

CLOUD IDENTITY AND ACCESS MANAGEMENT ARCHITECTURE & DESIGN

Service Definition
G-Cloud 15

REPLY

38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
info@reply.com

www.reply.com



TABLE of CONTENTS

CLOUD IDENTITY AND ACCESS MANAGEMENT ARCHITECTURE & DESIGN	1
SERVICE DEFINITION	1
TABLE OF CONTENTS	2
SERVICE DESCRIPTION	3
SERVICE FEATURES AND BENEFITS	4
ONBOARDING	7
KICK-OFF MEETING	7
ACCOUNT MANAGEMENT	7
<i>DESIGNATED ACCOUNT MANAGER</i>	7
<i>FORTNIGHTLY REVIEW MEETING</i>	7
OFFBOARDING	7
ACCESS TO DATA	7
SECURITY	8
PERSONNEL SECURITY	8
INFORMATION SECURITY	8
PHYSICAL SECURITY	8
TRAINING & KNOWLEDGE TRANSFER	9
ORDERING AND INVOICING PROCESS	10
CUSTOMER RESPONSIBILITIES	11
TECHNICAL AND CLIENT-SIDE REQUIREMENTS	11
OUTCOMES AND DELIVERABLES	11
ABOUT REPLY	12

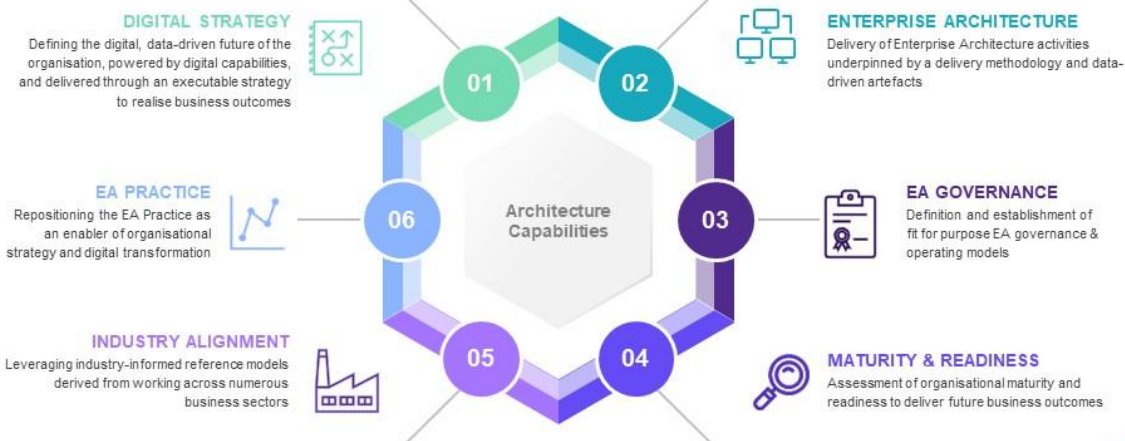


SERVICE DESCRIPTION

Reply specializes in designing IAM architectures that underpin robust, scalable, and secure identity management solutions. Our approach encompasses high-level and detailed IAM architectures, ensuring centralised authentication and authorisation for cloud-based services. We prioritise seamless integration, adherence to security standards and policies, and compatibility across technology stacks to facilitate digital transformation initiatives. By leveraging cloud technologies, we deliver scalable, sustainable, and cost-effective IAM solutions tailored to your organisation requirements, enhancing user experiences and ensuring secure access to digital services.

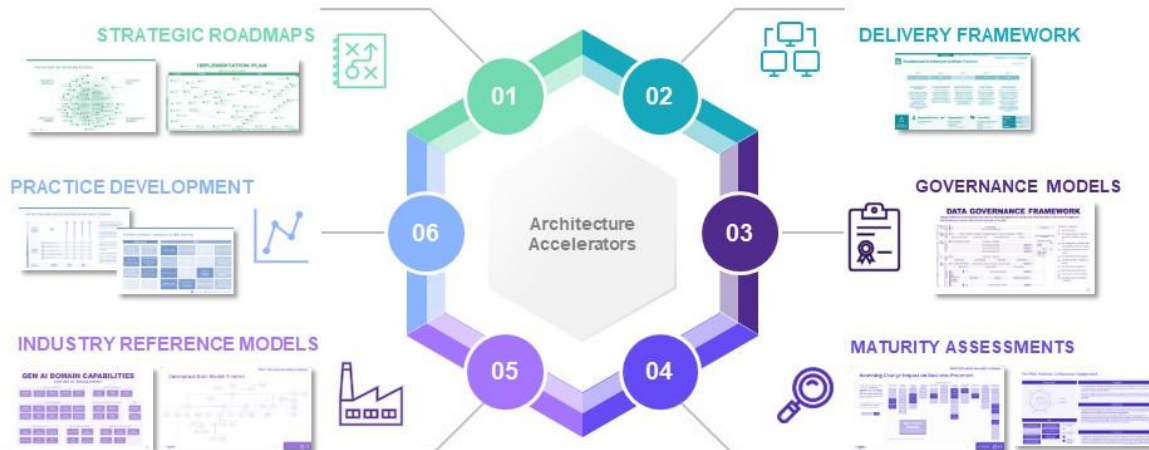
OUR CAPABILITIES

ENABLING ORGANISATIONS TO REALISE VALUE FROM THEIR ARCHITECTURE THROUGH EFFECTIVE EXECUTIVE ADVISORY, GOVERNANCE AND STRATEGIC PLANNING



OUR ACCELERATORS

ESTABLISHED METHODOLOGIES, TOOLKITS AND FRAMEWORKS TO MATURE ORGANISATIONS AND ADDRESS THEIR DATA CHALLENGES





RECOGNISED AS ARCHITECTURE LEADERS

 Market Guide for Business-Outcome-Driven Enterprise Architecture Consulting Recognised by Gartner in their Market Guide as a leader in business outcome driven EA consulting. The only UK based architecture consultancy to achieve this	 Platinum Approved by BCS, the highest level of accreditation only held by a handful of organisations. Recognised for furthering the IT profession
 Key Contributor to the Open Group Architecture Framework and an active Gold Member Led the development of the initial Business Capability Modelling concepts within TOGAF.	 Member of the Business Architecture Guild, contributing to the discipline and maturity of Business Architecture and Enterprise Architecture.
 Active Architecture contributor to DAMA, the Data Management Community. Our focus is on improving Data Governance across Financial Services.	 The Awards recognise projects that demonstrate improvements, or potential improvements, in innovation and collaboration across defence. The commended project, titled 'Governing Master Data within Defence Logistics', marks the second time the strategy and architecture specialist has received an award at the Team Defence Information Excellence Awards.



Service Features and Benefits

FEATURES

Definition of enterprise security principles and controls for consistency

We define and implement enterprise security principles and controls to ensure consistency and adherence to government security standards and regulatory requirements.

Scalable approach, from pilot to millions of users

We design IAM architectures that can scale seamlessly from small pilot projects to support millions of users, providing flexibility and agility to accommodate evolving business needs.

Robust auditing patterns, to ensure consistency of audit data

Our approach endows the establishment of robust auditing patterns that guarantee consistency and integrity of audit data, enabling government agencies to demonstrate compliance with regulatory requirements.

BENEFITS

Principles scaled and applied to all projects, reducing risk/costs

Our standardised security principles and controls can scale and be applied to all projects, reducing security risks and costs associated with disparate implementations.

Cost-controlled approach, use the same solution regardless of size

We adopt a cost-controlled approach by promoting the use of the same IAM solution regardless of project size, ensuring cost-effectiveness and consistency across DDaT initiatives.

Delivers compatibility through the use of industry standards

We ensure compatibility, interoperability and empower effective collaboration through the implementation of standards such as SAML, OpenID Connect and OAuth2, enabling users to authenticate once and access resources across multiple cloud environments seamlessly.



Delivery of identity mediation approach through robust policy management We facilitate implementation of identity mediation through robust policy management, enabling seamless integration and interoperability across disparate systems and domains.	Leverage audit records to identify issues and responsibility We leverage audit records to identify and address security issues promptly, ensuring accountability and transparency in access management and compliance.
Detailed, documented identity mapping between domains for entities and attributes We develop detailed and documented identity mapping between domains for entities and attributes, ensuring accurate and consistent identity resolution across applications and services.	Integrated management approach for both service providers and service requesters We implement an integrated management approach for both service providers and requesters, streamlining identity resolution and enhancing user experiences.
Browser-based/seamless integration as required by the technology stack We provide browser-based and seamless integration options tailored to the government's technology stack, ensuring ease of use and accessibility for service users.	Consistent definitions reduce the risk of incorrect access to systems Our consistent definitions reduce the risk of incorrect identity resolution leading to incorrect access to systems and data, ensuring compliance with access control policies and regulatory requirements.
Cloud Readiness/Maturity Assessment for federated identity We conduct Cloud Readiness/Maturity Assessments for federated identity, evaluating readiness and maturity levels to support seamless integration and interoperability in cloud environments.	Friction-less authentication for smooth and intuitive user experience Providing seamless and effortless authentication and authorisation to grant users access to digital resources or services, without unnecessary hurdles or interruptions, while maintaining strong security and compliance.
Hybrid/Multi-Cloud Architecture, including GCP, AWS, and Azure We design identity for Hybrid/Multi-Cloud solutions, catering for multi-cloud strategies and integration with major cloud platforms such as GCP, AWS and Azure; implementing federated identity and SSO capabilities to allow users to access resources across multiple cloud environments seamlessly.	Target areas for most effective improvement; maximising return on investment: We target the areas offering the most effective improvement based on timely and appropriate such as Cloud Readiness/Maturity Assessments, maximising return on investment and driving continuous improvement in IAM capabilities.
Standardised modelling using SAML, OpenID Connect, OAuth2 We implemented renowned standards enabling interoperable and friction-less	Platform-specific best practice for Federated Identity Architecture We architect federated identity applying platform-specific best practices, ensuring



authentication and authorisation across different systems and platforms.	optimal performance, scalability, and security in hybrid and multi-cloud environments.
Digital Identity (IAM, CIAM, IGA, IDaaS) Advisory Services We provide assessment, recommendation, guidance and support for adoption of different cloud identity approaches and solutions, including Identity Governance & Administration; that endorse your organisation's strategy and roadmap planning.	Improved, more reliable security for service users and data Our IAM solutions deliver improved, more reliable security for service users and data, reducing the risk of unauthorised access, data breaches, and compliance violations.



ONBOARDING

Kick-Off Meeting

When we start an engagement with a new client, we begin with a workshop introducing the team (from both Reply and the client), the project objectives, and our anticipated timelines and approach. This workshop is most impactful when the majority of client stakeholders involved in the project are present and involved (either in person or remotely). Where this is impossible, we can hold separate sessions with teams that cannot participate in the kick-off workshop to ensure all stakeholders are engaged and bought into the project's objectives.

Account Management

Designated Account Manager

Each client has a designated Account Manager, who will be the main point of contact throughout the engagement. This individual is responsible for ensuring that delivery progresses and is executed to the standards that Reply and our clients expect.

Fortnightly review meeting

Alongside regular ceremonies and informal daily interaction between the Reply project team and the client, we hold formal review meetings with key stakeholders, usually fortnightly. This includes critical client stakeholders, senior Reply project team members, and the Reply Account Manager. Where appropriate, these meetings will consist of a review of work completed and demonstrations or walk-throughs of deliverables.

Offboarding

Where an engagement continues to completion, unless the client requests an extension or new engagement, all client IT, documents, artefacts and deliverables will be returned to the client. Our team will ensure a complete handover of data and knowledge to client staff. An ongoing support or retained advisory service may be implemented where appropriate to provide additional continuity.

Access to Data

Ensuring secure access to client data upon exit is paramount to maintaining confidentiality and integrity. We begin by conducting a comprehensive inventory of all client data stored within our systems, encrypting it both in transit and at rest using industry-standard protocols. Strict access controls and authentication mechanisms are implemented to restrict access to authorized personnel only, with permissions regularly reviewed and updated. Client data is segregated from other data within our systems, ensuring isolation and protection. Upon exit, all access rights to client data are promptly revoked, including user account deactivation and permission removal. If requested, we securely delete or anonymise client data in accordance with retention policies and regulatory requirements. Detailed documentation and audit trails of data access are maintained, providing transparency and accountability. Before exiting, we verify with the client that all necessary data access has been revoked. Finally, we adhere to legal and regulatory obligations regarding data protection and privacy, ensuring compliance with contractual agreements and applicable laws such as GDPR or HIPAA. Through these measures, we ensure that client data remains secure throughout the exit process, mitigating the risk of unauthorized access or data breaches.



SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels. Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains. Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.



TRAINING & KNOWLEDGE TRANSFER

We enable customer teams throughout delivery by embedding knowledge transfer alongside implementation activities. Training is aligned to organisational roles, ensuring relevance for finance users, operational staff, and system administrators.

Knowledge transfer is delivered through:

- A train-the-trainer approach to establish internal subject matter experts.
- Technical training for administrators covering configuration, security roles, and integrations.
- Walkthroughs of system design, data structures, and operational processes.
- Provision of comprehensive documentation, including user guides and runbooks.

Formal training is supported by ongoing access to expert guidance during delivery and early life support. Where required, refresher sessions or additional enablement can be provided to support organisational change or onboarding of new users.



ORDERING AND INVOICING PROCESS

To begin the process, please contact glue.frameworks@reply.com with details of your organisation, role and high-level requirements.

Our Framework Manager will connect you to our experts and from here we will organise an introductory discussion to go into more detail and shape a proposed engagement that suits your needs.

We invoice for both fixed price and time and materials engagements one month in arrears. For fixed price engagements, this takes place upon completion of the deliverable(s), or in stages, if the size of the engagement is greater than £40,000 excluding VAT.

Payment terms are 30 days net of receipt of invoice.



CUSTOMER RESPONSIBILITIES

To deliver our responsibilities as a partner, we require the following:

- Full access to systems and data that are relevant to the specific project
- Reasonable and timely access to key stakeholders and internal SMEs for information gathering, requirements definition and other critical tasks associated with the delivery of our outputs

Technical and Client-Side Requirements

Other than the system access specified above, there are no specific technical or client-side requirements that would limit our capacity to begin work.

Outcomes and Deliverables

Our engagement's specific outcomes and deliverables will be determined during the scoping phase before beginning the project based on your goals and objectives and the level of depth you require. These will include:

- Workshop(s) to discuss and assess the existing architectural design
- Detailed assessment of design with identification of risks and opportunities
- Report with recommendations and proposed action plan



ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations