# MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY

**Objective**:

To understand the key components of the SEI's *Incident Management Maturity Model* and apply it to assess the maturity level of an organization's incident management capabilities.

**Scenario**:

Imagine Zenith Hospital, a regional healthcare provider with a growing network of clinics. They've recently experienced a surge in phishing attempts targeting staff. While IT has basic incident response procedures, staff awareness of cyber threats seems low. This scenario presents a challenge – how mature is Zenith's incident management, and what improvements are crucial to protect sensitive patient data and ensure business continuity in case of a cyberattack?

Your team, assigned Zenith Hospital, will utilize the SEI's Incident Management Maturity Model to assess their current state and develop a roadmap for improvement. Focus on prioritizing capabilities critical for healthcare, like incident identification, communication, and recovery. Remember, a robust incident management plan is vital to safeguarding patient privacy and mitigating disruption to critical medical services.

**Instructions**:

1. Divide the class into small groups of 3-4 students. Or work individually.
2. Use the provided scenario.
3. Using the information provided in the module notes, particularly the list of capabilities and their priorities, each group should:
    a. Identify the incident management capabilities their assigned organization should prioritize based on the organization's nature and potential risks.
    b. Assess the organization's maturity level for each of the prioritized capabilities, considering the indicators and scoring criteria provided in the notes.
    c. Develop a roadmap or action plan for improving the organization's incident management maturity, focusing on the highest priority capabilities that need improvement.
4. After 20 minutes of group work, each group will present their findings and proposed roadmap for 5 minutes.

**Expected Output:**

Each group should submit a written report (approximately 600 words) that includes:

1. A brief description of the assigned organization scenario.

2. A list of the prioritized incident management capabilities for the organization, with justifications.
3. An assessment of the organization's current maturity level for each prioritized capability, supported by evidence from the module notes.
4. A proposed roadmap or action plan for improving the organization's incident management maturity, with recommendations for addressing the identified areas for improvement.

This exercise will help you understand the practical application of the SEI's Incident Management Maturity Model, reinforce your knowledge of the different incident management capabilities, and develop skills in assessing an organization's maturity level and proposing improvement strategies.