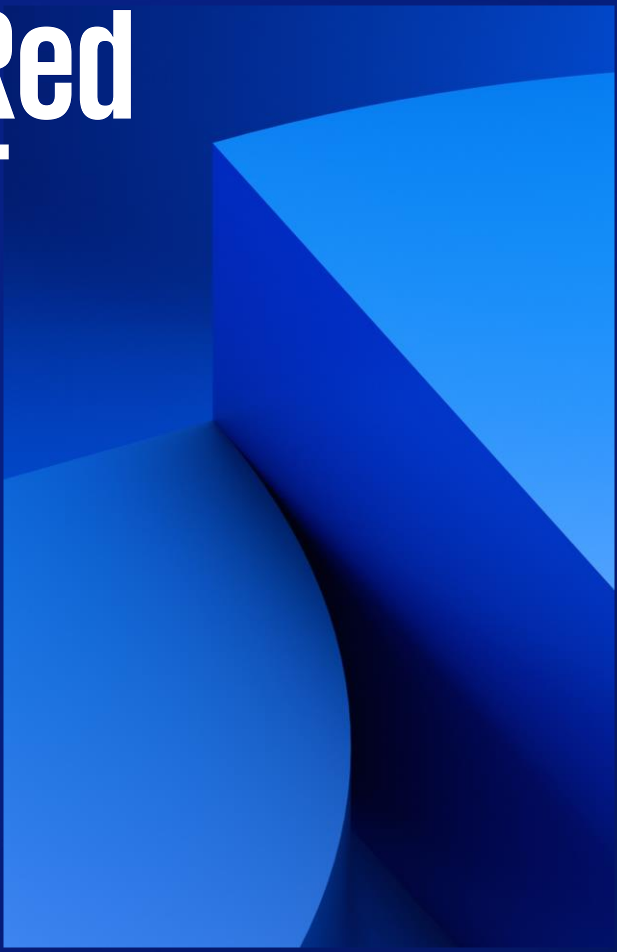
KPMG

Cyber Security Red Team and GBEST service

A KPMG Service for G-Cloud 14

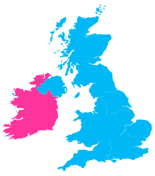


May 2024
kpmg.co.uk

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 trans-formation
- 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 Red Team and GBEST service

Service Description:

KPMG delivers simulated attack exercises for the most demanding of public sector organisations in the UK and globally. Our assessments focus on demonstrating the impact of realistic threat scenarios; shaped by our collaboration with threat intelligence providers, incident responders and SOC teams. KPMG's service will provide you with a realistic assessment of your security posture.

What are the benefits of KPMG Cyber Security Red Team and GBEST Service?

- Obtain holistic and independent assessment of your IT systems security
- Gain a clear view of cyber risks and their impact
- Enable you to effectively prioritise improvement activities
- Enable your firm to protect against cyber-attacks in practice
- Ensure IT initiatives appropriately reflect security risks facing your organisation

Our service features

- Deliver NCSC accredited GBEST services to public sector organisations
- Consider operational impact, and explain discovered vulnerabilities
- Simulate hacker actions to deliver a profile of internet-facing threats
- In-depth weakest link testing on your networks and back-end systems
- Assess level of access to visitors, facilities and internal roles
- Social engineering exercises to test your employees' security awareness
- Physical security testing ensuring unauthorized visitors cannot compromise security
- Includes phishing exercises by email spoofing or instant messaging

Our Approach

Overview

Cyber Security incidents are increasingly unpredictable in both their targets and their methods. KPMG combines field-leading expertise and thorough assessments to define and carry out realistic scenarios to help achieve actionable and relevant insights, keeping your organisation secure.

- Cyber security breaches are today more common and ever more public. Threat agents such as hacktivists, organised crime groups and state- sponsored cyber spies have a variety of motivations and almost any organisation can be a potential target.
- While organisations are already struggling to maintain a clear view of their complex and widely distributed IT environments, the traditional security assurance activities are not answering the fundamental question – can we be hacked?
- We can help refine your requirements, define and carry out realistic cyber security scenarios that combine breadth-first target identification, target prioritisation, and in-depth focus on your key problem areas.

Introducing Red Teaming and GBEST services

- We are accredited by NCSC to deliver GBEST services to government.
- We have helped many organisations and Central Government Departments understand how and why hackers can breach their IT environments. This includes running GBEST services.
- In the course of client engagements, we have been able to demonstrate many end-to-end attacks and trace these back to the underlying business process issues. The attacks have included obtaining full control over a client's corporate network through an involved breach of their internet-facing perimeter, and getting access to client bank account statements and email accounts over Wi-Fi from a public car park.
- Our work focusses on quality and clarity: we have helped clients define broad and meaningful initiatives to improve their information security posture.

What's in the box

Our Red Team services provide you with an independent and objective security assessment of your IT systems and business processes. We will work with you to define scenarios and test cases relevant to your organisation, carry these out with consideration to the operational impact, and clearly explain the discovered vulnerabilities and their business impact.

Red Team Light. Our Red Team Light service provides a rapid assessment at a reduced cost. This includes:

- Simulating the actions of a hacker aiming to breach your organisation from the internet
- Understanding the level of access available to office visitors, facilities staff and internal roles
- We will map out the internal resources available to the particular access level and aim to escalate our privileges on internal IT networks and systems.

CREST

Penetration Testing
Cyber Security
Incident Response

CESG

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

CREST STAR

CBEST

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

In the event of supplying software services, 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 plus Skype 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

This proposal is made by KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent firms affiliated with KPMG International Limited (“KPMG International”), a private English company limited by guarantee. The proposals set out in this document do not constitute an offer capable of acceptance. They are in all respects subject to satisfactory completion of KPMG's procedures to evaluate prospective clients and engagements, including independence and conflict checking procedures and, the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International and its related entities provide no services to clients. No member firm has any authority to obligate or bind KPMG International, any of its related entities or any other member firm vis-à-vis third parties, nor does KPMG International or any of its related entities have any such authority to obligate or bind any member firm.

Document classification: KPMG Public