KPMG

Cyber Risk Quantification Service with KPMG Cyber Risk Insights

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

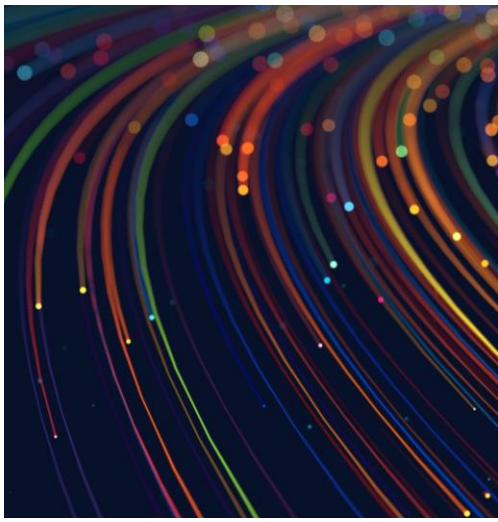
15 office locations

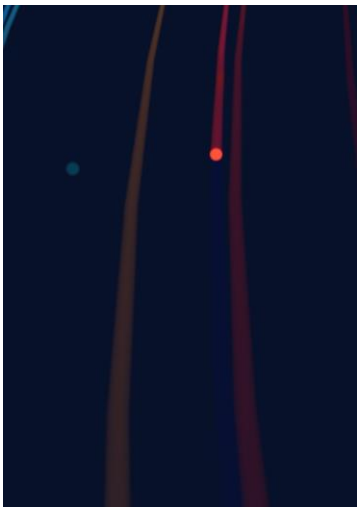
Part of a global team of 6200+ individuals

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.

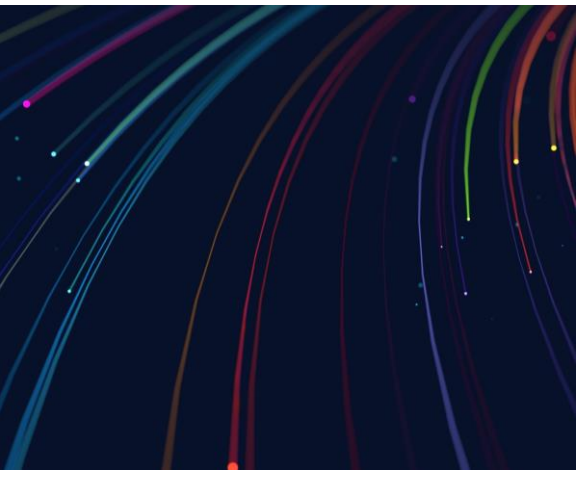
We have access to a 2000- strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

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

Cyber Risk Quantification Service with KPMG Cyber Risk Insights

Service Description:

KPMG cyber risk quantification subject matter experts can conduct analysis to help gain visibility of risk exposure and determine what actions will maximise risk reduction. They can also provide support services around KPMG Cyber Risk Insights, an intuitive Cyber Risk Quantification SaaS product to help you build the capability in-house.



What are the benefits of KPMG Cyber Risk Insights Services?

- Quantify your cyber risk exposure in financial terms
- Identify what capabilities maximise risk reduction
- Make more objective decisions on where to invest
- Understand what risk reduction could be achieved for your investment
- Communicate cyber risk posture to the Board in business terms
- Upskill in cyber risk quantification

Our service features

- Cyber risk quantification assessment
- Threat-modelling of scenarios relevant to your business
- Identify strengths and weaknesses in your defences
- Simulation analysis to test the effectiveness of defence mechanisms
- Measure risk reduction through cost-benefit analysis of your initiatives
- Cyber risk exposure report
- Cyber risk quantification services support

Cyber Risk Insights

A market leading product to help you make better cyber risk decisions

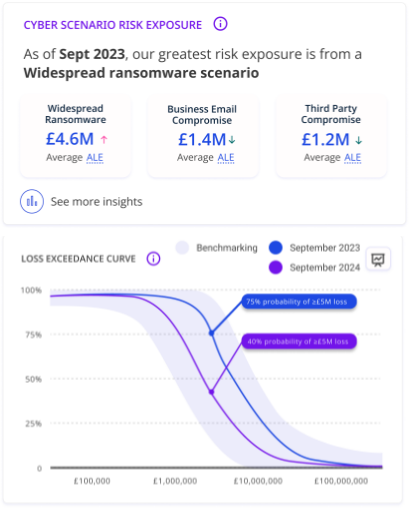
What is KPMG Cyber Risk Insights (CRI)?

CRI is a licensable SaaS product which takes a scenario-driven approach to more accurately assess the likelihood and impact of cyber-attacks. It uses powerful and intuitive dashboarding to show insights, with a strong user interface.

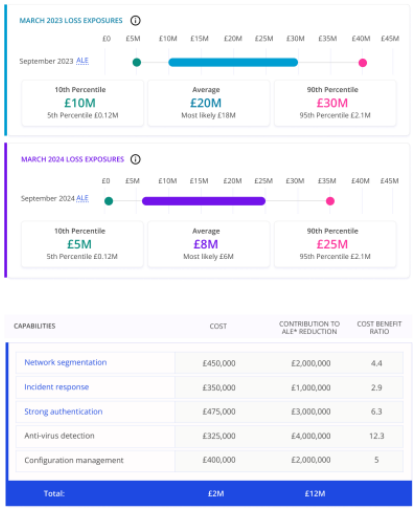
Key inputs	Cyber threat scenario modelling	Cyber capability effectiveness estimations	Attacker contact rate estimations	Financial impact estimations	Cyber investment data

Example 'insights'

Prioritise cyber risks

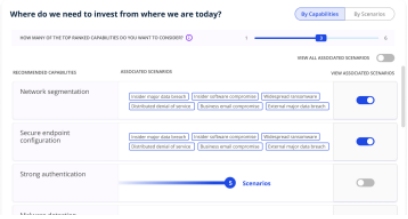


Optimise cyber spend



Fix weaknesses in defences

Identify optimal future improvements



Why use KPMG CRI?

CRI gives you a comprehensive view of the potential financial losses in the event of a cyber-attack, as well as the best 'bang for buck' investments to help mitigate those attacks. This allows you to make defensible and data-driven decisions and can help you prioritise your remediation efforts. The typical questions CRI helps answer are below.

Prioritise cyber risks	Regulator(s) Board CEO CFO COO CIO CRO CISO Business	What is our true risk exposure to cyber attack (likelihood in a year and potential financial impact)? Is it within our risk appetite? What cyber risks should we prioritise?
Optimise cyber spend	Board CEO CFO COO CIO CRO CISO Business	What cyber investments would deliver best bang-for-buck risk reduction? If we invest XM in cyber next year, is this too much or too little?
Improve communication	Board CEO COO CIO CRO CISO Business	I know cyber is a complex risk with many interdependencies – how can we simply explain our overall exposure in order to make effective well-informed decisions?
Comply with regulation	Regulator(s) Board CEO CRO CISO	How can I determine the potential 'material' impact of a cyber attack on my business? How can I communicate cyber risk to the Board to meet new cyber reporting requirements?

Assessment Approach

Below highlights the key phases and activities of a Cyber Risk Insights assessment at a high level.

Cyber threat scenarios

We have conducted threat modelling on 12 cyber risk scenarios. These attack paths are integral to the analysis, helping understand what capabilities deliver maximum risk reduction.

Cyber capability analysis

Our approach is to score the process maturity, technical effectiveness, and coverage of capabilities. This helps us understand the strengths or weaknesses in defences and, identify future areas of focus.

Attacker contact rate estimations

Attacker contact rate (ACR) is an estimation of the number of attack attempts in a given year, based on the frequency of historic incidents or protective monitoring data. ACR is used to make an annualised estimate of scenario likelihood rather than just a relative one.

Financial impact estimations

Our financial impact modelling uses Monte Carlo simulations to generate Loss Exceedance Curves. These curves demonstrate how a range of losses are possible (not just a point value as shown in a typical risk matrix), and that larger losses are less likely than smaller ones.

Cyber change projects / initiatives

Our cost-benefit analysis modelling uses information about your initiatives and their impact on risk reduction. This can be done proactively to simulate potential strategies or, reactively to demonstrate the impact of decisions.

- Identify scope
- Decide use case
- Select scenarios

- Assess cyber capabilities

- Estimate Loss Event Frequencies
- Estimate Loss Magnitudes
- Input Investment Data

- Report creation

How has CRI helped our clients?

Business case for investment

Healthcare

Enabled a national health organisation, to forecast the potential reduction in cyber risk exposure through executing on their multi-year cyber strategy.

- ✓ A baseline view of cyber risk exposure across Secondary Care, and forecasted risk reduction from the programme.
- ✓ National guidance documentation aligned to the National Cyber Security Centre Cyber Assessment Framework outcomes.
- ✓ Supported the central cyber risk management team on operationalising their cyber risk management lifecycle, enabled through risk quantification.

Prioritisation of a cyber roadmap

Insurance

A CISO was receiving Board-level challenge about the benefit of the cyber investment programme and was asked to reduce spend. CRI enabled:

- ✓ Identification of the priority controls for investment based on robust cost-benefit analysis.
- ✓ Demonstrable year-on-year reduction in cyber risk exposure tied to benefits tracking of change initiatives.
- ✓ Granular assessments of individual business units after the Group-wide assessment.

Managing exposure across a portfolio

Private Equity

Cyber risk assessment's and remediation plans were required across 20+ Portfolio Companies. CRI enabled:

- ✓ Each Portfolio Company to understand their cyber risk exposure, in financial terms.
- ✓ Each Portfolio Company to prioritise their cyber investments based on the specific threats to their business.
- ✓ The replacement of their 1-5 maturity assessment methodology, giving leaders better confidence in the security of their portfolio.

How can CRI help you?

Make the case to the board

CRI's logical and transparent approach helps you to communicate cyber risk to senior stakeholders, demonstrate the business benefits of cyber capabilities and make compelling investment cases.

Carry out systematic, consistent, data-driven assessments

CRI makes the adoption of quantitative techniques quick and simple and improves the objectivity of risk assessments by producing consistent, data-driven results.

Quantify likelihood and impact

Access to our tried and tested models, which quantify the likelihood of cyber-risk scenarios occurring, the possibility of attackers succeeding across the layers of defence and potential financial losses.

Target spend to reduce exposure

Graphical risk scenario models allow you to see where your cyber capabilities contribute to risk reduction across the layers of defence and which areas would benefit most from investment.

Help optimise investments

Determining the optimal investment portfolio of cyber capabilities, to help achieve a great return on investment in risk reduction.

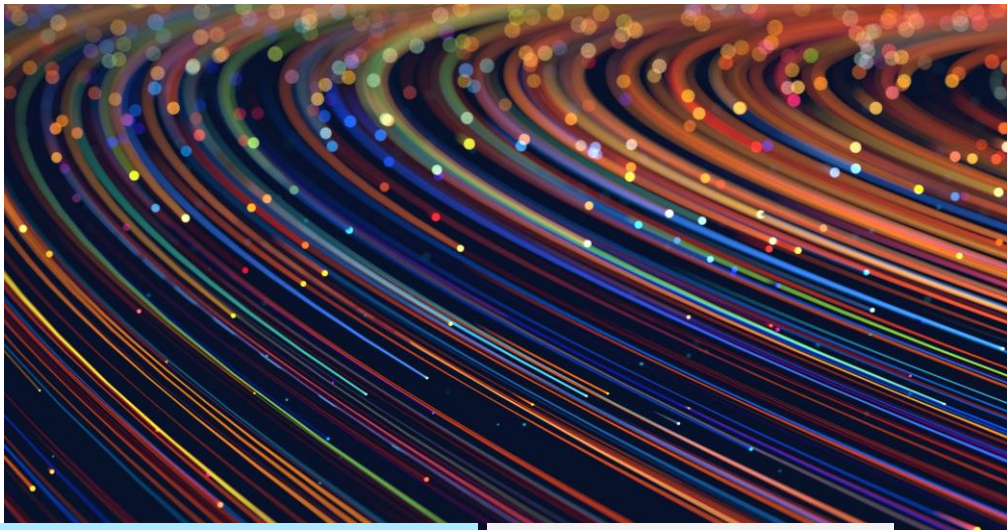
Test investments

Estimate the payback period for an investment or investment portfolio, based on a cost-benefit analysis of spend compared to the expected reduction in cyber losses.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/uk/en/CRI

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.

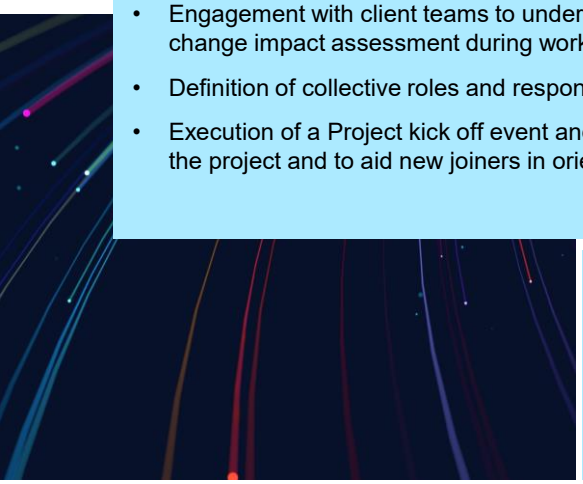
Service constraints like maintenance windows or the level of customisation allowed

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

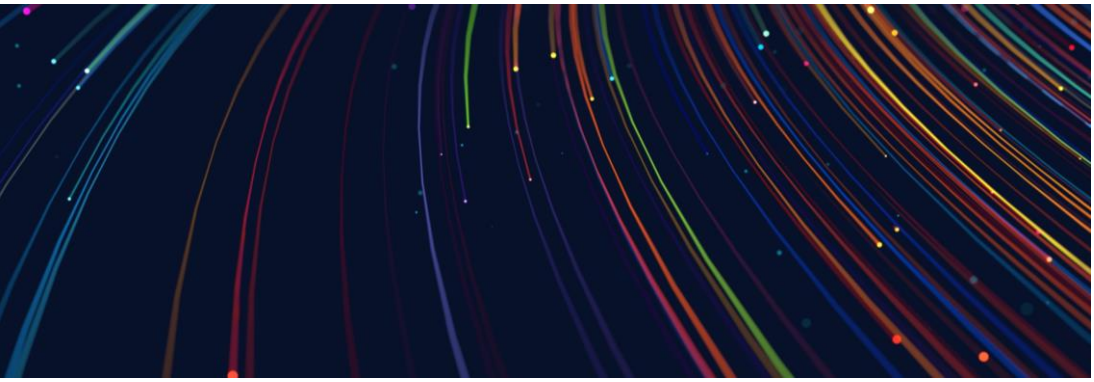
KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.

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