KPMG

KPMG Cyber Security Maturity Assessment and Cybersecurity Assessment Framework (CAF) compliance analysis

A KPMG Service for G-Cloud 14

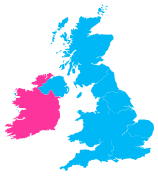
May 2024

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

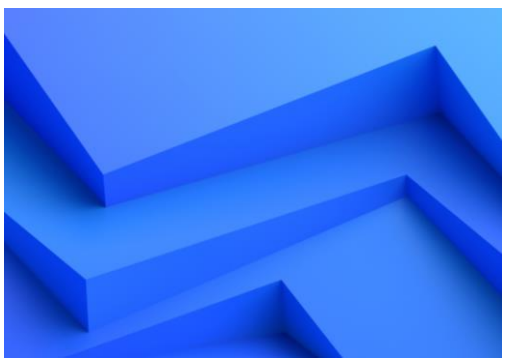
UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

- 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.



KPMG Cyber Security Maturity Assessment and Cybersecurity Assessment Framework (CAF) compliance analysis

Service Description:

KPMG's Cyber Maturity Assessment provides an in depth review of how prepared an organisation is to protect its information and assets against cyber threats in a cloud environment.

The Cyber Maturity Assessment (CMA) looks beyond your organisation's technical preparation for cyber threat and takes a rounded view of people, process and technology.

The CMA domains are mapped to the Cyber Assessment Framework and GovAssure domains. The CMA to be used to support pre-GovAssure assessments and the development of a tailored cyber security strategy and roadmap.

What are the benefits of KPMG Cyber Security Maturity Assessment?

- Understand your organisation's ability to protect against cyber threats.
- Benchmark your cyber security maturity levels against peers.
- Identify vulnerabilities before they are exploited.
- Identify and prioritise areas for remediation.
- Demonstrate both corporate and operational compliance.
- Identify and prioritise cyber security strategy remediation.
- The "platformed" CMA - the 9 domains of the core cyber security assessment sit as 247 control areas on our Cyber Strategy and Governance SaaS platform.
- The platform can conduct assessments across multiple parties concurrently and is optimised for remote working.

Our service features

- Fixed Price standalone or with complementary Extended ITSM Build
- CMA Domains as follows
  - Leadership and Governance
  - Human Factors
  - Information Risk
  - Management
  - Compliance
  - Security Operations
  - Security Architecture
  - Cyber Resilience
  - Technical Security
  - Third Parties
- Inherent control mapping capabilities can be used to conduct security audits.
- Assessment maturity can be replayed in real time to identify any critical risks, trends or errors.
- Real time reporting and analysis accelerates identification of risk exposures and high priority vulnerabilities.

Our Approach

The Challenge
Cyber risk is an evolving and increasing risk across public sector given the scale and complexity of digital and legacy infrastructure.

Where to start?

- What security controls do you have in place already?
- Baseline your current security posture in order to understand strengths and weaknesses and prioritise effort to establish and maintain the appropriate security posture.
- What are others doing and why? Is your security appropriate to your risk?

- KPMG's Cyber Maturity Assessment (CMA) provides a holistic view of an organisation's ability to protect its information assets and respond to an ever-changing cyber threat landscape. It is based on a number of international 'good practice' standards, including ISO27001, NIST, Cyber Assessment Framework (CAF) and ISF SoGP, designed to provide a point in time maturity score for the purposes of benchmarking.

A holistic cyber security framework that makes sense of cyber to the business

KPMG's Cyber Security Assessment domains are as follows

1. Leadership and Governance

The board and management, their due diligence, ownership and effective management of risk within the context of the organisation's goals, objectives and the external threat/risk landscape.

2. Human Factors

The level of security-focused culture that empowers and ensures the right people, skills, culture and knowledge come together.

3. Information Risk Management

The approach to achieve comprehensive and effective risk management of information throughout the organisation as well as its delivery and supply partners.

4. Compliance

The processes in place to identify and interpret cyber security and privacy implications of relevant laws and regulations. This includes cyber and privacy specific legislation, general legislation and regulation. This process should drive the implementation of controls enabling compliance to be measured and reported on.

5. Security Operations

The capability to monitor, assess and defend information systems from different cyber security threats. Activities including threat intelligence, vulnerability assessments, log and event correlation and incident response, which can be combined to ensure a more effective capability.

6. Security Architecture

The organisation has an appropriate and cohesive security architecture, which addresses the organisation's requirements and risks, and specifies what security controls are to be applied and where.

7. Cyber Resilience

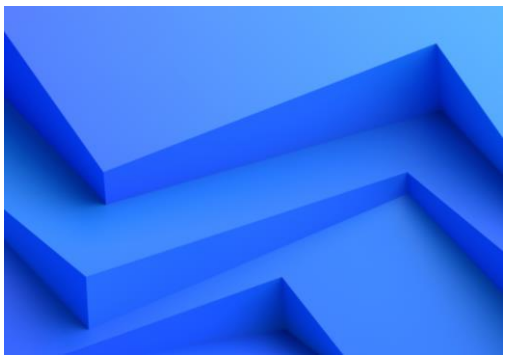
The organisation has the ability to recover from a successful cyber attack with as little business disruption, regulatory conflict, and reputational impact as possible. A holistic approach to crisis, integrating human irregularity with technical considerations outlines a good practice approach to resilience.

8. Technical Security

Integrating technical security solutions, which include: malware protection; identity and access management; intrusion detection and data leakage prevention.

9. Third Parties

Ensuring the successful development and deployment of a third party security due diligence and oversight programme. This includes the design of a risk triage model, assessment workflows, third party security evaluation methodology and execution of third party security assessments.



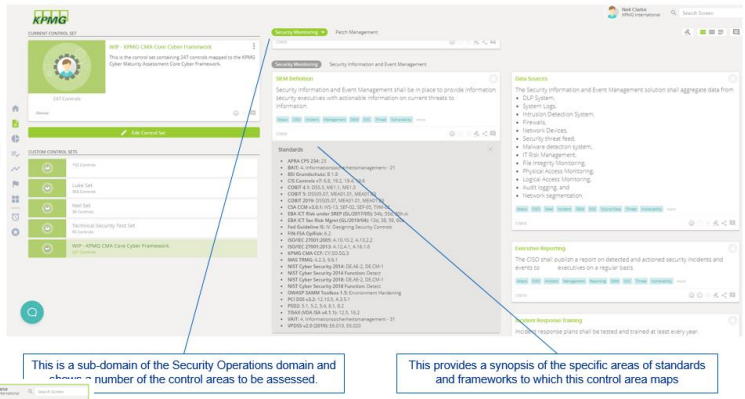
Our Approach

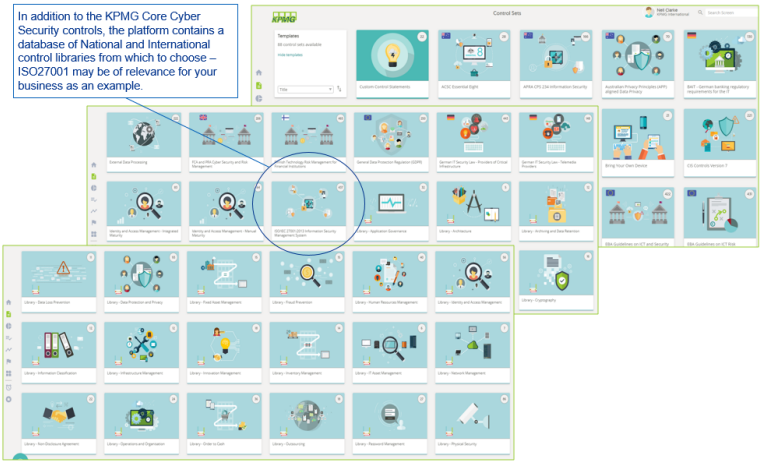
The Platform

The **9** domains of the core cyber security assessment sit as **247** control areas on our Cyber Strategy and Governance SaaS platform, enabling rapid concurrent assessment, correlation, comparison and mapping to aligned standards and frameworks. This would always be our default recommendation for a core, holistic set of controls by which to assess capability and maturity.

There are **88 control libraries** (and growing) from which assessments may be enabled integrated and ultimately mapped.

The platform can be employed to rapidly design and build bespoke control frameworks to conduct across multiple parties concurrently and is optimised for remote working.





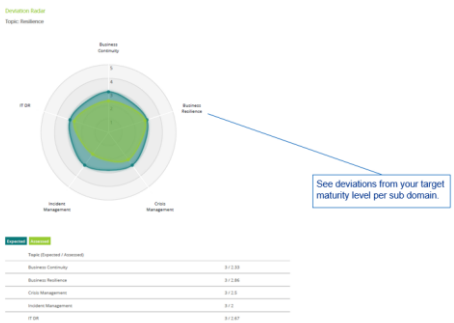
Once the relevant controls have been scoped an assessment can be built, including defining target maturity levels by domain and control area and if required, logic to direct detailed commentary. There is additional functionality by which to set filters to define logical categorisation of completed assessments e.g. high, medium, low risk – useful in the conduct of multiple assessments against multiple entities, ultimately to be compared to each other, such as third party and/or supply chain assessments.

Real Time Reporting

Assessment maturity can be replayed in real time as a mechanism by which to identify any critical risks, trends or errors.

Real time reporting can look at per domain measures at given points in time also – useful for rapid 'wash-up' sessions with specific business owners or stakeholders.

Such real time reporting allows for ready analysis and discussion of key findings as they present themselves. Accelerating the process of engaging with risks, findings and recommendations.



Why KPMG

We believe cyber security should be about what you can do – not what you can't. We bring a robust approach to this work, combining industry good practice with insights gained from working with our global clients.

We have experience in developing robust cyber security frameworks and in conducting large scale cyber security maturity assessments. We have in depth understanding of industry good practice and relevant security standards (e.g. NIST, COBIT, ISO 2700x) and we will leverage our experience to develop a framework that is effective, fit for purpose and relevant to our clients.

Case Study: Healthcare client
The Healthcare clients' core services including IT and Information Governance were outsourced to a separate organisation. On the clients' behalf, the third party was completing mandatory returns to the NHS covering Information Governance and wanted an independent fresh perspective due to concerns around breaches of electronic systems. There was also the concern that toolkit evidence and commentary was being rolled forward, year on year, rather than being refreshed. The client was keen to gain an understanding of the level of cyber maturity and to gain assurance over controls in place and third party contractual performance.

We completed a documentation review supported by workshops with the CIO, CFO, Emergency Planning Officer and Information Governance Leads using our CMA framework.

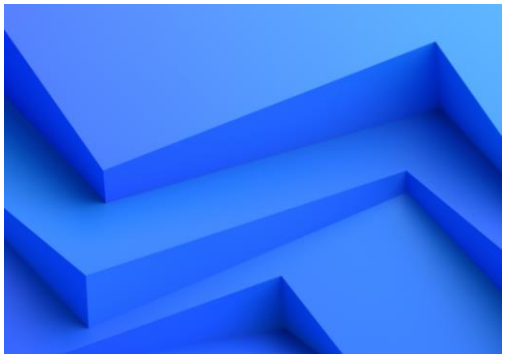
The benefit to the client was the provision of a holistic view of their cyber posture. We found that there was limited proactive Board engagement with cyber, ineffective identification of information assets and identifications of threats to those assets that could leave the client exposed. There was a mismatch between the clients expectation of what was achievable in a disaster recovery situation and what the third party was able to provide. Our report was well received and demystified areas by providing a clear and digestible report grouped by the six domains – Leadership & Governance, Human Factors, Information Risk Management, Business Continuity, Operations & Technology and Legal & Compliance.

Industry Insights
We will bring a fresh approach to this work, combining industry good practice with insights gained from working with our global clients

Track Record of Delivery
We are an award winning cyber security consultancy and take great pride in being recognised by Forrester as a leader in the market.

Pragmatic Approach
We have refined tools and methodologies available to be deployed immediately – this will enable accelerated delivery of the engagement.

Global Coverage
We have prioritised cyber security as a global business imperative and it is one of a handful of named 'Strategic Growth Initiatives' across our firm. This means we regard cyber security as an investment priority for us, both investment in our people and investment in our technology. We are determined to drive global best practice in this field.



Service Details

Service levels like performance, availability and support hours

This is not relevant as KPMG's Cyber Maturity Assessment as service does not involve a standard software solution.

Service levels like performance, availability and support hours

Not applicable.

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.

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.

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.

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.

kpmg.com/uk