Handling Instructions: For MASS and Crown Commercial Services only

MASS
A COHORT PLC COMPANY

Cyber Security Consultancy

Service Definition Document
Jan 2025

Contents

1. Introduction

1.1 Overview

With a wealth of experience spanning decades, MASS specialises in delivering cyber security consultancy services for both public and private sector organisations, regardless of project size or security classification. Our dedicated teams stay abreast of the latest advancements in cyber security project and task management, ensuring our methods reflect current best practices. We consistently deliver solutions on schedule and within budget, underpinned by rigorously defined business processes that safeguard the integrity and confidentiality of client information.

1.2 Purpose of the Document

The purpose of this document is to outline the Cyber Security Consultancy services and business processes delivered by MASS under the G Cloud 15 Framework, detailing the robust measures we employ to ensure effective, secure, and confidential service provision for our clients.

2. Service Overview

2.1 Description of Cyber Security Consultancy Services

MASS delivers comprehensive Cyber Security Consultancy services as part of the G Cloud Framework, supporting organisations across the public and private sectors in strengthening their security posture. Leveraging our extensive experience and deep sector knowledge, we provide end-to-end guidance and practical solutions tailored to the unique security challenges faced by each client.

- **Security Assessments and Risk Analysis** – We conduct thorough security assessments, including:
  - Gap Analyses
  - Risk Identification
  - Threat Modelling
  - Vulnerability Assessments
  - Penetration Testing
  - CIS Benchmarking

  Our consultants evaluate existing controls, policies, and technical measures, providing recommendations to address vulnerabilities and comply with relevant standards.
- **Darktrace** – MASS, as a Managed Service provider, is one of the only Darktrace delivery partners licensed to implement this best-of-breed software into secure environments. We currently use it on a large-scale managed service for central government department, using it to monitor and mitigate security threats in real time.
- **Policy, Process, and Strategy Development** – Our team assists clients in developing and refining cyber security policies, incident response plans, and business continuity strategies. We ensure that processes and documentation align with best practices and regulatory requirements.
- **Technical Security Consultancy** – We offer expert advice on the design, implementation, and management of secure IT systems and networks. This includes secure architecture reviews, vulnerability management, penetration testing, and cloud security guidance.
- **Compliance and Accreditation Support** – MASS supports organisations in achieving and maintaining compliance with standards such as, Cyber Essentials, NCSC guidance, and sector-specific frameworks. We guide clients through accreditation processes and help prepare necessary documentation.

2.2 Objectives

Each of the cyber security consultancy services outlined above can be delivered independently by our specialists, but they are also seamlessly integrated into the overall provision of our solutions. MASS embeds these core capabilities into every engagement, ensuring clients benefit from tailored cyber security services and products that address their unique requirements. We manage all aspects of these services throughout the contract lifecycle, from the initial consultation through to successful completion.

Guided by our highly experienced cyber security professionals, we take a flexible and responsive approach to service delivery, scaling resources up or down as needed to provide robust, adaptable solutions for every client.

3. Methodologies

MASS operates a specialised Cyber Security Consultancy team alongside our Product Management functions, collaborating closely to employ rigorous idea generation and service delivery frameworks. Our consultants are highly skilled in developing all essential documentation and materials required to ensure successful outcomes. With extensive experience in managing complex, multi-layered engagements across defence and public sector organisations, we consistently deliver tailored cyber security solutions that meet diverse client needs.

Our cyber security consultancy service applies a flexible project methodology tailored to the unique needs of each client and engagement. At the outset, our cyber security consultants collaborate closely with client stakeholders to define the scope and requirements, ensuring that all processes align with organisational objectives and security priorities. Our Project Managers possess extensive expertise in delivering projects using recognised frameworks such as Prince2, Agile, APM, P3M, and Waterfall, enabling us to select the most suitable approach for each cyber security engagement and deliver effective, resilient solutions.

3.1 Client Engagement

MASS adopts a transparent and proactive communication strategy throughout the delivery of our cyber security consultancy services, ensuring clients remain fully informed of progress and developments. Our approach encourages collaborative engagement, enabling clients to respond to evolving requirements and implement necessary adjustments promptly. At the initiation of each engagement, our Project Managers identify critical stakeholders and develop a tailored communication plan to support the project's lifecycle.

To facilitate clear allocation of responsibilities within cyber security projects, we employ Responsibility Assignment (RACI) Matrices. These matrices are instrumental in defining stakeholder roles for each task and deliverable, particularly in multi-disciplinary or cross-organisational environments. The RACI framework clarifies the following roles:

- Responsible: Individuals or teams tasked with executing specific cyber security activities.
- Accountable: The person who holds ultimate responsibility for the successful and compliant completion of cyber security deliverables.
- Consulted: Stakeholders whose expertise or opinion is sought to guide cyber security decisions and processes.
- Informed: Stakeholders who must be regularly updated on project progress and outcomes.

The RACI matrix is reviewed and communicated during project kick-off meetings and subsequent progress reviews. Additional key items communicated include:

- Cyber security project outputs
- Minutes from review and progress meetings
- Progress statements and updates

3.2 Communication Channels

From the outset of each consultancy engagement, MASS works collaboratively with clients to establish clear communication channels tailored to their preferences. Throughout the course of the project,

information is shared through a blend of formal and informal methods, ensuring that all stakeholders remain informed and engaged.

Among the formal communication approaches, regular verbal interactions play a significant role. These include scheduled meetings and presentations conducted at intervals agreed upon with the client, where thorough records are kept in the form of meeting minutes to ensure transparency and provide a reference point for future discussions.

3.3 Monitoring Progress

MASS works in collaboration with our clients to establish clear requirements for any services and products we are delivering. At the outset of any project, we ensure a method to measure the success of our delivery in a way that works well for the client themselves. This could include producing a balanced scorecard with Key Performance Indicators (KPIs) for things such as

- Delivery schedule adherence
- Quality right first time
- Risks and Opportunities identification
- Cost
- Relationship Management

Whilst this is a formal grading of performance, we also encourage a free-flowing relationship between any partners and our clients to identify and resolve risks and issues as early as possible.

3.4 Change Management

As good practice, MASS creates and aims to deliver according to an agreed upon project plan. However, we recognise that, at times, plans do not survive first contact and are adept and experienced at managing any changes in a controlled manner.

We ensure that any deviations to this agreed upon plan that affects clients or any other relevant stakeholder are communicated with an accomplished strategy to recover any lost time or cost.

As an organisation, MASS is agile, and we are committed to meeting our clients' requirements. As such, we have the ability to surge resources into problem areas to maintain agreed upon deadlines.

Any significant changes to the delivery of our services, as identified either by MASS or our clients, are supported, where appropriate, by impact assessments or any relevant contractual change notes when involving a change of scope.

3.5 Why MASS?

MASS brings a long-standing, high assurance security pedigree, ingraining Cyber Security in the delivery of all of our services. Handling classified data as a standard service, we maintain rigorous governance through our ISO27001:2022-ceritified Information Management System (with a full statement of applicability) and our role as a Cyber Essentials (CE)/CE+ certification body. Security is embedded end-to-end across our delivery cycle, from design through to development and ongoing management, underpinned by defence-grade standards. With extensive experience delivery secure solutions across Defence, Government, and other high-assurance sectors, MASS integrates cyber resilience into every

service we provide. As such our team are highly reliable consultants, with extensive expertise in the domain, assuring consistent advice and outcomes for our customers.

MASS has delivered Cyber Security consultancy for companies across Defence. Across the Cohort PLC Group (our parent company), we have conducted penetration testing for CHESS and Cohort itself, as well as Herald Investment Management. This was comprised of a scoping call to understand the system requirements, followed by a five-day remote security audit, with a report delivered afterward (with zero anomalies). We also conduct regular security testing (penetration testing, vulnerability scanning, and CIS benchmarking) on the systems we deliver and maintain, support secure and resilient project delivery.

4. Team

MASS's Company Security Controller (CSC) is responsible for all security policy, procedures, risk assessment, management, and general security processes. The CSC is the primary link between the company and Government Security Authorities. For every project, they have oversight of Security Aspects Letter (SAL), informing the security requirements which flow down to the project management and cyber staff.

4.1 Cyber Security Team Structure

MASS has a team of full-time Cyber Analysts to ensure continual delivery of our Cyber Security Consultancy services. We may also utilise Project Managers for each piece of work we do to ensure coherence and governance within the team, working in accordance with our quality standards. They may also act as a single point of contact for our clients.

4.2 Team Capabilities

Our team combines exemplary domain knowledge with excellent customer service to ensure continual advice in conjunction with assessments. As part of our company culture, with MASS delivering work in high-assurance industries (including extensive work for the MOD), both team members have experience working in highly secure environments. This means they are experts at implementing and maintaining systems that require extensive cyber security controls and have the deep knowledge to guide all customers through their relevant certifications.

Our team has a range of skills to ensure coverage of the whole area domain of cyber security. The team's lead is a certified Cyber Essentials Assessor, Cyber Essentials+ Assessor, and lead Auditor. The team also have qualifications including Vulnerability Assessment Plus (VA+), Crest Registered Security Tester (penetration testing qualification), ensuring they are qualified to conduct relevant support services for customers across Defence.

Where any new tool, process, or technology arises, we are able to utilise our deep understanding of fundamental aspects of the domain and apply them in order to ensure effective delivery in novel areas.

5. Assuring Quality

5.1 Relevant Standards

MASS delivers all services in accordance with our Quality Management System, certified to ISO9001:2015 Quality Management, ISO27001:2022 Information Security (with a full statement of applicability), and ISO20000-1:2018 Service Management. We are also Cyber Essentials and Cyber essentials+ certified ourselves and have assurances as part of the Information Assurance for Small and Medium Enterprises (IASME).

Our processes are regularly audited in accordance with our ISO accreditations. This includes our annual audit from an external body, as well as internal auditing of our projects through samples. MASS's Quality Assurance team also monitor customer satisfaction through surveys that are independent from individual projects, which customers can fill out as they see fit.

When testing the weaknesses of our customers' systems, we adhere to the Computer Misuse Act.

5.2 Project Management

Throughout delivery, MASS ensures effective communication with our clients to allow for the smooth operation and implementation of our services.

We are comfortable with the utilisation of various different channels of communication, both logical and physical, and will use both formal and informal methods to ensure consistent and coherent delivery of our services. During a kick-off meeting or during regular monthly meetings, our Team Lead will generally meet our client's team lead. On a more routine basis, our data engineers will speak to somebody at the same level on the customer side. We ensure frequency of communication appropriate to whatever the situation demands, generally daily or at least weekly.

5.3 Information Sharing

MASS ensures any information shared with our clients is done so in accordance with best practice and the relevant industry standards.

6. Security

6.1 Security Management

Organisation of Security at MASS is mandated by policy and legislation, and we are accredited to ISO27001. We focus on the MOD approach to Security role, structuring for Secure-By-Design, specifically JSP 440 Leaflet 5C and Industry Security Notice 2023-09. Several roles included, while not mandated in these policies, are a core requirement to assuring the Confidentiality, Integrity, and Availability of the system and its functions, specifically the UK Data Protection Act, JSP 490 and export legislation.

Security Management for the delivery of our services, including all aspects of physical, personnel, information, and technical security, is governed by MASS's Company Security Controller (CSC), who operates as Security Manager for individual contracts, in accordance with our defined MASS Security Instructions.

6.1.1 Physical Security

All MASS employees and visitors to our premises adhere to security protocols in accordance with the MASS Security Instructions. This includes controlled access to offices and secure storage of confidential materials.

6.1.2 Personnel Security

All MASS staff are required to have the appropriate security clearance as required.

6.1.3 Information Security

MASS staff work in accordance with the Government Security Classification Policy, JSP440, the Security Aspects Letter and the MASS Security Instructions when dealing with any protective marker information.

7. Previous Experience

MASS has a proven track record in delivering comprehensive security management solutions, underpinned by strict adherence to industry standards and governmental regulations. Our experience includes the successful implementation of Secure-By-Design principles across a variety of contracts, ensuring robust confidentiality, integrity, and availability for our clients. We have consistently demonstrated expertise in managing physical, personnel, and information security in accordance with MOD policies, UK Data Protection Act, and ISO27001 accreditation.

Our team has worked closely with government agencies and commercial organisations, providing tailored security strategies that align with specific legislative requirements. Previous projects have involved coordinating security clearances, establishing controlled access environments, and handling sensitive information with meticulous care. This breadth of experience positions MASS as a trusted partner in the field of security management.