

CLOUD SECURITY & COMPLIANCE ASSESSMENT

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

CLOUD SECURITY & COMPLIANCE ASSESSMENT	1
SERVICE DEFINITION	1
TABLE OF CONTENTS	2
SERVICE DESCRIPTION	3
<i>CLOUD SECURITY AND COMPLIANCE ASSESSMENT – SERVICE MODULES (II)</i>	<i>4</i>
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

Cyber Security in Public Cloud

While digitisation continues to unlock opportunities to engage customers, reduce cost, and accelerate product delivery, it also increases exposure to more sophisticated and targeted cyber threats. Public cloud environments introduce a distinct set of security challenges that must be addressed as part of any successful cloud programme.

Common challenges include:

- The inherently open and shared nature of public cloud environments
- Designing and building applications that are secure by default
- Maintaining security and compliance on a continuous, ongoing basis
- Managing risk across rapidly evolving and highly dynamic cloud services

Our service helps clients address these challenges.

Reply's Cloud Security and Compliance Assessment is designed to support organisations through a modular, flexible approach that can be tailored to specific objectives, risk appetite, and stage of cloud maturity. Our focus is on enabling organisations to adopt and scale cloud securely, both now and in the future.

We bring proven expertise, established frameworks, robust methodologies, and a strong track record of delivery across complex and regulated environments.

Ultimately, our service provides guidance, support, expertise, and capability that enable:

- The design and development of an effective cloud cyber security strategy
- A pragmatic and implementable roadmap to achieve that strategy
- Programmatic, technical, and operational support to execute
- Delivery of the key security components required to align cyber risk with business objectives

Overview of our Cloud Security and Compliance Assessment

Our Cloud Security and Compliance Assessment evaluates organisational maturity and capability across key security domains, based on Airwalk Reply's proprietary framework and extensive experience delivering cloud services at scale.

The assessment focuses on the following core areas:

1. Cloud Cyber Security Strategy
2. Information Security Risk Management
3. Controls Framework – Control Design and Implementation
4. Cyber Security Engineering and DevSecOps
5. Cyber Security Architecture
6. Cyber Security Testing
7. Security Incident and Event Management (SIEM)

Cloud Security and Compliance Assessment – Service Modules (i)

1. Cyber Security Strategy

- Review of organisational security strategy and its effectiveness in promoting a proactive security posture
- Assessment of objectives, priorities, investment levels, and cloud risk appetite
- Benchmarking against industry standards and regulatory expectations

2. Information Security Risk Management

- Review of Information Security policies and standards, with recommendations for cloud-specific



updates

- Assessment of security maturity against recognised best practices
- Provision of benchmarking to contextualise results

3. Controls Framework – Control Design and Implementation

- Review of frameworks used to assess and approve cloud workloads and designs
- Benchmarking against standards such as NIST, CIS, ISO, and industry best practice
- Assessment of cloud-native, third-party, and in-house services
- Review of control effectiveness and alignment to control objectives

4. Cyber Security Engineering and DevSecOps

- Review of engineering security controls and guardrails
- Assessment of CI/CD pipelines and security automation
- Review of governance, approval gates, and security review processes
- Assessment of monitoring, logging, and supporting tooling

5. Cyber Security Architecture

- Review of security patterns and deployment blueprints
- Assessment of the cloud cyber controls catalogue
- Review of security logging, monitoring, and cloud security operations strategy

Cloud Security and Compliance Assessment – Service Modules (ii)

6. Cyber Security Testing

- Review of infrastructure testing approaches and automation
- Assessment of application security testing within CI/CD pipelines
- Security build reviews, including infrastructure-as-code and standards
- Configuration hardening (operating systems, containers, images)
- Review of vulnerability management and scanning practices
- Phishing simulations and security awareness testing

7. Security Incident and Event Management (SIEM)

- Review of SIEM strategy and implementation
- Assessment of people, processes, and skills
- Review of tooling and technology, with recommendations where gaps exist
- Assessment of compliance with regulations such as GDPR, PCI, SOX, and HIPAA

Key Benefits of our Cloud Security and Compliance Assessment

By engaging with Reply, your organisation can achieve the following benefits:

- Reduced cyber security risk across cloud environments
- Increased maturity of cyber security capability with expert support
- Greater confidence for regulators, auditors, and senior management
- Comprehensive, standards-aligned control frameworks
- Clear visibility of cloud security posture across infrastructure and applications
- Consistent security policies and controls across the cloud estate
- Secure, automated, and scalable cloud security operations



- Applications and platforms that are secure by design
- Integration of automated security into delivery pipelines and code

Associated Services

Our Cloud Security and Compliance Assessment can be complemented by the following services:

- AWS Cloud Strategy
- Microsoft Azure Cloud Strategy
- Cloud Business Case Development
- Cloud Operating Model Assessment
- Cloud Security Strategy
- Continuous Compliance Framework
- Cloud Architecture Review Service
- DevOps Strategy and Transformation
- Cloud Migration Service



ONBOARDING

Kick-off Workshop

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.

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

Termination

The client can terminate an engagement at any stage by providing four weeks' notice in writing to the Account Manager.

Off-Boarding

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/handed over 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 to provide additional continuity.



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

Our primary approach to training – Enablement

We work closely with our clients and their teams to ensure that their skills, knowledge, and experience develop and evolve during our engagement. We describe this as Enablement—our goal is to leave our clients behind much stronger than we found them.

Whilst formal training is part of this, we strongly believe in the effectiveness of working in blended delivery teams with our clients. We use methods such as peer programming and mentoring to transfer knowledge and skills to client team members, over time providing them with greater ownership and responsibility as Reply steps back from hands-on delivery and hands over to the client.

Where appropriate, we will structure formal training in specific areas (e.g., DevOps, Terraform, etc.), which can be incorporated into the programme as an additional module—specifically, our Reply Academy.

Reply Academy

A structured training programme - Cloud Academy – provides internal client resources and new external hires with the requisite skills to support cloud services for their relevant project or functional teams.

Key outcomes

- Permanent resources with the requisite skills to support the growing use of cloud services across your organisation
- Faster up-skilling of resources, allowing them to become productive members of teams much more quickly
- Reduced reliance on external service providers for operational and BAU and support functions
- An enduring, evolving and growing operational capability within your organisation to support cloud services

Implementation Plan

We collaborate with our clients to help them define the key objectives for their project or programme and their broader organisational strategy.

Understanding these drivers, alongside analysing the services, applications, and use cases they have in mind for use on the public cloud, enables us to work with the client to define a strategic roadmap for implementing the cloud and an appropriate security strategy to facilitate this.

Our analysis through the Cloud Security Assessment will drive recommendations and a prioritised plan.

Reply works closely with the client to manage this process, delivering all artefacts while managing the client's input. Ultimately, Airwalk Reply provides robust outputs that the client team can use to gain senior management buy-in and move forward with implementation at their own desired pace and scale.

Service Management

The nature of this service means that Reply does not provide service-level metrics, as we need to provide the technology or hosting capabilities themselves. As such, service management, service constraints, SLAs and outage or maintenance management are not applicable.



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, no specific technical or client-side requirements 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 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