Cyber Security

Privileged Access Management (PAM)

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

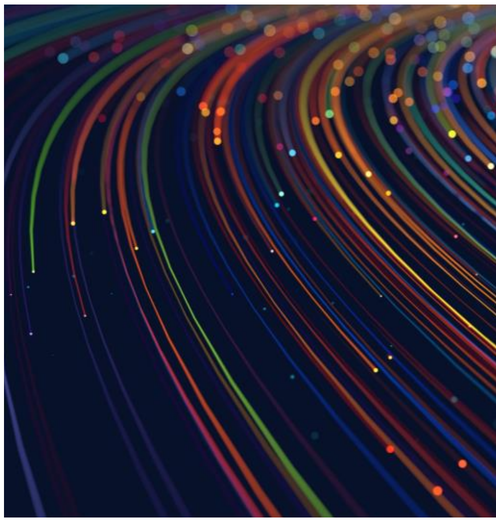
15 office locations

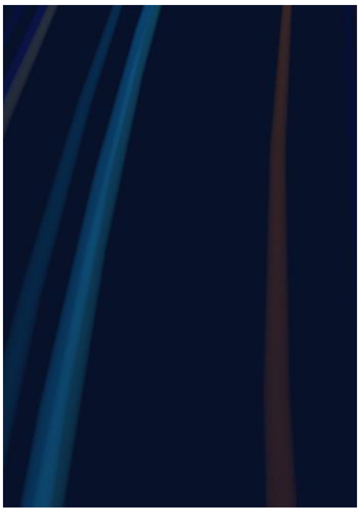
Part of a global team of 6200+ individuals

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.

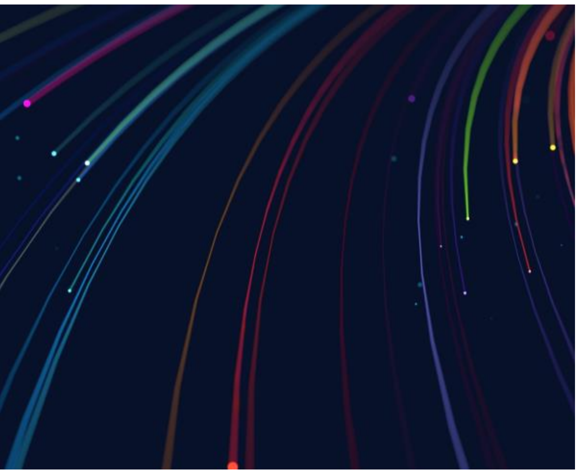
We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

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

KPMG Cyber Security Privileged Access Management (PAM)

Service Description:

KPMG will help you to improve your privileged access management controls. KPMG can work with you from strategy through to delivery on projects to manage passwords, implement session monitoring and implement a least privilege model.



What are the benefits of KPMG's Cyber Security Privileged Access Management (PAM) service?

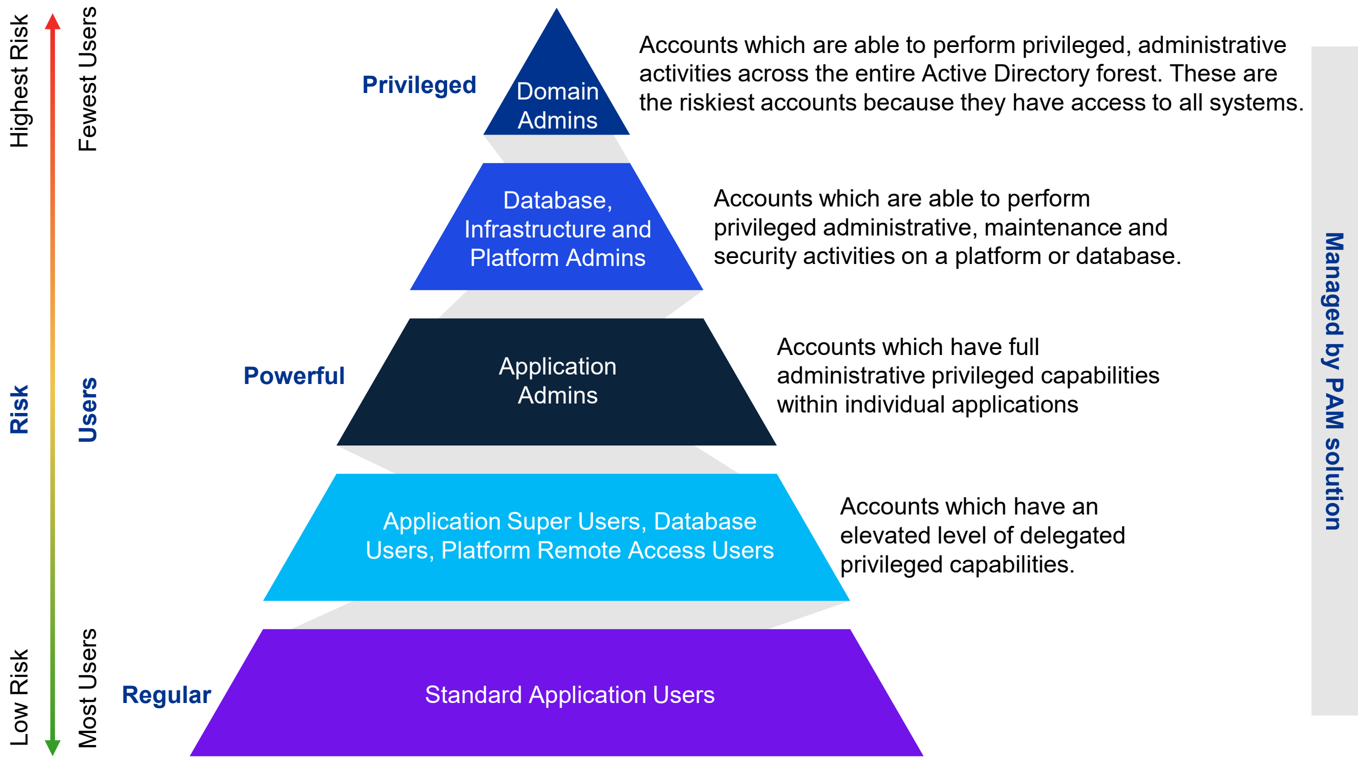
- Improve user experience by centralizing privileged password management
- Increased assurance on the management and use of privileged access
- Risk reduction due to increased control over privileged access
- Improved auditability of the use of privileged access
- Reduced risk relating to malicious insiders
- Increases visibility of use of shared accounts
- Reduced risk of privileged account creation going unnoticed
- Hybrid cloud and on premise deployment methodologies possible
- Digital management of privileged access reduces manual workload

Our service features

- We have relationships with the best vendor partners for implementation activities and leverage our global knowledge to guide clients. We are agnostic on the solution, providing you with independent advice.
- Assurance and assessment of current state with recommendations
- Strategy, roadmap and target operating model (TOM) development
- Business change management to bring IT stakeholders on board
- Connection to legacy applications using customization
- Technology and vendor assessments
- Solution design and architecture
- Password safe and vault design using knowledge of good practice
- Business requirements analysis and roadmap definition

KPMG Approach

Privileged Account Management (PAM) is a special sub discipline within Identity and Access Management focussing on accounts that are not directly mapped to one specific person. PAM solutions deal with the specific challenges associated with the privileged shared and individually assigned accounts used to manage the applications, databases and several other platforms. The pyramid represents various account types and the solutions that help manage the access.



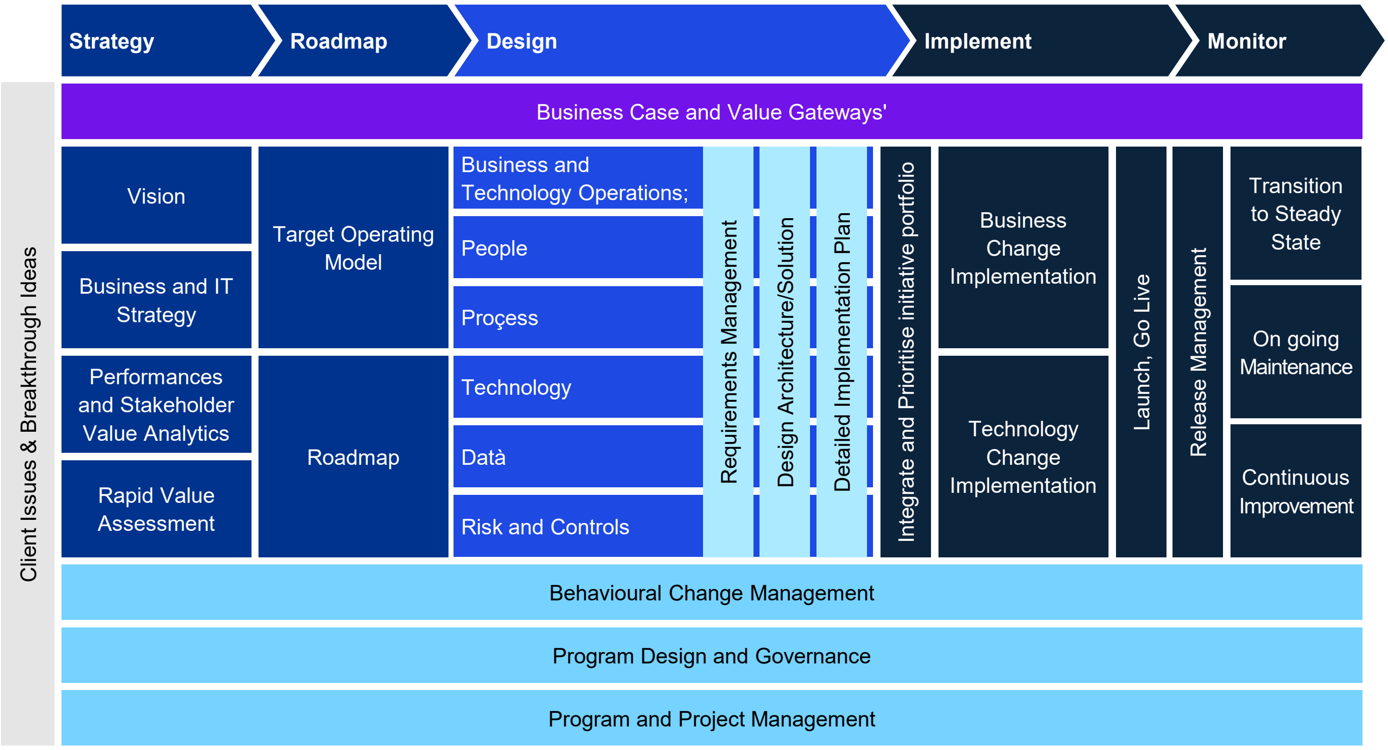
Integrating the PAM solution with the broader IAM programme will allow important controls which are key to both PAM and IAM to be handled centrally and consistently for all users across the organisation, whether privileged or otherwise. This will reduce the administrative time and resource costs associated with monitoring, requesting and reviewing access while providing a richer and more comprehensive view of who has access to what. The following controls should be used across privileged and non-privileged users:

- Privileged user accounts password must be managed by a PAM solution;
- An approved change or active incident ticket shall be available in order to receive the privileged password;
- All the activities performed using privileged accounts shall be regularly audited and monitored for appropriateness.

Power and Regular user account types will be managed by the identity and access management solution in accordance with the Access Control policy.

Why KPMG

KPMG offers an extensive set of services, based on KPMG's umbrella Value Delivery Framework (VDF) Approach. This approach lays out what we offer against a client's transformational Privileged Access Management (PAM) journey and consists of best practices, templates and other tools to efficiently execute the project.



Led by experienced PAM architects, business analysts and implementers, the KPMG Privileged Access Management team is well placed to ensure customers maximise value from their PAM solution.

Discovery and Analysis

Discover accounts, SSH keys and create an inventory of privileged accounts.

Policies and Process enhancements

Review of privileged access management processes, identifying opportunities for improvement in accordance with industry good practices. Develop effective target operating model to manage the PAM solution on an ongoing basis.

Solution Architecture and Design

Solution design and planning services. Infrastructure planning, hardware and sizing options.

Solution Configuration and Customisation

Deployment and configuration of privileged access management solution.

Quality Assurance and Health Check Assessments

Quality assurance services. Deep dive diagnostic review of existing PAM solution deployments, with recommendations for improvements.

Why KPMG

Global pharmaceutical company

- The client had an urgent requirement to address key external audit findings relating to the control of privileged accounts in its IT estate.
- Specifically, these findings identified control issues around privileged account access to applications used for Sarbanes Oxley (SOX) compliance reporting purposes, and their associated underlying infrastructure. The client had previously selected CyberArk to meet its privileged access management (PAM) requirements and had an existing PAM implementation program in place. However, the program had run into delays over the last 18 months.
- Following on from the initial success, the client extended the piece of work to onboard further applications in further phases of work.

- KPMG performed current state assessment on the client's privileged accounts across its estate.
- Conducted workshops and interviews with key stakeholders to gather requirements on privileged accounts and underlying infrastructure systems and to identify gaps and make recommendations where further discovery is needed
- Identified account requirements for audit monitoring and keystroke logging, two critical CyberArk functionalities necessary to pass audit finding.
- Built and tested the CyberArk solution in client's UAT environment
- Supported move of CyberArk to Production environment and transfer of accounts from UAT into Production
- Delivered CyberArk documentation for the CyberArk solution build and deployment, including: High Level Design, Low Level Design, build guide, admin guide, use case, test case documentation and service operations guide.

- Implementation of the CyberArk solution within 6 months, the fastest KPMG CyberArk implementation to date to reduce critical audit findings relating to SOxapplications.
- Effectively manage and control privileged account assets.
- Built a client support team applying the “Follow The Sun” model to support the CyberArk Production environment.
- Successful onboarding of SOX privileged accounts and implementation of CyberArk solution which significantly reduced risk relating to external audit findings.

Multinational telecommunications company

- The client is expanding their business internationally, the pool of people necessary to efficiently support that growth also increases and so manual and monitored privileged access to customer
- The client therefore deployed PAM software to manage internal privileged users.

- KPMG utilised a phased approach working closely with the client throughout the engagement.
- The initial phase covered a readiness assessment, requirements analysis, technology environment and infrastructure analysis, rollout approach planning and user case development.
- This was followed by a design phase which included the PAM solution design and pre-implementation data gathering.
- The build and implementation phases were deployed first in a test environment where the solution was configured and implemented, system tested and use case tested.
- Regular status reviews held with the client and weekly progress reports produced.

- PAM solution has been deployed to Windows, Unix, HP ILO and VMWare ESX platforms in the environments covering over 7,500 devices/servers with approximately 15,000 separate accounts.
- PAM solution enabled the client to align themselves to the best practices outlined by CESG, ISO27001 and the client's own Security Catalogue.
- Helped protect the brand and sales pipeline from any reputational damage.

Our Approach

Implementation Plan:

Privileged Access Management projects are delivered over four phases as follows:

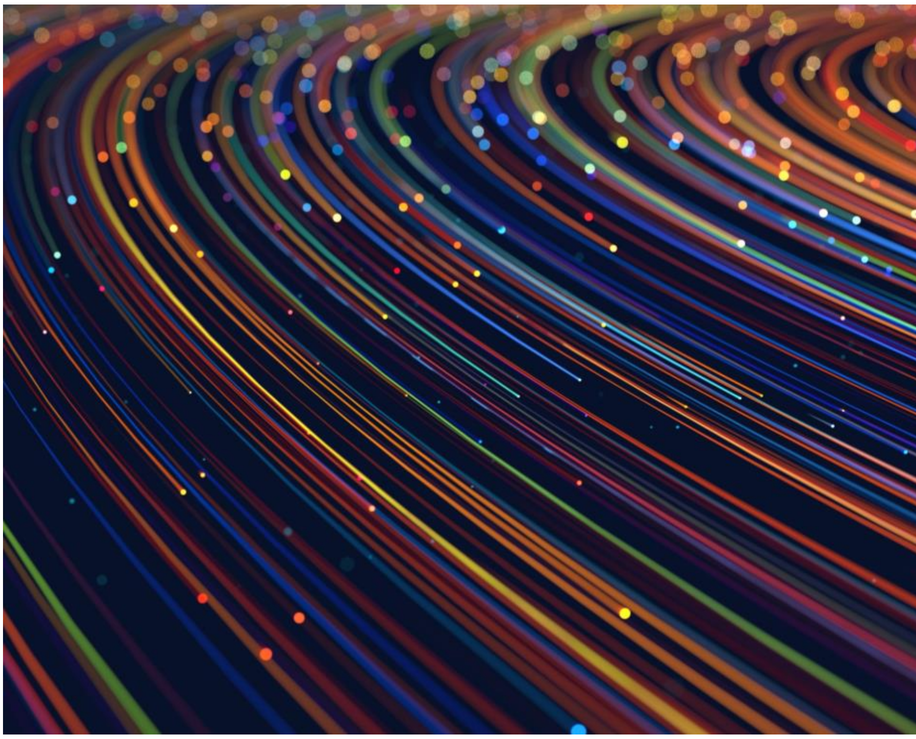
Assess: In this phase the high-level scope, the project plan, the approaches and strategies for how the project will be implemented during the remainder of the project are documented and accepted. In addition, during this phase preparation for activities in the Validate phase take place.

Transform: In this phase the designs for the items in scope will be finalised, documented and accepted by the Customer to facilitate entry into the Construct phase.

Operate: In this phase the processes and new products are configured, and integrations built in accordance with the design. A series of test phases collectively determine if the system was built in accordance with the design. Data is also cleansed in preparation for migration and tests will be conducted to confirm the ability to migrate and reconcile data from the legacy platforms to the new platform.

Evolve: During this phase the new platform is in production and the Customer starts operating the target processes on it, with the agreed level of post-go live Hypercare support.

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 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 Methodology 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.

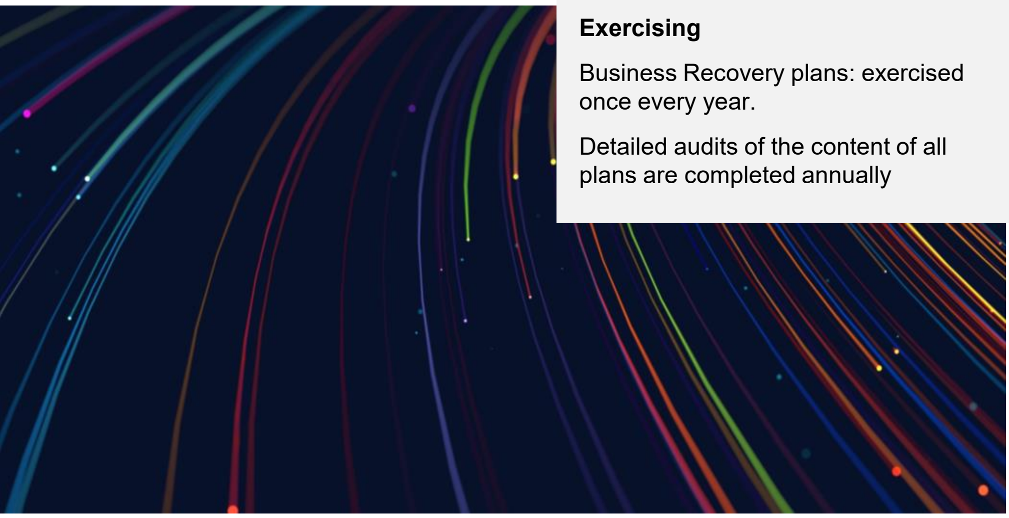
KPMG has comprehensive business continuity and physical security procedures in place to cover its day to day and business operations.

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

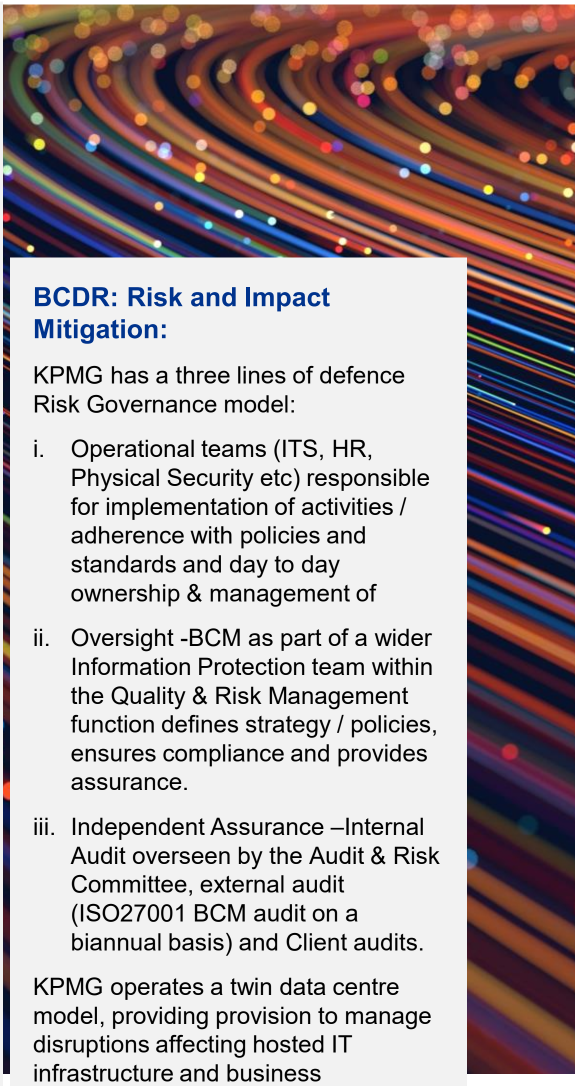
Business Continuity Co-ordinators are responsible for the maintenance and execution of client service recovery plans.The business recovery plans are reviewed within an ongoing programme of scenario based tabletop exercises.

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.

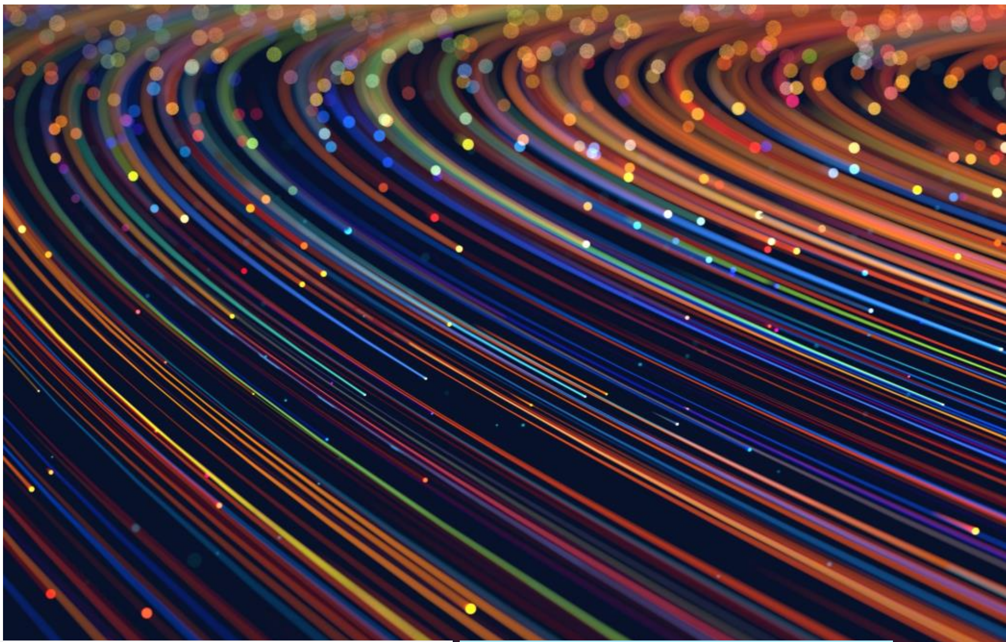
iii. Independent Assurance –Internal Audit overseen by the Audit & Risk Committee, external audit (ISO27001 BCM audit on a biannual basis) and Client audits.

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.

Service Details



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.

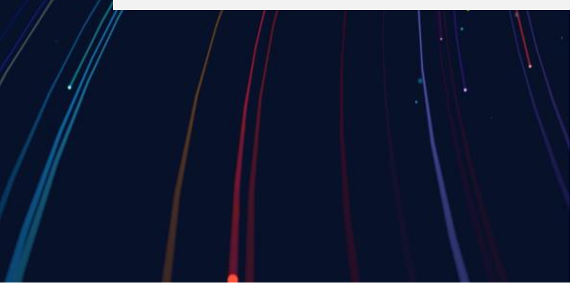
Both facilities are located in the UK. Production IT systems are typically hosted on an active passive infrastructure design, providing high availability and managed failover between data centres, underpinned by resilient fibre links.

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. Most Cloud software vendors restrict the capability to customise the core application as it impacts on the ability to service and support a common code base and the associated financial model.hpg

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.

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:

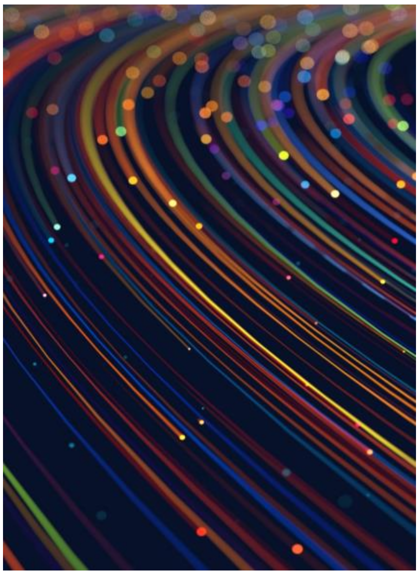
Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- 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.



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

Contact Us

KPMG G-Cloud Services Team
T+44 (0) 207 311 5767
Euk-g-cloud@kpmg.co.uk
www.kpmg.com

kpmg.com/uk

CREATE. | CRT164925A January 2026