

AI-DRIVEN LEGACY MODERNISATION & INTEGRATION SERVICES

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

Many public sector organisations depend on legacy systems that are critical to day-to-day service delivery but difficult to change. These platforms often lack modern integration capabilities, rely on undocumented logic and present significant risk when touched. Attempts to replace them wholesale frequently fail or introduce unacceptable service disruption, leaving organisations trapped between the need to modernise and the fear of breaking essential services.

Reply's AI-Driven Legacy Modernisation & Integration Services for G-Cloud 15 address this challenge through an integration-led, incremental approach to modernisation. We use AI-assisted analysis, automation and modern integration patterns to safely expose legacy systems via APIs and events, enabling gradual change without disrupting live services.

Our approach avoids high-risk “big bang” replacement programmes. Instead, we help organisations understand legacy behaviour, dependencies and risks, then modernise step-by-step while maintaining continuity of service. AI is applied pragmatically to accelerate analysis and improve confidence in change, not to replace engineering judgement.

Crucially, we treat legacy modernisation as a long-term transformation rather than a one-off technical exercise. By enabling coexistence between old and new systems, we create a controlled pathway to modern platforms that supports policy change, digital service improvement and future innovation.

FEATURES

Our service combines legacy integration expertise, AI-assisted analysis and public-sector delivery experience to modernise critical systems safely and sustainably.

- **Legacy System Assessment and Integration Strategy**
We conduct a detailed assessment of legacy systems, focusing on business criticality, technical constraints, dependencies and integration options. This forms the basis for a pragmatic integration and modernisation strategy that reflects operational reality rather than theoretical target states.
- **API Enablement for Legacy Platforms**
We design and implement APIs that safely expose legacy functionality and data without invasive change. These APIs provide controlled access to legacy systems, enabling reuse by modern services and reducing reliance on brittle point-to-point connections.
- **AI-Assisted Dependency and Impact Analysis**
We use AI-assisted techniques to analyse codebases, data flows and interface usage to identify hidden dependencies, usage patterns and potential impact areas. This improves visibility and reduces the risk of unintended consequences when making changes.

AI augments human expertise by accelerating analysis across large, poorly documented estates.

- **Event-Driven Integration for Legacy Environments**
Where appropriate, we introduce event-driven patterns to legacy environments, enabling systems to publish and consume events without tight coupling. This allows legacy platforms to participate in modern, responsive architectures without wholesale replacement.
- **Incremental Modernisation Approaches**



We support incremental modernisation techniques such as strangler patterns, façade layers and selective refactoring. These approaches reduce risk by allowing change to be introduced gradually while legacy systems continue to operate.

- **Data Extraction and Integration Support**

We enable secure, reliable extraction and integration of data from legacy platforms into modern data and analytics environments. This improves data availability while respecting performance and operational constraints of older systems.

- **Security and Compliance Controls**

Security, access control and compliance considerations are embedded throughout legacy integration and modernisation. Controls are designed to mitigate known legacy risks while meeting current public sector security expectations.

- **Co-existence of Old and New Systems**

Architectures are designed to support long-term coexistence between legacy and modern systems. This ensures business continuity while modern services are introduced and legacy components are progressively retired.

- **Documentation and Transition Planning**

We produce clear documentation of legacy behaviour, integration interfaces and transition stages. This supports assurance, future change and continuity as teams and suppliers evolve.

- **Knowledge Transfer to Internal Teams**

We actively transfer knowledge to internal teams, reducing reliance on specialist individuals and enabling organisations to take ownership of their modernisation journey.

BENEFITS

Our AI-Driven Legacy Modernisation & Integration Services enable organisations to modernise critical systems safely, incrementally and with confidence. The benefits focus on **maintaining service continuity while unlocking long-term transformation**, recognising the operational and reputational risk inherent in public sector legacy estates.

- **Reduced Risk When Modernising Business-Critical Systems**

Legacy platforms often support essential citizen and operational services, making uncontrolled change unacceptable. By combining detailed assessment, AI-assisted dependency analysis and incremental integration patterns, organisations significantly reduce the risk of service disruption. Changes are introduced in controlled steps, enabling testing, rollback and validation without exposing services to “all-or-nothing” failure scenarios.

- **Improved Accessibility of Legacy Systems Without Rewriting Them**

API enablement exposes legacy functionality and data in a controlled way, allowing modern digital services, cloud platforms and automation tools to interact with older systems safely.

This avoids invasive modification of fragile platforms while enabling reuse and interoperability across the wider technology estate.



- **Safer Change Management Through Greater Visibility**

Legacy estates often contain undocumented logic and hidden dependencies that make change unpredictable. AI-assisted analysis improves visibility into usage patterns, dependencies and impact areas, enabling teams to understand consequences before changes are made.

This reduces unexpected failures, emergency fixes and operational instability.

- **Modern Interaction Patterns Without Large-Scale Replacement**

Event-driven integration enables legacy systems to participate in modern, responsive architectures without requiring full re-platforming. Systems can publish and react to events, supporting near real-time services and analytics.

This allows organisations to modernise behaviour before modernising infrastructure.

- **Avoidance of High-Risk, Large-Scale Replacement Programmes**

Incremental modernisation spreads cost, effort and risk over time, avoiding disruptive replacement initiatives that frequently overrun, fail or are cancelled.

Organisations can demonstrate continuous progress while retaining flexibility to adapt plans as priorities or funding change.

- **Improved Data Availability From Legacy Platforms**

Secure data extraction and integration unlock data trapped in legacy systems, enabling analytics, reporting and operational insight without compromising system stability.

This improves decision-making while respecting performance and availability constraints.

- **Reduced Security and Compliance Risk in Legacy Estates**

Modern security controls, access management and monitoring reduce exposure to well-known legacy vulnerabilities. Integration security provides containment, reducing the blast radius of incidents affecting older platforms.

This supports alignment with current public sector security and assurance expectations.

- **Maintained Business Continuity Throughout Transformation**

Co-existence patterns ensure that old and new systems operate together safely over extended periods. Services remain available while modern components are introduced, migrated and validated.

Citizens and staff experience continuity rather than disruption.

- **Clear, Defensible Modernisation Roadmap**

Documented strategies and transition plans provide clarity for senior leaders, auditors and assurance bodies. Decisions are evidence-based and defensible, reducing uncertainty and governance friction.

- **Improved Capability to Integrate With Modern Platforms**



Knowledge transfer and modern integration patterns improve long-term organisational capability, enabling legacy systems to interact reliably with cloud services, data platforms, automation and AI solutions.

WHAT THE SERVICE INCLUDES

Reply provides a comprehensive, end-to-end service that supports safe, incremental legacy modernisation through integration, AI-assisted insight and strong governance. The service is designed to evolve over time rather than impose a single, disruptive change.

1. Legacy Estate Discovery and Contextual Understanding

We begin by developing a deep understanding of the legacy landscape and its role in service delivery. This includes:

- Identification of critical legacy systems and services
- Understanding operational importance and failure impact
- Review of existing interfaces, integrations and data flows
- Identification of key stakeholders and operational constraints

This establishes a realistic baseline for modernisation planning.

2. AI-Assisted Dependency and Impact Analysis

We apply AI-assisted techniques to analyse codebases, interfaces, data relationships and historical usage patterns. This accelerates discovery and highlights areas of risk that may not be visible through documentation alone.

Outputs include:

- Identification of hidden dependencies
- Insight into system usage and change sensitivity
- Improved confidence in impact assessment

AI supports engineering judgement; it does not replace it.

3. Integration-Led Modernisation Strategy Definition

We define a pragmatic modernisation strategy centred on integration rather than replacement. The strategy balances ambition with risk, cost and operational reality.

This includes:

- Selection of appropriate modernisation patterns
- Sequencing of changes over time
- Identification of quick wins and dependency blockers
- Alignment with enterprise and integration architecture

4. API Enablement for Legacy Systems

We design and implement APIs that safely expose legacy functionality and data. APIs act as a controlled façade, insulating modern services from legacy complexity.

This includes:

- Design of stable, well-governed interfaces
- Access control and throttling
- Versioning and lifecycle management
- Documentation for reuse

5. Event-Driven Enablement Where Appropriate

Where feasible, we introduce event publishing and consumption capabilities, allowing legacy systems to participate in event-driven architectures.



This supports:

- Looser coupling between systems
- Improved responsiveness
- Gradual migration to modern patterns

6. Incremental Modernisation Delivery

We support step-by-step delivery of modern components alongside existing systems.

Activities include:

- Implementation of façade and strangler patterns
- Validation of coexistence in live environments
- Controlled migration of functionality over time
- Safe retirement of legacy components when appropriate

7. Data Integration and Extraction Support

We enable secure, efficient extraction and integration of legacy data into modern data platforms.

This includes:

- Design of non-intrusive data access
- Performance-aware extraction approaches
- Data quality and validation controls
- Alignment with governance and privacy requirements

8. Security, Compliance and Assurance Embedded by Design

Security controls are applied consistently to legacy integrations, reducing exposure to risk.

This includes:

- Identity and access enforcement
- Data protection and encryption
- Support for audit and assurance activities
- Alignment with public sector standards

9. Documentation and Transition Planning

We produce and maintain documentation describing legacy behaviour, integration interfaces and transition stages.

This provides:

- Clarity for delivery and operations teams
- Evidence for assurance and audit
- Continuity as teams and suppliers change

10. Knowledge Transfer and Capability Enablement

We actively transfer knowledge to internal teams, reducing reliance on specialists and improving long-term sustainability.

This includes:

- Walkthroughs of legacy behaviour and risks
- Explanation of modernisation patterns
- Support for operational readiness

11. Ongoing Review and Roadmap Adjustment

Legacy modernisation is rarely linear. We support ongoing review of progress, emerging risks and changing priorities, updating the roadmap as needed.

**WHY THIS MATTERS**

Together, these services replace risky, disruptive legacy replacement approaches with a controlled, integration-led pathway to modernisation. Organisations gain confidence that critical systems can evolve safely over time, enabling digital transformation, policy change and innovation without putting essential public services at risk.



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