

CRISIS MANAGEMENT EXERCISE





A Crisis Management Exercise offers organisations a safe and controlled environment to rehearse their incident management and response processes.

It evaluates the readiness of teams to respond to and recover from relevant cyber incident scenarios, focusing on people, process, and technology aspects. The exercise structure involves a series of discussion points or 'injects,' presenting key questions to the team to discuss suitable responses, identify process gaps, and demonstrate the business impact of decisions.

Purpose:

The purpose of a Crisis Management Exercise is to assess the readiness of organisations to effectively manage and respond to cyber incidents. By simulating realistic scenarios and evaluating responses, the exercise aims to identify strengths and weaknesses in people, processes, and technology. It provides an opportunity for teams to practice incident management roles, highlight process gaps, and understand the potential business impact of their decisions.

Features:

-  **Simulated Scenarios:** Realistic cyber incident scenarios are simulated to test the organisation's response capabilities.
-  **Evaluation of Readiness:** Assess the readiness of teams in terms of people, process, and technology to respond to and recover from incidents.
-  **Discussion Points (Injects):** Series of discussion points or 'injects' prompt teams to discuss suitable responses and identify process gaps.
-  **Business Impact Analysis:** Demonstrate the business impact of decisions made during the exercise to emphasise the importance of effective incident management.

Benefits:



People:

- **Skill Enhancement:** Provides employees with the opportunity to practice their incident management roles, improving their readiness to respond to cyber incidents effectively.
- **Team Collaboration:** Promotes collaboration and communication among team members during crisis situations, enhancing overall teamwork and coordination.

Technology:

- **Process Improvement:** Identifies process gaps and areas for improvement in technology infrastructure and tools used for incident response.
- **Technology Validation:** Validates the effectiveness of existing technology solutions in detecting, containing, and mitigating cyber incidents.

Commercials:

- **Risk Reduction:** Helps mitigate the risk of business disruption and financial losses by identifying weaknesses in incident response processes and addressing them proactively.
- **Regulatory Compliance:** Assists in meeting regulatory compliance requirements by demonstrating a proactive approach to incident management and response readiness.