REPLY

SECURITY GOVERNANCE AND RISK COMPLIANCE

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 DESCRIPTION

Reply offers governance, risk and compliance as a service. We specialise in providing tailored solutions to ensure that your organisation meets all regulatory requirements and industry standards. Our team of dedicated experts understands the intricacies of compliance and we're here to guide you through every step of the process. From initial assessments to ongoing monitoring, we'll ensure your organisation thrives in today's complex compliance landscape. Our experienced team provide comprehensive GRC services, including Threat Modelling, PCI-DSS Gap Assessments, ISO 27001 Gap Assessments, NIST Assessments and Cyber Essentials Assessments. We help you identify and document risks and achieve compliance goals with ease.

Features

- Threat Modelling
- PCI-DSS Gap Assessment
- ISO 27001 Gap Assessment
- NIST Gap Assessment
- Cyber Assessments

Benefits

Governance, Risk, and Compliance (GRC) offer significant benefits to organizations, making it imperative for them to prioritize these aspects seriously. GRC provides a holistic approach to managing operational complexities by aligning processes with regulatory standards, mitigating risks effectively, and fostering a culture of ethical conduct. By implementing robust GRC frameworks, organizations can enhance decision-making processes, improve operational efficiency, and strengthen stakeholder trust. Furthermore, GRC helps organizations anticipate and mitigate risks, reducing the likelihood of financial losses, legal penalties, and reputational damage. Compliance within the GRC framework ensures adherence to relevant laws, regulations, and industry standards, safeguarding the organization's integrity and credibility. Ultimately, by embracing GRC, organizations can enhance resilience, drive sustainable growth, and achieve long-term success in today's dynamic business landscape.

ONBOARDING

We will start the GRC Service with an initial discovery assessment to understand your existing security measures and identify any gaps or areas for improvement. Based on the assessment results, we will create a customised roadmap outlining the steps needed to achieve compliance with ISO 27001, NIST 2, PCI-DSS and Cyber Essentials. This roadmap will be tailored to your organisation's specific needs, resources and timelines. We'll provide hands-on assistance with implementing the necessary security measures and controls outlined in the roadmap. This may include updating policies and procedures, implementing new technologies and providing comprehensive training and awareness programs to educate your team on security best practices. We'll conduct regular audits and assessments to ensure that your organisation remains compliant with ISO 27001, NIST 2, PCI-DSS and Cyber Essentials requirements. These audits will help identity any areas where improvements are needed and provide assurance to stakeholders. If certification is your goal, we will assist you in preparing for external certification audits. We'll help gather the required documentation, address any findings or non-conformities and guide you through the certification process to achieve compliance successfully. Our relationship doesn't end once you achieve compliance. We'll continue to be your trusted partner, providing ongoing support, guidance and expertise to help you navigate any security challenges that arise and stay ahead of emerging threats.

Offboarding

We securely transfer any data, documents, or records that belong to the client and are necessary for ongoing compliance and risk management activities. We ensure compliance with data privacy regulations and client confidentiality agreements throughout the transfer process. We verify that all sensitive information is handled and transmitted securely to prevent unauthorized access or breaches.

Upon completion of the data and documentation transfer process, we formally close out the engagement with the client and document the final status of all activities, deliverables, and agreements. We obtain confirmation from the client that all requirements have been met and that they are satisfied with the transition process. We ensure that all contractual obligations, including termination clauses and exit procedures, are fulfilled according to the terms of the agreement.

Access to Data

We initiate discussions with the client well in advance to discuss the decision to transition or terminate the GRC services. We clearly communicate the reasons for the transition, whether it's due to the completion of the engagement, changes in business needs, or other factors. We work with the client to develop a detailed transition plan outlining the steps, timelines, and responsibilities for both parties.

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 offer comprehensive training programs designed to empower our clients with the knowledge and skills needed to effectively manage GRC within their organisations. Our training covers a wide range of topics, including GRC principles, regulatory compliance, risk management strategies, and best practices for governance frameworks. We provide in-depth instruction on utilising GRC tools and technologies to streamline processes and enhance efficiency. Our training sessions are tailored to the specific needs and objectives of each client, ensuring relevance and practical application. We offer both onsite and virtual training options to accommodate diverse learning preferences and logistical considerations. Throughout the training process, we foster interactive discussions, case studies, and hands-on exercises to reinforce learning and encourage active participation. Our goal is to equip our clients with the expertise and confidence needed to navigate complex GRC challenges, drive organizational excellence, and achieve sustainable success.

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 of Governance, Risk, and Compliance (GRC) services, we require several key elements from our customers:

- Clear Objectives and Expectations: We need a clear understanding of our customer's objectives, priorities, and expectations for the GRC engagement. This includes defining specific goals, desired outcomes, and any unique requirements or constraints that may impact our delivery.
- Access to Relevant Information and Documentation: We rely on access to relevant information, documentation, and data related to our customer's business operations, regulatory environment, risk profiles, and existing GRC practices. This information enables us to conduct thorough assessments and develop customized solutions tailored to their needs.
- Engagement and Commitment from Key Stakeholders: We depend on active engagement and commitment from key stakeholders within our customer's organisation, including senior leadership, department heads, and subject matter experts. Their involvement is crucial for providing insights, making decisions, and driving implementation efforts.
- Timely Feedback and Communication: Timely feedback and open communication are essential for addressing questions, resolving issues, and ensuring alignment between our team and the customer. We encourage regular check-ins, progress updates, and status meetings to maintain transparency and keep the project on track.
- Compliance with Agreed-upon Responsibilities and Deadlines: We expect our customers to fulfil any agreed-upon responsibilities and commitments within the specified timelines. This may include providing requested information, participating in training sessions, or reviewing deliverables as part of the GRC implementation process.
- Flexibility and Willingness to Adapt: Given the dynamic nature of GRC environments, we appreciate our customer's flexibility and willingness to adapt to changes, challenges, and evolving requirements as they arise. Collaboration and partnership are essential for navigating complexities and achieving successful outcomes together.

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