G-Cloud 14

PwC and G-Cloud: Knowledge, Experience, Value

Identity and Access Management (IdAM) Services

May 2024

pwc

Contents

Transforming Business using the Cloud

We have worked with many Central and Local Government clients to support the implementation of their business objectives using cloud technology. Enabling business and enterprise transformation using cloud is a complex, strategic consideration facing many private and public sector organisations.

Cloud technology and services have the potential to reduce cost, remove technology bottlenecks, and facilitate rapid business innovation. As a result, for most organisations globally, adopting cloud technology has become a question of “when and how” rather than “if”.

Opportunities for enterprises generally include a combination of one or more of the following:

- Implementing private and/or hybrid clouds for infrastructure and applications;
- Smarter use of public cloud infrastructure for optimising existing business functions;
- Using cloud for implementing new business services or digital operations; and,
- Reducing cost by moving to consumption based pricing models that only charge for the actual IT capacity and services used.

Migration or adoption of cloud must be properly choreographed for success. We understand the realities and the business and technical risks that should be fully considered, understood and mitigated before such a move. Critical considerations include:

- Alignment of business and technology objectives. This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions;
- Availability and reliability of services. The avoidance of operational downtime to mitigate in lost revenue, unnecessary operational cost or reputational damage that can disrupt a business’ operations;
- Decentralised support structures. The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information.
- Data handling practices. Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data.
- Data privacy. Compliance with GDPR to understand where and how information can be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out of office experiences.
- Future Technology Trends. Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

A careful assessment of an organisation’s needs and different cloud service provider’s controls is required, enabling concerns to be addressed and the correct path to the cloud is selected.

As a trusted advisor PwC provides the framework, and the wealth of private and public sector experience, to consider the combination of Business, customer experience and Technology activities outlined above. There is no single answer that covers each and every client organisation; we tailor our frameworks to client circumstances to support clients:

- As a partner through the complete lifecycle of strategy through to execution; and,
- With point business issues encountered during implementation or running the business.

Identity and Access Management (IdAM) Services

This section describes in more detail the service features and benefits included within this service definition document.

Identity and Access Management (IdAM) Services Description

PwC provides a wide range of services that can help you assess, define or implement the people, processes and technology you need for your IdAM capability. We view IdAM as a whole-organisation challenge, establishing organisational change in parallel with technology to enable rapid digital transformation for customers, partners & themselves.

Identity and Access Management (IdAM) Services Features

- Digital Identity for workforce covering assigning unique digital identifiers for staff, granting, amending and revoking access to employees, contractors,suppliers, partners, guests, and other contingency staff.
- Identity Verification and the design and implementation of capability to deliver Role Based Access Control (RBAC) for the workforce.
- Access Governance including identifying and remediating access in violation of policies such as Dormancy, Segregation of Duties (SoD), Toxic Access Combination, and any other inappropriate access.
- Access Management capability covering strong Multi Factor Authentication (MFA), providing seamless access to applications using Passwordless, Single Sign-On (SSO), Federation, and other Identity Orchestration capabilities.
- Identifying and securing Privileged access (PAM) and application of policies to rotate Passwords, provide Just in Time (JiT) access, record privileged sessions and secure secrets.
- Use Identity Threat Detection and Response (ITDR) capabilities and Cloud Infrastructure and Entitlement Management (CIEM) capabilities to detect access anomalies and take remediation measures to reduce risk.
- Customer Identity or Consumer Identity and Access Management (CIAM), Consent Management, Single Customer View, API Security
- Directories including Azure AD, Active Directory, LDAP, Universal Directory
- Supported vendors include: Sailpoint, Saviynt, CyberArk, Microsoft, Ping / ForgeRock, Okta, Delinea, MicroFocus, Centrify
- Apply IdAM Standards: PSD2, FIDO, SAML, OAuth, OpenID Connect, UMA.

Identity and Access Management (IdAM) Services Benefits

- Review access policies, security controls to identify gaps and gain insights on the practical recommendations to address gaps.
- Review current IdAM capability maturity to assess access risks due to inappropriate access (e.g, access compromise, access misuse, unused access, policy violations etc) and take measures to minimise risks.
- Review the current access management practices to assess their alignment with industry good practices, regulatory requirements and standards to address gaps
- Advise on IdAM vision, strategy, target state architecture, roadmap and operating models.
- Support IdAM vendor selection and comparison, create RFP documents, and define requirements and use cases covering people, process, technology and security, and create IdAM business cases to seek funding.
- Create IdAM solution architecture/design, implement tools to streamline and standardise the IdAM processes to improve efficiencies, user experience and user productivity.
- Deliver business and technology transformation changes using IdAM as an enabler.
- Provide IdAM programme governance, SME support, change oversight and expertise.
- Provide an independent assurance on the IdAM capability delivered by other delivery partners.
- Provide IdAM managed services including L1/L2 and L3 operational support to minimise the burden on in house teams.

PwC provides a range of UK government and public sector focused IdAM related services that can help your organisation build public trust and enhance value for your internal employees, stakeholders, third-parties and citizens. We can help you achieve core drivers of:

- Business enablement
- Digital Transformation
- Risk and compliance management
- Cost savings and efficiencies
- Operational resilience

We can provide you with the full range of IdAM trained cyber security expertise. This ranges from business focussed experts who can design and implement an IdAM strategy, maturity assessment and Target Operating Model (TOM) to establish the necessary organisational culture, to helping you analyse your requirements, assess vendors and provide RFP support. As part of our Digital Transformation function, we can provide a team of specialised consultants who will follow our 'Transform' delivery methodology to assess, design, construct, implement, operate and review the IdAM solution for your organisation.

1. General Advice and Assurance

PwC can help you with every stage in understanding the effectiveness of how your enterprise is currently managing the identities and access of users (e.g. employees, citizens, contractors, partners, vendors, things, etc.) to assets (e.g. applications, infrastructure, structured and unstructured data, devices, IoT, and physical). We can conduct objective reviews of your current IdAM capabilities to give you assurance that your current access and authorisations controls are both comprehensive, well aligned to your threats, risks, policies and business drivers. Previous engagements include:

- Access reviews
- Threat and risk assessments
- Maturity assessments
- Project & programme assurance

2. Strategy Development

We can work with you to create a long term vision and strategies that are both for the business and understood by the business. This helps you build your internal business case for prioritising and investing in your IdAM capability, and the confidence that you will get the right solution for you when you go to market for solution elements. Once you go to the market we can help you with vendor and market assessments, and provide RFP support throughout the selection and procurement processes. Previous engagements include:

- Maturity models
- Current & target states
- Policy & process improvements (JML, etc.)
- Architecture & Enterprise technology frameworks
- Digital Transformation
- Capability based planning
- Roadmap definition & transition plans
- RFP Support & requirement gathering
- Vendor assessments & selection

3. Target Operating Model Design

The target operating model for IdAM is used to give clients a holistic perspective of how access should be governed in an organisation. We leverage industry best practice and our experience in large, complex organisations. The target operating model establishes good practices for access processes, roles, responsibilities, reporting, how to build, deliver, operate and integrate any solution, and other various tasks throughout your organisation's different business areas and geographic locations. Previous engagements include:

- Framework, scope and charter
- Processes

- Roles and responsibilities
- Communication and training
- Operations

4. Solution Design, Delivery and Managed Services

At PwC for IdAM we use our Transform IT Delivery Framework which allows us to propose an accelerated delivery over a record period of time. This agile approach for designing, building and integrating digital platforms defines governance, delivery management process and roles, support tools, integration to programme management, deliverables and transition processes and controls.

We are the largest solution delivery partner of SailPoint globally and are a leading specialist in the design and implementation of Sailpoint, CyberArk, Saviynt, Ping / ForgeRock, Microsoft Azure, OKTA, Delinea, IDAX, and Micro Focus (NetIQ) solutions. Outside these technologies we are also skilled in IdAM vendor offerings from BeyondTrust, RSA, Oracle, IBM and CA. Engagements are typically run across the following phases: (including change management and programme delivery)

- Assess and advise
- Design
- Construct
- Test
- Implement
- Operate and review

5. Solution Areas

At PwC we can provide you with expertise across the four key pillars of IdAM. These are the four areas of IdAM that allow the logical grouping of all capabilities that can be implemented as part of an IdAM solution, collectively or individually. They are typically delivered by one or more technology vendors in the IdAM space. Previous engagements have included delivery of capabilities across any combination of the following pillars:

- **Access & Data Governance** – Provide a single view of who has access to what systems and data (structured and unstructured) across the entire organisation. Monitor and detect violations to corporate policies such as Segregation of Duties (SoD), detect orphan and dormant accounts, and ensure that JML processes are effective. Ensure access is appropriate by providing regular automated reviews of access (recertification/attestation) and provide a platform for Role and Attribute Based Access Control (RBAC/ABAC).
- **Identity Management (Enterprise & Consumer)** – Enforce and manage access to systems for both enterprise users (staff, third-parties, contractors, etc) and consumers (customers, citizens). Capabilities including automated provisioning, Access Request, Self-Service Password Reset, Third Party Integration, Cloud Management and automated policy enforcement.
- **Privileged Access Management (PAM)** – Control, manage and monitor access to your ‘crown jewels’ by all types of users, from staff to third parties. Be able to replay who did what and when to high risk systems in your organisation. Enforce security best practices by never needing to provide passwords to your most privileged accounts and systems, replacing the round the clock standing privileged access with Just-in-Time (JIT) privileged access, and control who has access to what at the most granular of levels.
- **Access Management (Enterprise & Consumer)** – Provide secure, frictionless access for enterprise users and consumers to your systems. Adopt a “Zero Trust” approach in order to protect against internal and external threats, leveraging capabilities such as the latest security standards and protocols (e.g. SAML2, OAuth2, OpenID Connect), Multi Factor Authentication (MFA), and Context/Risk based access controls. Improve the user experience, enable administrators, and reduce costs, by leveraging capabilities such as Federated Authentication and Single Sign On (SSO).

Our IdAM experience

PwC has completed many IdAM engagements, covering the full range of IdAM services, for UK clients. Selected examples are shown below, but if you would like to talk to us about our service offerings, or to find examples that are relevant to your market sector or scale, please do get in touch.

A World Top 100 Research University	Our client, a UK research University, ranked as one of the world's top 100, invited PwC to assist them define an Identity and Access Management (IdAM) strategy. This was to improve the efficiency and effectiveness of their existing operations. The PwC UK IdAM Practice was asked to leverage identity and access management to help the University deliver more modern, flexible and sustainable academic services, whilst reducing costs and complexity. • We worked closely with the university to put together a strategy that mapped IdAM capabilities to its strategic aims and vision. • We reviewed the University's overall vision and business drivers, then identified appropriate stakeholders across all departments and faculties. • We undertook stakeholder interviews to identify challenges, risks and issues with the current system, and understand what was on each person's strategic agenda. A maturity assessment was undertaken, an as-is assessment and GAP analysis. • A requirements gathering exercise was carried out which led to the design of a vendor agnostic solution, defining architectural principles and producing capability based plans that allows the University to adopt a phased delivery approach, realising business benefit at each delivery stage. As a result PwC defined an identity and access management strategy to meet the requirements of the University, demonstrate the capabilities that are required to provide a new digital platform to improve services and the student journey, and provide a plan of how to achieve it. Also providing an agnostic design, and an assessment of which vendors would be able to meet the requirements of the University to deliver the capabilities it needed.Played back the strategy to the executive board and Information Service Steering Groups to help the University progress to the technology selection phase, which we subsequently requested to assist with
A Critical Research Driven Independent Intergovernmental Organisation	Our client is a critical independent intergovernmental organisation. It operates one of the largest supercomputer complexes in Europe and the world's largest archive of numerical weather prediction data. PwC were invited to help the organisation design an Identity and Access Management (IdAM) strategy along with a roadmap to improve the overall IdAM posture of the organisation and replace the legacy IdAM system as part of a significant move to a new data centre. We worked closely with the organisation to put together an iterative and incremental delivery approach by decomposing this complex project into work packages to suit the organisation's culture and assist them in the gradual knowledge growth. It helped to realise the business drivers by focusing on one specific section of the strategy at a time and considering the impact from

	various ongoing changes including the move to a new data centre. The Strategy included: ● Current State and Future State assessment ● Gap Analysis ● Vision and Architecture Principles ● Transitional Architecture ● Current and Future JML processes ● Vendor comparison ● Roadmap As a result, PwC developed a strategy and vision which will drive the IDAM transition programme in the organisation for the coming 3 years. Provided capability based plans for the organisation to illustrate the architectural transition from the current maturity state to the target maturity state. Developed an implementation plan that details all the initiatives identified and the priorities of implementation considering the resources available and impact from the data centre move.
Large UK Higher Education Institution	The client's initial engagement was for PwC to develop an IdAM capability strategy as part of their overarching digital transformation program. PwC worked closely with the client to put together an IdAM strategy and roadmap that would enable them to manage their identities, reduce costs, and improve their security controls. Being satisfied with the strategy PwC was then requested to deliver the following: ● Vendor selection ● Business process redesign ● High level and low level designs ● Implementation of the solution (joiner, mover, leaver and recertification) ● Design and prototype of a federated single sign-on solution As a result of the work completed, the client was provided with a tested IdAM capability that could be taken into production, as well as detailed designs to build upon for subsequent capability phases.
UK Regulatory Body	PwC was selected as the client's security acceleration partner with a remit to re-shape and execute a multi-year cyber security programme with the aim of rapidly reducing their cyber risk exposure and re-architecting their security controls to support their new multi-cloud ecosystem. This included the planning, mobilisation, management and execution of their IAM sub-programme covering PAM, IGA, access management and CIAM. All IAM solutions were SaaS based. Key areas of PwC assistance included: ● Implementation of quick wins such as enforcing Azure PIM for elevated access on Azure AD, MFA on network access and risk based access policies to achieve accelerated risk reduction in < 6 months. ● Implementation of Delinea PAM solution to secure their Tier 0 access across Azure, AWS and on premises infrastructure at a rapid pace. ● Implementation of Saviynt IGA solution to automate their workforce / 3rd party joiners and leavers process for standard and privileged users.

	● Integration of Saviynt and Delinea to enable automated access provisioning and certification capabilities.
National Government	Client had limited business wide governance of IAM capability and controls, and had a limited view on who is accountable for access risks, defining the controls, responsible for monitoring the controls; and responsible for executing the controls. Client had issues with multiple IAM processes and teams with manual processes that duplicated effort and left process, capability and ownership gap. PwC assisted the client across the following areas: **Project Management and Business Change** ● Coordinate with business on the broader Cyber Security Programme ● Facilitate business change enabled by the IAM Project ● Manage the end to end delivery of the IAM project **Discovery** ● Discover and analyse the existing IAM processes, policies and tools ● Determine the business drivers for IAM ● Establish the IAM requirements and roadmap ● Define the target state architecture & operating model for IAM services **Tooling Delivery** ● Conduct validation, design, implementation, testing and handover of a SailPoint Identity Governance and Administration (IGA) tool and Delinea Privileged Access Management (PAM) tool. ● Provide tooling strategies and plans in line with the Roadmap.
Global Entity	Client had an urgent need to improve privileged access management (PAM) controls after a security incident.They are the largest in their industry with 40,000 employees across 50+ countries. Each with localised IT functions, processes, technology and governance. PwC delivered the following: ● Coordinated a global effort to analyse current PAM processes, technology, attack vectors, strengths and weakness with the organisation ● PwC performed a gap analysis against our PwC PAM capability matrix and leading industry standards ● Developed a target state for PAM; processes, requirements, logical services and component architecture ● Created a common taxonomy, governance, delivery and operating model ● Developed an implementation plan and technical architecture ● Provided proactive technical assurance over the project team and system integrator. This included building an architecture specification, reviewing all design documents, providing ad-hoc advisory and creating On-boarding framework for BAU migrations. In addition, controls and technical configuration testing was across each environment via stage gates. ● Provided a project officer to support the programme delivery manager for daily project governance.

As a result, we worked with the client to rapidly identify the highest risk accounts to bring immediate value back to the client.Created a global approach for the client. Educated the client across PAM controls and the mitigation they bring to the risks most relevant to the client's industry. Ensured quality of the solution and return on value through a proactive assurance regime across the solution's delivery.

This was done using specialist PAM resources