KPMG

KPMG Cyber Security Identity and Access Management (IAM/IDAM) Authentication and Authorisation

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

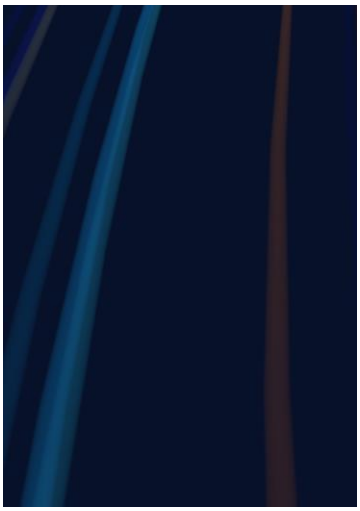
15 office locations

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.

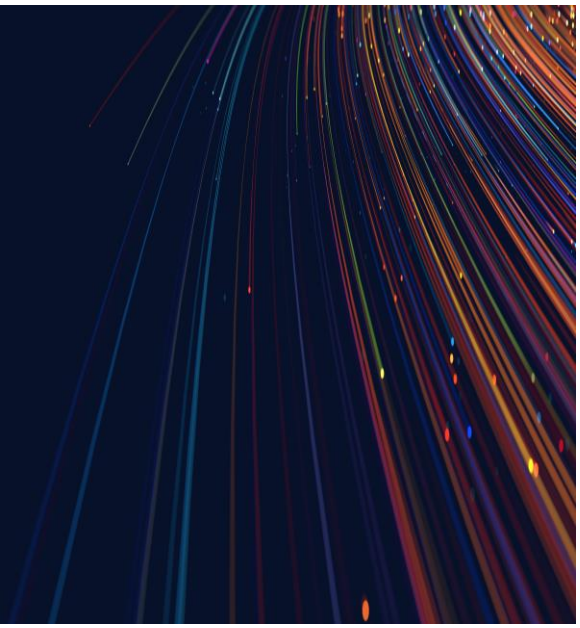
© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

KPMG Cyber Security Identity and Access Management (IAM/IDAM) – Authentication and Authorisation

Service Description:

KPMG delivers strategy through to implementation. KPMG implement industry leading vendor solutions to implement single sign on (SSO) in the cloud, multi-factor authentication, citizen access, social login, supplier/federated access and employee access.

KPMG implements business controls (e.g. Role Based Access Controls), process optimisation, industrialisation of onboarding and change management.



What are the benefits of KPMG Cyber Security Authentication and Authorisation service?

- Improve user experience with SSO by reducing remembered credentials
- Digital access management reduces manual workload
- Risk reduction due to increased controls over critical applications
- Self-service platforms reduce administrative effort
- Effectively manage federated access to third parties
- Experienced access management professionals knowledgeable about industry good practice
- Increase assurance over managed credentials
- Improve employee efficiency with easy to use multi-factor authentication
- Reduced risk relating to malicious insiders
- Increased security with Multi-Factor Authentication (MFA)

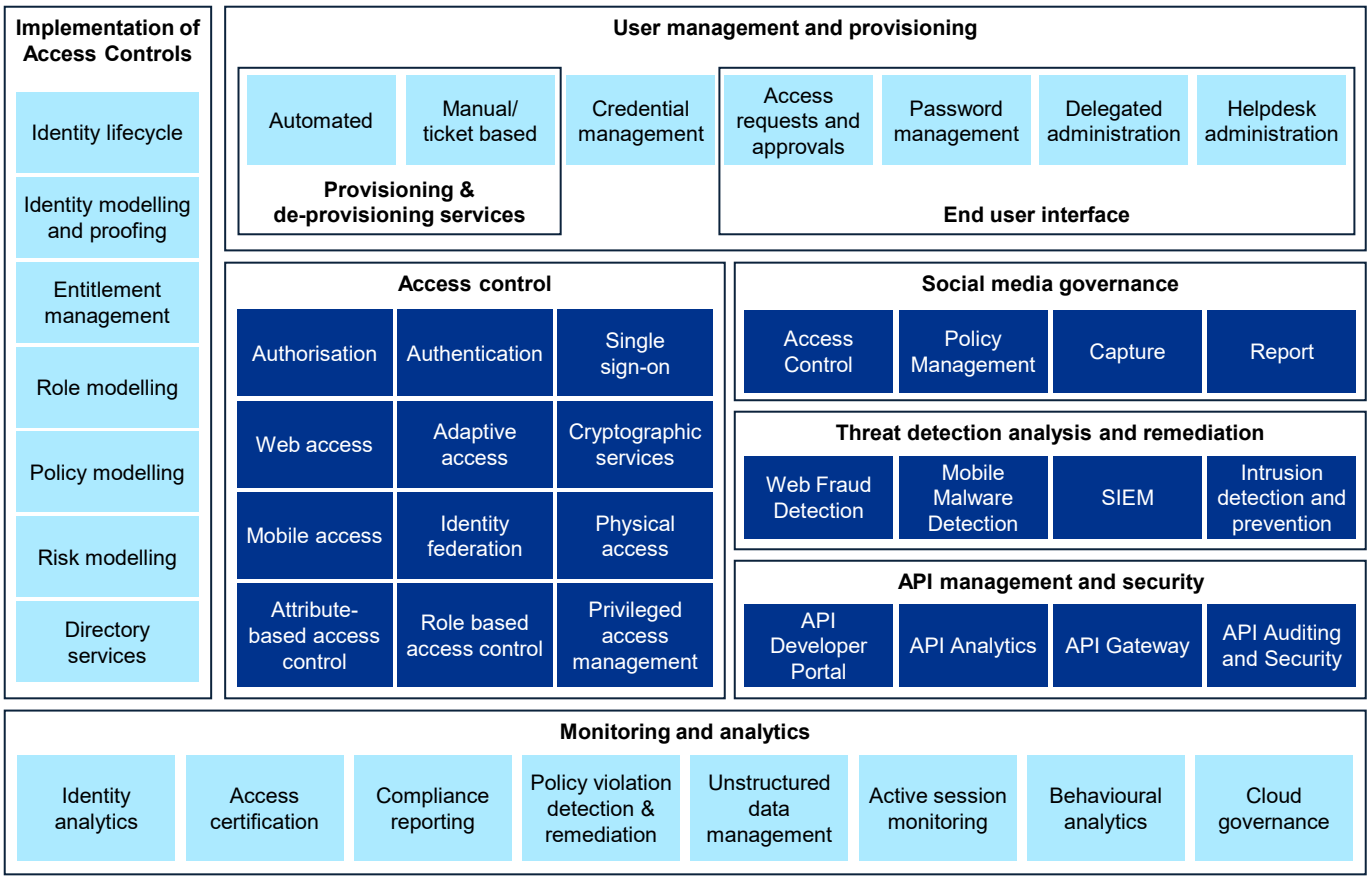
Our service features

- Experience with vendors: Ping, Oracle, Okta, Microsoft and ForgeRock
- Assurance and assessment of current state with recommendations
- Strategy, roadmap and target operating model (TOM) development
- Migration from legacy applications to cloud solutions
- Technology and vendor assessments
- Business requirements analysis and roadmap definition
- Business process design and implementation
- Business change management
- Solution design and architecture
- Hybrid cloud and on premise deployment methodologies possible

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

Our Approach

Implementation of Access Controls



Authorisation

The IAM solution ensures users have the appropriate authorisation to access resources. Authorisation is performed based on assigned roles and entitlements in the IAM solution.

Web access

Seamless access to internal web applications and external/third party web applications is supported. Single Sign On improves user experience by removing need to re-supported.

Mobile access

Seamless access for managed mobile devices and unmanaged mobile devices is supported. Some resources are only accessible via managed devices or BYOD.

Attribute-based access control

Access control is enforced by a series of attribute parameters (e.g. location, job title) applicable to a specific user. Rules can be formulated based on these attributes which control access.

Authentication

Future state authentication capabilities include step-up multi-factor authentication which accounts for risk context. Passwordless authentication will be standard for managed devices.

Adaptive access

Access control enforced based on intelligent policies that consider location, time and user behaviour. For example, MFA is enforced when access is attempted at a specific location or time.

Identity federation

Identify federation enables Single Sign-On across different identity domains – external and internal apps and resources. Federated SSO creates a seamless user experience.

Role-based access control

Access rights are grouped into logical roles related to a users' job function and responsibilities. Access is controlled to resources a user is authorised to access based on roles and entitlements.

Single Sign-On

Single Sign-On application on-boarding is self-service and the SSO experience is consistent for web and mobile applications. Easy SSO improves UX by removing need to re-authenticate.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

Why KPMG

What we do

Advisory services

- Define and review Access Management strategy, roadmaps and business case that meet specific regulatory, compliance and/or business enablement objectives
- Perform assessments, including review of the clients Access Management maturity, provide business analysis and project staff to facilitate requirements and process documentation.
- Assist with vendor selection, running RFP or POC evaluation activities.
- Conduct Thematic Access Management Audits.

Transformation Programmes

- Deliver Access Management Transformation programmes by bringing together expertise in Governance, Processes, Implementation, Support and Operational delivery models.
- Infrastructure and product architectural assessments, implementation planning, technical strategy services, architectural and solution design.

Enterprise Access Elements Delivered

- Multifactor Authentication (MFA)
- Architecture and strategic road maps
- Governance and compliance (roles, data, certify)
- Solution implementation

Education services

- Facilitate business enablement or stakeholder education sessions during the lifecycle of an Access Management program.
- Strategy and business case development.
- Enable clients to become more proficient in the use of Access Management toolsets, with sessions aligned to toolset end users or administrators who may require focused training on specific functionality of the toolset.

Target State Authentication

Strong Authentication

- **Step-up authentication** can be used to achieve trust when required.
- **Multi-factor authentication (MFA)** is used to combine different factors of authentication leading to enhanced security**.**

Passwordless Authentication

- **Authenticator apps, physical keys, or biometrics** can be used for login.
- Passwordless authentication can be used instead of passwords where appropriate.
- Passwordless authentication can be used in conjunction with passwords for **step-up authentication and MFA**.

Risk based Authentication

- Dynamically determined assurance based on risks of individual requests.
- Requests **may be denied**or users **may be subjected to strong authentication**.
- Risk analytics are based on factors such as **location, device posture, network, travel context, user behaviours, and threat intelligence**.

Self service

- **Self-service portal** is used to enrol and manage passwords and passwordless authentication.
- Unlock accounts and change forgotten passwords through self service portal (verify ‘who I am’ using passwordless authentication).
- Self service application onboarding is based on pre-defined templates and patterns.

Service availability

- A **predictive service monitoring** capability to alert support team of deteriorating service and provides granular component level metrics to pinpoint likely fault location.
- **Production-like test environments** to assist with troubleshooting and to improve test coverage and quality.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

Why KPMG

British Fashion and Clothing

The challenge

- The client had a number of applications with employees, contractors and third parties having access but with individual credentials and with each having their own password complexity requirements. This lead to different password policies and standards, large volume of password reset requests and weaker overall controls for access and authorisation.
- The organisation also faced a large number of phishing attempts due to compromise of weaker passwords and sharing of credentials.
- Lack of appropriate challenge for un-authorised access e.g. out of hours, unknown network/location.
- Adoption of cloud based services added to the complexity as employees now had access to applications without having to log into the corporate network

KPMG approach

Discovery

KPMG engaged with the client's business and technical stakeholders to conduct a two week discovery and assessment exercise with an aim to identify the suitability of the applications for modern SSO technologies like SAML2.0, OpenID Connect, OAuth and multi factor authentication and provided the client with a prioritised list of applications based on suitability and risk to client data due to exposure. We performed an initial assessment of suitability of available technology (PingID) to what's available in the market.

Delivery, Support and Enablement

- We assisted the client with the development of requirements, performed requirements validation and obtained sign-off
- The requirements were then mapped to the functionality within current toolset to see the coverage and gaps.
- We then captured the technical and functional design, test criteria, resilience and failover aspects and user interface and functionality to produce the low level design. This was augmented by producing the requirements traceability matrix, test plan and proof of concept for a sample user set.
- On successful completion of the POC and sign-off, we developed a project plan, communications plan, user training and enablement plan and obtained further sign-offs to assess feasibility and delivery of the plan.
- We then performed application on boarding in a phased manner rolling out federated SSO and Multi factor authentication to 8 applications (5 cloud and 3 on premise) using on premise AD as the Identity provider and mobile devices/sms/email for second factor authentication (2FA).
- During the roll out phase, we performed employee enablement exercises by providing training using webex, quick user guides and FAQs.
- We provided support with arranging and during the UAT sessions.
- We trained and enabled the local IT teams, helpdesk teams and regional IT leads to improve user acceptance of the solution and aid usability.
- We also provided the hyper care & post go live support to enable smooth transition to service/BAU.

Client benefits

- Single sign-on access to 8 applications (cloud and on-premise) with a single set of domain credentials, standardised access protocols across the estate.
- Robust enforcement of stronger password polices compliant with the organisation's IT security policy by performing authentication against the corporate AD
- Elevated access challenges (2FA) based on access location and network used.
- Reduced number of help desk calls for password reset.
- Reduction in number of phishing attempts and date compromise due to inability to use just the credentials.

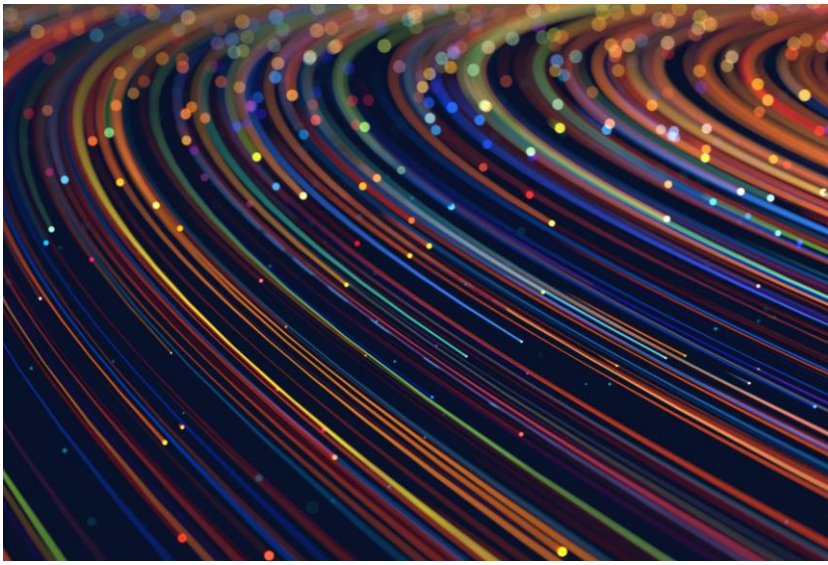
Summary

- 8 applications on boarded for SSO and 2FA within 6-8 months. 30 plus applications assessed for suitability during the discovery phase.
- Delivery collaterals produced: Requirements traceability matrix, Low level design, Build Guides, Test plan, Comms& Training Plan, Comms material & training guides and service design document.
- Knowledge transfer and transition of the solution to BAU.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

Our Approach



Implementation Plan:

Identity and 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.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

Our Approach

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

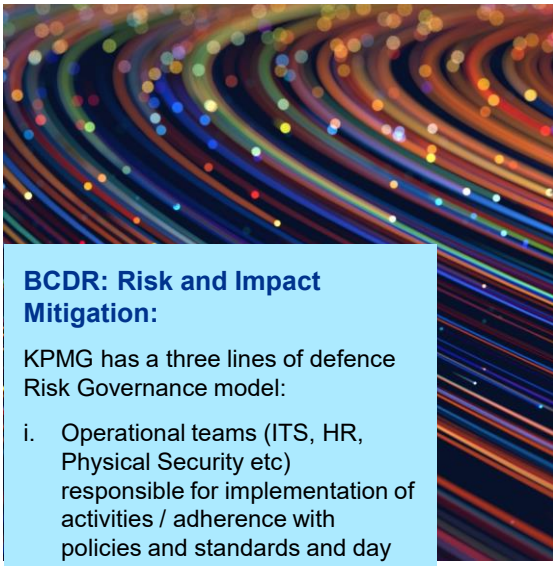
Business Continuity Co-ordinators are responsible for the maintenance and execution of client service recovery plans. The business recovery plans are reviewed within an ongoing programme of scenario based tabletop exercises.

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.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

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.

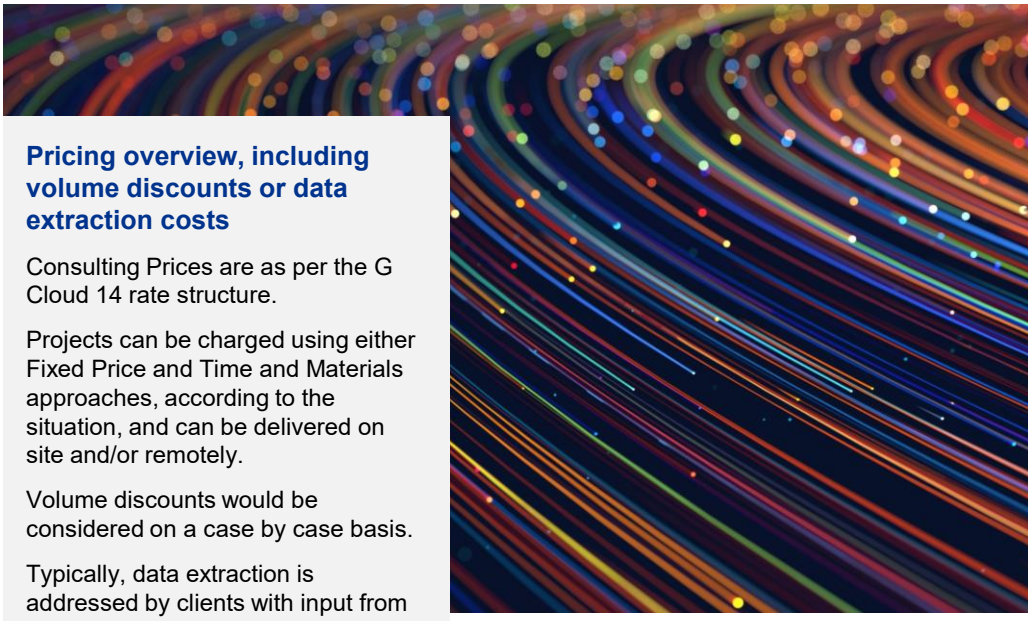
Both facilities are located in the UK. Production IT systems are typically hosted on an active passive infrastructure design, providing high availability and managed failover between data centres, underpinned by resilient fibre links.

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.



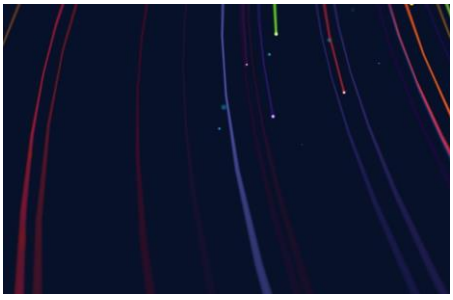
Pricing overview, including volume discounts or data extraction costs

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.

KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

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.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: **KPMG Confidential**

kpmg.com/uk

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: KPMG Confidential

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026