Incident Response Tabletop Exercise

G-Cloud 15

January 2026

HM Government
G-Cloud
Supplier

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	Maple Networks, The Print Rooms, 164/180 Union Street, Waterloo, London, SE1 0LH		
Telephone	0203 858 0048		
Primary Contact	Graham Tetley	**Role**	Chief Technical Officer

Revision History

Issue Date	Author	Version	Revision Description
28/01/2026	Tim Luck	0.1	Initial Draft
09/01/2026	Ben Archer	1.0	Release

Table of Contents

1 Service Overview

Maple's Incident Response (IR) Tabletop Exercise (TTX) is a scenario-driven simulation designed to provide credible assurance that your organisation can manage a serious cyber incident in line with regulatory expectations, industry standards, and board-level governance requirements.

Delivered by an NCSC Assured and CREST-accredited Incident Response provider, this service helps organisations:

- Validate real-world readiness, not just documented plans
- Demonstrate alignment with NCSC Cyber Assessment Framework (CAF) outcomes
- Support ISO/IEC 27001 incident management and continual improvement obligations
- Reduce regulatory, financial, and reputational risk during a cyber incident

Outputs from the exercise can be used as supporting evidence for audits, assurance reviews, insurer discussions, and regulatory engagement.

2 Service Scope – General

An Incident Response Tabletop Exercise is a facilitated, discussion-based simulation of a realistic cyber-attack, testing your playbook(s). Participants respond as they would during a live incident, making decisions with incomplete information, time pressure, and competing business priorities. The exercise goes beyond technical containment to test:

- Executive decision-making and governance
- Incident escalation and authority
- Legal, regulatory, and notification considerations
- Internal and external communications (including media and stakeholders)
- Coordination with third parties such as insurers, suppliers, and regulators

The result is a clear, defensible view of organisational readiness, grounded in how people actually behave under pressure.

2.1 Service Package - General

Objective	To assess, validate, and strengthen the organisation's ability to manage a serious cyber incident through a realistic, scenario-driven simulation that tests decision-making, governance, communication, and technical coordination across all levels of the organisation.
Description	A facilitated, discussion-based cyber incident simulation tailored to the organisation's sector, risk profile, and maturity. Participants work through a realistic attack scenario under time pressure, responding as they would during a live incident. The exercise evaluates strategic, tactical, and operational readiness, highlighting strengths, gaps, and improvement opportunities. Delivered by an NCSC Assured and CREST-accredited Incident Response provider, the exercise provides credible assurance aligned to regulatory, audit, and governance expectations.
Hosted-in	Delivered either on-site at the customer's premises or remotely via secure virtual training platforms.
Supported from	Delivered and supported by Maple's UK-based, NCSC Assured and CREST-accredited Incident Response team, operating from secure facilities with 24/7 access to active incident responders.
Support level	Professional services engagement with full facilitation, scenario development, exercise delivery, and post-exercise reporting. Includes access to senior incident responders, tailored scenario design, and a comprehensive improvement roadmap.
Required connection types	For remote delivery: secure video conferencing (Teams) and access to shared training materials. For on-site delivery: standard meeting room facilities with projector/screen and attendee devices (optional).