e2e assure

Tabletop Exercise

Service Definition Document

Tabletop Exercise

Service Definition Document – G-Cloud 15

CONTENTS

Service Introduction

Businesses regularly test IT failover and building safety systems to ensure systems and communication channels work as expected, there is often an assumption that their Cybersecurity Incident and crisis escalation processes are equally as robust. Unfortunately, an increasing number of organisations are discovering in a live cyber-attack scenario that not all staff understand their responsibilities, who and how to escalate to, and what to do in a potentially catastrophic level event.

In the pressurised environment of a real incident, any gaps in incident preparedness quickly become apparent. If documentation is missing, processes not fully understood, and escalation points hit a dead-end, it can mean the difference between containing an attack with minimal impact versus having to re-build systems and reputation from the ground up.

Service Overview

The e2e-assure Tabletop Incident Exercise is designed to stress test a business's attack readiness by simulating a cyber incident as it might unfold in the real world, but with time to observe and reflect.

Starting with the technical identification and triage, through third-party engagement, and up to senior stakeholder management, the exercise provides the opportunity to test all aspects of incident response, communications & escalation, and business continuity.

Observations and recommendations identified during the exercise will be documented in a final report, guidance and advice will cover technical remediation, playbook development, process improvements, and communications optimisation.

SCOPE OF ACTIVITIES

The assignment will include the following actions and areas of assessment:

Stage	Tasks
Initial Consultation	• Initiation & Scoping meeting to review objectives and scenarios • Stakeholder assessment and session tailoring • Session deck delivered to client for internal distribution
Incident Exercise	• Facilitated exercise scenario at customer site • Review end to end performance across technical identification, triage, recovery, management responses, escalations, and communications.
Reporting & Recommendations	• Executive summary of scenarios tested and list of attendees • Detailed findings across people, process, and technology • Prioritised recommendations to improve incident response readiness and adjacent activities

SCOPE OF DELIVERABLES

The following output artifacts will be provided as part of the exercise sign-off:

Output	Description
Tabletop Incident Exercise Presentation Slides	• The content used to facilitate and guide the session
Tabletop Incident Exercise Findings Report	• An in-depth documented review of the exercise and progressive scenario with key observations • Areas for improvement across the end-to-end identification to crisis stand-down process

Service outcomes

- Identify potential gaps in current ability to respond to, and manage, a business disrupting cyber-attack and address issues within a controlled environment
- Ensure a common and coherent understanding of responsibilities and accountabilities across all stakeholders and involved parties across the Incident Response lifecycle
- Inform security engineering roadmaps, user awareness training plans, and risk assessment activities with empirical data and areas needing improvement and remediation
- Understand potential risks with external 3rd parties which only surface during a crisis incident