

Service Definition Document: Cyber Risk Assessment and Assurance

Collaborate

Innovate

Accelerate

Introduction: We deliver programmes across sectors for government, regulators, industry bodies and businesses. Our experience provides insight into the latest trends, technology and challenges to shape how projects are designed and executed to achieve maximum positive impact. We offer professional services in support of business objectives.

Purpose: A risk assessment provides risk identification, analysis and evaluation. Effective risk management improves performance, encourages innovation and supports the achievement of business objectives. We provide a robust, consistent and repeatable, risk assessment service for public/private sector organisations in the Cloud or considering moving to the Cloud.

Overview: Our highly qualified and experienced cyber security consultants, under the direction of a lead consultant, will liaise with key stakeholders, senior management, business owners and third-party suppliers to create risk assessments in support of business change, including project/programme/organisational objectives.

A risk assessment considers the context of each risk, categorization and prioritization, risk ownership, acceptance criteria, proportionate mitigation options, escalation and management throughout the lifecycle.

The risk assessment methodology uses best practice principles, frameworks and processes, including ISO25005, ISO27030, NSCS guidance and the NIST Cyber Security Framework, designed to help an organisation manage the effects of uncertainty on its key objectives.

We advise organisations to help provide a better understanding of risks and risk management, to enable informed decision-making. We assess third party access to data and provide expertise relating to engaging or changing Cloud service providers. The review encompasses security and data privacy risks considerations. A gap-analysis highlights where organisations are not implementing security good practices, the associated business risks, and makes recommendations of proportionate measures to take.

We consider compliance against General Data Protection Regulation (GDPR) and Digital Operational Regulations Act (DORA). Our consultancy is designed to enable organisations understand their current security risk exposure, make good decisions and help them to meet legal, regulatory and contractual security requirements, whilst at the same deriving the significant benefits of working in the Cloud and the opportunities arising from it.

Elements of the wider security service offering include cyber and risk management strategy, operational security, cyber threat intelligence, security risk assessments, security architecture and design, compliance management, penetration testing, security awareness training, incident management, compromise assessment, and forensic analysis.

www.atomicrisk.com

Collaborate

Innovate

Accelerate

Service Definition Document: Cyber Risk Assessment and Assurance

Quality Assurance and Performance Testing:

- Assesses organisations against legal, regulatory and contractual obligations, as well as industry standards ISO27001, ISO27005, ISO27017, ISO27030 and NIST Cyber Security Framework
- Gap-analysis based on security and data privacy good practices
- Articulate risks to enable informed management decisions around the implementation and maintenance of secure Cloud services.
- Supports overall corporate strategy and business objectives.
- Enables organisations to meet legal, regulatory and contractual security requirements.

Security Services:

- Promotes positive security culture and awareness
- Enables organisations to meet legal, regulatory and contractual security requirements
- Significantly enhances business resilience
- Key risks are identified and managed in a proportionate manner

Ongoing Support:

- Tailored support to meet organisational requirements
- Flexible resourcing to meet demand surges
- Mapping of continuous and continuous improvement
- Skills transfer from our highly experienced consultants to organizational teams

Information Assurance: We employ highly qualified and experienced security-cleared personnel. Services are offered for data at all classifications, as per the Government Security Classification (GSC) scheme.

Pricing: Resources are charged in accordance with SFIA day rates, based on the anticipated requirement. Pricing models include, but are not limited to:

- Fixed price. Based on expected resource requirement including a contingency based on experience and available information, including anticipated travel and subsistence requirements, at the time of quoting. Payment to be made by the Customer against agreed milestones. Full details to be agreed before service commencement.
- Time and material, limited liability. Based on anticipated resource requirement and charged monthly in arrears against actual effort based on timesheets or similar records. Travel and subsistence limits may also be agreed in advance. These will also be charged at cost monthly in arrears. Full details to be agreed before service commencement.
- Flexible or subscription pricing. Based on Customer requirements or service usage. Full details to be agreed before service commencement.

Service Definition Document: Cyber Risk Assessment and Assurance

Service Management and Constraints: A lead consultant will be responsible for liaising with the Customer lead, managing resources and delivery the required services. All contracts are managed by an account manager with oversight by a director, who is also an escalation point. Support is available by phone, email or on-site during normal working hours and we aim to respond to all enquiries within one working day. Extended support hours can be arranged where required.

Data Backup and Business Continuity: We can process data at OFFICIAL on our systems. Data at any classification may be processed on Customer systems subject to suitable accreditation of that system. We carry out regular backups of corporate systems and devices to ensure we can continue to provide services in the event of any disruption

Onboarding/offboarding: Our standard onboarding process may be used, or we can align with Customer requirements. Offboarding will include a project review against organizational objectives and industry good practices.

Ordering and invoicing process: Initial enquiries should be sent via email to enquiries@atomicrisk.com or submitted using the contact form at www.atomicrisk.com. Once the requirements have been agreed with the Customer, Atomic Risk Management will provide a costed proposal detailing the services and initial engagement information. Subject to receipt of a signed approval and valid purchase order, we will then agree a start date, plan and payment schedule for the activities. Payment terms are thirty days from invoice date.

Customer responsibilities: Collaborate with the lead consultant throughout the duration of the agreement and facilitate access to key stakeholders, systems and such information as may reasonably be required to meet the terms of the agreement.

Why work with us?

We are skilled in delivering programs of work that help Customers achieve their business goals. Our expertise lies in managing and delivering public and private sector programs amidst constantly changing technical, regulatory and commercial pressures. We collaborate closely with you and offer support throughout every aspect of the service. We can flex resources to meet changing requirements or a surge in demand to help deliver business change and unlock your organisation's potential.

To find out more please contact us:

t: 0118 907 1001

e: enquiries@atomicrisk.com

w: <https://www.atomicrisk.com>

www.atomicrisk.com

Collaborate

Innovate

Accelerate