Handling Instructions: For MASS and Crown Commercial Services only

MASS
A COHORT PLC COMPANY

Cyber Essentials and Cyber Essentials+

Service Definition Document

Jan 2026

Copyright © [2026] MASS Consultants Limited. All rights reserved

Contents

1. Introduction 3
1.1 Overview 3
1.2 Purpose of the Document 3
2. Service Overview 4
2.1 Description of Cyber Essentials & Cyber Essentials+ Services 4
2.2 Objectives 4
3. Methodologies 5
3.1 Process 5
3.2 Why MASS? 5
4. Team 6
4.1 Cyber Security Team Structure 6
4.2 Team Capabilities 6
5. Assuring Quality 7
5.1 Relevant Standards 7
5.2 Project Management 7
5.3 Information Sharing 7
6. Security 8
6.1 Security Management 8
6.1.1 Physical Security 8
6.1.2 Personnel Security 8
6.1.3 Information Security 8
7. Prior Experience 9

1. Introduction

1.1 Overview

MASS has extensive experience delivering Cyber Essentials and Cyber Essentials+ assessment and advisory services to organisations across both the public and private sectors. We ensure all projects are managed efficiently and securely, regardless of size or required security clearance. Our teams remain fully trained in the latest cyber security best practices and project management methodologies, guaranteeing our clients receive up-to-date and compliant advice and assessments. We consistently achieve successful certification outcomes on schedule and within budget, underpinned by our robust and clearly defined business processes.

1.2 Purpose of the Document

The purpose of this document is to outline the Business Processes and Consultancy Services that MASS delivers in support of Cyber Essentials and Cyber Essentials Plus certifications, and to demonstrate how we facilitate their effective implementation and ongoing compliance for our clients.

2. Service Overview

2.1 Description of Cyber Essentials & Cyber Essentials+ Services

MASS provides expert Cyber Essentials services to our clients, utilising our experience and expertise to guide suppliers through assessment periods. As a Certification Body, we deliver:

- **Cyber Essentials** – This is an NSCS-run cyber security framework, aimed at protecting against internet-born commodity threats. It focuses on easily found malware online, and the security needed to prevent it. As a standard cyber security framework, it is required by all suppliers delivering government work. MASS operates as an assessment body for individual suppliers, supporting them through certification with guidance and advice ahead of their self-assessments. Our expert Cyber Analysts then mark the assessments, with further guidance on strengths and shortfalls, as required.
- **Cyber Essentials+** - This certification builds on Cyber Essentials, with a technical verification added to the assessment. This provides additional assurance and proof of security measures in place to deliver contracts with security is a priority. In addition to all services delivered for Cyber Essentials, MASS conducts a live audit with the customer to check the validity of the self-assessment.
- **Cyber Adviser** – MASS also provides Cyber essentials-focused cyber consultancy. We provide cyber security guidance to businesses in any sector, on any topic, with a focus on getting them through their Cyber Essentials assessments.

2.2 Objectives

The ultimate objective of our delivery is to get customers through their Cyber essentials and Cyber Essentials+ certifications. We undertake efforts to expedite this, often getting them through the process at pace. Through our expert analysts, we improve customers' knowledge of the cyber security domain so that they are in a place to deliver their own services securely.

3. Methodologies

3.1 Process

To assess other companies, and guide them through their assessments, MASS will first meet with customer teams to understand their experience and history with Cyber Essentials. This will help form a baseline of understanding that can be built on to ensure they pass their assessment.

For each assessment itself, we do the following:

- **Cyber Essentials** – MASS marks the customer's self-assessment according to a mark scheme, with freedom given to our assessors. As such, this requires an extensive knowledge of the subject matter, with three years of experience (as a minimum) in IT for all team members.
- **Cyber Essentials+** - Our expert cyber analysts perform a remote technical verification of the customer's self-assessment, validating the controls they have in place and providing further assurance of cyber security. MASS follows the Test Specification Document, assessing through:
  - A remote vulnerability scan.
  - An internal vulnerability scan.
  - A malware protection check.
  - A multi-factor authentication check for cloud services.
  - Account separation.

We also provide ad-hoc advice to communicate knowledge of specific subject matter. This helps to upskill our customers' teams and ensure improved self-sufficiency with regards to cyber security.

Once the process has been completed, we include customers on our mailing list, ensuring they are kept aware of any updates to the scheme.

3.2 Why MASS?

MASS is a high-security focused company, delivering services across Defence, the MOD, and for customers who require high-assurance environments. This means our domain knowledge is exemplary, which we use to guide all Cyber Essentials customers through their relevant assessments. We often fold our Cyber Adviser role into the assessments, answering any queries they may have to accrue further knowledge and improve their cyber resilience.

Our customers in this area range from large UK Defence Organisations to national government agencies, with an exceptional pass rate, and specific referrals coming to us from other Certification Bodies. With a retention rate of over 95%, very few customers leave once they have engaged our services. Some of our customers include BAE Systems, Thales UK, Teledine, Ultra Maritime and Ultra Precision Control, AIG, Skanska, and Royal Mail. In the past twelve months alone, a total of 154 certificates have been generated through our assessment work.

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 Essentials assessment and advisory services. The team's lead is a certified Cyber Essentials Assessor, Cyber Essentials+ Assessor, and lead Auditor.

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. 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.

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.

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. Prior Experience

MASS brings a wealth of prior experience in security management, underpinned by our long-standing accreditation to ISO27001 and adherence to MOD security frameworks. Our expertise spans the implementation of Secure-By-Design principles, specifically aligned with JSP 440 and related Defence standards, as well as compliance with the UK Data Protection Act and export legislation. Over the years, we have successfully delivered robust security solutions for a range of contracts, ensuring the confidentiality, integrity, and availability of sensitive information and systems.

Our track record includes managing all facets of security, from physical and personnel protection to information and technical safeguards. We have consistently demonstrated our ability to operate under strict regulatory environments, with our Company Security Controller leading teams to meet and exceed client requirements. This extensive experience positions MASS as a trusted partner for delivering secure services in complex and demanding settings.