

AWS PLATFORM AS A SERVICE (PAAS)

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
HOSTING INFRASTRUCTURE	5
DISASTER RECOVERY	5
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's AWS Platform as a Service (PaaS) is designed to empower organizations by providing a robust and flexible cloud infrastructure. This service harnesses the power of Amazon Web Services to offer an environment that supports agile development methodologies, enabling rapid deployment and scaling of applications.

At the core of our offering is a methodically architected solution that promotes resilience, high availability, and seamless scalability. Businesses can leverage our PaaS to innovate faster, reduce time-to-market, and focus on creating value, while we manage the underlying infrastructure complexities.

Our integrated Service Desk stands as a pillar of support, ensuring uninterrupted service and immediate response to your needs. This proactive support model is geared towards maintaining operational excellence and enabling continuous improvement of applications in the cloud ecosystem.

Hosted exclusively in EU data centers, our service guarantees adherence to the stringent compliance and data sovereignty requirements that European businesses face. This localization also means that your data is processed with the highest security standards, aligning with GDPR and other regulatory frameworks.

The platform is engineered to foster innovation, providing a sandbox for experimentation, quick pivots, and embracing cutting-edge technologies. It is scalable to accommodate growth, elastic to manage fluctuating demands, and resilient to ensure uninterrupted service.

Security is a paramount concern, and our AWS PaaS embeds top-notch security measures at every layer. From network firewalls and encryption to IAM roles and policy enforcement, we ensure that your applications and data are protected against the most sophisticated threats.

By choosing Reply's AWS PaaS, businesses of all sizes can accelerate their digital transformation journey, benefiting from a service that is not only performance-optimized but also cost-effective and future-proof. Our commitment is to provide a platform that not only meets today's demands but also anticipates and adapts to the needs of tomorrow.

Use Multi-factor Authentication: Multi-factor authentication (MFA) significantly enhances the security of your platform by requiring users to provide two or more verification factors to gain access to resources. This additional layer of security minimizes the risk of unauthorized access, ensuring that sensitive data and applications are accessible only to authenticated users. MFA is crucial in protecting against various security threats, including phishing attacks, credential compromise, and unauthorized access attempts, thereby safeguarding your business's integrity and customer trust.

End-to-end Encryption: Implementing end-to-end encryption ensures that data is encrypted at its origin and decrypted only by the intended recipient, making it inaccessible to unauthorized entities during transmission or storage. This stringent security measure protects sensitive information from interception, breaches, and external threats, guaranteeing the confidentiality and integrity of your data. It's particularly beneficial for maintaining privacy, securing communication channels, and complying with stringent regulatory requirements.

Monitor Compliance Continuously with Automatic Security Updates: Continuous compliance monitoring combined with automatic security updates ensures that your system remains in line with industry standards and regulatory requirements. This proactive stance on security helps in identifying and rectifying vulnerabilities swiftly, maintaining the robustness of your defence mechanisms. Automatic updates reduce the window of exposure to new threats, keeping your infrastructure secure against emerging vulnerabilities and ensuring uninterrupted compliance.

Allocate Resources Dynamically for Optimized Performance and Cost: Dynamic resource allocation allows for the efficient utilization of cloud resources, adjusting capacity based on real-time demand. This not only optimizes performance, ensuring applications run smoothly without lag, but also reduces costs by avoiding over-provisioning. You pay only for the resources you use, enhancing operational efficiency and enabling a scalable, flexible approach to infrastructure management.

Automatically Scale to Meet Real-time Application Demands: Automatic scaling responds to changes in demand in real-time, providing the necessary resources to handle spikes in traffic seamlessly. This ensures consistent application performance, regardless of the number of requests, and maintains high availability without manual intervention. It's crucial for handling unpredictable workloads, improving user satisfaction, and maintaining service reliability.



Deploy Rapidly with Integrated CI/CD Tools: Integrated Continuous Integration and Continuous Deployment (CI/CD) tools streamline the development lifecycle, enabling rapid deployment of new features, updates, and fixes. This accelerates time-to-market, fosters innovation, and ensures that your application remains responsive to evolving business needs and customer feedback. It enhances collaboration, reduces deployment errors, and promotes a culture of continuous improvement.

Implement Blue-green Deployment to Minimize Downtime: Blue-green deployment is a strategy that reduces downtime and risk by running two identical production environments, only one of which is live at any given time. This allows you to deploy new versions to the inactive environment and thoroughly test them before making a switch. Such an approach ensures minimal disruption, facilitates easy rollbacks if issues arise, and enhances overall user experience by providing a seamless transition between old and new versions.

Choose Data Residency Options for EU Data Protection Laws: Data residency options enable you to choose where your data is stored, ensuring compliance with EU data protection laws and regulations. This feature is particularly beneficial for organizations needing to meet specific geographic or jurisdictional data storage requirements, offering greater control over data localization, sovereignty, and adherence to legal frameworks like GDPR.

Conduct Regular Data Audits for GDPR Compliance: Regular data audits are essential for maintaining GDPR compliance, providing a systematic review of how personal data is handled, stored, and processed. These audits help in identifying potential non-compliance areas, ensuring that data processing activities are transparent, secure, and in line with data protection principles, thereby safeguarding individual privacy rights and enhancing organizational accountability.

Monitor Application Performance in Real-time: Real-time monitoring of application performance offers immediate insights into the health and efficiency of your services. This enables swift identification and resolution of issues before they impact users, optimizing the end-user experience, and ensuring high availability and reliability of your applications. Continuous performance monitoring is key to proactive system management and maintaining operational excellence.

Access Customizable Dashboards for System Insights: Customizable dashboards provide a centralized, intuitive interface for monitoring your system's health and performance metrics. These dashboards can be tailored to meet specific monitoring needs, offering real-time visibility into system operations, aiding in quick decision-making, and enabling efficient management of cloud resources. They are instrumental in maintaining transparency, enhancing control, and driving strategic IT decisions.

Utilize Pre-configured Development Environments for Various Languages: Pre-configured development environments streamline the setup process for developers, providing them with ready-to-use, standardized environments for various programming languages. This reduces the time and effort involved in configuring development settings, accelerates the development process, and ensures consistency across development teams. It supports rapid application development and fosters an agile, efficient development culture.

Enable Easy Integration with API-driven Design: An API-driven design facilitates easy integration with external services and applications, enabling a more flexible, modular approach to software development. This design principle allows for the seamless extension and enhancement of your platform's capabilities, encouraging innovation, and ensuring that your service can adapt quickly to new business requirements or technological advancements.



HOSTING INFRASTRUCTURE

Our AWS PaaS solution is hosted on the world-renowned Amazon Web Services (AWS) cloud infrastructure, known for its reliability, scalability, and comprehensive security. This hosting setup provides a resilient environment for deploying, managing, and scaling applications with ease and efficiency. Here are the key aspects and options of our hosting infrastructure:

Cloud-Based Hosting on AWS: The core of our hosting infrastructure utilizes AWS's cloud services, ensuring high availability, fault tolerance, and global reach. This enables your applications to leverage the full spectrum of AWS capabilities, including compute, storage, and database services, all optimized for high performance and reliability.

Scalability Options: Our solution is inherently scalable, designed to adjust resource allocation dynamically in response to changing demand. This ensures optimal performance and cost-efficiency, with the ability to scale up or down automatically without requiring manual intervention.

Multi-Region Deployment: We offer the flexibility to deploy your applications in multiple AWS regions across the globe. This not only enhances application performance by reducing latency but also increases resilience through geographical diversification, ensuring your services remain uninterrupted and accessible even in the face of regional disruptions.

Compliance and Data Residency: Recognizing the importance of compliance and data sovereignty, our hosting solution provides options to choose data centers located in specific regions to comply with local regulations and data residency requirements, such as GDPR in Europe. This ensures that your data is stored and processed in accordance with the legal requirements of your chosen jurisdiction.

Security-First Architecture: Our infrastructure is designed with a security-first approach, incorporating multiple layers of security measures, including network firewalls, encryption, access controls, and continuous monitoring, to protect your data and applications from threats and vulnerabilities.

Environment Customization: We understand that each business has unique requirements. Therefore, we provide customizable hosting environments that can be tailored to meet your specific operational needs, whether you require a dedicated environment, a shared one, or a hybrid setup.

Backup and Disaster Recovery: Ensuring business continuity, our hosting infrastructure includes robust backup solutions and disaster recovery strategies. This minimizes data loss and downtime, providing peace of mind that your critical applications and data are safeguarded against unexpected incidents.

Integrated Development and Deployment Tools: Our platform supports integrated development and operational tools, facilitating continuous integration and continuous deployment (CI/CD) practices. This enables streamlined workflows for code deployment, automated testing, and efficient release management, enhancing the agility and responsiveness of your development teams.

Disaster Recovery

Our AWS PaaS includes a comprehensive disaster recovery (DR) strategy, centred on minimizing data loss and downtime while maximizing reliability and operational continuity. The key provisions of our disaster recovery strategy include:

Highly Available Architecture: Our service is built on a highly available infrastructure that spans multiple AWS Availability Zones (AZs) within a region. This design ensures that, in the event of an AZ failure, the system can automatically failover to the remaining operational AZs, thereby maintaining service availability and access.

Data Replication: We implement real-time data replication across geographically dispersed AWS regions and AZs. This ensures that your data is consistently backed up and can be quickly restored to the most recent state in case of a disaster, reducing the risk of data loss.

Automated Backups: Regular, automated backups of your data and applications are a cornerstone of our DR strategy. These backups are encrypted and stored in multiple secure locations, ensuring they can be rapidly retrieved and restored to reinstate your application environment promptly.

Rapid Recovery: Our DR plan is designed for rapid recovery, with clearly defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that align with the criticality of your applications.



This ensures that key systems can be quickly restored to full functionality with minimal data loss, adhering to the business's continuity requirements.

Failover and Failback Procedures: We have established failover procedures to switch operations to a secondary environment without human intervention automatically. Our failback procedures are equally robust, ensuring a smooth transition back to the primary environment after the resolution of the disaster scenario.

Testing and Documentation: Regular DR testing is conducted to ensure our recovery procedures are effective and can be executed as planned. Comprehensive documentation is maintained, detailing the DR strategy, procedures, roles, and responsibilities, ensuring clarity and preparedness among all stakeholders.

Compliance and Standards: Our DR provisions are in strict compliance with industry standards and best practices, ensuring alignment with regulatory requirements and business expectations. This compliance is regularly reviewed and updated to reflect the evolving landscape of threats and technological advancements.

Customizable DR Options: Recognizing that different applications may have varying levels of criticality, we offer customizable DR solutions tailored to the specific needs and risk profiles of your business, allowing you to optimize your investment in DR resources.

Continuous Monitoring and Improvement: Our infrastructure is continuously monitored, and the DR strategy is regularly reviewed and updated to incorporate improvements, adapt to new threats, and reflect changes in the business or technological environment.



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