

CONSULTANCY SERVICE

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

REPLY CONSULTANCY SERVICES

ERROR! BOOKMARK NOT DEFINED.

TABLE OF CONTENTS	2
SERVICE DESCRIPTION	3
WHY US?	5
ONBOARDING	6
OFFBOARDING	7
SECURITY	8
PERSONNEL SECURITY	8
INFORMATION SECURITY	8
PHYSICAL SECURITY	8
TRAINING & KNOWLEDGE TRANSFER	9
ORDERING AND INVOICING PROCESS	10
CUSTOMER RESPONSIBILITIES	11
ABOUT REPLY	12



SERVICE DESCRIPTION

SHIELD REPLY IS A DIGITAL CONSULTANCY FIRM, DELIVERING BESPOKE APPLICATIONS AND INNOVATIVE SOLUTIONS FOR THE DEFENCE, INTELLIGENCE AND SECURITY SECTORS.

We provide expert advice and innovative digital solutions that enable faster, smarter decision-making in defence, intelligence and security.

From bespoke Oracle APEX applications to UK Classified Cloud Platforms, we deliver practical solutions to complex challenges.

Our analytics expertise helps organisations uncover actionable insights from data, equipping them with the right tools, skills, and strategies to drive digital transformation at pace.

OUR SERVICES



BESPOKE APPLICATIONS



ACCREDITED CLOUD PLATFORM



BUSINESS ANALYTICS



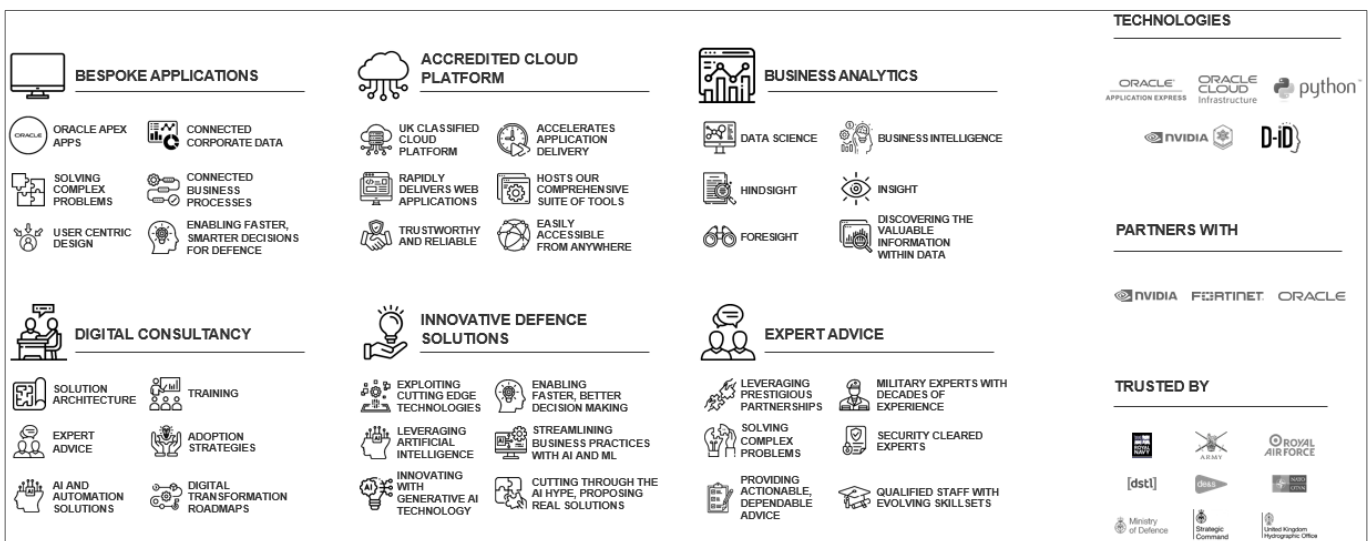
DIGITAL CONSULTANCY



INNOVATIVE DEFENCE SOLUTIONS



EXPERT ADVICE



Shield Reply, as the defence focused element of Reply, offer support services to Military and Government projects including: Requirements Management and Capture; Consultancy and Subject Matter Expert provision; Security Management and Assurance; and Developmental and Operational Design, Testing and Evaluation for Acceptance. We deliver embedded consultancy and programme management expertise to strengthen defence capability development and operational output, supporting the Government's objectives for resilience, efficiency, and innovation. Our approach ensures continuity and coherence across departments, agencies, and suppliers to align strategic priorities to capability delivery requirements whilst ensuring compliance.

Our team works side-by-side with Service Commands, Delivery Teams, and MoD Headquarters, integrating seamlessly into existing structures to accelerate delivery and drive strong governance. Our collaborative model supports whole-of-government outcomes by bridging operational requirements with technical realities.

Leveraging decades of former military insight and advanced technical expertise, we provide consultancy across the full spectrum of defence and security domains. Our experience spans multiple portfolios, including capability development, complex mission, platform and weapons systems, electromagnetic warfare, and security. From concept development and programme management to integrated test and evaluation, mission data solutions, and security services, we deliver end-to-end support for complex programmes.



We also reinforce programme management functions, currently exemplified by our work in the Army ASGARD programme, by implementing proportionate governance and ensuring coherence across workstreams. This activity includes programme planning, monitoring, RAID management, stakeholder engagement, governance, change control, and lessons learned tracking, alongside administrative support for programme headquarters.



WHY US?

Choosing us means partnering with a team that possess significant and deep understanding of Government defence and security priorities having operated in that environment for numerous decades and who are adept at listening to customer needs to and deliver tangible outcomes. Our differentiators which help ensure value for money, high levels of security, and significant operational application across all engagements are shown below:

Embedded Expertise:

- Our consultants work within MoD structures for seamless collaboration and immediate impact.

Proven Military and Technical Knowledge:

- Combining operational insight with deep technical expertise.

Consultancy Across Defence Domains:

- Extensive experience across multiple portfolios for integrated solutions.

End-to-End Capability Support:

- From concept development to integration and mission data solutions.

Governance and Delivery Rigour:

- Reinforcing programme management with SQEP resources for efficiency and risk control.

Innovation and Future Readiness:

- Delivering multi-domain solutions aligned with the UK MoD's 2035 vision.

Compliance and Standards:

- Adhering to MoD security policies, ISO 27001, ITIL, GDPR, and G-Cloud requirements.

Our Services Include:

- Managed Private Cloud, using our proven security model for UK MOD, Gov, and NATO.
- Project management and governance, delivered by our experienced Military and Defence industry PM team.
- Capability analysis, scrutiny provided by our highly experienced ex-Military Requirements and Capability Managers.
- Managed Hybrid Cloud, Proven model for UK MOD, Gov, and NATO.
- Security strategy, UK MOD and NATO experienced security support.
- Assurance/testing design, Qualified Military Test and Assurance Engineers and multi-cloud technical auditors.
- Operational readiness testing, Qualified Military planners and operational readiness assurance staff.



ONBOARDING

Our onboarding process ensures rapid, secure integration of personnel and services into the client environment in line with G-Cloud and MoD standards.

Timelines:

- Onboarding typically occurs within 5–10 working days from contract signature, subject to security clearance verification.

Roles and Responsibilities:

- Consultant: Complete mandatory training, provide required documentation, and attend induction sessions.
- Client: Facilitate access to systems, provide workspace, and confirm governance structures.
- Reply Ltd: All consultants will be managed by Reply Ltd throughout the engagement. Reply Ltd provides governance, oversight, and accountability, ensuring consultants adhere to agreed processes and deliverables. Reporting lines are clearly defined, with consultants reporting to Reply Ltd's engagement lead, who coordinates directly with client stakeholders.

Compliance Checks:

- All personnel undergo security clearance verification, GDPR compliance training, and security protocol briefings before deployment.

Knowledge Transfer:

- Initial sessions include programme objectives, governance, reporting lines, and access to relevant documentation. A structured induction pack is provided to ensure alignment with operational requirements.



OFFBOARDING

Our offboarding process guarantees a controlled, secure exit while preserving knowledge and minimising disruption.

Timelines

- Offboarding is completed within 5 working days of contract termination or project completion.

Roles and Responsibilities

- Consultant: Deliver final reports, transfer all documentation, and participate in exit review sessions.
- Client: Confirm receipt of deliverables, revoke system access, and approve final sign-off.
- Reply Ltd: Reply Ltd manages the offboarding process, ensuring consultants complete all exit requirements, deliverables are handed over, and compliance checks are met. Reply Ltd coordinates with client stakeholders to confirm smooth transition and accountability.

Compliance Checks

- Removal of system access, return of all issued equipment, and confirmation of MoD security compliance.

Knowledge Transfer

- Includes final handover of RAID logs, lessons learned, and project documentation. A formal exit review ensures continuity and captures feedback for continuous improvement.



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. It also incorporates a Facility Security Clearance (FSC) from the UK Security Vetting Agency to allow storage of classified material and classified meetings.
- All Laptops/Phones are stored securely overnight.
- When working on a client-site our consultants adhere to client security policies.



TRAINING & KNOWLEDGE TRANSFER

To ensure consultants deliver maximum value and maintain compliance with Government and MoD standards, we provide a structured training and knowledge transfer process:

Pre-Engagement Training

- Mandatory security and data protection training (GDPR, MoD security protocols).
- Familiarisation with G-Cloud framework requirements and client governance.
- Technical upskilling aligned with project scope (e.g., ITIL, ISO 27001, cloud technologies).

Role-Specific Induction

- Consultants receive tailored induction packs covering programme objectives, reporting lines, and governance structures.
- Training on client-specific tools, systems, and processes.

Technical Specialties

- Our consultants bring expertise across key technical domains, including:
- Cloud Architecture & Migration
- Cybersecurity & Information Assurance
- Data Analytics & Mission Systems
- Electromagnetic Warfare & Mission Data
- Programme Management Tools
- Integration & Test Planning

Continuous Professional Development

- Access to ongoing training resources and certifications relevant to defence and cloud environments.
- Regular knowledge-sharing sessions within the consultancy team to maintain best practices.

Knowledge Transfer During Engagement

- Consultants document processes, decisions, and lessons learned throughout the project.
- Scheduled handover sessions with client teams to ensure continuity.
- Use of secure collaboration platforms for sharing documentation and updates.
- Centralised knowledge repositories provide continuous access to critical insights - anytime, anywhere.

Exit Knowledge Transfer

- Formal handover of all deliverables, RAID logs, and technical documentation.
- Exit workshops to transfer operational knowledge and ensure smooth transition.
- Lessons learned captured and shared with client stakeholders for continuous improvement.



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 ensure successful delivery, the customer must provide clear governance and decision-making structures, timely approvals, secure access to systems and environments, and relevant programme documentation. They must support security clearance processes, enable stakeholder engagement for workshops and reviews, and commit to knowledge transfer activities. Additionally, the customer should collaborate on change control and risk management, ensuring all required information, infrastructure, and compliance measures are in place.

Governance & Decision-Making

- Clear Points of Contact: Nominate a primary stakeholder and decision-maker for approvals and escalations.
- Defined Governance Structure: Provide programme governance documents, reporting lines, and escalation routes.
- Timely Approvals: Ensure decisions on deliverables, scope changes, and risks are made promptly to avoid delays.

Access & Infrastructure

- System Access: Grant secure access to required platforms, tools, and environments (e.g., MODCloud, Jira, SharePoint).
- Workspace & Facilities: Provide physical or virtual workspace for embedded consultants.
- Connectivity & Security: Ensure consultants can connect securely to client networks in compliance with MoD protocols.

Information & Documentation

- Programme Documentation: Share relevant programme objectives, governance frameworks, and technical specifications.
- Existing Artefacts: Provide access to RAID logs, previous lessons learned, and current project plans.
- Data Availability: Ensure required datasets and mission information are available for analysis and integration.

Security & Compliance

- Security Clearance Support: Facilitate clearance verification and onboarding checks.
- Compliance Briefings: Provide client-specific security and governance briefings where applicable.

Collaboration & Engagement

- Stakeholder Availability: Ensure key stakeholders attend workshops, reviews, and knowledge transfer sessions.
- Regular Communication: Participate in scheduled progress meetings and provide feedback promptly.
- Knowledge Transfer Commitment: Engage in handover sessions and adopt shared documentation practices.

Change & Risk Management

- Change Control Process: Agree on a structured process for scope changes and impact assessments.
- Risk Ownership: Collaborate on RAID management and mitigation strategies.



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. We are able to consistently deliver to meet our clients' needs because of our knowledge of advanced technological solutions and our considerable consolidated experience, through which we address the main core issues of the various industrial sectors.

Through our 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 16,000 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.