

AI-ASSISTED INTEGRATION ASSURANCE & DESIGN AUTHORITY

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 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

Large public sector digital programmes increasingly rely on complex integration architectures spanning cloud platforms, legacy systems, APIs and, more recently, AI and agentic AI components. These environments evolve quickly, often under delivery pressure, making it difficult to maintain architectural coherence, security and compliance over time. Without independent challenge and assurance, integration design decisions can drift, technical debt can accumulate and risks may only surface once services are live.

Reply's AI-Assisted Integration Assurance & Design Authority service for G-Cloud 15 provides independent, expert oversight of integration architecture, design and delivery. We combine experienced integration architects with AI-assisted analysis to review designs, patterns and delivery approaches, identifying risk early and supporting consistent, high-quality decision-making across programmes.

Our service acts as an independent design authority, ensuring integration solutions remain aligned with GDS standards, security expectations and architectural best practice. We review traditional integration approaches alongside AI and agentic AI designs, helping organisations adopt innovation safely without undermining reliability, compliance or assurance.

Crucially, our assurance approach is collaborative rather than obstructive. We focus on enabling delivery teams to move faster with confidence, improving quality and reducing rework through early, evidence-based feedback rather than late-stage remediation.

FEATURES

Our service combines independent design authority, deep integration expertise and AI-assisted analysis to provide proportionate, effective assurance across complex delivery environments.

- **AI-Assisted Review of Integration Architectures**

We use AI-assisted techniques alongside expert review to analyse integration architectures, diagrams and design artefacts. This supports rapid identification of structural weaknesses, anti-patterns, dependency risks and inconsistencies that may be difficult to spot manually across large estates.

AI augments, rather than replaces, expert judgement by enabling broader and faster coverage of complex architecture landscapes.

- **Design Authority and Assurance Services**

We operate as an independent integration design authority, providing clear guidance, challenge and approval where required. This ensures architectural decisions are made consistently across teams and suppliers, reducing fragmentation and conflicting approaches.

Design authority services bring coherence and continuity to long-running programmes.

- **Review of AI and Agentic AI Designs**

We assess AI and agentic AI integration designs to ensure they align with enterprise integration architectures, security models and governance expectations. This includes reviewing how AI components access data, invoke actions and interact with workflows.

This reduces the risk of AI solutions bypassing established controls or introducing opaque behaviour.

- **Compliance Assessment Against GDS Standards**



We review integration designs against GDS Service Standard and relevant public sector architectural and delivery guidance. This ensures solutions are defensible during assurance, spend control and audit processes.

Compliance is assessed pragmatically, focusing on intent and outcomes rather than rigid interpretation.

- **Integration Pattern and Design Validation**

We validate integration patterns, ensuring appropriate use of APIs, messaging, event-driven approaches and data flows. This helps avoid brittle point-to-point connections and improves long-term maintainability.

Pattern validation supports reuse and architectural consistency.

- **Security and Resilience Assessment**

We review integration security, resilience and failure handling, including identity, access control, data protection and recovery mechanisms. This ensures integrations remain robust under failure scenarios and meet public sector security expectations.

Security and resilience are assessed as architectural qualities, not bolt-on features.

- **Independent Delivery Quality Checks**

We provide independent checks on delivery quality, reviewing whether implemented integrations align with agreed designs and standards. This identifies drift between architecture intent and delivery reality early.

Independent quality checks increase confidence for programme leadership and SROs.

- **Architecture Decision Documentation Support**

We support documentation of key architectural decisions, including rationale, trade-offs and risks. This creates a clear audit trail that supports assurance, future change and organisational learning.

- **Continuous Assurance During Delivery**

Rather than a one-off review, we provide continuous assurance throughout delivery phases. This allows issues to be identified and addressed early as designs evolve.

Continuous assurance reduces late-stage rework and delivery risk.

- **Knowledge Sharing and Recommendations**

We actively share insights, lessons learned and recommendations with delivery teams, helping improve capability and decision-making over time.

BENEFITS

Our AI-Assisted Integration Assurance & Design Authority service enables organisations to deliver complex integration and AI-enabled programmes with confidence, consistency and control. The benefits extend beyond technical quality to improved governance, stronger assurance outcomes and reduced delivery risk at scale.



- **Early Identification and Reduction of Architectural Risk**

Complex integration estates accumulate risk quickly, particularly when multiple teams, suppliers and technologies are involved. By reviewing integration and AI designs early and repeatedly, this service identifies structural weaknesses, inappropriate patterns and hidden dependencies before they become embedded.

Early identification enables corrective action at a point where change is cheaper, faster and less disruptive, significantly reducing long-term technical debt and delivery risk.

- **Consistent and Defensible Architectural Decision-Making**

In large programmes, inconsistent architectural decisions are a common cause of fragmentation and rework. Acting as an independent design authority ensures decisions are made using consistent principles, evidence and standards rather than local preference or supplier bias.

This consistency strengthens architectural coherence and provides a defensible basis for decisions during assurance reviews, audits and senior governance forums.

- **Safer Adoption of AI and Agentic AI**

AI and agentic AI introduce new risks around access, autonomy, explainability and governance. Independent review ensures AI designs are aligned with enterprise integration architecture, security controls and operating models, rather than bypassing them.

This enables innovation to proceed without exposing organisations to unmanaged security, compliance or reputational risk.

- **Improved Governance and Assurance Outcomes**

Integration and architecture decisions are often scrutinised through spend controls, portfolio reviews and audits. Clear evidence of independent assurance, alignment with GDS standards and documented decision-making improves confidence among reviewers and approving authorities.

This reduces friction at governance gates and avoids late-stage rework driven by assurance concerns.

- **Higher Quality, More Maintainable Integration Solutions**

Validation of integration patterns and designs improves solution quality by encouraging reuse, discouraging brittle point-to-point connections and promoting scalable, well-understood approaches.

Over time, this improves maintainability, reduces operational incidents and lowers the cost of change.

- **Improved Security and Service Resilience**

Security and resilience are assessed as core architectural qualities rather than technical afterthoughts. This reduces the likelihood of outages, data exposure or service degradation caused by poorly designed integrations or insufficient failure handling.

Organisations gain more robust, predictable services as a result.



- **Increased Confidence for Programme Leaders and SROs**

Independent assurance provides senior leaders with confidence that integration and AI risks are understood, visible and actively managed. This is particularly valuable where programmes are complex, politically sensitive or high-profile.

Confidence is grounded in evidence rather than assumption.

- **Clear and Auditable Architecture Decision Trail**

Well-documented architecture decisions provide a clear audit trail explaining why specific approaches were chosen, what alternatives were considered and what risks were accepted.

This supports future change, regulatory scrutiny and organisational learning.

- **Early Detection of Design Drift During Delivery**

Continuous assurance identifies divergence between agreed architecture and what is actually being built. This allows issues to be addressed before they reach production rather than being discovered during late testing or live operation.

- **Better-Managed Digital and AI-Enabled Programmes**

Through challenge, guidance and knowledge sharing, the service raises architectural maturity across delivery teams. Programmes benefit from clearer direction, reduced rework and improved outcomes over time.

WHAT THE SERVICE INCLUDES

Reply delivers a comprehensive, end-to-end assurance and design authority service covering integration, cloud and AI-enabled delivery. The service is designed to strengthen delivery rather than slow it down, providing proportionate, evidence-based assurance throughout the lifecycle.

1. Programme Context Understanding and Assurance Scoping

We begin by understanding the programme context, delivery pressures and risk profile. Assurance is tailored to the complexity, scale and criticality of the programme rather than applied as a generic checklist. This includes:

- Understanding programme objectives and constraints
- Identifying critical integrations and AI components
- Agreeing assurance scope, depth and cadence
- Defining escalation and decision-making routes

This ensures assurance effort is focused where it adds most value.

2. Target, Transition and Solution Architecture Review

We review architectural artefacts at key stages, including target architectures, transition states and solution designs. Reviews consider alignment with enterprise strategy, integration principles and delivery constraints.

Activities include:

- Assessment of architectural coherence and layering
- Review of integration approaches and dependencies
- Identification of architectural trade-offs and risks
- Practical recommendations for improvement

3. AI-Assisted Architecture and Integration Analysis



We apply AI-assisted techniques to analyse architecture artefacts, integration inventories and design documentation. This supports faster identification of complexity hotspots, duplication and failure risks across large estates.

AI augments human expertise by improving coverage and consistency, not replacing expert judgement.

4. Review of AI and Agentic AI Designs

We assess AI and agentic AI designs to ensure they integrate safely into enterprise architecture. Reviews cover how AI components access data, invoke actions, interact with workflows and are governed.

This includes:

- Alignment with integration and identity patterns
- Review of autonomy and control mechanisms
- Assessment of auditability and explainability
- Identification of AI-specific architectural risks

5. Security, Resilience and Compliance Assessment

We evaluate security and resilience at an architectural level, ensuring integrations meet public sector expectations for confidentiality, integrity and availability.

This includes:

- Identity and access control design
- Data protection and encryption approaches
- Failure handling and recovery mechanisms
- Alignment with GDS and security standards

6. Design Authority Operation and Decision Support

We support or operate design authority forums, providing independent challenge, guidance and recommendations. Where required, we help structure decision processes and criteria to improve clarity and consistency.

7. Continuous Assurance During Delivery

Rather than one-off reviews, we provide ongoing assurance aligned with delivery milestones. This enables early detection of emerging risks and supports course correction as designs evolve.

8. Architecture Decision Record (ADR) Development

We support the creation and maintenance of clear Architecture Decision Records, capturing rationale, assumptions and implications.

This ensures decisions remain understandable long after teams or suppliers change.

9. Risk Reporting and Actionable Recommendations

We provide clear, prioritised findings and recommendations written for delivery leaders rather than architects alone. Reports focus on practical action rather than abstract critique.

10. Knowledge Sharing and Capability Uplift

We actively share lessons learned, patterns and good practice with delivery teams, improving architectural maturity and reducing reliance on future assurance intervention.

WHY THIS MATTERS:

Together, these service components provide proportionate, independent assurance that improves delivery quality without introducing bureaucracy. Organisations gain confidence that integration and AI-enabled solutions are well designed, secure and aligned with public sector standards, enabling faster, safer digital transformation while protecting public services and trust.





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