

# Cyber Incident Exercise

Ensure your organisation can respond effectively to real-world threats.

Rapid and effective incident response is critical to minimising the disruptions that organisations can face in an ever-evolving cyber-threat landscape. Teams must be able to act decisively, following established protocols to contain the impact and restore operations when an attack occurs. Without regular testing, gaps in incident response processes may go unnoticed until a real breach happens.

Roc's Cyber Incident Exercise provides a structured simulation of a cyber crisis, designed to test your organisation's ability to detect, respond to, and recover from an attack. Delivered in a controlled environment, this exercise enhances coordination across teams, validates response plans, and strengthens cyber resilience—ensuring your business can respond confidently and effectively when it matters most.

## Ideal for you if...

- ▶ You need to assess and validate your cyber incident response plan
- ▶ You want to improve cross-team coordination and decision-making in a cyber crisis
- ▶ Your organisation is preparing for cyber security audits, certifications, or regulatory compliance
- ▶ You require expert-led insights to enhance security strategy and operational resilience

## Why Roc?

24/7/365 In house MSOC	100% UK coverage	70+ highly trained engineers	100% engineers SC or DV cleared
CYBER ESSENTIALS PLUS accredited	ISO9001 accredited	14001 accredited	27001 accredited

## Service benefits

- ▶ Identifies gaps in cyber-security processes
- ▶ Improves coordination between IT and leadership teams
- ▶ Enhances regulatory compliance and governance
- ▶ Strengthens cyber resilience and readiness
- ▶ Reduces risks of downtime and financial impact



## Service overview

### Realistic cyber-incident simulation

The exercise replicates a real-world cyber attack scenario tailored to your organisation's specific risks. The simulated attack session tests how well your teams work together to mitigate the impact of an attack, refining decision-making and response protocols.

### Assessment of response capabilities

Organisations gain a clear understanding of their strengths and areas for improvement by walking through an incident step-by-step. The exercise evaluates how effectively teams detect, assess, and contain threats, as well as how leadership responds under pressure. Gaps are addressed before a real breach occurs.

### Compliance and governance alignment

Regulatory compliance ensures your cyber response processes align with industry standards. The exercise supports adherence to ISO 27001, Cyber Essentials, and other frameworks, ensuring businesses demonstrate due diligence and improve their overall security governance.

### Actionable insights and continuous improvement

Following the exercise, Roc provides a comprehensive debrief outlining key takeaways, strengths, and areas requiring further development. The recommendations help you fine-tune your response strategies, reduce the risk of downtime, financial and reputational damage, whilst strengthening defences against future threats.

### Cyber Incident Exercise

Roc offers four approaches to an Incident Exercise. These can be tailored according to the needs of your organization.

- ▶ **Paper-based desktop exercise:** our consultants will work with you to test your incident response policies, assessing effectiveness and identifying risks or weaknesses to be remediated
- ▶ **Technical exercise:** working in partnership with your technical team, we will assess your ability to recover your technical environment in the wake of an incident
- ▶ **Scenario-based exercise:** we will create multiple incident scenarios based on current threat trends; we then work through a dynamic simulation with your team to assess overall response capability
- ▶ **Gamified exercises:** Gamification tools such as cyber escape rooms and capture the flag provide an engaging, team building exercise

