**Logan Risk – G-Cloud 15 Cyber Vulnerability Investigations (CVI) Service Definition Document**

**About Us**

Logan Risk Ltd is a specialist cyber security consultancy. We provide cyber and information assurance services through qualified professionals to assess cyber security risk and to provide customers with independent advice on the selection of appropriate security controls in proportion to their risk. Our services enable our customers to manage the risks to their information throughout project lifecycles, enabling them to adopt change more effectively. All work is conducted in line with industry security best practices and relevant legislation, frameworks and standards.

**Our Services**

Logan Risk Ltd's specialist consultants provide high-quality cyber security advice, support, leadership and solutions. Our services include:

- Cyber Security Risk Management;
- Cyber Vulnerability Investigation (CVI) services;
- Cyber Security Risk Assessment;
- Information Assurance support;
- Secure architecture design;
- Policy development;
- Security accreditation support and artefact production;
- Security testing and assessment;
- Cyber security consultancy;
- Security auditing services;
- Technical assurance, Governance, Risk and Compliance (GRC);
- Cyber security training and awareness; and
- Cyber security compliance and framework support.

**Our People**

Our consultants boast a wealth of Public Sector cyber security expertise, each with over 10 years' experience of working with customers across Defence, Critical National Infrastructure (CNI), Energy, Healthcare, Finance and Communications sectors. We also hold several industry-leading qualifications, certifications and skills showcasing our knowledge, including:

- Certified Cyber Professional (CCP);
- Certified Information Systems Security Professional (CISSP);
- Chartered Engineer (CEng);
- Chartered Information Technology Professional (CITP);

• Systems engineering for complex systems;

• ‘Soft skills’ to facilitate interactions with a wide range of stakeholders;

• Domain experience across core defence domains (Air, Land, Maritime, Space, Cyber);

• Cyber threat understanding across both Industry and MOD sectors;

• Cyber Vulnerability Investigation techniques including attack path analysis, technical, organisational and cultural assessments;

• Risk assessment, including quantification and identification of themes, mitigations and interventions;

• Risk management, including specification and implementation of mitigations; and

• DV clearance across all consultants.

**Service Features and Benefits**

For our Risk Management Service, our Cyber Security consultants define your current cyber security baseline, enabling you to gain an understanding of your current levels of risk. We then identify the key information assets that could be affected by a cyber-attack and highlight risks that potentially affect those assets. With this baseline in place, we then create and maintain an effective cyber security risk management plan, ensuring that all areas are assessed regularly and the impact and likelihood of risks occurring is greatly reduced.

Our Cyber Vulnerability Investigations service is an Agile socio-technical assessment methodology used to identify cyber risks. CVIs take on the view of an attacker, applying agile methodologies to highlight vulnerabilities, test viable attacks paths and develop risk mitigations, moving swiftly to areas of most concern.

Outputs of our service benefit a wide stakeholder audience, and a programme of CVIs can support both enterprise-level and individual capability or system risk management. As sociotechnical investigations, focus is given to people, processes and technology and the potential vulnerabilities these create, which are often key to an attacker exploiting a vulnerability.

Across each of our cyber security service offerings, we offer a number of benefits for our customers:

• Holistic and realistic assessments,

• Scalable approaches to cyber risk management,

• Methodical approaches which lead to effective interventions,

• Agile and adaptable approaches,

• Effective and valuable outputs,

• Evidence for scrutiny and compliance,

• System discovery and baselining;

• Identification and selection of security controls;

- Implementation of security controls;
- Assessment of security controls;
- Preparation of documentation suite;
- Authorisation of security controls;
- Monitoring of security controls;
- Risk-based, mission-driven methodology;
- Risks assessed early and continuously;
- Security architecture developed early with periodic lifecycle updates; and
- Delivers increased capability to protect, detect, react and restore.

**Planning Service**

Our planning service helps buyers to gain an early understanding of their capability's cyber security risk. It also delivers a cyber security system architecture baseline whilst recommending the necessary controls to be implemented in order to successfully manage and monitor cyber security risk throughout the capability's lifecycle, often as part of a wider, integrated risk management framework.

**Security and Assurance Services**

Our security and assurance services comprise of strategy, risk management, secure design, testing and auditing, utilising specialist security subject matter experts (SMEs). We provide expert security advice on all aspects of information assurance and security, including the government cyber security schemes, Cyber Essentials, US NIST standards and the International Standard on Information Security Management (ISO 27001).

**Training Services**

Logan Risk Ltd can supply customers with appropriately skilled training consultants for desired training needs across the full breadth of cyber security and awareness requirements. All training is aligned to the specific needs of end user groups across the customer's organisation.

Training is tailored to the customer’s requirements, and ranges from security awareness training to technical and specific system security training. Training can be undertaken on customer site or remotely and is designed to be interactive and relevant to real life situations. Ongoing refresher courses and knowledge updates can also be provided on a continuous basis to ensure success and relevance of security training programme.