

CENTRES OF ENABLEMENT FOR CLOUD SOLUTIONS

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

SERVICE DEFINITION	1
TABLE OF CONTENTS	2
SERVICE DESCRIPTION	3
ONBOARDING	5
KICK-OFF MEETING	5
ACCOUNT MANAGEMENT	5
<i>DESIGNATED ACCOUNT MANAGER</i>	5
<i>FORTNIGHTLY REVIEW MEETING</i>	5
OFFBOARDING	5
ACCESS TO DATA	5
SECURITY	6
PERSONNEL SECURITY	6
INFORMATION SECURITY	6
PHYSICAL SECURITY	6
TRAINING & KNOWLEDGE TRANSFER	7
ORDERING AND INVOICING PROCESS	8
CUSTOMER RESPONSIBILITIES	9
TECHNICAL AND CLIENT-SIDE REQUIREMENTS	9
OUTCOMES AND DELIVERABLES	9
ABOUT REPLY	10



SERVICE DESCRIPTION

Centres of enablement for cloud solutions are dedicated organisational functions who have a remit to disseminate, facilitate and lead competencies and capabilities in cloud technology for the overall organisation.

The emphasis is on serving as a facilitator to the rest of the organisation so that those departments can develop their own specialised capabilities with the support of the Centre of Enablement. Setting the overall strategy and structuring an enablement framework working in partnership with the rest of the organisation.

Centres of Enablement

- Define and lead the strategic direction for cloud architecture and technology for different government entities and help other departments develop expertise and capability. Establish approach for IaaS, PaaS and SaaS models based on organisational use cases.
- Establish a clear governance framework and Cloud Enablement Board ensuring policies, technologies, processes and resources are utilised efficiently and effectively.
- Manage key resources from a central shared pool, deploying expertise across the organisation and establish a targeted training programme to improve knowledge in the cloud computing domain.
- Ensuring the correct protocols are being followed in terms of Data Protection and Security protecting the public's data and conforming to legal regulation.
- At the forefront of innovations in cloud technology and be able to recommend the best architectural approaches and technological solutions.
- Manage and build a central asset repository where vetted and approved software code libraries reside and can be distributed to the wider organisation.

Establishing a Cloud Centre for Enablement

- Each government department or entity will follow a tailored approach which is broadly in-line with the following steps and following the GDP methodology of Discovery, Alpha, Beta and Live.

Define Objectives and Scope

- Identify clear goals and service outcomes for the enablement centre.
- Set a clear set of capabilities in the short, mid and long term.

Audit Existing Processes and Capabilities

- Understand which capabilities and processes are already effective and incorporate them in the go-to ways of working. Eliminate broken processes or those that add little value.

Define Governance Framework

- Establish the Governance Board as the decision-making executive branch of the Centre for Cloud Enablement responsible for steering and guiding initiatives managing risk, resources, policies, governance and technology decisions.
- The governance framework maps out a blue-print for how to consistently, rapidly and securely kick-off cloud initiatives within the government organisation.



Data Integrity and Security

- Ensure the organisation or government entity is aware and adheres to all regulatory and legal obligations such as GDPR, the Data Protection Act 2018 and other relevant compliance requirements

Technology Standards

- Establish technical guidelines, standards and policies when working with cloud-based technology to ensure consistency and integrity of use. This includes design patterns, technology stack, key use cases, security and compliance protocols.

Training and development

- Guide training and development programme ensuring consistent level of expertise throughout the organisation.

Operational Planning

- Guide training and development programme ensuring consistent level of expertise throughout the organisation.

Continuous Improvement

- Ongoing monitoring and feedback of the process is essential to maintain high standards and ensure the cloud enablement centre is fit for purpose.

Benefits

Moving to a cloud centric architecture and establishing a centre of enablement can have enormous benefits for a government organization both in terms of cost savings and process efficiencies.



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