

SUPPLIER, PARTNER, ECOSYETM INTEGRATION WITH AI

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	9
KICK-OFF MEETING	9
ACCOUNT MANAGEMENT	9
<i>DESIGNATED ACCOUNT MANAGER</i>	9
<i>FORTNIGHTLY REVIEW MEETING</i>	9
OFFBOARDING	9
ACCESS TO DATA	9
SECURITY	10
PERSONNEL SECURITY	10
INFORMATION SECURITY	10
PHYSICAL SECURITY	10
TRAINING & KNOWLEDGE TRANSFER	11
ORDERING AND INVOICING PROCESS	12
CUSTOMER RESPONSIBILITIES	13
TECHNICAL AND CLIENT-SIDE REQUIREMENTS	13
OUTCOMES AND DELIVERABLES	13
ABOUT REPLY	14



SERVICE DESCRIPTION

Public sector organisations increasingly operate within complex delivery ecosystems involving multiple suppliers, delivery partners, arms-length bodies and external data providers. While these partnerships are essential to service delivery, integration across organisational boundaries is often fragile, inconsistent and difficult to govern. Point-to-point integrations, bespoke data exchanges and manual coordination create operational risk, slow onboarding of new partners and limit visibility across the wider ecosystem.

Reply's Supplier, Partner & Ecosystem Integration with AI service for G-Cloud 15 addresses these challenges by designing and delivering secure, standardised and scalable integration foundations that support collaboration across multiple organisations. We enable data and process exchange through well-governed APIs and event-driven architectures, reducing complexity while maintaining strong control over access, security and compliance.

Our service is enhanced with AI-assisted monitoring and analysis to provide operational insight across partner integrations. This enables early detection of exceptions, performance issues and emerging risks, supporting proactive management rather than reactive escalation. Integration becomes a managed, observable capability rather than a collection of fragile interfaces.

Crucially, we recognise that partner integration is as much about governance, accountability and operating models as technology. Our approach supports faster onboarding, clearer ownership and improved transparency across supplier ecosystems, enabling organisations to collaborate effectively while protecting public services, data and trust.

FEATURES

Our service combines secure integration design, ecosystem governance and AI-enabled operational intelligence to support collaboration at scale.

- **Secure Supplier and Partner Integration Design**

We design integrations that securely connect organisational boundaries, ensuring data and processes are exchanged safely between internal systems and external partners. Security controls are embedded by design, including identity, access management and data protection.

This enables collaboration without exposing internal systems to unmanaged risk.

- **API and Data Exchange Standardisation**

We define and implement standardised APIs, data contracts and event formats for partner interactions. Standardisation reduces bespoke development, improves consistency and simplifies onboarding of new suppliers or partners.

This creates a shared integration language across the ecosystem.

- **AI-Assisted Exception Detection**

AI-assisted analysis is used to identify unusual patterns, failures or delays across partner integrations. This includes detecting data anomalies, message backlogs or deviations from expected behaviour.

Early detection reduces operational overhead and prevents small issues escalating into major incidents.

- **Event-Driven Partner Integration Models**



We design event-driven architectures that enable real-time data and process exchange across organisational boundaries. Partners can publish and consume events without tight coupling, supporting timely coordination and responsiveness.

This improves visibility and reduces reliance on batch or manual processes.

- **Governance and Access Controls**

We implement governance frameworks that define how partners access services, data and APIs. Controls include role-based access, policy enforcement and lifecycle management.

Governance provides clarity while enabling agility.

- **Performance Monitoring and Reporting**

We enable monitoring and reporting across partner integrations to track availability, performance and usage. This provides visibility into how suppliers and partners are interacting with systems and where risks or inefficiencies lie.

Insight supports informed supplier and contract management.

- **Integration Onboarding Frameworks**

We establish repeatable onboarding frameworks covering technical standards, security requirements and operational expectations. New partners can be onboarded quickly without re-inventing integration approaches.

This accelerates delivery while maintaining consistency.

- **Audit and Compliance Support**

Integration interactions are logged and auditable, providing evidence for assurance, audit and regulatory review. This is particularly important in multi-organisation environments where accountability must be clear.

- **Scalable Multi-Party Architectures**

Architectures are designed to scale as the ecosystem grows, enabling additional partners to be integrated without redesign. This supports future delivery models and shared services.

- **Knowledge Transfer and Documentation**

We provide clear documentation and knowledge transfer to internal teams and partners, reducing dependency on individuals and improving long-term sustainability.

BENEFITS

Our Supplier, Partner & Ecosystem Integration with AI service enables public sector organisations to collaborate effectively across complex delivery ecosystems **without losing control, security or accountability**. The benefits focus on improving **operational confidence, agility and transparency** in multi-organisation environments.

- **Stronger Collaboration Across Organisational Boundaries**



Well-designed, standardised integrations allow suppliers and partners to exchange data and processes reliably and predictably. This removes friction caused by bespoke interfaces, manual hand-offs and unclear responsibilities.

As a result, collaboration improves across delivery chains, enabling services to be delivered more smoothly even when responsibility spans multiple organisations.

- **Reduced Integration Complexity and Technical Debt**

Standard APIs, data contracts and event models replace one-off, point-to-point integrations. This reduces structural complexity and prevents ecosystems from becoming increasingly brittle as new partners are added.

Over time, this significantly lowers maintenance effort, rework and the accumulation of technical debt.

- **Lower Cost and Effort Managing Partner Integrations**

AI-assisted monitoring and exception detection reduce the operational overhead required to manage integrations across multiple organisations. Issues are identified early and prioritised intelligently, reducing manual investigation and reactive firefighting.

Operational teams spend less time resolving avoidable incidents and more time improving services.

- **Real-Time Visibility Into Ecosystem Health**

Event-driven integration and AI-enhanced monitoring provide real-time insight into data flows, service interactions and partner performance. Organisations can see how the ecosystem is behaving as a whole, rather than relying on fragmented reports from individual suppliers.

This visibility supports faster, more informed decision-making.

- **Increased Agility When Onboarding or Changing Partners**

Clear integration standards and onboarding frameworks enable new suppliers or partners to be integrated more quickly and consistently. Changes to suppliers can be managed without large-scale redesign or disruption.

This agility supports competitive procurement, innovation and evolving delivery models.

- **Improved Supplier Performance Management**

Operational metrics, trend analysis and AI-assisted insight provide evidence-based understanding of how suppliers and partners interact with systems. This supports more constructive performance conversations grounded in data rather than anecdote.

Supplier management becomes proactive rather than reactive.

- **Clearer Accountability Across Multi-Party Services**

Audit logging and traceability provide transparency into who exchanged what data, when and under which controls. This clarity supports governance, accountability and dispute resolution in complex delivery environments.



Accountability is retained even when services span multiple organisations.

- **Reduced Risk to Public Services and Data**

Strong governance, access controls and security-by-design integration reduce the risk of data leakage, unauthorised access or uncontrolled changes introduced via partners.

Public services remain protected as collaboration increases.

- **Scalable, Future-Proof Ecosystem Foundations**

Architectures designed for multi-party interaction allow ecosystems to grow without repeated re-engineering. New services, partners and data exchanges can be added predictably.

This future-proofs integration foundations against policy, organisational and supplier change.

- **Reduced Reliance on Individual or Supplier-Specific Knowledge**

Documentation, standards and knowledge transfer reduce dependency on informal or supplier-specific expertise. Internal teams gain confidence in how integrations work and how partners interact.

This improves resilience and continuity over time.

WHAT THE SERVICE INCLUDES

Reply delivers a comprehensive, end-to-end service that treats supplier and partner integration as a **strategic ecosystem capability**, not a set of one-off technical connections.

The service is designed to scale, adapt and endure across changing delivery models.

1. Ecosystem Discovery and Integration Landscape Assessment

We begin by building a detailed understanding of the delivery ecosystem and its integration challenges. This includes:

- Identification of suppliers, partners and third parties
- Mapping of data, process and service dependencies
- Review of existing integration approaches and pain points
- Understanding contractual, governance and risk constraints

This ensures integration design reflects real organisational complexity.

2. Partner Integration Strategy and Operating Model

We define a clear integration strategy that sets out how the organisation will collaborate with partners in a controlled, consistent way.

This includes:

- Definition of integration principles and standards
- Partner roles and responsibilities
- Ownership and accountability models
- Alignment with enterprise and integration architecture

3. Secure, Standardised Integration Design

We design secure APIs, data exchange mechanisms and event-driven patterns that enable consistent interaction with partners.

Design covers:



- API exposure and consumption patterns
- Data contracts and schemas
- Identity, authentication and authorisation
- Failure handling and resilience

Security and scalability are embedded by design.

4. Governance and Access Control Frameworks

We establish governance frameworks defining how partners access systems and data, how integrations evolve and how changes are approved.

This includes:

- Role-based and policy-driven access controls
- API lifecycle and version management
- Change and approval processes
- Compliance and assurance alignment

Governance supports collaboration without unnecessary bureaucracy.

5. AI-Enhanced Monitoring and Exception Detection

We implement AI-assisted monitoring across partner integrations to surface anomalies, failures and performance issues early.

This includes:

- Detection of unusual patterns or delays
- Identification of repeated integration failures
- Context-aware alerting and prioritisation

AI enhances visibility while reducing manual effort.

6. Event-Driven Ecosystem Enablement

Where appropriate, we introduce event-driven patterns enabling partners to publish and subscribe to events safely.

This supports:

- Near real-time collaboration
- Looser coupling between organisations
- Improved responsiveness to change

7. Partner Onboarding Framework Implementation

We design and implement repeatable onboarding frameworks to enable faster, safer partner integration.

This includes:

- Technical onboarding guides and templates
- Security and assurance requirements
- Testing and validation processes
- Operational readiness checks

New partners can be enabled without reinventing approaches.

8. Performance Monitoring and Reporting

We enable dashboards and reports that show how partner integrations are performing over time.

Reporting supports:

- Supplier performance management
- Operational oversight
- Risk and trend identification

9. Audit, Compliance and Assurance Support



Integration activity is logged and retained to support audit, regulatory review and assurance processes. This provides:

- Clear traceability across organisational boundaries
- Evidence of control and compliance
- Support for investigations or reviews

10. Documentation and Knowledge Transfer

We produce and maintain integration standards, documentation and runbooks, and transfer knowledge to internal teams.

This reduces reliance on suppliers and improves long-term sustainability.

11. Continuous Improvement and Ecosystem Evolution

We support ongoing optimisation of integration patterns, governance and monitoring as the ecosystem evolves.

Integration capability matures rather than degrading over time.

WHY THIS MATTERS

Together, these service components replace fragile, bespoke partner integrations with a governed, scalable and observable ecosystem capability. Organisations gain confidence that collaboration with suppliers and partners improves delivery rather than increasing risk, enabling more agile, transparent and resilient public services across complex multi-organisation environments.



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