REPLY

MANAGED CLOUD INTEGRATION 24X7 SUPPORT

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
infouk@reply.com

www.reply.com

TABLE of CONTENTS

SERVICE DESCRIPTION

Many public sector organisations rely on complex integration platforms to keep critical services running, yet support for these platforms is often reactive, fragmented and limited to office hours. Issues are detected late, incidents take too long to resolve, and responsibility is split across suppliers, creating avoidable downtime, operational risk and pressure on internal teams. As integration estates grow, the lack of consistent monitoring, clear ownership and proactive optimisation becomes a major threat to service reliability.

Reply's Managed Cloud Integration & 24×7 Support Services for G-Cloud 15 address this challenge by providing fully managed, round-the-clock support for mission-critical integration platforms. We take responsibility for monitoring, incident management, optimisation and continuous improvement, ensuring integrations remain available, secure and performant at all times.

Our service combines 24×7 monitoring, SLA-backed support and proactive operational management to move organisations away from fire-fighting towards stable, predictable service operation. We detect issues early, resolve incidents quickly and systematically improve platform health, reducing disruption to citizens, staff and dependent services.

Crucially, we focus not just on keeping systems running, but on strengthening them over time. Through root-cause analysis, optimisation and knowledge transfer, we help organisations build more resilient integration services while reducing operational burden on internal teams.

FEATURES
Our managed service combines continuous monitoring, proactive incident management, AI-assisted alerting and disciplined service management to provide reliable, accountable integration support at scale.

- **24×7 Monitoring of Integration Platforms**
  We provide continuous, round-the-clock monitoring of integration platforms, interfaces and critical message flows. This includes tracking availability, throughput, latency, error rates and platform health indicators across cloud, hybrid and legacy environments.

  Monitoring is designed around service outcomes, not just infrastructure metrics, ensuring issues are identified before they impact dependent systems or end users.

- **Proactive Incident Management and Resolution**
  Incidents are actively managed by experienced integration specialists using defined runbooks, prioritisation models and escalation paths. We take ownership of triage, diagnosis and resolution, coordinating across suppliers and internal teams where necessary.

  This proactive approach minimises time to resolution and avoids the delays and confusion that arise when responsibility is unclear or fragmented.

- **SLA-Backed Support and Service Management**
  Services are delivered against clearly defined SLAs covering response times, resolution times and service availability. Performance is tracked and reported transparently, providing operational assurance and commercial accountability.

  This ensures support is predictable, measurable and aligned with the criticality of public sector services.

- **Integration Platform Health and Performance Monitoring**
  Beyond basic availability, we continuously assess platform capacity, resource utilisation and performance trends. This allows us to anticipate stress points and degradation before they become incidents.

  Health monitoring supports informed operational decisions, such as capacity scaling, configuration changes or targeted optimisation activities.

- **AI-Assisted Alerting and Anomaly Detection**
  Where appropriate, AI-assisted techniques are used to identify abnormal patterns, unexpected behaviour or emerging risks across integration platforms. This complements traditional rule-based alerts and helps surface issues that may otherwise go unnoticed.

  Earlier detection enables faster investigation and resolution, particularly in complex, high-volume environments.

- **Integration Optimisation and Performance Tuning**
  We regularly review integration flows, configurations and platform settings to improve performance, reliability and efficiency. This includes tuning message handling, retry strategies, resource allocation and integration patterns as usage evolves.

  Optimisation ensures platforms continue to perform effectively as demand grows or service usage changes.

- **Release, Patching and Upgrade Management**
  We manage releases, patches and upgrades in a controlled and auditable manner, aligned with change management processes. This reduces the risk associated with platform change while ensuring systems remain supported, secure and up to date.

  Changes are planned to minimise service disruption and are validated through appropriate testing before deployment.

- **Security Monitoring and Compliance Support**
  Integration platforms are monitored for security-related events, misconfigurations and potential vulnerabilities. We support compliance with public sector security expectations by maintaining visibility, auditability and evidence across live services.

  This reduces exposure to security risks and supports assurance and governance activities.

- **Root-Cause Analysis and Operational Reporting**
  Following incidents, we perform structured root-cause analysis to understand underlying causes rather than treating symptoms. Findings are documented and used to implement corrective actions that prevent recurrence.

  Regular reporting provides insight into trends, risks and improvement opportunities across the integration estate.

- **Knowledge Transfer and Documentation Updates**

Operational knowledge, runbooks and documentation are kept up to date and shared with client teams as appropriate. This reduces dependency on individuals, improves resilience and supports continuity of service.

BENEFITS

Our Managed Cloud Integration & 24×7 Support Services deliver both immediate operational assurance and long-term improvement in how integration platforms are managed.

- **Improved Availability of Critical Systems**
  Continuous monitoring and rapid response reduce unplanned outages and protect the availability of services that underpin public sector operations.

- **Reduced Service Disruption and Downtime**
  Proactive issue detection and disciplined incident management prevent minor issues escalating into major disruptions.

- **Predictable and Accountable Service Delivery**
  Clear SLAs, reporting and ownership provide confidence that support performance is understood, measured and managed.

- **Early Detection of Potential Failures**
  Health monitoring and trend analysis surface risks early, enabling preventative action rather than reactive firefighting.

- **Faster Issue Identification and Resolution**
  AI-assisted alerting and experienced integration specialists reduce time spent diagnosing issues and restoring service.

- **Improved Efficiency and Response Times**
  Ongoing optimisation ensures integration platforms continue to perform efficiently as usage patterns evolve.

- **Reduced Risk for Critical Government Services**
  Controlled patching, upgrades and change management lower the likelihood of change-related incidents.

- **Improved Security Posture and Compliance**
  Continuous security monitoring and audit support help organisations meet governance and regulatory expectations.

- **Continuous Improvement Through Insight**
  Root-cause analysis and performance reporting drive learning and improvement over time.

- **Increased Resilience of Integration Services**
  Documentation and knowledge transfer reduce reliance on individual suppliers or staff and strengthen long-term resilience.

WHAT THE SERVICE INCLUDES

Reply provides a structured, end-to-end managed service for cloud integration platforms, designed to ensure operational stability, predictable performance and continuous improvement. The service combines technical operations with consulting-led service management, ensuring platforms remain reliable today while becoming more resilient over time.

Our managed service is delivered as a continuous lifecycle, rather than a set of disconnected operational tasks.

1. **Service Onboarding and Transition**
   - We begin with a structured transition into live support, ensuring continuity and reducing risk from day one. This includes understanding existing architectures, integrations, operating procedures, known risks and service dependencies.
   - During onboarding, we:
   - Review current integration platforms, interfaces and data flows
   - Validate monitoring, alerting and incident processes
   - Establish clear service ownership, escalation paths and SLAs
   - Capture and refine operational documentation and runbooks
   - This approach ensures a controlled transition into 24×7 support without disrupting live services.

2. **Continuous Monitoring and Observability**
   - We provide round-the-clock monitoring of integration platforms, interfaces and critical message flows across cloud, hybrid and legacy environments. Monitoring is configured to provide insight into service health, performance and capacity, not just infrastructure availability.
   - This includes:
   - Platform and integration availability
   - Message throughput, latency and error rates
   - Capacity and performance trends
   - Early warning indicators of degradation or failure
   - The objective is early visibility, enabling issues to be addressed before users or dependent services are affected.

3. **Incident Management and Service Restoration**
   - When incidents occur, we take ownership of managing them end-to-end. Issues are triaged, prioritised and resolved by experienced integration specialists using defined processes and escalation paths.
   - Our incident management approach focuses on:
   - Rapid identification and containment of issues
   - Clear communication to stakeholders during incidents
   - Coordinated resolution across internal teams and third-party suppliers
   - Timely restoration of normal service
   - This reduces uncertainty, shortens outages and avoids the delays that often arise when responsibility is unclear.

4. **Root-Cause Analysis and Problem Management**
   - Following service incidents, we carry out structured root-cause analysis to understand underlying issues rather than applying temporary fixes. Findings are documented and translated into corrective actions.

- Problem management activities include:
- Analysis of recurring incidents and systemic issues
- Implementation of permanent fixes and preventative measures
- Tracking of actions to completion
- Reporting on trends and lessons learned
- This ensures service stability improves over time rather than deteriorating through repeated firefighting.

5. Performance, Capacity and Platform Optimisation

- We continuously assess integration platform performance and capacity to ensure services remain efficient and responsive as demand changes. Optimisation activities are planned and prioritised based on evidence rather than assumptions.
- This includes:
- Performance tuning of integrations and message flows
- Capacity planning and scaling recommendations
- Optimisation of configurations and platform usage
- Optimisation reduces operational overhead, improves responsiveness and supports growing service demand.

6. Release, Change and Environment Management

- We manage integration releases, patches and upgrades in a controlled and auditable manner, aligned with change management processes. This ensures platforms remain secure and supported without introducing unnecessary risk.
- Activities include:
- Planning and coordinating releases and upgrades
- Managing patching and platform updates
- Supporting testing and validation activities
- Minimising disruption to live services
- This disciplined approach reduces the risk of change-related incidents.

7. Security Monitoring and Compliance Support

- Security is managed as an ongoing operational concern rather than a one-off exercise. We monitor integration platforms for security events, configuration issues and policy deviations.
- Our service supports:
- Ongoing security monitoring
- Identification and remediation of configuration risks
- Evidence collection for audit and assurance
- Alignment with public sector security expectations
- This helps maintain a strong security posture throughout live operation.

8. Service Reporting and Governance

- We provide regular service reporting to support transparency, governance and continuous improvement. Reports focus on service performance, incidents, risks and improvement actions rather than raw technical metrics.
- Governance activities include:
- SLA and service performance reporting
- Incident and problem trend analysis
- Risk and improvement tracking

- Service review meetings with stakeholders
- This enables informed decision-making and effective oversight.

9. Knowledge Management and Continuous Improvement

- Operational knowledge is actively maintained and shared. Documentation, runbooks and support materials are updated as platforms evolve, reducing reliance on individuals and improving resilience.
- Continuous improvement is driven through:
- Lessons learned from incidents and changes
- Identification of recurring inefficiencies or risks
- Incremental automation and optimisation
- Knowledge transfer to internal teams where required
- Over time, this creates a more stable, well-understood and self-sustaining integration service.

Why This Matters

Together, these service components provide consistent, reliable and well-governed support for integration platforms that underpin critical public services. Organisations gain confidence that integrations are monitored, supported and improved proactively, reducing operational risk and allowing teams to focus on delivering better services rather than managing incidents.

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