CLOUDGUARD

ADVISORY

Incident Response Tabletop Exercise (TTX) Services

Turning incident response from assumed capability to proven execution

Service overview

Many organisations have an Incident Response Plan in place but lack confidence that it will perform effectively during a real-world cyber incident. Without structured validation, gaps in decision-making, communication, and coordination often only surface under pressure, when the business impact is already escalating.

CloudGuard's Tabletop Exercise (TTX) service enables organisations to validate their incident response capability in a controlled, scenario-driven environment. Through realistic, business-aligned simulations, we test how stakeholders respond to a developing cyber incidents by assessing coordination, escalation, and decision-making across both technical and business teams.

The outcome is a clear understanding of how effectively your organisation can respond in practice, supported by actionable insights to strengthen readiness. This ensures your Incident Response Plan is not only documented, but tested, refined, and capable of supporting controlled and effective response when it matters most.

- **Readiness** – A tested plan, defined roles, and people who know their part.
- **Responsiveness** – Contain the incident in hours, not weeks. Reduce blast radius.
- **Resilience** – Keep the business functioning, even when the unexpected hits

Service overview

Tabletop Exercise service value:

- Validates incident response capability against a multitude of realistic, controlled scenarios.
- Tests decision-making, coordination, and escalation across stakeholders
- Identifies gaps in response execution before a real incident occurs
- Strengthens process alignment between technical teams and business leadership
- Improves confidence in responding effectively under pressure.
- Provides clear, actionable insights to enhance response readiness
- Transitions incident response from documented plan to a measurable capability

Why this matters now

Cyber incidents are inevitable, but effective response is not. Without a tested Incident Response Plan, organisations lose valuable time, struggle to make confident decisions and face greater disruption when pressure is at its highest. A mature, tested Incident Response Plan turns a chaotic, high-pressure event into a coordinated strategic execution of a well-defined process, when it matters most.

CLOUDGUARD

Tabletop Exercise (TTX) Service scope

Scenario Design & Planning
Development of realistic, business-aligned cyber incident scenarios to reflect relevant threats, organisational risks, and operational priorities.

Stakeholder Engagement
Identification and participation of key business and technical stakeholders to validate roles, responsibilities, and coordination during an incident.

Operational Simulation
Delivery of a structured, scenario-led tabletop exercise to simulate a live cyber incident and guide participants through each phase of response

Response Validation
Assessment of decision making, communication, escalation, and coordination to evaluate the effectiveness of the Incident Response Plan in practice.

Continuous Improvement
Provision of detailed feedback and actionable recommendations to improve response capability, readiness, and overall resilience.

Our approach

Engagement Initiation - Confirm objectives, scope, and stakeholder participation to align the exercise with business priorities and outcomes.

Scenario Design – realistic, business cyber incident scenarios tailored to organisational risks and industry context.

Exercise Execution- Facilitate a structured, scenario-based simulation to guide stakeholders through a developing cyber incident and response activities.

Response Validation – Assess decision-making, communication, escalation, and coordination to evaluate the effectiveness of the response in practice.

Debrief & Insights- Validate the plan with key stakeholders to ensure it is practical, understood, and aligned to business and regulatory requirements.

Reporting & Recommendations - Deliver a clear outcome report with actionable recommendations to strengthen incident response readiness and resilience.

Why CloudGuard

CloudGuard delivers enterprise-grade cybersecurity for growing businesses. Combining automation-led technology with UK-based experts, we provide 24/7 protection, without the complexity or cost of traditional platforms. Our fully managed approach simplifies detection, protection and improvement, so you can focus on growing with confidence.

Get in touch