KPMG

Cyber Security NCSC – accredited Cyber Incident Response

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

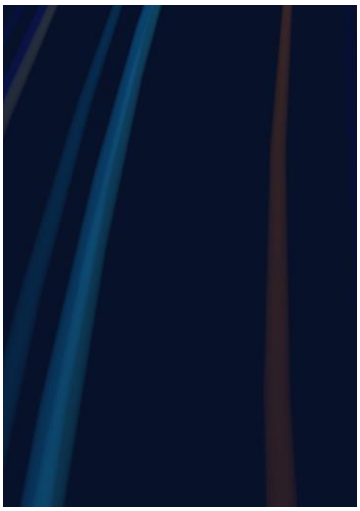
15 office locations

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 risk
Cyber and enterprise resilience	Privacy compliance
Cyber tech transformation	Identity and access management
Cyber defence services	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.

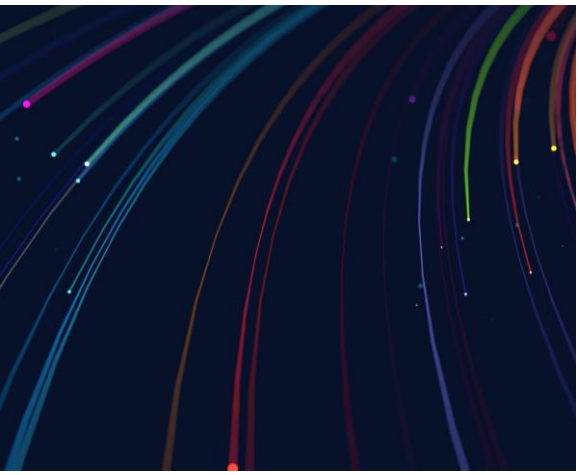
We apply a data and technology driven approach to drive change through our digital transformation services.

KPMG Cyber Security NCSC – accredited Cyber Incident Response

Service Description:

KPMG's Cyber Security NCSC-accredited Cyber Incident Response service draws on technical security experts, experienced incident managers, forensic specialists and legal advisors.

KPMG helps clients security staff detect, contain and recover from cyber-attacks. We handle insider threats, cloud incidents, hacking, ransomware, Denial of Service and bespoke scenarios; targeting in-house or cloud-based estates working to restore client to a secure state.



What are the benefits of KPMG Cyber Security NCSC – accredited Cyber Incident Response services?

- Obtain an independent view of the risks your organisation faces.
- Gain improved cost-effective Cyber Response capabilities.
- Manage any Cyber Attacks that your organisation may experience.
- Gain confidence in the state of your Cyber Incident Response procedures.
- Improve insight into emerging issues and solutions to ever-increasing threats.

Our service features

- Cyber incident response maturity and readiness assessment.
- Incident response governance; policy, planning, and playbook development.
- Threat Intelligence Collection.
- First Responder Training.
- Deploy tools and systems to identify potential attacker behaviour.
- On call 24/7 to provide advice and guidance.
- Work with technical and security staff on recovery strategies.
- Collate technical details and losses due to an incident.
- Information updates on emerging threats on a regular basis.
- A truly global capability via 146 country network of offices.
- Incident Response & Crisis Management Simulations.
- Crisis Management & Incident Coordination.

KPMG Approach

Cyber Incident response services: A look at our capabilities

Digital investigations

- Business Email Compromise Ransomware
- Network intrusion Intellectual property (IP) theft Botnets and malicious code
- Spear phishing & account takeovers
- Court-appointed neutral expert
- Expert testimony
- On-demand cyber response

Digital strategy

- Privilege consulting Tabletop exercises
- Adversary simulation/cyber exercises Proactive consulting
- Compromise assessment IR Program Assessment Staff augmentation

Digital disciplines

- Digital evidence preservation Digital evidence recovery Network forensics
- Host forensics Mobile forensics
- Memory forensics Malicious code analysis Database and log analysis

We provide complete coverage protection. Our experts will help safeguard both IT and OT assets, ultimately protecting business operations and people. Our incident response service goes beyond cyber to support the business during crisis. See below.

Incident Response

In the case of a cyber incident, resources from out team of highly skilled incident responders will be mobilized and triage activities initiated.

Incident Preparation

To mitigate the effects of a cyber incident, proper preparation is essential. KPMG is able to help ensure your organisation is prepared in the event of a cyber-attack.

Incident Recovery

Following an incident, the KPMG team will be on hand to ensure your mind is at ease and will help your organisation return to business as usual as quickly as possible.

Crisis Management

In the event of a cyber crisis having a comprehensive crisis management strategy is invaluable. KPMG's crisis management experts regularly assist with designing and implementing crisis management procedures

Monitoring

During and after a cyber-attack, it is essential to monitor the network for any indicators of compromise.

Forensic Investigation

In line with recent regulations, it is often necessary for companies to run forensic investigations if they are the subject of a cyber incident. Our forensic team assists wit initial triage and investigation.

Communication

In event of Incident KPMG's communication team are able to minimise the impact by providing advice on speaking to media and clients

Legal help

The recent GDPR privacy and data protection law contains detailed regulations which must be followed in the event of a breach. Our team of IR and Crisis management is trained to assist legal firms in such situations

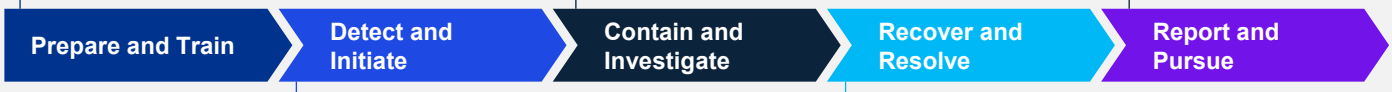
Our Approach

High level incident response methodology

With our tailored onboarding sessions, we work with the relevant client stakeholders to understand their business, infrastructure and systems. This helps us to be fully prepared to assist them in the event of a cyber attack, not only with our in-depth expertise, skills and knowledge but also with being up to speed on their organisation and processes.

Depending on the incident, our experts will make sure the right response is chosen to contain the incident and minimise the impact on the affected client. Should the need arise, we would deploy Cylance (endpoint detection and response tool) to our clients endpoints to help with containment. We would also request them to run specific tooling to gather data and logs for investigation and analysis.

Once the incident response has concluded, we will create a detailed report for our client that covers the incident, analysis, resolution, findings and recommendations. This can then also feed into their continuous security improvement process. We will provide our cross-industry insight and advise them on the most effective remedial actions to minimise the impact of similar incidents in the future.



As part of the clients SOC operations, generally they will already be monitoring for threats and vulnerabilities. Should anything be detected or the client experiences a cyber attack of any sort, they will call us on our dedicated hotline. We will initiate the response and arrange a scoping call within the agreed SLA. We would mobilise resources according to the incident type in terms of required skills, and location. We would be good to go as soon as we receive email notification from the client to proceed.

We will work with them to prioritise the recovery of the most critical assets and assist them with getting back to business as usual operations.
The onboarding workshops, assessments and reviews of the organisation will help to guide us in the right direction for a speedy recovery and give us a head start on our approach.

Our Approach

This slide gives an overview of the tools we can leverage for gathering forensic artefacts and carrying out incident investigation process.

KPMG Evidence Management System

KPMG uses industry-leading collection, preservation and analysis. KPMG's digital evidence handling protocols include chain-of-custody procedures, authenticity of evidence, encryption, and tracking of physical/logical evidence.

KPMG understands the importance of simplifying evidence management for large and diverse data sets, staying in control of budgets, and maintaining project timelines, all while providing a defensible audit trail to avoid adverse rulings levied in court.

KPMG believes that evidence tracking should be integrated into the incident response process in order to help ensure accuracy, efficiency, and awareness of the data through out the various phases of a project.

Tool Agnostic

KPMG is tool agnostic and vendor neutral. KPMG uses tools including but not limited to the below and can provide independent assurance of their efficacy and applicability.

Network forensics
- Fidelis Cyber security™
- RSA NetWitness™
- Suricata™
- Wireshark™

Log data
- ArcSight™
- Elastic search, Logstash, Kibana™
- LogRhythm™
- Plaso™
- QRadar™
- Splunk™

Endpoint detection response
- Carbon Black™
- Crowdstrike Falcon™
- Cylance Optics™
- FireEye HX™
- Google Rapid Response™
- Microsoft Defender ATP™
- Tanium™
- Sysmon™

KPMG's Evidence Management System

Host forensics
- Encase™
- Access Data Forensic™
- F-Response Enterprise™
- NUIX™
- Axiom Forensics suite™
- TZworks™

Memory forensics
- Volatility Framework™
- Rekall™

Malware analysis
- Cuckoo Sandbox™
- Falcon Sandbox™
- Ghidra™
- IDA Pro™
- REMnux™
- Threat Analyzer™

Why KPMG

Create Note: Due to non clarity of the map we have kept as an image, please review and advice

Our Cyber Response professionals are experienced in responding to cyber crime incidents, including insider threats, data breaches, hacktivism, cyber terrorism, organised crime frauds and Advanced Persistent Threats.

Frost & Sullivan recognises KPMG for its innovative KPMG digital responder cyber application

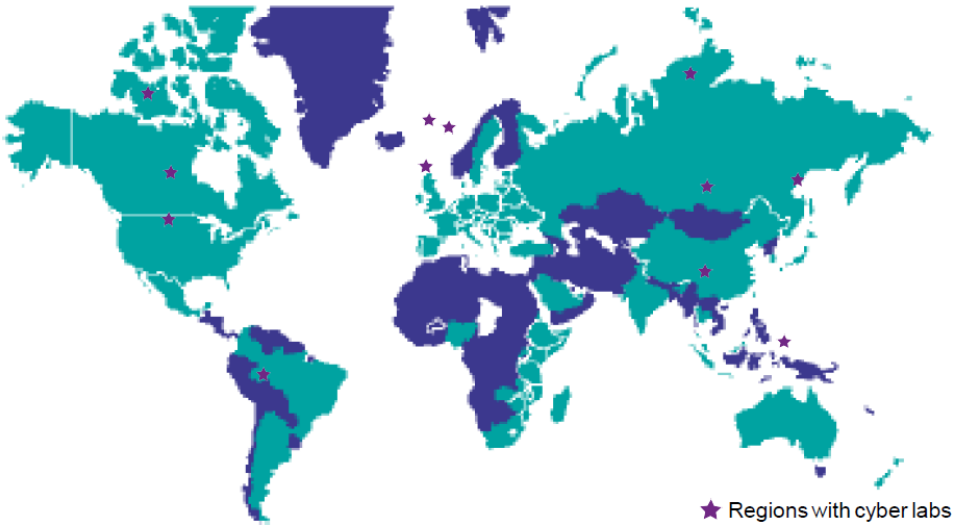
Frost & Sullivan recognised KPMG with its 2017 Global New Product Innovation Award for the firm's innovative KPMG Digital Responder, an automated forensic collection, analysis, and reporting solution.

Distilled from its years of digital forensic and incident response field investigations, KPMG Digital Responder is a flat-rate cyber investigations tool that allows KPMG to automate cyber response from the point of collection to reporting—at a predictable fixed price. It can reduce costs of cyber investigations; shift time spent from collecting data to actual analysis, and provides more time to organisations to make faster, more informed strategic business decisions to manage potential cybersecurity risks.

Global consistency and local capability

KPMG has over 3,500 cyber professionals in offices around the globe with cyber labs across major regions including but not limited to the United Kingdom, as well as primary cyber labs in the United States, Spain, Australia, Japan, Netherlands, Russia, Singapore, Malaysia, Canada, China, Mexico, and Argentina.

- Consistent global approach, common methodology
- Rapid response through single point-of-contact and institutional strength



Why KPMG Cyber response?

KPMG Cyber has an extensive professional network within KPMG member firms across the globe that can assist organisations in transforming their security, privacy, and continuity controls into business-enabling platforms. All while maintaining the confidentiality, integrity, and availability of critical business functions. KPMG's approach aligns with our clients' business priorities and compliance needs:

- Our experienced cyber response professionals possess leading technical experience.
- Many of these professionals are leaders in the cyber community, helping to develop the tools and methodologies used to combat cyber crime on a daily basis.
- We have extensive experience building, delivering, and supporting cybersecurity programs for FORTUNE 500 and Global 2000 companies across a multitude of industries.

KPMG Cyber's approach—*Prevent, Improve, Detect, Respond*—is designed to be simple and effective, and most importantly aligned with your business needs.

Our professionals have experience countering various forms of cyber crime, including insider threats, data breaches, hacktivism, and advanced persistent threat-style intrusions by highly motivated adversaries. Our services include on-demand malicious code analysis, hostand enterprise-based forensics, network forensics, threat intelligence, and witness testimony.

KPMG is involved in the information security community. This involvement provides us with early insight into emerging issues, which we share with our clients and the project support teams as a component of our advisory role. Our advice and the services are continually refined by our experience gained serving clients of various sizes, scopes, and complexities.

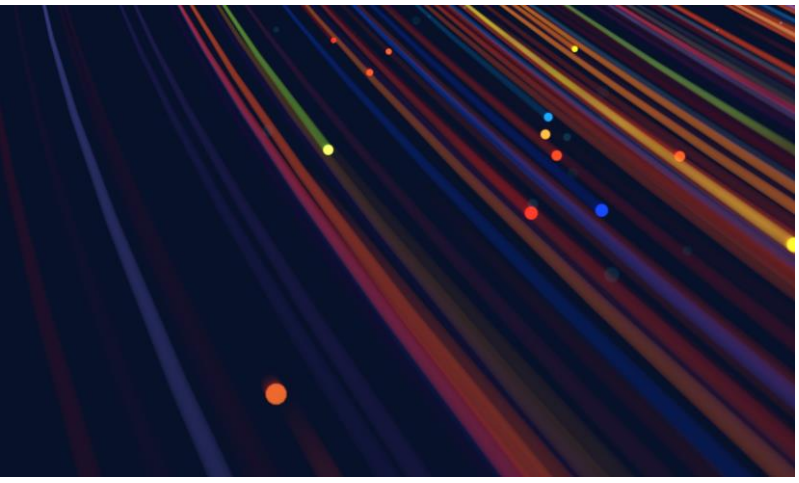
KPMG is a preferred provider of Cyber Response Services to many organisations and acts as an extension of other organisations' internal teams. Lastly, our services are tool agnostic and vendor neutral.

Why KPMG

Case Study #1: Health Organisation—Digital evidence collection

As part of ongoing litigation and anticipation of a government investigation, KPMG was retained by one of the largest health organisations to coordinate the collection of digital media and hard copy documents from an active research facility. To meet the client's request to minimise disruption to the research facility and quickly complete the collections, KPMG assembled a team of 25 forensic professionals to collect over 130 TB of electronically stored information from 3,900 Cyber media devices and 500 boxes of hard copy documents in 108 hours.

The media collected was part of the hospital's infrastructure and bring your own device (BYOD) program with varying specifications and configurations, including Macintosh (MAC), Windows, and Linux systems. KPMG had to work with outside counsel, in-house counsel, IT professionals and the medical staff to develop the most effective way to collect the data with minimal operational disruption to the ongoing research. KPMG followed its standard operating procedures to help ensure forensic imaging and document the transfer of chain of custody per leading industry practices. KPMG also developed a customised methodology to meet the client's expectations and successfully collected data from the individual custodians, lab workstations, medical equipment, external media, network shares, personal shares, e-mail servers, and hard copy documents leveraging the industry leading and proprietary forensic tools.



Case Study #2 Large hospital—ransomware

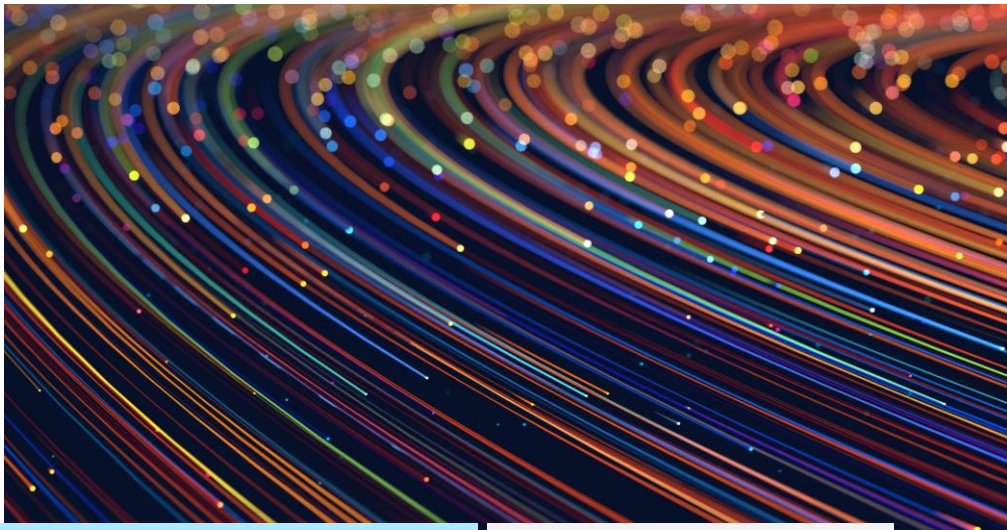
For a large affiliated hospital network, KPMG led the recovery following a ransomware attack that resulted in complete loss of access to its electronic health records database—to the point which impacted multiple hospitals from servicing patients. After another IR vendor was unsuccessful, KPMG reverse-engineered the ransomware to determine how it encrypted the data and developed an innovative approach to fully recover their data and help restore operations—an effort most would have considered impossible. KPMG was then further engaged to assist with the structured data sensitive data review to assist with notification obligations.

Case Study #3 Large public company—incident response

For a large public company, KPMG coordinated global IR to a cyberattack involving Shamoon malware. This malware was known to first target the oil and gas industry in August 2012, when reported tens of thousands of computers in the Middle East were destroyed. KPMG's client was impacted by a variant of this malware which researchers publicly attributed to the Iranian hacking group APT33. This resulted in tens of thousands of computers across the company being inoperable—and losses of millions of dollars a day

in productivity. In response, KPMG helped coordinate a multinational team including U.K., U.S., and Singapore to stand up a 24x7 enterprise monitoring and containment operation to isolate the propagation of malware. We further assisted with the investigation of root cause analysis and remediation.

Why KPMG



Implementation Plan

Timescales are driven by a number of variables including the scale and complexity of each Customer's scope together with quality of data and availability of resources. We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG Powered service would be agreed as part of the procurement of the service. As part of the service we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs. Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop / articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement
- Provision of orientation sessions in our methodologies and assets, for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account in change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a Project kick off event and associated materials to formally launch the project and to aid new joiners in orientation

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.

Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

This is not applicable for this service.

Customisation:

This is not applicable for this service.

Offboarding:

Each implementation has a post go live ("Evolve phase") in which KPMG will provide post go live support working with each Clients Business as Usual (BAU) team to fully transition on going service delivery to the Clients' BAU support team according to the agreed plan.

Service Details

Service levels like performance, availability and support hours

This is not relevant as this service does not involve a standard software solution.

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

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026