SECURITY ASSESSMENTS

G-CLOUD 14

SERVICE DEFINITION DOCUMENT

Author	Created	Version	Changes
ID	05/03/2024	1.0	Created

Table of Contents

REPLY
SPIKE

OUR SERVICE

Service Description

Spike Reply is part of the Reply Group, specializes in delivering comprehensive managed multi-cloud security services. Our portfolio encompasses security incident management, vulnerability management, and pentesting services tailored for organizations of all sizes. As accredited partners with leading cloud vendors such as AWS, Azure, and Google Cloud Platforms, we ensure your business benefits from top-tier cyber threat protection. Our services are underpinned by rigorous service assurance standards, positioning us as either your full IT security service partner or an adjunct to your existing IT security efforts.

Our team has over 40 years of cumulative experience in both the public and private sectors, is dedicated to offering bespoke Cyber Security Services and Security Service Solutions. Our offerings are particularly tailored for UK Public Sector Organisations and Private Organisations, designed to mitigate business risks, manage threats proactively, and secure your operations against the evolving threat landscape. Spike Reply is your steadfast partner throughout your digital transformation journey, providing flexible and robust security service options.

Our Service

Spike Reply extensive experience with central government projects has enabled us with a deep understanding of the unique challenges, regulatory requirements, and security mandates these projects entail. Our value lies in our proven track record of deploying innovative solutions that adhere to Agile methodologies, DevSecOps principles, and stringent compliance standards such as NCSC guidelines, ISO, GDPR, and more. Our approach ensures not just compliance but also the achievement of strategic objectives, making us the ideal partner for departments seeking to navigate the complexities of government IT projects.

Our Cloud Security Services is specifically designed to protect your multi-cloud and hybrid environment. In the offering, we include cloud security consultancy and advisory, strategy planning & technology road-mapping, security implementations and optimisations and more security services.

Features:

- Security maturity assessment and roadmap planning.
- Security solution design, build, configuration and operation.
- Security Design and Advisory
- Cyber Security Consultancy
- Security Pentesting
- Vulnerability Management Service
- Security Incident Management
- Security Audit Services
- Cyber Security Governance
- Cloud Migration and Security
- Security Engineering Services
- Identity Security
- Data Security
- Cloud Workload Security
- Security awareness and training programmes.

Benefits:

We constantly review and optimise your workloads to avoid overspend:

- Aligned to Business and ICT and Compliance Strategies.
- Reduced data/reputation/finance risk through 24x7 security monitoring, incidents and alerts.
- Increased transparency of security posture through insightful reporting and guidance.
- Improved compliance of security policies and regulatory requirements.
- Flexible service to support customer across SOC & tooling domain.
- Service can also be applied to other security cloud platforms.
- Ability to try before you buy cloud technologies and services.
- Architects produce secure and robust design artefacts ensuring no over-design.

Onboarding

Spike Reply will carry out series of meetings, workshops with stakeholders and system owners, Floor walk, technical discussion with architecture team and functional discussion with business to define the scope of work. Prior to the execution of the Order, the Supplier and the Buyer will agree the scope of the exit plan for the Security Services and a timescale for delivering an exit plan to ensure continuity of service. Once the scope of work is agreed a project manager will be assigned to deliver the project.

Offboarding

The offboarding process is designed to ensure a smooth transition and continuity of service. Spike Reply collaborates with clients to establish a detailed exit plan, outlining the activities required for a seamless service discontinuation. This plan is developed in accordance with the agreed terms in the Call-Off Contract, ensuring all parties are aligned on expectations and deliverables.

Access to Data

At Spike Reply, we prioritize ensuring our clients have complete and uninterrupted access to their data when our services come to an end. Our exit strategy includes a clear and straightforward process for transferring all client data back to the client, securely and efficiently. We use encrypted methods for data transfer, whether it’s through direct online channels or encrypted physical media, to maintain security and integrity.

We are committed to make the data handover as smooth as possible and we support to integrate the transferred data back into your systems with minimal disruption. Our approach is tailored to meet your specific needs, ensuring you receive your data in a format that's ready to use. Throughout the exit process, we ensure transparency and support to facilitate a seamless transition, reaffirming our dedication to your data's security and your business 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

Spike Reply ensures that every client gets the most out of our solutions and services through comprehensive training and knowledge transfer sessions. Our training programs are designed to empower your team with the knowledge and skills they need to manage and maintain security effectively. These sessions cover everything from basic security awareness to advanced operational techniques, tailored to the specific tools and services we've implemented for your business.

We focus on practical, hands-on training that allows your team to confidently handle security tasks, respond to incidents, and use our security solutions efficiently. Additionally, we provide detailed documentation and resources for ongoing reference, ensuring that your team can continue to apply best practices long after the initial training period. Our goal is to leave your team well-equipped and knowledgeable, ensuring a smooth transition and sustained security effectiveness.

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

For the successful delivery of our services, we rely on a collaborative partnership with our customers. It is essential for customers to provide us with timely access to their systems, relevant data, and necessary resources throughout the duration of our service. This access enables us to perform comprehensive assessments, implement solutions, and conduct thorough testing to ensure the security measures are effectively in place.

Additionally, we ask our customers to maintain open lines of communication with our team. Regular updates, feedback, and discussions about any changes in your IT environment help us to adapt our services to best meet your needs. Your engagement and responsiveness are crucial in addressing issues promptly and making informed decisions, ensuring the success of our security solutions in protecting your organization.

ABOUT REPLY

About Spike Reply

Spike Reply is the company within the Reply Group focusing on cybersecurity and personal data protection. Its mission is to safeguard the values and privacy of people, companies and processes in order to support the growth of a global, sustainable digital world through innovation. Confidentiality, integrity and availability of systems are top priorities. Together with its partners, the company provides vendor-independent consulting services to help enterprises achieve a group-wide, security-oriented culture.

IDENTITY AND ACCESS MANAGEMENT

Identity management, also known as identity and access management (IAM or IdAM), is a framework of policies and technologies to ensure that the right users (that are part of the ecosystem connected to or within an enterprise) have the appropriate access to technology resources. IAM systems fall under the overarching umbrellas of IT security and data management. Identity and access management systems not only identify, authenticate, and control access for individuals who will be utilizing IT resources but also the hardware and applications employees need to access.

SECURITY ASSESSMENTS

Security Assessments ensure that necessary security controls are integrated into the design and implementation of a project/product or an operation. Our security assessments provide documentation outlining any security gaps between a project design and approved corporate security policies. Security gaps can be addressed in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gaps, or accept the risk based on an informed risk / reward analysis. Spike Reply will evaluate security controls to examine the overall organisation’s security infrastructure, provide you with a gap analysis against most current information and best practice recommendation relative to your security posture, and finally help develop an appropriate roadmap to prioritise and resolve them.

CLOUD SECURITY POSTURE MANAGEMENT – CSPM

Cloud security data breaches are commonplace today, with most breaches involving a misconfiguration in the Cloud infrastructure settings. Cloud Security Posture Management (CSPM), offers a policy-based tools that empower security personnel to automate thousands of settings in a consistent manner and give them a standing chance of managing the drift. Spike Reply consultancy offers advice for policy setting by providing automated visibility, continuous monitoring and remediation workflows for your Cloud computing services.

WORKLOAD PROTECTION - CNAPP OR CWPP

As Applications have evolved to now also be delivered as serverless functions or containers, the collective noun in use seems to be the Workloads. Workload protection refers to a collection of security tools that safeguard Workloads across different Cloud environments. CNAPP tools are an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production.

The most significant benefit of a CNAPP approach is better visibility and control of cloud-native application risk. Attempts to identify and remediate application risk have been fragmented across multiple toolsets spanning development and runtime. By integrating vulnerabilities, context and relationships across the development life cycle, excessive risk can be surfaced, enabling development teams and product owners to focus on remediating the areas of the application that represent the most risk.

GOVERNANCE, RISK AND COMPLIANCE

Spike Reply's expertise makes it possible to tailor cyber security programs and controls according to client's business missions. Standards and best practices are integrated with approaches gathered in fieldwork and innovation aptitude. The experts guide clients towards managing security risks and compliance with standards and regulations, working towards a continuous improvement on the security maturity level.

SECURITY OPERATION SERVICES

Especially larger companies are attempting to deliver as many critical services as possible with their own employees. While this can be an efficient method for critical and large scaled topics, it can become very expensive for smaller or customer-individual solutions. Long-term operation is another challenge due to a shortage of skilled IT personnel. To assist businesses with these topics, Spike Reply has setup a Managed Security Services department.

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 decentralized 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