fixed Price and Time and Materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Data extraction is not included in this service.

Service constraints like maintenance windows or the level of customisation allowed

This is not relevant to this service.

Service levels like performance, availability and support hours

Not relevant to this service.

How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

The ordering and invoicing process

The ordering process for G Cloud services is laid out in the 'G Cloud buyers' guide on the www.gov.uk website.

Invoicing arrangements will be as per the agreed G Cloud order form and will vary from engagement to engagement.

How buyers or suppliers can terminate a contract:

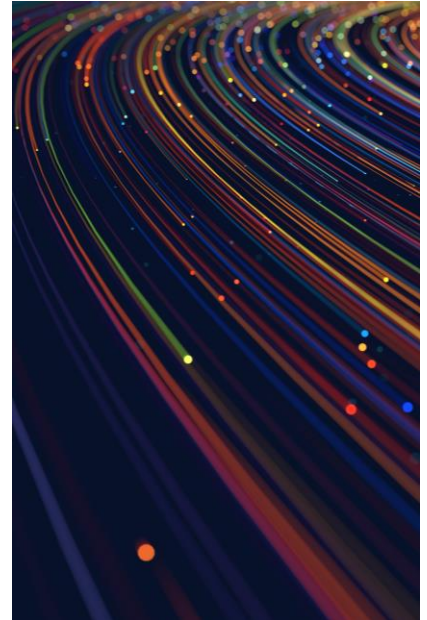
Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- convenience,
- failure to remedy a material breach and
- insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.



Any technical requirements

Each Cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for the majority of organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the Services. Microsoft Office 365 & Teams are used by all colleagues within the firm, with other tools such as Jira and Confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.



kpmg.com/uk

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: KPMG Confidential

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026