

Operational Resilience

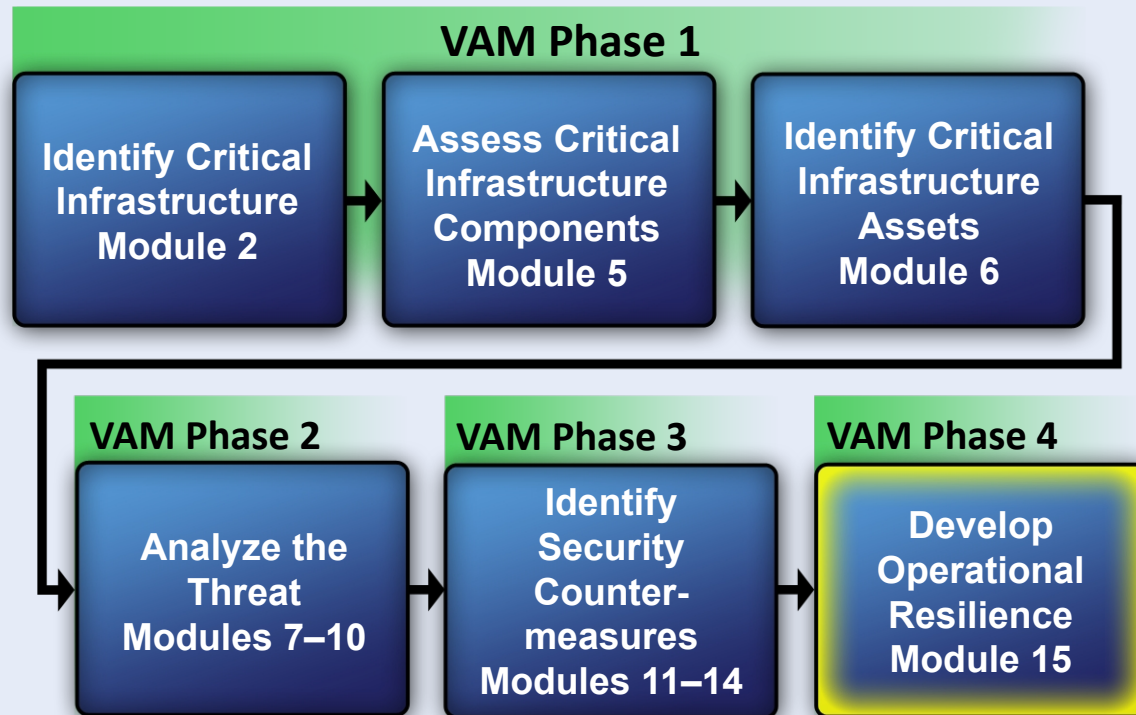


Module Objective

- **By the end of this module, you will be able to describe how to apply operational resilience strategies for your country after a terrorist attack, natural disaster, or other threat**



Course Map Diagram



Terms Related to Critical Infrastructure Resilience

- **Resilience — to prepare and adapt, withstand and recover rapidly**
- **Collaboration — to work together to achieve shared goals**
- **Protection — the capabilities necessary to secure the homeland**



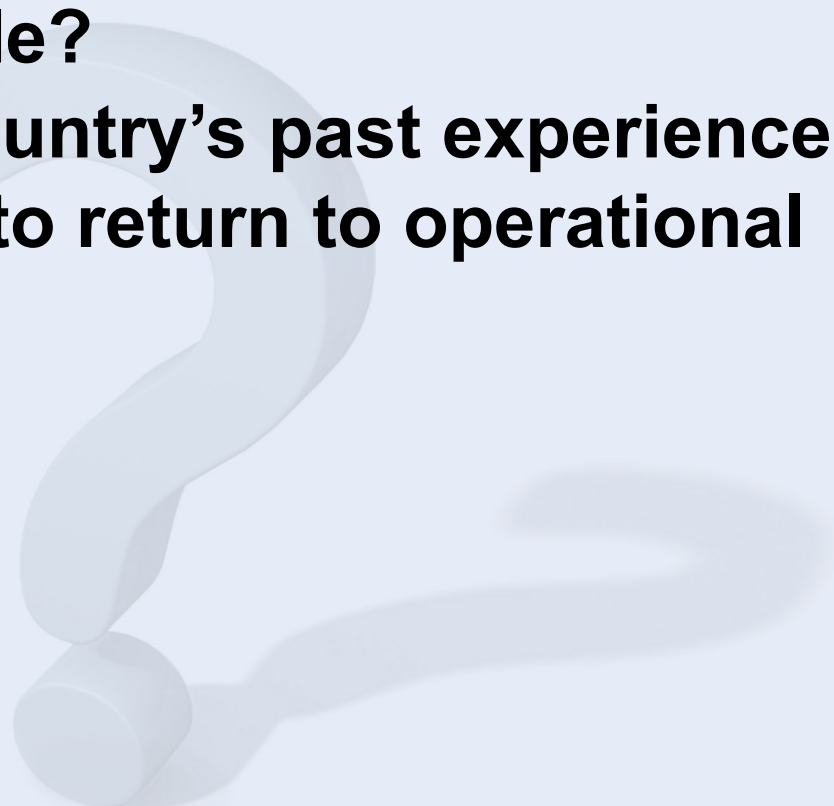
Resilience in Your Country (1 of 2)

- **What strategies does your country currently have for resilience?**
- **What types of capabilities does your country have to protect against threats and natural disasters?**



Resilience in Your Country (2 of 2)

- **What type of preparations for resilience has your country made?**
- **Based on your country's past experience, how long has it taken to return to operational status?**



Critical Infrastructure Security and Resilience Policy Example

- **High-level national directive to serve as a template for other sectors; may include:**
 - **Introduction**
 - **Policies**
 - **Roles and responsibilities**
 - **Strategic imperatives**
 - **Innovations and research and development**
 - **Actions to implement the directive**



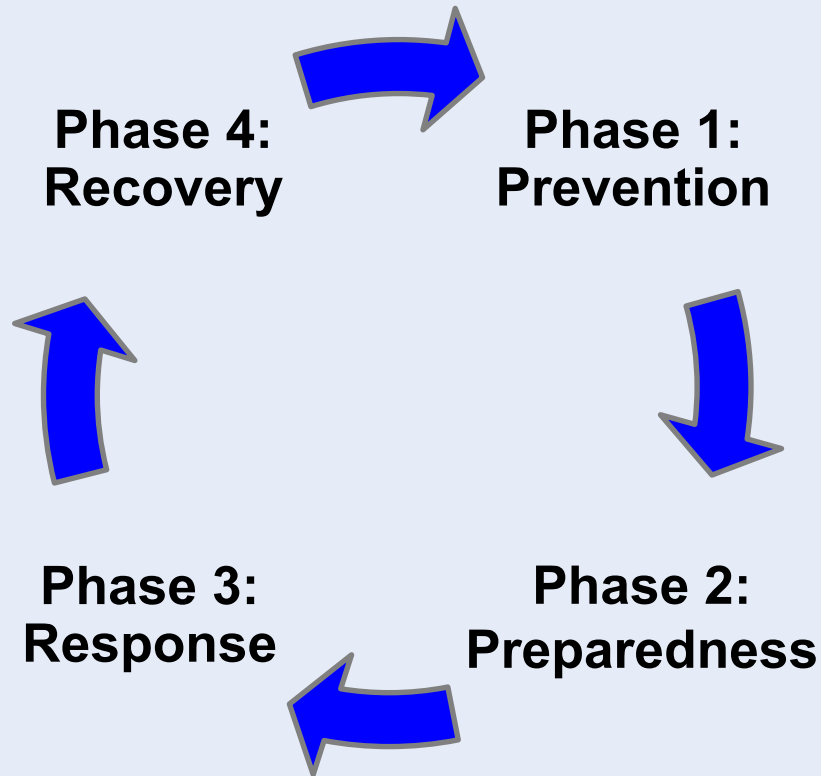
Critical Infrastructure Security Introduction (1 of 3)

- **Requires coordinated efforts**
- **Includes both physical space, cyberspace, and multinational ownership**
- **Requires managing risk and determining effective strategies for resilience**
- **Helps rapid recovery**



Critical Infrastructure Security Introduction (2 of 3)

Requires security systems integration across:



Critical Infrastructure Security Introduction (3 of 3)

- **Requires all stakeholders to share policies and action**
- **Compels national governments to strengthen internal security and resilience**



Critical Infrastructure Resilience Policies (1 of 2)

- **Governments and stakeholders work to:**
 - Take proactive steps to manage risk
 - Consider all hazards to security, economy, health, and safety
 - Integrate policies to reflect interdependencies
 - Identify critical energy and communication systems
 - Protect all information in compliance with law



Critical Infrastructure Resilience Policies (2 of 2)

- **Reduce vulnerabilities**
- **Minimize consequences**
- **Identify and disrupt threats**
- **Hasten response and recovery efforts**



Roles and Responsibilities (1 of 2)

- **Minister or secretary of national security and resilience organization:**
 - Provide high-level strategic guidance
 - Promote and coordinate national unity
 - Evaluate national capabilities and analyze threats
 - Identify security and resilience functions
 - Develop a national plan and report effectiveness



Roles and Responsibilities (2 of 2)

- **Sector-specific agencies:**
 - Unique characteristics, operating models, and risk profiles
 - Institutional knowledge and specialized expertise
 - Knowledge of specific recovery and resilience needs



Roles and Responsibilities of Other Stakeholders

- Finance and contracts division
- Human resources division
- Information technology division
- Legal division
- Operational area specialists
- Security operations team



Source: Ready.gov



Three Strategic Imperatives (1 of 3)

- 1. Refine and clarify functional relationships across the government to advance the national unity of effort to strengthen critical infrastructure security and resilience:**
 - Guided by a national plan
 - Informed by expertise, experience, capabilities, and responsibilities of all stakeholders



Three Strategic Imperatives (2 of 3)

2. Enable efficient information exchange by identifying baseline data and systems requirements for the government:

- Timely exchange
- Situational awareness capability
- System requirements
- Respect of privacy and civil liberties



Three Strategic Imperatives (3 of 3)

3. **Implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure**



Innovation and Research and Development (1 of 2)

- **Align research and development activities**
- **Research innovations in construction and cybersecurity methods**
- **Enhance research on various scenario responses**



Innovation and Research and Development (2 of 2)

- **Facilitate incentives for investments in designs**
- **Prioritize efforts to implement critical infrastructure security and resilience policies**



Planning for Resilience

- Adequacy and deficiency
- Timely recovery
- Policy applies across all sectors
- Each sector responsible for implementing in their area



Gap Analysis Process (1 of 2)

- The steps that security managers use to compare the actual performance of an existing physical protection system with its potential performance
 - Does the system design meet requirements?
 - Does the system meet expected outcomes?



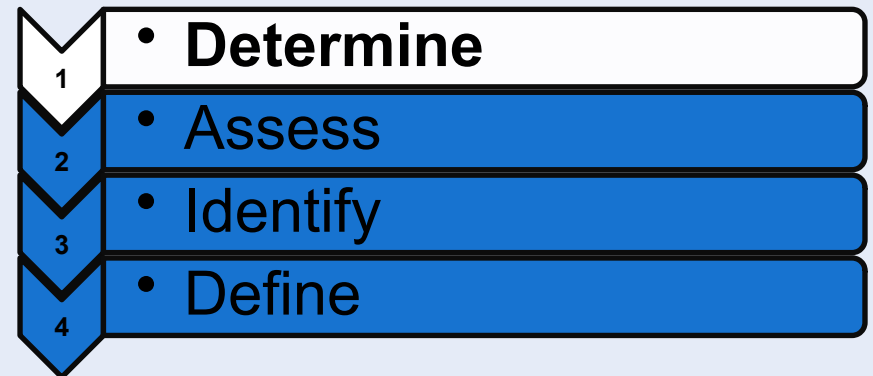
Gap Analysis (2 of 2)

- **Step 1: Determine expected standard requirements**
- **Step 2: Assess existing performance levels**
- **Step 3: Identify gaps**
- **Step 4: Define risk management plan**



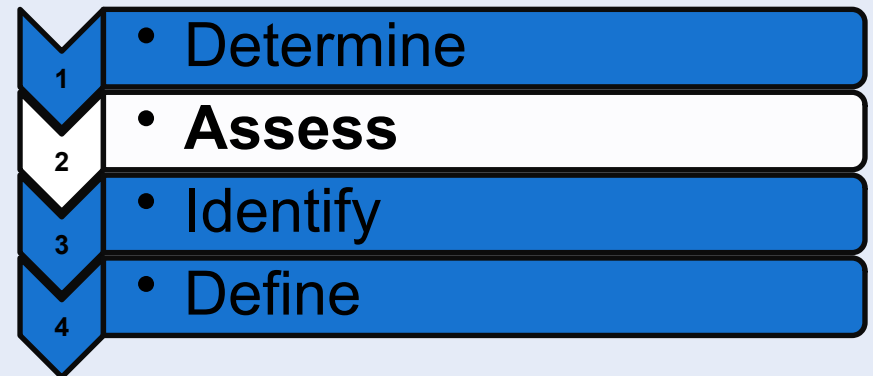
Step 1: Determine Expected Standard Requirements

- Identify the performance requirements and expectations for a specific security countermeasure



Step 2: Assess Existing Performance Levels

- Decide how the existing performance levels will be measured



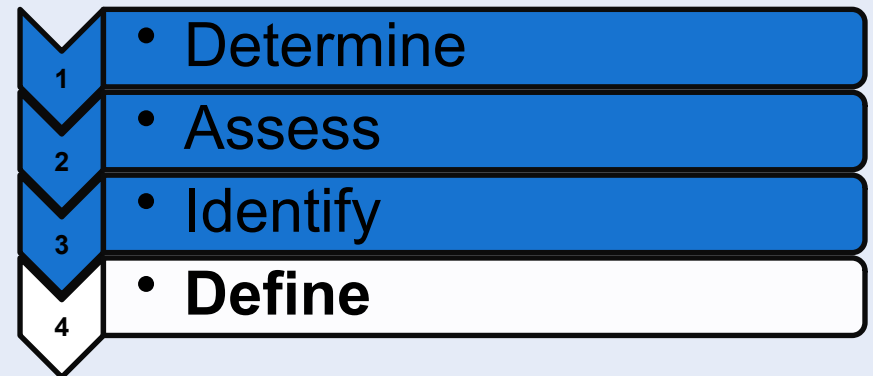
Step 3: Identify Gaps

- **Determine what areas (risks) do not meet the pre-established performance standards or expectations**



Step 4: Define Risk Management Plan

- **Determine the best countermeasures to manage the risks**



Gap Analysis

Process Scenario Activity

Refer To:

Handout 15.1



- **Purpose:** to identify the steps of the gap analysis process in a given scenario
 - **Duration:** 40 minutes (30-activity; 10-discussion)
 - **Group composition:** table groups
 - **Debrief:** large-group discussion



Proposed Security Countermeasures

- Formulate how the proposed countermeasures will resolve the gap
- Prioritize the recommendations from security inspection and validation report:
 - Importance and vulnerability
 - Greatest risks are highest priority



Discussion Questions

- In your experience, which type of security countermeasure is the most consistently well planned and budgeted? Why?
- In your experience, which type of security countermeasure is the least planned and budgeted? Why?



Develop National Resilience Plan (1 of 2)

- **National security and resilience organization and minister must develop the national plan that each sector will use as a model**
- **Integrate:**
 - **Prevention**
 - **Preparedness**
 - **Response**
 - **Recovery**



Develop National Resilience Plan (2 of 2)

- **Stakeholders, government agencies, and advisory groups must coordinate together to:**
 - **Assess gaps in current conditions**
 - **Evaluate effectiveness of current practices**
 - **Develop expected outcomes and performance relative to resilience**
 - **Prepare plan of prioritized recommendations for high-level national policies, procedures, and actions**



TeachBack Moment



- **What are the definitions of resilience, collaboration, and protection as they relate to critical infrastructure resilience?**
- **What are the important elements of a critical infrastructure security and resilience directive?**
- **What are the necessary actions to develop an operational resilience plan?**



Threaded Exercise — National Ministries Building Part 8

Refer To:

Threaded Exercise
Workbook Part 8



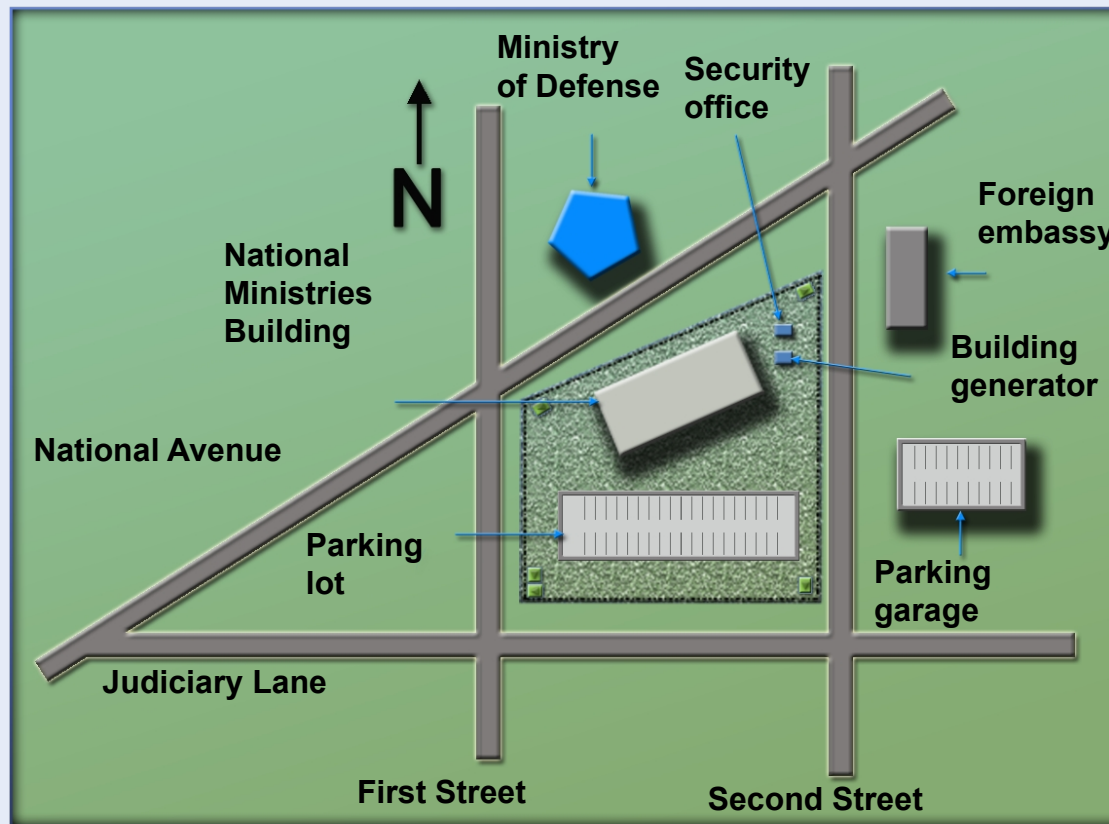
- **Purpose:** to present four main points of an operational resilience plan statement that includes recommended security countermeasures for a given scenario
 - **Duration:** 70 minutes (40-preparation; 30-debrief)
 - **Group composition:** table groups
 - **Debrief:** group presentations and facilitator feedback



National Ministries Building Complex Map

Refer To:

Threaded Exercise
Workbook Part 8



Module Summary

- **Critical infrastructure resilience**
- **Critical infrastructure security and resilience directive example**
- **Planning for resilience**

