

CLOUD SECURITY STRATEGY ADVISORY AND IMPLEMENTATION 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
infouk@reply.com

www.reply.com



TABLE of CONTENTS

CLOUD SECURITY STRATEGY ADVISORY AND IMPLEMENTATION SERVICE	1
SERVICE DEFINITION	1
TABLE OF CONTENTS	2
SERVICE DESCRIPTION	3
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

Cloud Security Strategy Advisory and Implementation

Whilst digitisation is increasing opportunities to engage with customers, reduce cost and accelerate product delivery, it also has the potential to expose businesses to more creative and advanced cyber-attacks. This leads to multiple complex challenges that need to be overcome as part of any cloud programme:

- Inherent open nature of public cloud environments
- The challenge of designing and building secure applications
- Maintaining security and continuous on an ongoing basis
- Dealing with evolving, dynamic services on the cloud

Our service helps clients address these challenges.

Our Cloud Security Strategy Advisory and Implementation service is designed to help clients address these issues and many others by providing a modular approach that can be adapted to your specific goals.

Our focus is on enabling you to achieve your goals securely and make the most of the cloud for your organisation now and in the future.

We bring unique expertise, frameworks, methodologies, significant experience, and a track record of successful delivery to make this happen.

Ultimately, our service provides clients with guidance, support, expertise and capabilities that enable:

- The design and development of a Cyber Security strategy
- A pragmatic and implementable plan to achieve that strategy
- Programmatic, technical and operational support to execute
- Delivery of the critical components required to align your cyber risk with business objectives

Overview of our Cloud Security Strategy Advisory and Implementation service

Our Cloud Security Strategy Advisory and Implementation service comprises multiple components or modules, allowing clients to select the elements that will add the most value to their organisation or take the full suite of options for a comprehensive and holistic cloud security strategy where appropriate.

The key modules that form our service include:

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

Cloud Security Strategy Advisory and Implementation Service Modules (i)

1. Cyber Security Strategy

- Formulation of a security strategy which helps your organisation design and implement a proactive approach to cloud security
- An approach designed to improve the security and resilience of your services, together with a roadmap and timeline for implementation
- A strategy aligned to the business requirements and risk appetite of your organisation



2. Information Security Risk Management

- Review and assessment of Information Security policies and standards, with potential recommendations for amendments and updates for cloud
- Assessment of your security maturity level against security good practice and processes, CESG, National Cyber Security Centre (NCSC)
- Identification of gaps and areas for improvement
- Industry benchmark against which to compare the results

3. Controls Framework - Control Design and Implementation

- Development of a comprehensive control framework with which to assess existing and future systems and applications
- Framework based on industry standards including NCSC, National Institute of Standards and Technology (NIST), Centre for Internet Security (CIS), ISO and good practice
- Assessment of cloud provider, 3rd party and in-house services
- Implementation of controls, cloud native and engineered, to support control objectives

4. Reply's Continuous Compliance

Reply's Continuous Compliance is a lightweight serverless framework which enables your organisation to apply consistent security policies and controls across your cloud estate.

- Controls can be implemented in four ways: preventative, detective, corrective, and exemption. It is a crucial enabler of innovation, providing guardrails for many cloud services whilst providing information to cyber security teams, allowing them to manage risk in their cloud environments

5. Cyber Security Assessment

- Detailed assessment of the security posture of your cloud infrastructure, applications and information
- Report of findings and recommendations for improvement with a prioritised plan for implementation

Cloud Security Strategy Advisory and Implementation Service Modules (ii)

6. Cyber Security Strategy

- Engineering of security controls and guardrails using cloud-native, 3rd party tooling and in-house developed solutions
- Secure CI/CD software delivery pipelines with integrated and automated security for effective and secure engineering and development in the cloud
- Strategies to shift security left and automate away the traditional security gates
- Build and integrate security monitoring and logging

7. Information Security Risk Management

- Development of secure patterns and blueprints for deployment of cloud services
- Development of a catalogue of cyber controls for cloud
- Definition of security logging and monitoring, observability, strategy
- Design of cloud security operations strategy, including potential changes for existing teams and processes

8. Controls Framework - Control Design and Implementation

- Cyber Security infrastructure testing
- Application Security Testing, including support to select and implement tools into your CI/CD pipeline and code reviews
- Security Build Review, infrastructure as code, standards, configuration hardening including operating



systems and container images

- DevSecOps strategy and approach
- Social Engineering Engagements, simulated attacks and training

9. Reply's Continuous Compliance

- Implementation of Reply's Consolidated Observability platform to collect, ingest, process and analyse log events from across the estate
- Development of additional integrations from any data source
- Help demonstrate compliance with regulations such as HIPAA, PCI, SOX, and GDPR

Associated Services

Our Cloud Security Strategy Advisory and Implementation service can complement several other services that Airwalk Reply offers through G-Cloud 14. If any of the following interests you, please let us know, and we would be happy to discuss them further. Further information can also be found on Airwalk Reply's corresponding service pages on G-Cloud 14.

Security and Compliance Assessment

This service provides an architectural assessment against organisational, regulatory and industry security control guidance and our own proprietary cloud security framework.

Continuous Compliance Framework

Reply's CCF is a comprehensive, automated approach to delivering ongoing, dynamic management of your cloud estate, ensuring visibility and active management of security and compliance.

Cloud Architecture Review service

Our certified experts analyse your design's cloud and on-premise components in detail to ensure you are delivering efficient, robust, and secure digital services on AWS or Azure.

Cloud Operating Model Assessment

We comprehensively assess your cloud operating model, reviewing foundational areas such as engineering, architecture, cloud security, governance, people, skills, and service operations.

DevOps Strategy and Transformation

This service helps clients modernise their working practices and tooling, accelerate release cycles, drive security through automation, and improve delivery quality and consistency.

Cloud Migration service

Our Cloud Migration service helps clients design and execute the migration of key applications and services to the public cloud securely, efficiently and effectively.

AWS Cloud Strategy

Our AWS Cloud Strategy service helps organisations design and successfully implement their AWS migration programmes securely and at scale whilst delivering maximum benefit.

Microsoft Azure Cloud Strategy

Our Azure Cloud Strategy service helps organisations design and successfully implement their Azure migration programmes securely and at scale while delivering maximum benefit.



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

Implementation Plan

We collaborate with our clients to help them define their cloud security project's key objectives and broader organisational strategy.

Understanding these drivers and analysing the services, applications, and use cases they are using (or plan to use) on the public cloud enables us to work with the client to define a strategic roadmap for implementing enhanced cloud security in their organisation.

This process includes:

- A detailed analysis of the existing Cloud Cyber Security operating model (see slide 9 for further detail on this analysis)
- A prioritisation of the critical actions, risks and opportunities to mature and enhance Cloud Cyber Security over the subsequent 6-18 months (depending on the scale and complexity of the challenge)

Once this has been defined, an implementation plan can be developed, including identification of the critical foundational elements that would need to be delivered for successful realisation of the action plan and associated benefits.

Service Management

The nature of this service means that Airwalk 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, outages, and 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