Penetration Testing

Service Definition Document

October 2025

HM Government
G-Cloud
Supplier

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
24/06/2025	Jonny Zammer	0.1	Initial Draft
13/10/2025	Jasmine Gillard	0.2	Updates for G-Cloud 15
28/01/2025	Jonny Zammer	0.3	Further updates for G-Cloud 15

HM Government
G-Cloud
Supplier

Table of Contents

Contents

Document Control ***2***
Revision History ***2***
Table of Contents ***3***
Services Overview ***4***

Service Description **5**

Maple Networks Penetration Testing Services **5**
Service Overview 5
Service Package 6

HM Government
G-Cloud
Supplier

Services Overview

Maple Networks are next generation Digital and IT service provider in the UK, with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Network's CREST-certified Penetration Testing Services.

HM Government
G-Cloud
Supplier

Service Description

Maple Networks Penetration Testing Services

The world of cyber security is innovating at an incredible rate. Almost weekly a new product is announced that is the “silver bullet” you need. The reality is always something different.

At Maple we believe an effective cyber security strategy is a healthy combination of people, process and technology. Our objective is to ensure that every penny you spend on cyber security brings tangible benefit to your business.

How do we do this? First, we help customers identify the threats relevant to their organisation, their assets, and their regulatory or governance obligations. Then we align any new investment in protective controls to those threats, the organisation’s risk appetite and budget. Finally, we consider the people. Without the right skills to configure and manage a control, the investment can be wasted.

At Maple, we recognise the need for penetration testing, a crucial tool in helping our clients stay resilient against cyber-attacks and threat actors. We align to the NIST Cybersecurity framework and use CVSS v3 risk scoring to give clients an accurate insight into their security posture across applications, API’s, Infrastructure and networks.

Service Overview

Maple Networks have significant experience across a wide range of organisation types and structures. Across all sectors, we have delivered numerous successful engagements at different stakeholder levels, aligning our reports and presentations to executive teams, senior leadership and technical staff alike.

Maple’s technical expertise spans multiple platforms and technologies, including:

- Hybrid multi-cloud
- Backup
- Cyber security
- Disaster Recovery
- Business Continuity

This expertise means Maple are well positioned to deliver on such engagements by leveraging all our accrued experience and knowledge. Maple have developed a proven methodology which has delivered defined outcomes for our customers.

Maple’s proven methodology has been developed over several years, leading to successful delivery of large-scale reviews, roadmaps, and implementation projects for many commercial organisations including within the NHS, local government and higher education.

HM Government
G-Cloud
Supplier

Service Package

Objective	To identify and safely exploit security vulnerabilities in order to improve an organisation's resilience and validate the effectiveness of its security controls.
Description	Maple Networks' penetration testing services provide an independent assessment of an organisation's attack surface. Our consultants simulate real-world adversary techniques to identify weaknesses and flaws across infrastructure, applications and cloud environments, before they can be exploited and leveraged by attackers. Each engagement is tailored to the client's environment, technology stack and objectives, ensuring the assessment is relevant and meaningful and not just a tick-box exercise.

HM Government G-Cloud Supplier

Supported from	Remotely, from within the UK
Testing Areas	• Web applications Assessment • API Assessment • Thick Client Assessment • Internal Infrastructure Assessment • External Infrastructure Assessment • Wireless Infrastructure Assessment • Internal Vulnerability Assessment • External Vulnerability Assessment • Wireless/Wi-Fi Testing • Code Review • Host Build Review • Authenticated Host Scan • Switch/router Configuration Review • Firewall Ruleset Review • AWS/Azure/O365/Google Security Review • Breakout Assessment • IoT Assessment • CI/CD Pipeline Review • Compiled Application Security Assessment • Web Service / API Security Assessment • Cloud Security Testing (AWS, Azure, GCP, Kubernetes etc.) • Continuous Threat Exposure Management (CTEM) • AI Penetration Testing • Automated Penetration Testing • IT Health Check (ITHC) Assessment • PSN-Aligned Security Testing
Process	**All Maple penetration testing services are CREST-certified.** All testing is performed under formal signed authorisation and the testing follows recognised industry standards, including: • Open Web Application Security Project (OWASP) • ISECOM's Open-Source Security Testing Methodology Manual (OSSTM) • Penetration Testing Execution Standard (PTES) • National Institute of Standard and Technology (NIST) • NCSC CHECK principles where applicable ○ Public-sector assessments can also be delivered in line with IT Health Check (ITHC) and PSN Code of Connection security testing requirements.

Commented [JZ1]: Or on site?

HM Government
G-Cloud
Supplier

	Engagements typically follow these stages: • Scoping and Authorisation: Define the scope and objectives of the assessment, identify any constraints (including scope constraints), and obtain formal written authorisation. A Statement of Work and/or Rules of Engagement will be issued to confirm the aforementioned, along with test dates and communication plan. A call is scheduled between the client and technical consultant ahead of the assessment date to ensure all pre-requisites and access requirements are in place, to avoid any delays to the scheduled penetration test. • Test Execution: All testing is conducted by qualified penetration testers using a blend of automated and manual techniques. All testers follow methodologies created by the Lead tester adhering to and following the above-mentioned industry standards. • Analysis and Validation: All findings are verified, and where authorised, safely exploited to demonstrate real-world impact. Each issue is individually mapped against CVSS v3, considering business logic, context and mitigations. • Reporting: Delivery of a detailed technical report, including executive summary, summary of recommendations, and detailed technical findings for each issue. Each finding includes a detailed summary, impact, proof of concept, reproduction steps, and remediation guidance. • Debrief and Retest: The technical findings are presented to the client by the consultant in a debrief call, providing a chance for a thorough explanation to the client and giving the client the opportunity to ask any questions. A retest can be scheduled to confirm that vulnerabilities have been successfully remediated.
Output	**Report** Upon the completion of the penetration test, Maple will produce a comprehensive report detailing all identified vulnerabilities, complete with their CVSS scores, impact analysis, reproduction steps and recommended actions. **Debrief** A follow-up call with the technical consultant will be scheduled to review the findings, remediation steps and answer any questions. **Optional Retest** A retest can be arranged to confirm that vulnerabilities have been successfully remediated.