



KPMG Evidence-Backed Cyber Security Identity and Access Management (IAM/IDAM) Transformation

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 client's range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.



330+ professionals

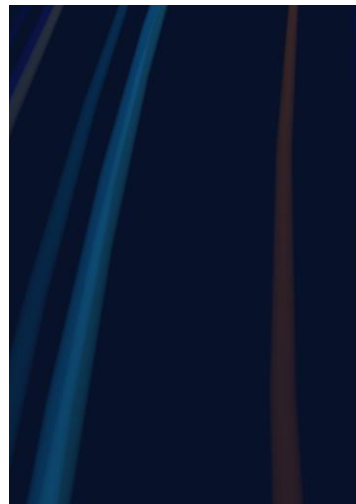
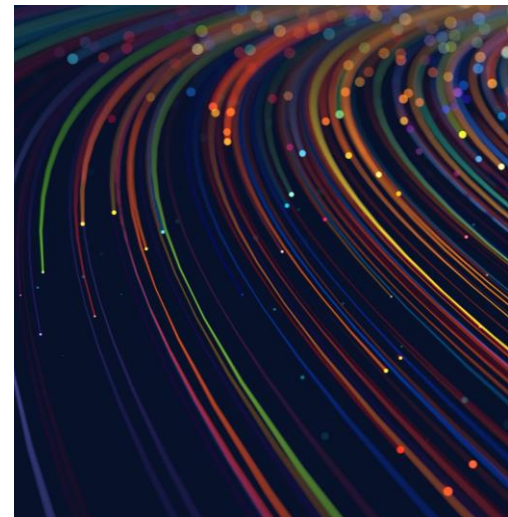
15+ office locations

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 Cyber Security Identity and Access Management (IAM/IDAM) - Transformation



Service Description:

KPMG will help you develop, design and deliver essential evidence-backed set of controls to prevent insider risk from inappropriate access to a cloud environment. The range of services include - Thematic audits and JML processes, strategy and roadmap development, deployment of Identity and Access Management (IAM) solutions and providing solution support.



What are the benefits of KPMG Cyber Security Identity and Access Management (IAM/IDAM) Transformation service?

- Reduce risk of unauthorised access to your critical business systems
- Reduce costs by operating sustainable business processes
- Reduce costs by technology solutions tailored to your needs
- Increase administrative effectiveness to your most critical systems
- Apply industry good practice to effective identity and access management
- Increase security across the organisation
- Improve employee efficiency with easy-to-use multi-factor authentication (MFA)
- Increased security with MFA



Our service features

- IAM Audits & Assessments
- IAM Analytics & Monitoring services
- Strategy and business case development
- IAM programme assurance and delivery
- Technology assessments, selection and implementations (Privileged Access Management & Identity Access Management)
- Managed Service
- Development of Service and Target Operating Models
- Implementation and configuration of IAM solutions
- Solution design and architecture

KPMG Approach

What we do

Advisory services

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

Transformation Programmes

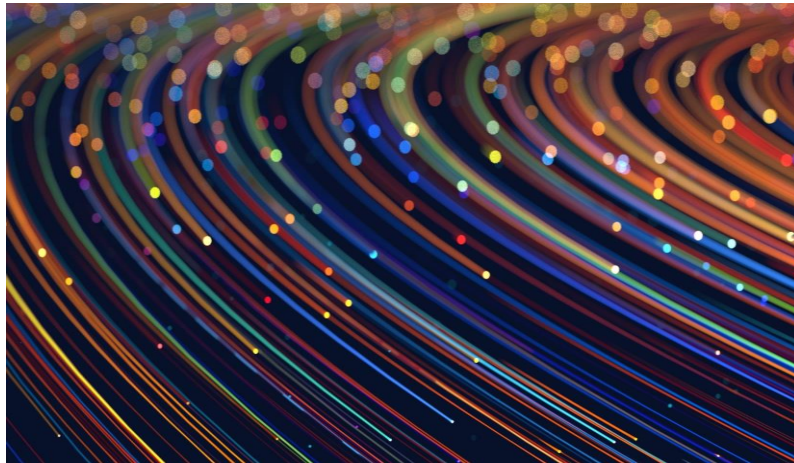
- Deliver IAM Transformation Programmes by bringing together expertise in IAM Governance, Processes, Implementation, Support and Operational delivery models
- Infrastructure and product architectural assessments, implementation planning, technical strategy services, architectural and solution design

Education services

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

Managed services

- Scale existing IAM implementations covering the on boarding of applications, ongoing definition of roles or segregation of duties.



The methodology we follow



Why we are different in the market

- We take a threat led approach with focus on automation and compliance
- End to end transformation services (Advisory and Technology)
- Based on methodology and framework
- We have the right expertise & global footprint
- 100+ IAM implementations so far around the globe
- Our framework can be tailored to the needs and objectives of the organisation

Why KPMG

How we can help

We have the Right Team and Experience

Our teams are composed of individuals who have extensive experience in IAM across many industries, and we have been involved in some of the biggest IAM deployments in the UK in the past few years.

We have experience in implementation and assessment of user management, authentication management, authorisation management, provisioning and ongoing monitoring. Our team is comprised of professionals who are experienced not only in designing and implementing IAM processes, but who are also able to help deliver business effectiveness and change through the sustenance of delivered IAM initiatives.

Our Focus is on Risk and Control

Unlike 'traditional' advisors who focus only on implementing systems, our professionals focus on the business process, risks and controls supporting your policies, processes, and technologies.

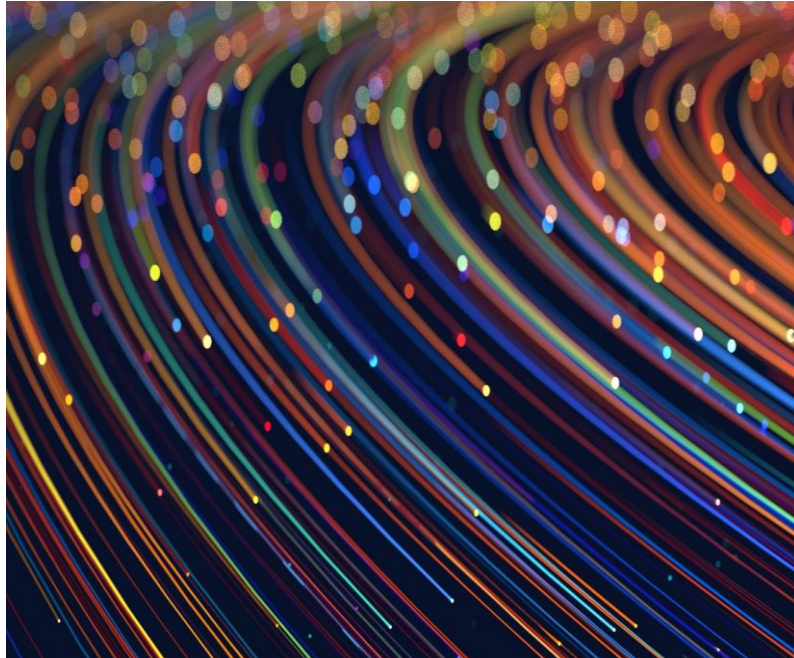
The combination of these professionals, along with our audit and support background, enables KPMG to help our clients develop strategic and sustainable processes and not a point-in-time plan.

Vendor Insights

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.



Client Issues

Regulatory compliance: Failure to implement adequate internal controls can result in non-compliance of regulations.

Audit requirements: Lack of centralised recording of all user management and user activity can result in unmonitored user access to business critical systems.

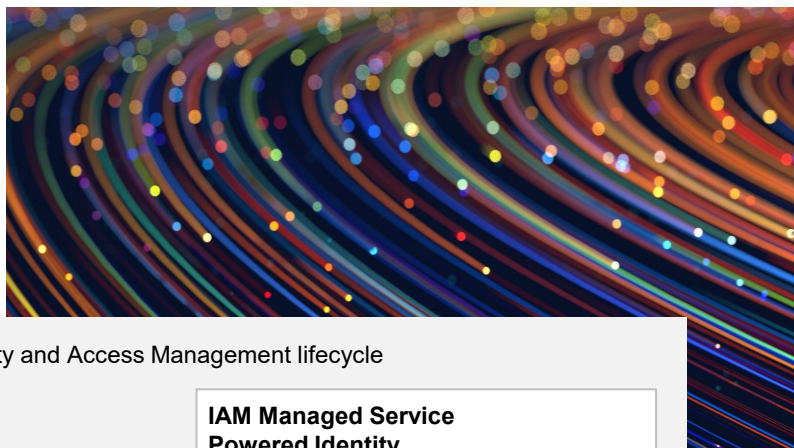
Insider threat: Inadequate access controls can allow internal users to exploit the elevated access they may have to business critical systems. Lack of Segregation of Duties for user access increases the opportunity of wrongdoing.

Data breaches: Lack of periodic access review and effective Joiner/Mover/Leaver process can result in continued access to sensitive information by users who should not access the business systems.

Operational efficiency: Manual processes for executing access requests, password resets and other access changes can result in operational inefficiency and results in high IT costs in Help Desk and other IT staff.

Risk Management: An effective IAM solution can play a significant role in strengthening security and mitigate risk by helping your organisation detect and remediate vulnerabilities: users with excess or inappropriate access privileges, policy violations and poorly-managed privileged user accounts.

Why KPMG (cont.)



Our services

We offer comprehensive IAM services across the entire Identity and Access Management lifecycle

Pre-implementation

Understand drivers and opportunities and tailor IAM initiatives to business needs

Example activities

- Requirements gathering
- Future state modelling
- Planning and roadmap
- Business case development
- Capability & maturity assessment
- Vendor and product evaluation
- Operating model design
- Role and policy modelling
- IAM Strategy
- Whole of business transformation

Implementation

Implement and deploy technology solution and infrastructure to deliver the required IAM capabilities

Example activities

- Solution architecture & design
- Project management
- Solution implementation
- Development and integration
- Data analysis and remediation
- Platform / product migration
- Change management
- SME Resource augmentation

IAM Managed Service

Powered Identity

IAM Maturity Assessments

Post-Implementation

'Keeping the lights on' – sustain and evolve the solution to meet changing business needs

Example activities

- Managed services
- Health checks
- Solution support
- Maintenance / Upgrades

Key clients and case studies

International Luxury Retail Brand

- Single sign-on to cloud and on-premise applications with standardised access protocols across the estate
- Enforcement of password policies compliant with the organisation's IT security policy and delegated authentication to a trusted source
- Elevated access challenges Two Factor Authentication (2FA) based on location and network segregation.
- Reduced help desk calls related to forgotten credentials and password fatigue
- Reduced the impact of phishing attacks by significant reduction due to 2FA challenges

Global Financial Services Company

- Significant risk reduction by ensuring that all terminated user accounts are promptly revoked, and the prevention of accounts becoming 'orphaned'
- Operational benefits delivered as a result of greater reliability of the leavers controls, meaning that manual processing of revoking leavers accounts is no longer required.

International Luxury Retail Brand

- Successful on boarding of SOX (Sarbanes-Oxley Act) privileged accounts and implementation of CyberArk solution within 6 months, the fastest KPMG CyberArk implementation to date.
- KPMG helped the client to effectively manage and control privileged account assets in the face of a constantly evolving threat landscape and an increasingly challenging regulatory environment. The client successfully remediated their critical audit findings around the SOX applications.

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 several 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, and when in relation to the changes the project is planning to implement
- Provision of orientation sessions in the Methodology 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

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 15 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.

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
- 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 most 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.



Contact Us



**Amit
Kumar**

Director,
**Head of AI and
Cloud Propositions**

KPMG LLP,
CIO Advisory
15 Canada Square
London E14 5GL
amit.m.kumar@kpmg.co.uk



**Douglas
Dick**

Partner,
**Head of Cloud Engineering
Risk Controls**

KPMG LLP, FS Tech Risk
15 Canada Square
London E14 5GL
douglas.dick@kpmg.co.uk



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