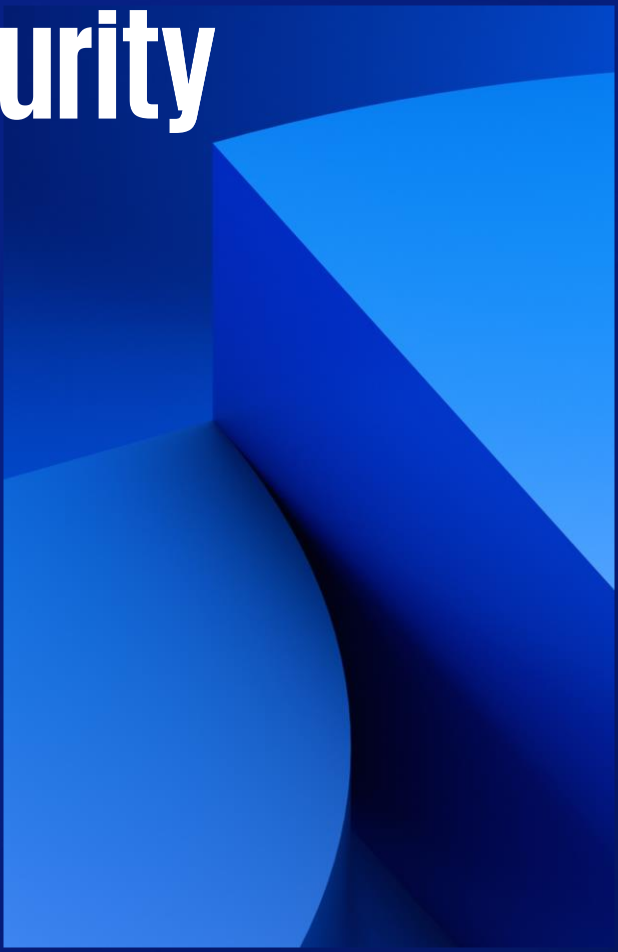
KPMG Cyber Security Strategy and Transformation service

A KPMG Service for G-Cloud 14

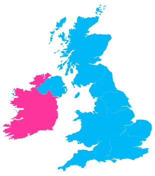


May 2024
kpmg.co.uk

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 risk
- Cyber and enterprise resilience
- Privacy compliance
- Cyber tech trans-formation
- 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's Cyber Security Strategy and Transformation service

Service Description:

This service helps you design and implement a practical cyber security strategy, in line with your business / cloud goals enabling you to respond to the evolving cyber threat landscape.

Our end-to-end solution supports your organisation in setting its security vision and direction and achieving your target state through security transformation.

What are the benefits of KPMG Cyber Security Strategy and Transformation service?

- Wider business understands information security contribution better
- Benchmarking across peers
- Pragmatic security programmes focused on business benefits
- Change integration across the whole business
- Use of approaches that have been successful in other organisations
- Confidence that information risks are understood and managed
- Cost effective compliance with regulations and legislation such as the Cyber Assessment Framework (CAF)

Our service features

- Security strategy and governance
- Security programme management
- Security policies, processes and standards
- Cyber Target operating model
- Controls implementation

Service Overview

Overview

Chief Security Officer and Chief Information Security Officers are faced with important questions:

- Who is trying to target you or has a credible interest in targeting you?
- What information and / or business process are they seeking to compromise and why?
- What methods would they use to achieve compromise?
- How effective is your current technical control environment across your cloud infrastructure and legacy infrastructure?
- Where are the identified vulnerabilities; which are highest priority?
- How much do you need to invest in order to reduce your cyber risk vulnerabilities?
- How can you cyber security strategy become an enabler for your enterprise digital strategy?
- How can manage your delivery programme to make the best use of third party vendors and external delivery organisations?
- How can you develop a business case for investment that complies with Treasury Green Book Guidance and sets out a compelling case for change?

Introducing Cyber Strategy and Transformation

KPMG cyber security and transformation solution framework is outlined below:

- **Threat model -** a summary of your threat profile and the business impact of compromise.
- **Security demand -** business requirements for security based on your mission and delivery priorities.
- **Risks / vulnerabilities -** Identified risks and current vs target security maturity
- **Improvement options -** These will cover governance, people, process, information / data and technology.
- **Culture and sustainability -** To sustain improvements and a culture of continuous improvement.
- **Organisation design** - Organisational structures, headcount requirements, and governance.
- **Cyber Target Operating Model (TOM) -** Development of a Cyber TOM for your organisation to outline key cyber capabilities, roles and accountabilities.
- **Business case -** based on the HMG 5 case model.
- **Roadmap design** details the duration of each intervention, sequencing between interventions, critical path and interdependencies.
- **Implementation partner support-** Ongoing support to implement your programme and realise the business benefits. This includes specialist programme management support depending on the complexity and reach of the programme.

What's in the scope of the service?

Our cyber security strategy and transformation service includes the following components:

1. **KPMG Threat Modelling –** outlining the key threats to your business.
2. **KPMG Strategy Services** - including analysis of HMT Green Book requirements
3. **People consulting services**– providing industry leading organisation design, behavioural change and security culture services
4. **Cyber Target Operating Model (TOM)** - Development of a Cyber TOM for your organisation to outline key cyber capabilities, roles and accountabilities.
5. **Vendor analysis**–market assessments of leading security vendors and market testing of products
6. **Major Projects Advisory**– provision of specialist PMO services for large complex security programmes
7. **Cloud Advisory Services**– professional services to align security to your enterprise cloud strategy and delivery programme
8. **Customer**–Industry leading methodologies to map and develop customer journeys for your key internal and external customers
9. **Security policy and control implementation**–Implementation of new and enhanced policies, standards, controls along with integration of key controls into your enterprise risk operating model
10. **Benefits realisation** –benefits tracking, analysis and reporting

Why KPMG

- Our breadth and depth of skills, knowledge and experience across cyber Security Strategy and Transformation enables us to tackle complex client cyber challenges. We have experience across major cyber transformation programmes.
- We are market focused – Our team understands the complexities of government and public sector organisations.
- We are proven – our case studies outline the client challenges we have supported our clients with (see below and overleaf).

Client Challenge	**Case Study – Cyber Target Operating Model** **The client needed support to**: Develop a Cyber Target operating Model (TOM) which took account of the clients federated operating structure, enabling them to outline future accountabilities and responsibilities for the future state 2030.
KPMG Response	**Design principles** - Developed guiding Design Principles for the development of the Cyber TOM. **Cyber refence Model -** Developed an Cyber Refence model which was the anchor for the cyber TOM. This was based upon the Cyber Assessment Framework (CAF), NIST and ISO27001. **Target state to 2030** - Defined new and improved organisational capabilities aligned to the departmental vision and anchored in security culture. **Workshop** - Conducted workshops with key stakeholders to map out critical accountabilities and responsibilities. **Gap analysis** - Cyber TOM design approach and plan developed, key activities including an as-is assessment, gap analysis, change impact assessment and ROM cost for new capability and business plan requirements. **Stature Design Options** - Structure key design questions to facilitate decision making and develop the 2030 Cyber vision for the National Team. Develop National Cyber Team structural options, pros and cons and key implications across the system for consideration to guide decision on National TOM structure and detailed design of accountabilities and responsibilities. **Validation of TOM** - Held a major workshop with 50+ CIOs and c-suite representatives across the system to validate the design and outline key success factors the implement the TOM across the system
Benefits to Client	• A cyber TOM with agreed accountabilities and responsibilities across the federated system based upon National, Regional and Local approach. • A roadmap to develop the 2030 capabilities including ROM costs for the development of the new capabilities • A list of requirements and input enabling the development of a strategic 5 year business case. • Detailed analysis of future organisation design options supporting decision making. • "*Incredible job by the team. This has put us in a really strong position going forward to implement the Cyber TOM.* " – Client Lead

Why KPMG

Client Challenge	**Case Study – Cyber Security Business Case for a Central Government Department** **The client required support** developing and gaining approval for a cyber transformation business case, based upon risk reduction, plus designing a programme governance approach to enable effective delivery
KPMG Response	**Cyber Risk Quantification** – Assessed the cyber-risk exposure to the department and regulatory system, using KPMG's risk-quantification software, 'Cyber Risk Insights', to baseline cyber security maturity. **Business Case Risk Support -** Supported development of a cyber transformation programme business case, aligned to HMT's Green Book, focusing on an economic 'risk reduction' model that evidenced the investment impact of strengthening cyber maturity. **Cyber Risk Investment Guidance** - Develop a guide for CIOs across the client's federated system, enabling CIOs to prioritise cyber-security investment decisions. **Intervention Design -** Provide cyber expertise to client teams, enabling the design of programme interventions to achieve desired cyber risk and resilience outcomes. **Programme PMO creation** - Stand up the transformation programme's cyber PMO, including the development of programme's security governance, processes and artefacts.
Benefits to Client	• The result was a step-change for the UK Government: a national transformation and resilience programme, measuring the benefits of investments in cyber-risk reduction across the health and adult social care system. • In addition, the investment guide has helped over 200 providers across the country to make data-driven, cyber-investment decisions, underpinned by our risk-quantification methodology. • The Programme transitioned to BAU and is in delivery mode. • *"This has completely changed the dial for how the system sees us as a national team."* - Director of Cyber Operations.

Client Challenge	**Case Study – Cyber Security Strategy for a Central Government Department** The client needed support to: evidence key cyber risks; define a target state and portfolio of improvement interventions, and; gain board-level approval to an Outline Business Case (OBC).
KPMG Response	**Threat model -** Compelling analysis of the motivations, tactics and techniques employed by priority threat actors. **Business lens** - Value chain mapping with business stakeholders to understand how cyber security enables business priorities. **Risk analysis** - Identification of known and unknown gaps in controls and capabilities across organisation, technology and people. We used a cyber security psychologist to assess organisational culture and behaviours. **Target state-** Defined new and improved organisational capabilities aligned to the departmental vision and anchored in security culture. **Improvement interventions** - Costed improvement interventions to deliver the future state, comprising defined benefit metrics and quantified risk reduction impact. Included a delivery roadmap for implementation. **Outline Business Case**- HMG-compliant product detailed the case for change, benefits and investment options to deliver the proposed cyber security portfolio.
Benefits to Client	• Strategic risks and risk reduction measures approved at board-level • Cyber security embedded into the Digital Data and Technology operating model • Strengthened governance and accountability across the global organisation • Defined cyber security improvement portfolio to reduce risk and build an effective security culture across the global workforce • A compelling OBC a board-level decision to make major investment in the new cyber programme (approved by the SRO). • *"This was one of the best security projects I have worked on in government and the level of detail we now have to help shape and drive its security posture, processes and governance is outstanding."* - Head of Technology Services

Service Details

Implementation Plan:

Our strategy projects are primarily delivered over five phases as follows:

Vision: In this phase the high-level scope, the project plan, the approaches and strategies for the security function will be defined, documented and accepted. In addition, during this phase preparation for all subsequent phases take place.

Macro Risk Analysis: In this phase we assess the macro risks to the organisation's core business strategy that the security strategy is seeking to reduce and remediate – this establishes the case for change.

Business Case: In this phase we set out the various elements of the case for change using Treasury 5 case model. This phase will be used to secure the investment requirements for the security programme and identify the core target benefits

Deploy: Mobilisation of the programme and execution of quick wins to deliver immediate risk reduction. This phase will be managed by a PMO function, either provided by KPMG or in-house with KPMG provide project management support as required.

Measure and evolve: During this phase the benefits of the programme are measured and traceability is established between the initial risk reduction target outcomes and what has been delivered in the programme. We will establish key performance and risk metrics that can be used to drive accountability for delivery across your organisation.

Implementation Plan, continued

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

Onboarding and offboarding support:

Onboarding…continued

- 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

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.

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.

Service Details

Service levels like performance, availability and support hours

This is not relevant as KPMG's Strategy and Transformation 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

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