



COGNISYS

PENETRATION TESTING

Tabletop exercise

Prepare your team for real-world incidents with our tabletop exercise service.

What's the purpose of a tabletop exercise?

A tabletop exercise is essential for assessing and improving your organisation's incident response capabilities. It enables your team to discuss, simulate, and analyse how they would react in a real-world security breach, disaster, or any other emergency. By walking through various hypothetical scenarios, your team can identify process gaps, enhance communication, and improve department coordination.

This proactive approach helps strengthen your security posture, enhance decision-making during a crisis, and ensure that response plans are comprehensive and actionable.

Scoping and planning

Define objectives

We work closely with your team to establish the key goals of the tabletop exercise. Whether focusing on a ransomware attack, insider threat, or business continuity during a cyber incident, we tailor the exercise to address your primary concerns and prepare for realistic threats.

Requirements

We gather relevant information about your network, existing security procedures, and incident response plans to set up the exercise. We aim to simulate realistic and impactful scenarios based on your organisational environment and critical assets.

Custom scenario design

Each tabletop exercise is tailored to your industry and specific organisational needs. We create realistic scenarios based on current threat landscapes, considering your network architecture, attack surface, and existing security protocols.

Methodology

Scenario simulation

We design and run simulations that mimic real-world cyber incidents, allowing your team to explore how they would respond. These scenarios include threats such as data breaches, ransomware attacks, or insider attacks, testing your response strategies in a controlled environment.

Interactive group discussion

Our facilitator leads an interactive discussion with key stakeholders, focusing on decision-making, role allocation, and procedural review. These discussions help identify weaknesses, communication issues, and opportunities to strengthen your team's readiness.

Post-exercise evaluation

After the exercise, we thoroughly evaluate your team's performance, highlighting strengths and areas for improvement. This process allows for a deeper understanding of response efficiency, highlighting the need for better coordination, policy adjustments, or tool optimisations.

Why choose Cognisys' tabletop exercise?

Choose our tabletop exercise service to boost your team's preparedness for cyber incidents.

Our certified experts design tailored scenarios that reflect your organisation's real-world risks. Through structured simulations and group analysis, we provide actionable insights and detailed feedback, enabling you to refine your incident response strategies.

[BACK TO CONTENTS](#)

