Start Grow Manage Exercise Briefing

Nicholas Zink

October 17, 2024

Welcome

Nicholas Zink
Outreach Coordinator
Cybersecurity & Infrastructure Security Agency (CISA)
Region 2: NY, NJ, Puerto Rico, & U.S.V.I.

Exercise Overview

CISA offers cybersecurity and physical security exercises at **no cost** to enhance security and resilience of critical infrastructure owner/operators. These exercises provide stakeholders with mechanisms to examine plans and procedures, identify areas for improvement, share best practices, and enhance preparedness against cyber-attacks and physical security incidents.

Discussion-Based Exercise Types:

- **Seminar:** Provide a common framework of understanding
- **Workshop:** Increased participant interaction with a focus on achieving or building a product
- **Tabletop Exercise (TTX):** Facilitate conceptual understanding, identify strengths and areas for improvement, and/or achieve changes in perceptions
- **Game:** Simulation of operations that explore the consequences of player decisions and actions

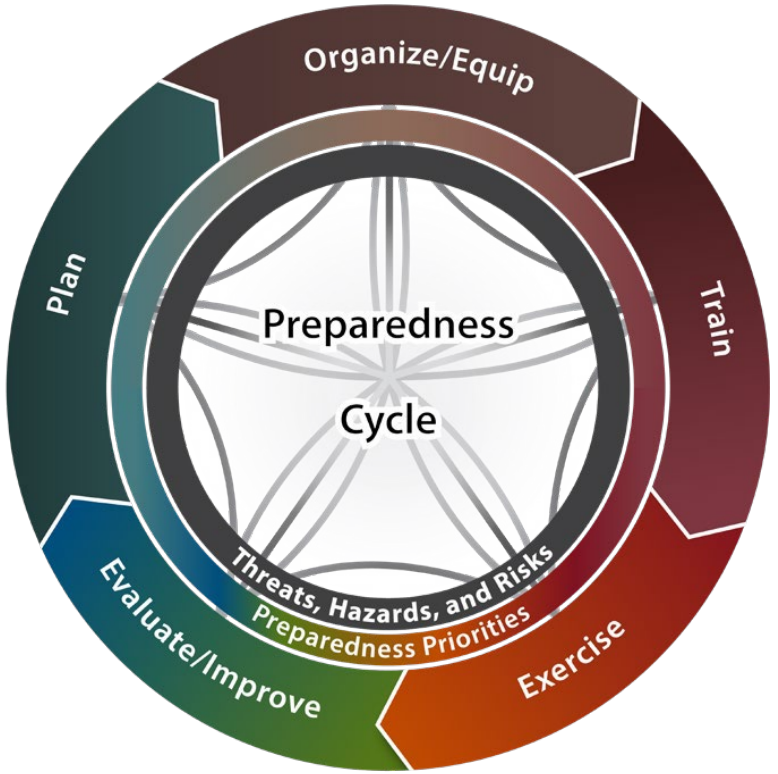
Operations-Based Exercise Types:

- **Drill:** Coordinated, supervised activity to validate a specific function or capability
- **Functional Exercise (FE):** Validate and evaluate capabilities, multiple functions and/or sub-functions under crisis conditions
- **Full-Scale Exercise (FSE):** Focus on implementing and analyzing the plans, policies, and procedures that may have been developed in discussion-based exercises and honed during previous, smaller exercises

Integrated Preparedness Cycle

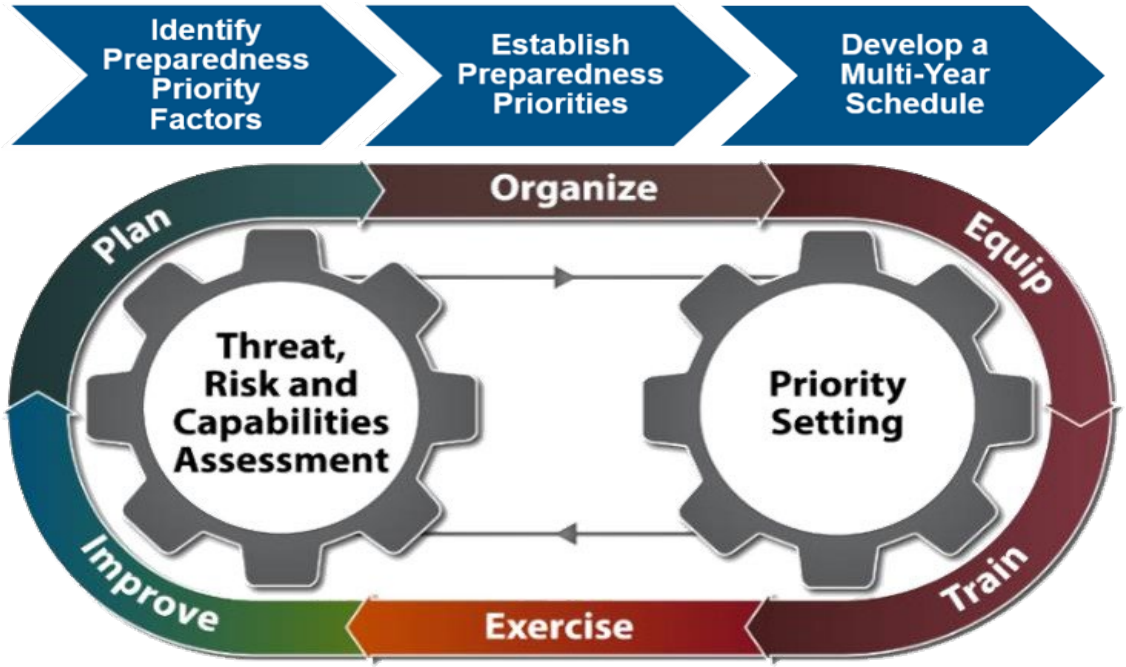
- The **Integrated Preparedness Cycle** of planning, organizing/equipping, training, exercising, and evaluating/improving is a continuous process that ensures the regular examination of ever-changing threats, hazards, and risks

- This cycle provides a continual and reliable approach to support decision making, resource allocation, and measure progress toward building, sustaining, and delivering capabilities based on an organization's threats, hazards, and risks.



Integrated Preparedness Cycle Planning

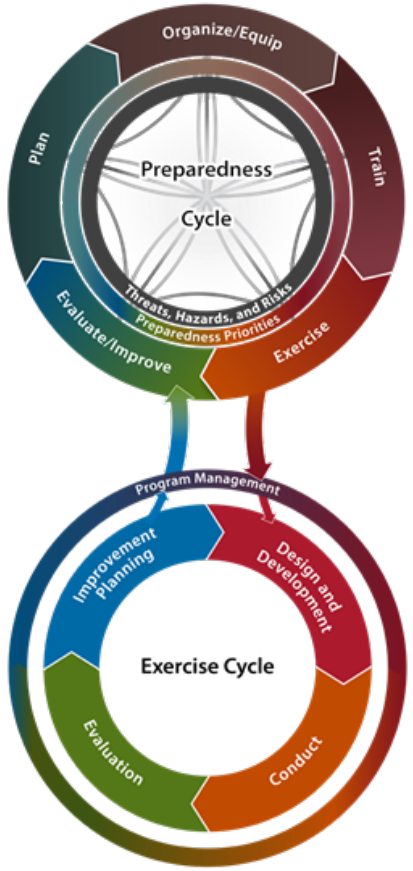
The purpose of the **Integrated Preparedness Cycle Planning** is to consider the range of preparedness activities within the Integrated Preparedness Cycle, and along with the guidance provided by senior leaders, identify and set preparedness priorities, and schedule preparedness activities for the multi-year Integrated Preparedness Plan.



Homeland Security Exercise and Evaluation Program

- **Homeland Security Exercise and Evaluation Program (HSEEP)** uses a common approach for planning, conducting, and evaluating individual exercises.

- The exercise phase of the Integrated Preparedness Cycle is linked to the program management process and starts the design and development of individual exercises within HSEEP. Multi-year preparedness priorities guide the exercise program to produce quality individual exercises. These individual exercises are used to build, sustain, and deliver capabilities.



Tabletop Exercise Planning Process

- Design and development
  - Concept & Objectives Meeting (C&O)
  - Initial Planning Meeting (IPM)
  - Midterm Planning Meeting (MPM)
  - Final Planning Meeting (FPM)
  - *In-Progress Review (IPR) as necessary*
- Conduct
- After Action
- Improvement Planning & Support

* This is generally a 3–4-month process

Exercise Objectives

- Exercise objectives should incorporate senior leaders' intent; exercise participants' plans, policies, and procedures; operating environment; corrective actions from previous exercises and real-world incidents; and desired outcomes.
- The exercise planning team should select a reasonable number of objectives to facilitate effective scenario design, exercise conduct, and evaluation.
- An objective should be specific, measurable, achievable, relevant, and time-bound (SMART).

SMART Guidelines for Exercise Objectives	
Specific	Objectives should address the five Ws- who, what, when, where, and why. The objective specifies what needs to be done with a timeline for completion.
Measurable	Objectives should include numeric or descriptive measures that define quantity, quality, cost, etc. Their focus should be on observable actions and outcomes.
Achievable	Objectives should be within the control, influence, and resources of exercise play and participant actions.
Relevant	Objectives should be instrumental to the mission of the organization and link to its goals or strategic intent.
Time-bound	A specified and reasonable timeframe should be incorporated into all objectives.

Participant Selection

Considerations for Participant Selection

- Internal:
  - Core Team/Business Group
  - Supporting/Supported Business Groups
  - Decision Makers
  - Communications Team
  - Legal/HR/Corporate Security
- External:
  - Vendors/Third Party Contractors
  - Public Sector Entities
    - State/Local
    - Federal
  - Non-Profits/Non-Governmental Organizations

Effective Exercise Guidelines

- Exercise should be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Encourage participants to respond to the scenario using their knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from their training and experience.
- Decisions made in an exercise are not precedent setting and may not reflect your organization's final position on a given issue. Exercises are an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions or recommended actions that could improve organizational efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

After-Action Reports

- The After-Action Report (AAR) is a document that generally includes an exercise overview, analysis of capabilities, and a list of corrective actions. The length, format, and development timeframe of the AAR depend on the exercise type and scope.
- The observations developed for the AAR should be categorized as either **strengths** or **areas for improvement**. Observations do not have to be lengthy to be impactful. A strongly written observation includes a clear and direct statement of the issue identified, a brief description of the analysis, and the impact or result of the issue.
- **Area for Improvement** observations should include:
  - Description
  - Analysis
  - Options for consideration

CISA Exercise Products

CISA Tabletop Exercise Package (CTEP) also known as "tabletops in a box", are designed to assist stakeholders in conducting their own customizable exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of cybersecurity and physical security threat scenarios. With over 100 CTEPs available, including CTEPs designed specifically for the election infrastructure subsector, stakeholders can easily find resources to meet their specific exercise needs.

CISA Tabletop Exercise Packages | CISA

CISA Tabletop Exercise Package (CTEP)

Cybersecurity Scenarios

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Physical Security Scenarios

Active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aircraft systems (UASs), and many more. There are also CTEPs that are geared towards specific industries or facilities to allow for discussion of their unique needs.

Cyber-Physical Convergence Scenarios

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

CTEP Documents

Leverage pre-built templates to develop a full understanding of roles and responsibilities for exercise planners, facilitators / evaluators, and participants. Additionally, the documentation includes templates for the initial invitation to participants, a slide deck to use for both planning meetings and conduct, a feedback form to distribute to participants post-exercise, and an After Action Report. In conjunction with selecting one of the above situation manuals, your exercise planning team will be able to fully develop your own tabletop exercise and update information sharing processes; emergency response protocols; and recovery plans, policies, and procedures.

- Emergency Services Sector CTEP Situation Manual (DOCX, 5.43 MB)
- Federal Distributed Denial of Service (DDoS) CTEP Situation Manual (DOCX, 5.77 MB)
- Healthcare and Public Sector CTEP Situation Manual (DOCX, 4.40 MB)
- Industrial Controls CTEP Situation Manual (DOCX, 3.74 MB)
- K-12 Schools CTEP Situation Manual (DOCX, 3.60 MB)
- Local Governments CTEP Situation Manual (DOCX, 4.07 MB)
- Maritime Ports CTEP Situation Manual (DOCX, 4.87 MB)
- Ransomware CTEP Situation Manual (DOCX, 4.12 MB)
- Ransomware Third Party Vendor CTEP Situation Manual (DOCX, 3.16 MB)
- Vendor Phishing CTEP Situation Manual (DOCX, 3.64 MB)

CTEP Situation Manual

TLP:WHITE

[Enter Client Name]

CISA Tabletop Exercise Package – Industrial Controls

<Exercise Date>

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

TLP:WHITE

TLP:WHITE

<Exercise Title>
Situation Manual

Table of Contents

TLP:WHITE

Exercise Resources

- CISA CTEP: CISA Tabletop Exercise Packages | CISA
- HSEEP: Homeland Security Exercise and Evaluation Program | FEMA.gov
- FEMA EMI Training: EMI | National Standard Exercise Curriculum | HSEEP (fema.gov)
- Business Continuity in a Box: Business Continuity in a Box | CISA
- CISA Continuity Planning: Continuity Planning Suite | CISA

Questions

Nicholas Zink
Outreach Coordinator
CISA Region 2: NY, NJ, PR, & USVI
Cell: (202) 923-6093
Nicholas.Zink@cisa.dhs.gov

Phillip Milbouer
Cyber Training & Exercise Coordinator
CISA Region 2: NY, NJ, PR, & USVI
Cell: (771) 217-1421
Phillip.Milbouer@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY