KPMG

KPMG Cyber Security Secure by Design (SbD)

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

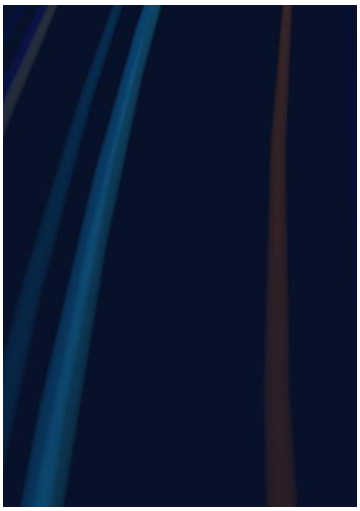
15 office locations

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.

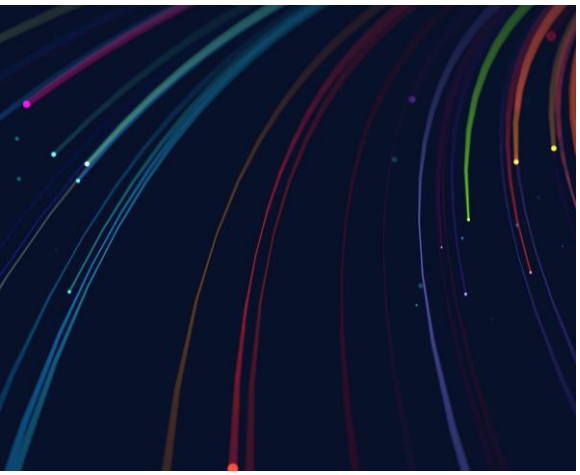
We apply a data and technology driven approach to drive change through our digital transformation services.

KPMG's Secure by Design: Summary Serving

Service Description:

KPMG seamlessly integrates Secure by Design (SbD) principles into digital and cloud transformations, establishing consistent governance for building effective and proportionate security controls throughout the entire digital service lifecycle.

We underpin our 'Secure by Design' approach with a taxonomy of cyber controls, enabling organisations to quantify risk, streamline security processes and rationalise employee time by minimising retrospective security assurance and response to security incidents.



What are the benefits of KPMG's Cyber Security Secure by Design (SbD) Service

- **Reduce risk of cyber security attacks,** considering security at every stage of digital and cloud transformations.
- **Improved security posture,** with digital systems and products resilient to attacks and data breaches
- **Reduced organisational costs** responding to security incidents and conducting retrospective security assurance reviews.
- **Improved productivity** among employees, reducing their time spent dealing with security vulnerability and non-compliance issues.
- **Enhanced security culture,** with security responsibilities and considerations embed into all roles associated with the delivery of digital and cloud transformation.
- **Improved compliance** to evolving digital, data and cloud based security regulations and standards.
- **Enhanced trust and reputation** among end customer users, who become faster adopters of digital and cloud transformations.

Our service features

- **Generate tailored 'Secure by Design' Principles**, aligned to organisation and regulatory (i.e CAF) outcomes
- Develop a single, **cyber controls taxonomy**, with tailorable security 'Activities' directing 'Principle' implementation.
- Harness **KPMG's Cyber Risk Insight,** quantifying cyber risk exposure and the prioritisation of security controls into digital service lifecycles.
- Embed **security governance** into digital and cloud solution architecture design and operation.
- Integrate **secure development practices** into the software, modelling and testing of digital services.
- Implement a **culture of security awareness,** training personnel involved in digital service lifecycles.
- **Rationalise compliance** with relevant security regulations and standards.
- Set **transparent security behaviours**, communicating with end users about security practices and requirements.

Service Overview

Secure by Design

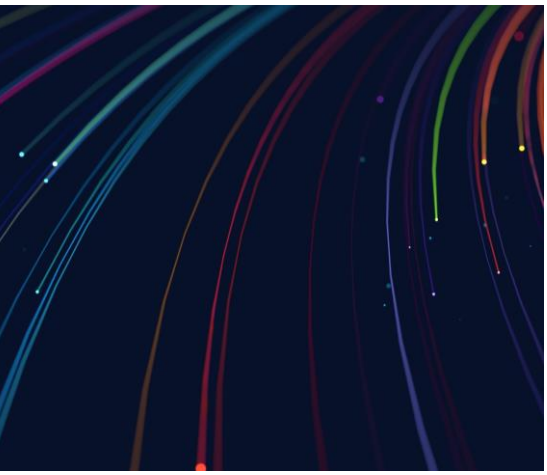
Vision: Strengthen cyber resilience, ensuring security is consider at every stage of digital and cloud transformation lifecycles.

Deployment: We leverage the combined power of human expertise and technology to deliver our 'Secure by Design' service.

Our team of security and digital design specialists **partner with client teams** to develop, integrate and assure Secure by Design Principles throughout digital and cloud transformation service lifecycles.

Learning: We **build internal client capabilities** for operating and evolving a Secure by Design framework.

We train teams to integrate security controls, assure their effectiveness, and communicate the value of enhanced security practices within digital and cloud service lifecycle, embedding a culture of continuous security improvement.



Secure by Design: Service Phases

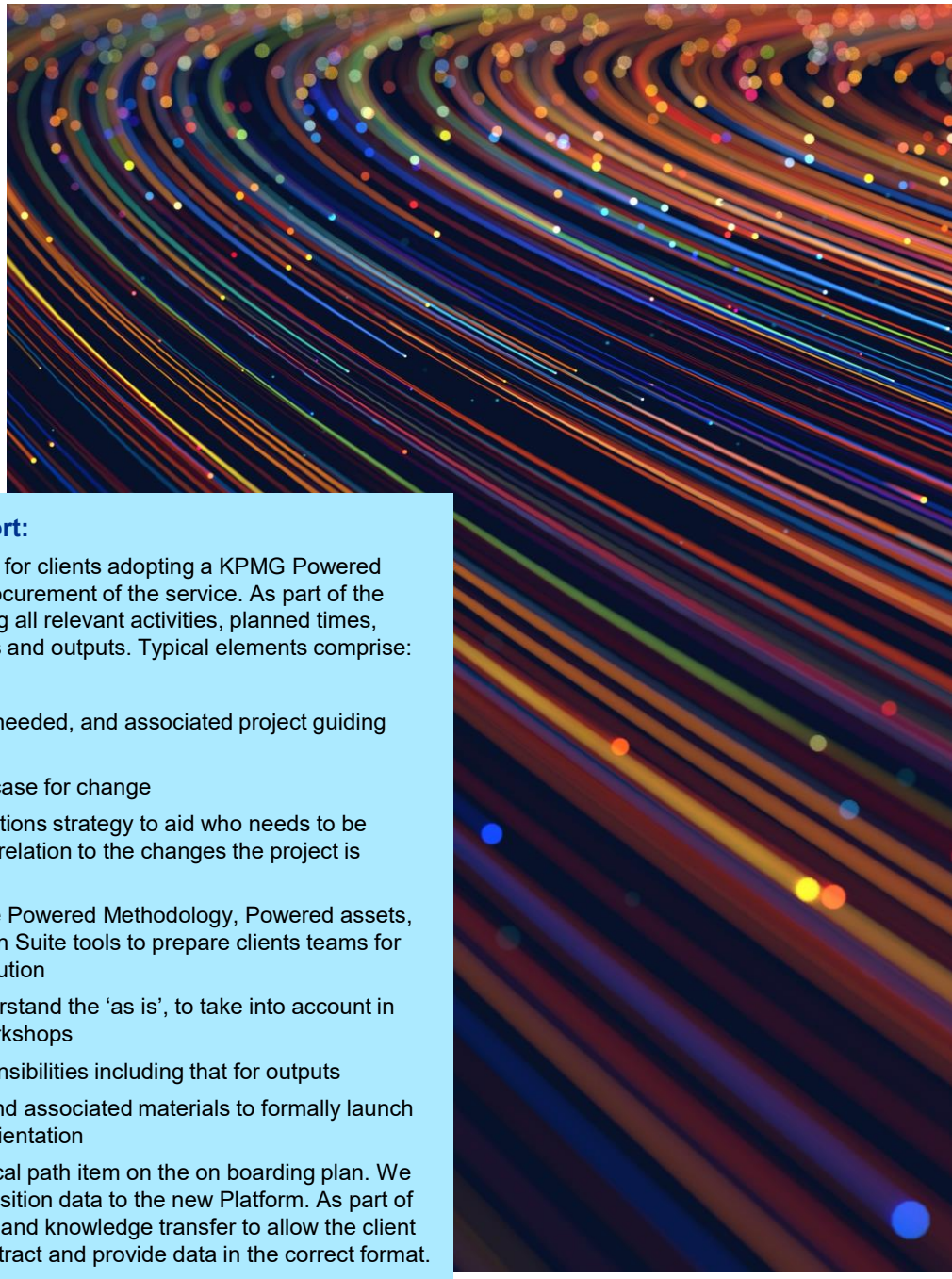
KPMG's Secure by Design by Design Service is structured via four phases: **Requirement**, **Principles**, **Integration**, **Governance & Assurance**.

01 **Secure By Design: Requirement**	**Aim**: Set Secure by Design within organisational security, digital and cloud transformation outcomes. **Approach**Define the value, role, and scope of Secure by Design in service lifecycles, considering business, policy, and regulatory compliance drivers.
02 **Secure By Design: Principles**	**Aim:** Define 'Secure by Design' outcomes for embedding security practices. **Approach:** Tailor security 'Principles', 'Activities' and set a consistent controls taxonomy, which must be adhered to by delivery teams.
03 **Secure By Design: Integration**	**Aim:** Embed security principles into the building and operation of digital and cloud technologies. **Approach**: Create an implementation plan to schedule and assist team in adopting security principles and controls.
04 **Secure by Design: Governance & Assurance**	**Aim**: Build an environment of continuous assurance and improvement. **Approach**: Set governance processes to assure adherence to security principle, communicating the value and role of security in digital and cloud transformation.

Our Powered (Technology) Capabilities for 'Secure by Design'

Cyber Risk Insights	Cyber Arena	4DI Incident Simulation	Powered SecDevOps
Cyber risk quantification and control decision making	Cyber controls simulation and testing environment	Scenario based security building and resilience testing	Automated secure engineering, monitoring and governance assurance.

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.

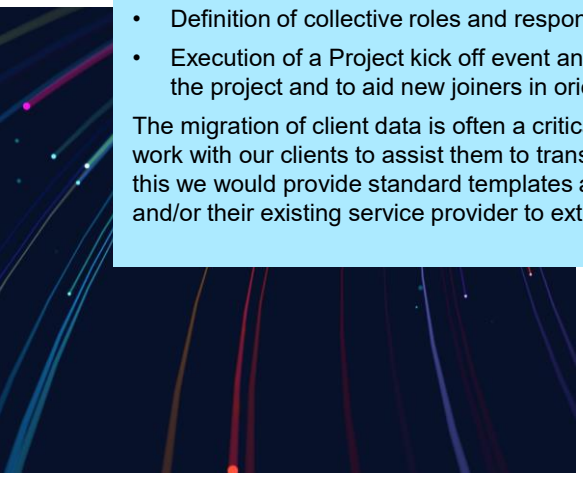
Onboarding and offboarding support:

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 the Powered Methodology, Powered assets, Platform principles, Powered Execution Suite tools to prepare clients teams 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

The migration of client data is often a critical path item on the on boarding plan. We work with our clients to assist them to transition data to the new Platform. As part of this we would provide standard templates and knowledge transfer to allow the client and/or their existing service provider to extract and provide data in the correct format.



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

The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans.

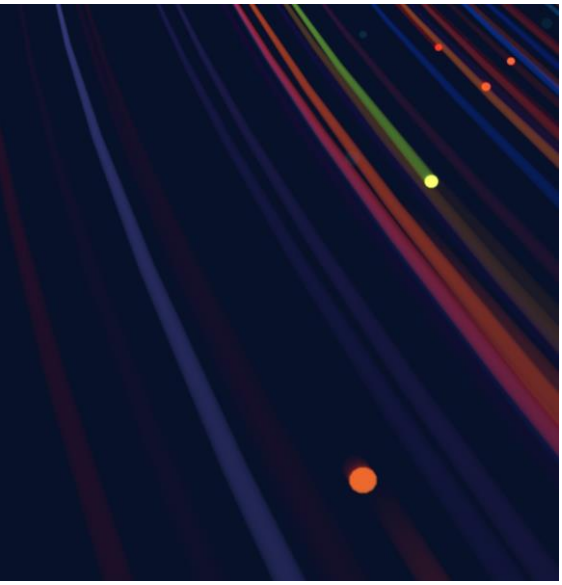
KPMG has comprehensive business continuity and physical security procedures in place to cover its day to day and business operations.

The KPMG Business Continuity and Readiness Statement Executive summary dated November 2022 includes the following:

The Business Continuity team follow the Business Continuity Institute best practice guidelines and comply with the International Standard ISO22301: 2012.

The firm has ISO27001 accreditation, the scope of the external audit extended for the first time in 2010 to include the Business Continuity Management across the UK firm externally audited every six months.

Incident & Crisis Management response: role holders are trained and exercised.



Business Recovery Readiness:

Strategy

The firm's recovery strategy is based on the use of the KPMG UK office network to provide workplace and Information & Communications Technology contingencies in the event of the loss of one (or more) of the firm's offices.

The firm's business recovery strategy is based on using the offices throughout the UK as alternate site contingencies for building denial events with remote working at home and client site completing the response by leveraging KPMG's agile working capability: high capacity VPN, all staff have laptops and Smart phones.

Plans

Business Continuity Co-ordinators are responsible for the maintenance and execution of client service recovery plans.The business recovery plans are reviewed within an ongoing programme of scenario based tabletop exercises.

The plans are maintained and centrally monitored using business continuity planning software. These plans are supported by the firm's infrastructure (ITS, Facilities and HR) support plans

Exercising

Business Recovery plans: exercised once every year.

Detailed audits of the content of all plans are completed annually

BCDR: Risk and Impact Mitigation:

KPMG has a three lines of defence Risk Governance model:

i. Operational teams (ITS, HR, Physical Security etc) responsible for implementation of activities / adherence with policies and standards and day to day ownership & management of

ii. Oversight -BCM as part of a wider Information Protection team within the Quality & Risk Management function defines strategy / policies, ensures compliance and provides assurance.

iii. Independent Assurance –Internal Audit overseen by the Audit & Risk Committee, external audit (ISO27001 BCM audit on a biannual basis) and Client audits.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted IT infrastructure and business applications.

The primary and secondary data centres are dedicated data halls hosted in purpose built UI Tier III equivalent facilities. The buildings are separately owned by two of the market leaders in data centre colocation.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted IT infrastructure and business applications.

Why KPMG

BCDR Risk and Impact Mitigation, (cont.):

The data centres are sufficiently physically separated to minimise exposure to shared risk/threat occurrence, whilst within distances to support synchronous replication of data to minimise data loss opportunity in the event of DR.

Both facilities are located in the UK. Production IT systems are typically hosted on an active passive infrastructure design, providing high availability and managed failover between data centres, underpinned by resilient fibre links.

KPMG provides a disk to disk backup strategy supplemented by snapshot and clone solutions to provide the lowest RTO. Disk backups are replicated between data centres for additional assurance. Long term data retention is provided through a choice of archive disk or tape backup where required.

The KPMG network is fully resilient, with all offices linked by dual network paths into an MPLS Wide Area Network, providing connectivity to KPMG's Data Centres.

KPMG has several risk assessments for suppliers in place, which cover business continuity, health and safety and data security.

KPMG provides related consulting services to clients.

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.

Typically, data extraction is addressed by clients with input from KPMG but we work closely with our clients to develop the data migration strategy and plan, providing templates with the target Platform format, to enable our clients to cleanse and map extracted data. We can apply varying levels of data migration automation techniques to address large volumes or complex requirements.

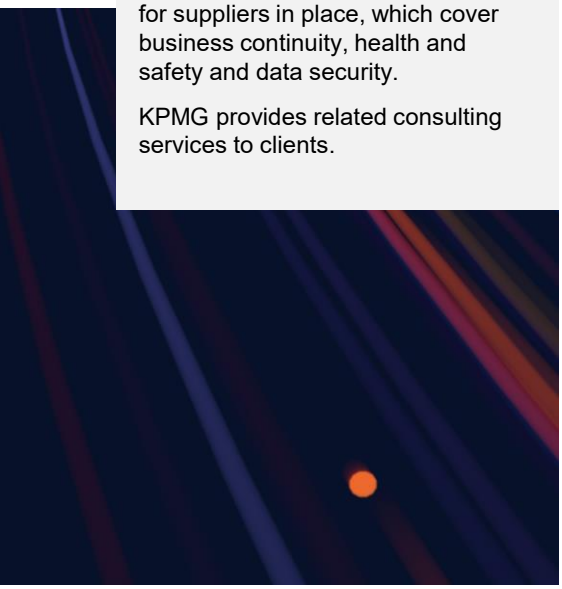
Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

Cloud software is updated regularly to apply minor fixes and to a schedule for more significant updates. These types of maintenance activities are usually well documented and pre advised by the Cloud software vendor and, where notified, are considered in project planning and particularly design and regression testing activities.

Customisation:

Our approach is to 'configure rather than customise', adopting standard Cloud software functionality to enable ease of upgrade and to take advantage of new updates and releases with minimal issues.



Service Details

Service levels like performance, availability and support hours

The service levels and support hours for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

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