

Tabletop Incident Exercise



How confident are you that your plans to deal with cyber breaches stand up to contact with the enemy?

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.

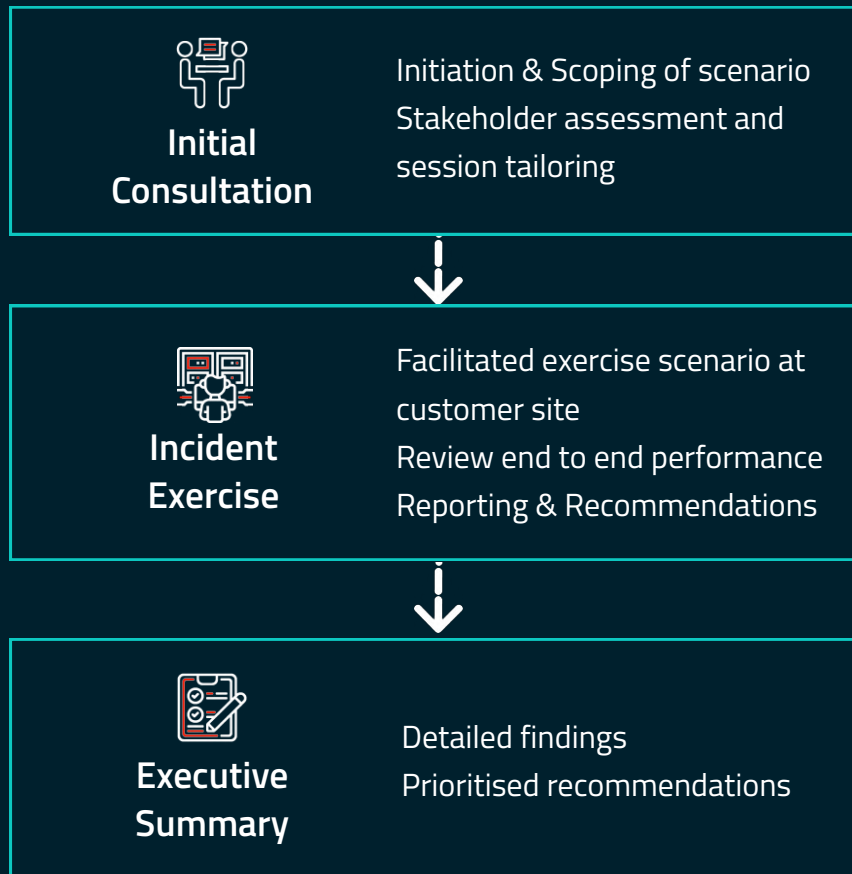
What we offer

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 on expectation versus reality.

From 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.

The Exercise



Outcomes and deliverables

At the end of the Tabletop Incident Exercise, you will leave with:

- An in-depth documented review of the exercise with recommended areas for improvement across the end-to-end Incident Response lifecycle
- The presentation content used to facilitate the session
- Identified potential gaps in current ability to respond to, and manage, a business disrupting cyber-attack and address issues within a controlled environment
- A roadmap to ensure common and coherent understanding of responsibilities and accountabilities across all stakeholders and involved
- Data to Inform security engineering roadmaps, user awareness training plans, and risk assessment activities with empirical data and areas needing improvement and remediation
- Understanding of potential risks with external 3rd parties which only surface during a crisis incident