Conducting Exercises to Improve Incident Response
ITU-D 2021 Global CyberDrill

Olivier CALEFF on behalf of FIRST

October 11th, 2021 - online

Copyright

FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Course Goals

After the full 2-days course, attendees are able to:

- Plan exercise programs and projects
- Marshal people and resources that contribute to an organization's strategic objectives
- Create exercise programs that:
  - Demonstrate
  - Train
  - Increase proficiency
  - Assess
  - Certify

- ***Today, attendees will be presented with the best and most important parts***

Module 1: Defining Exercises and Their Organizational Benefits

- At the end of this module, you will be able to:
  - Define and describe an incident response readiness program and its benefits
  - Articulate the role of exercises in improving an incident response readiness program
  - Detail how exercises can directly benefit an organization

Incident Response Readiness Program Definition

- **Multiyear program** to periodically validate preparedness for unexpected events, emergencies and catastrophes

- It provides:
  - **Roadmap** for ensuring a viable capability and outline of organization's approach to maintaining plans, as well as enhancing and managing the capability
  - Program to ensure **continual** enhancement and adequacy of emergency plans, policies and procedures
  - Umbrella program to manage periodic IT preparedness projects
  - Steps, resources, and processes to take to ensure and improve readiness

Benefits of an Incident Response Readiness Program

- Offer a **coordinated approach** to building and maturing the **organization’s capabilities**
- Identify **deficiencies, weaknesses, and risks**, and define and execute improvement plans to increase an organization’s resilience
- Ensure that **staff are fully prepared and capable of responding** to incidents by efficiently following business continuity and disaster-recovery procedures
- Increase **cooperation and teamwork** across the organization to more efficiently respond to cyberattacks
- **Identify interdependencies and exchange best practices** with other organizations

Comprehensive Incident Response Policy

- An incident response policy helps ensure that your organization is ready to respond to incidents
- An incident response readiness program should include a policy that outlines the **organization's internal and external requirements** that forms the framework for the purpose and objectives of the program
- Prepare for, respond to, manage, and recover from disasters affecting its mission

What Do We Mean by Exercise?

- Common types of IT plans:
  - Contingency plans
  - Incident response plans

- The major types of events used to maintain these plans:
  - Tests: using quantifiable metrics to validate the operability of a system or system component
  - Training: informing personnel of their roles and responsibilities within a particular IT plan

Exercises: a simulation of an emergency designed to confirm the viability of one or more aspects of an IT plan.

Exercise Purposes

Demonstrate: Show how the situation could be handled

Train: Create a playbook on how to handle events
in an organization

Increase proficiency: Allow people in the organization to practice response tasks

Assess: Analyze whether the current processes are still
valid or need to be updated

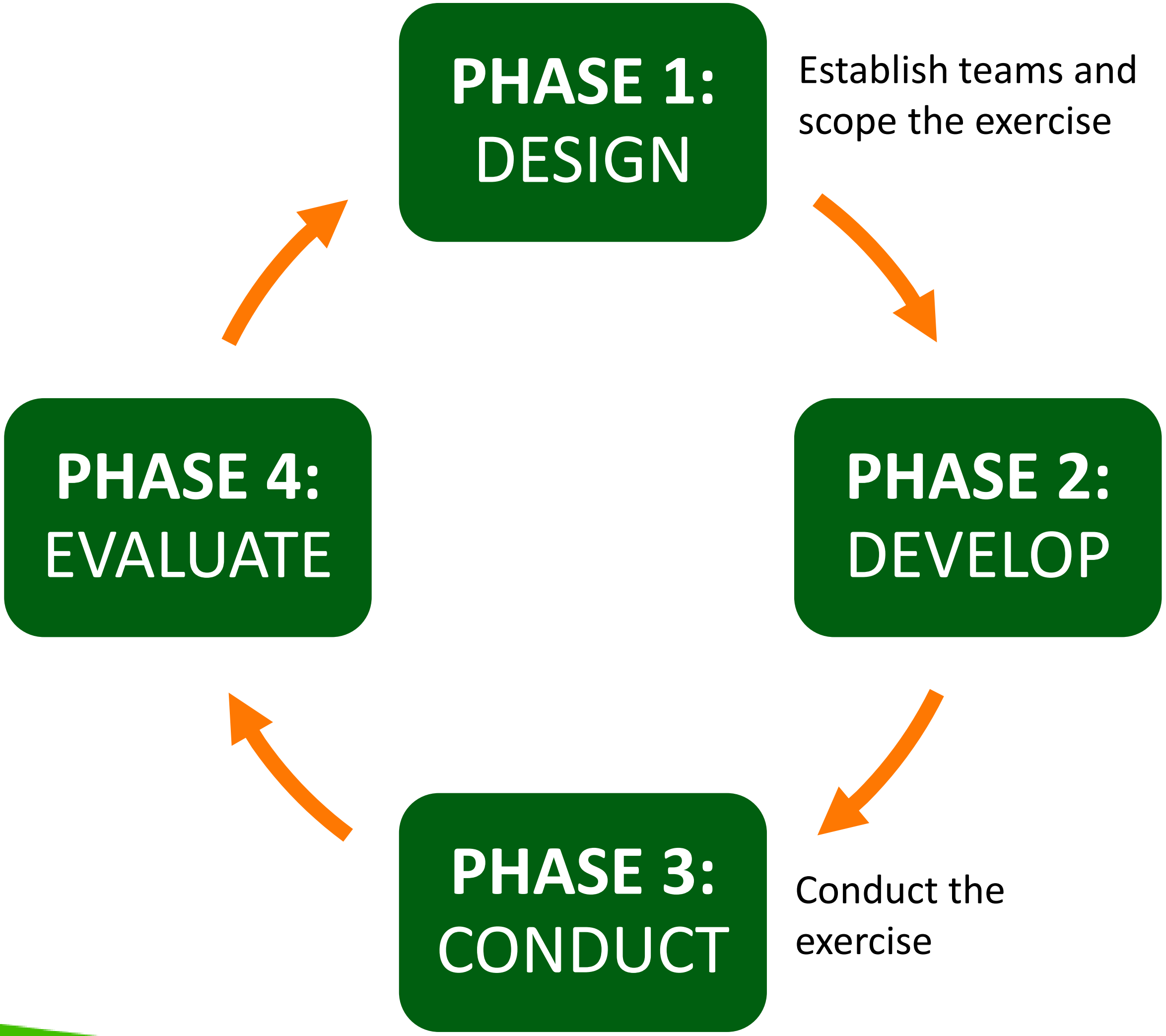
Certify: Demonstrate the organization’s compliance

Exercises must NOT be used for performance evaluation/assessment of individuals

Integrating Exercises in a Program Plan

- Plan out 3–5 years but anticipate changes along the way
- Progressively move toward more complex exercises
  - Starting point based on organization’s capabilities
  - Avoid rushing into full-scale exercise resulting in wasted resources
- Best practices:
  - **Address known shortfalls prior to start of exercises**
  - **Identify expected outcomes and distribution methodology early**
  - **Provide regular, frequent updates of exercise trends**
- Exercises dictated by organizational requirements

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation of the exercise

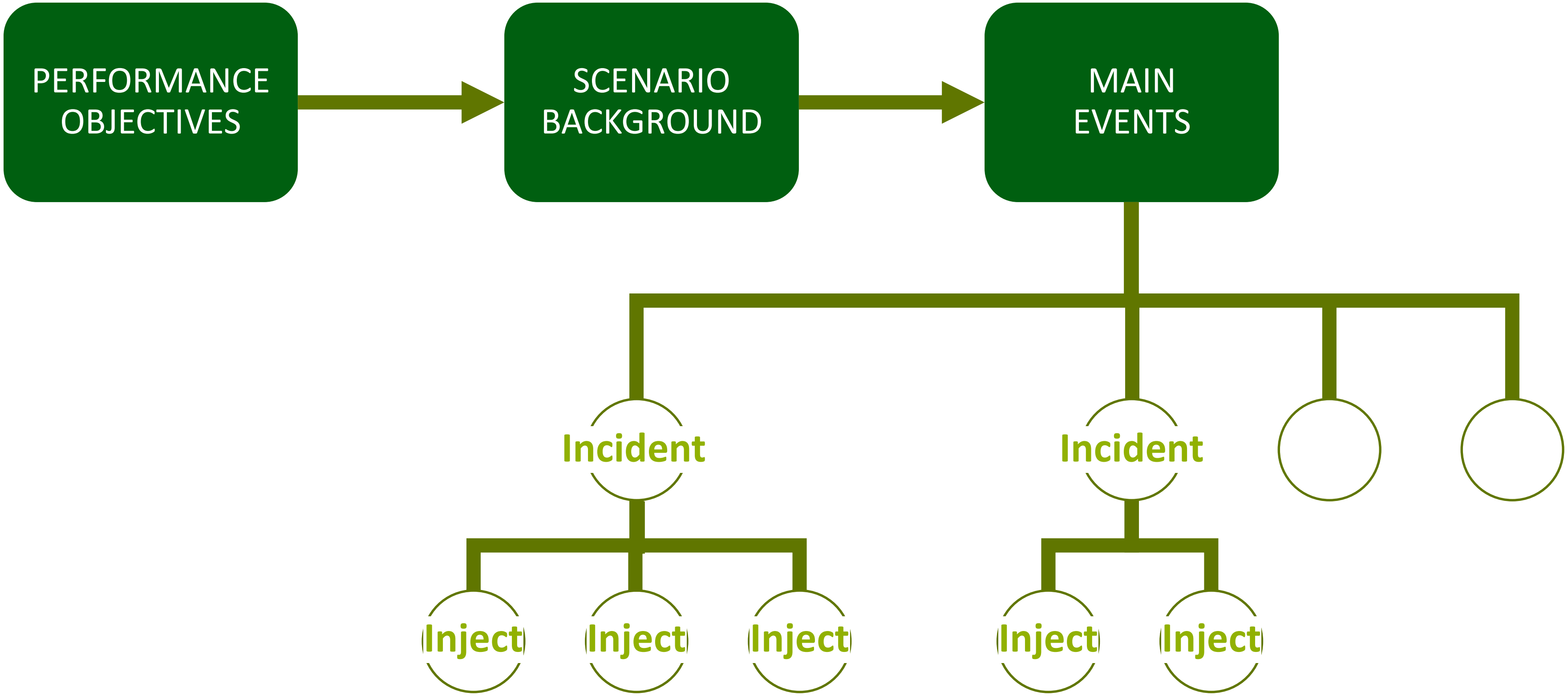
PHASE 3: CONDUCT

Conduct the exercise

PHASE 4: EVALUATE

Document lessons learned from the event

Well-Designed Exercises Central to Incident Response Readiness Program

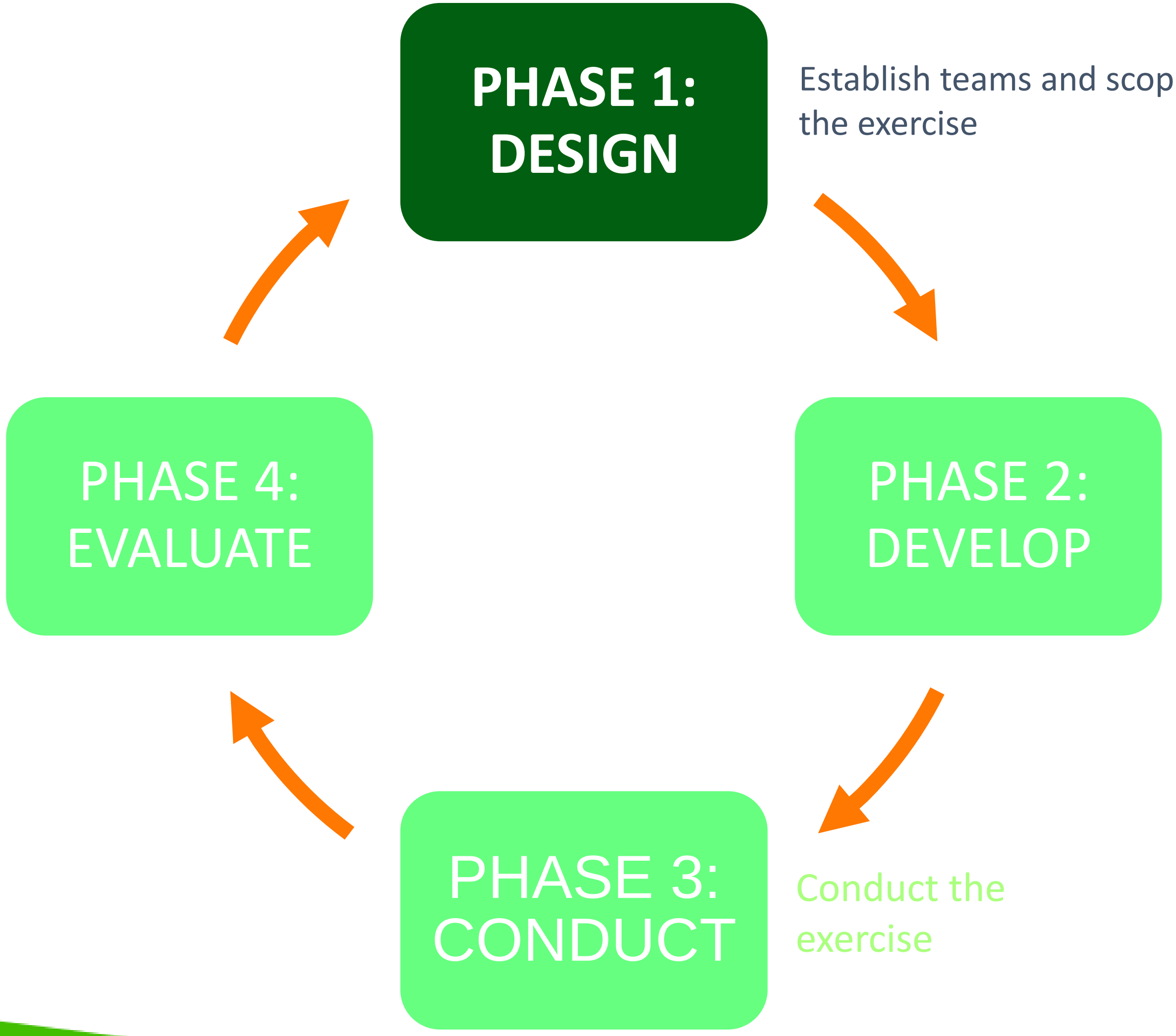


Module 2: Determining Exercise Roles

At the end of this module, you will be able to:

- Define the need for upper management support in creating an exercise program
- Outline **roles and responsibilities** involved in creating exercises

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation of the exercise

PHASE 3: CONDUCT

Conduct the exercise

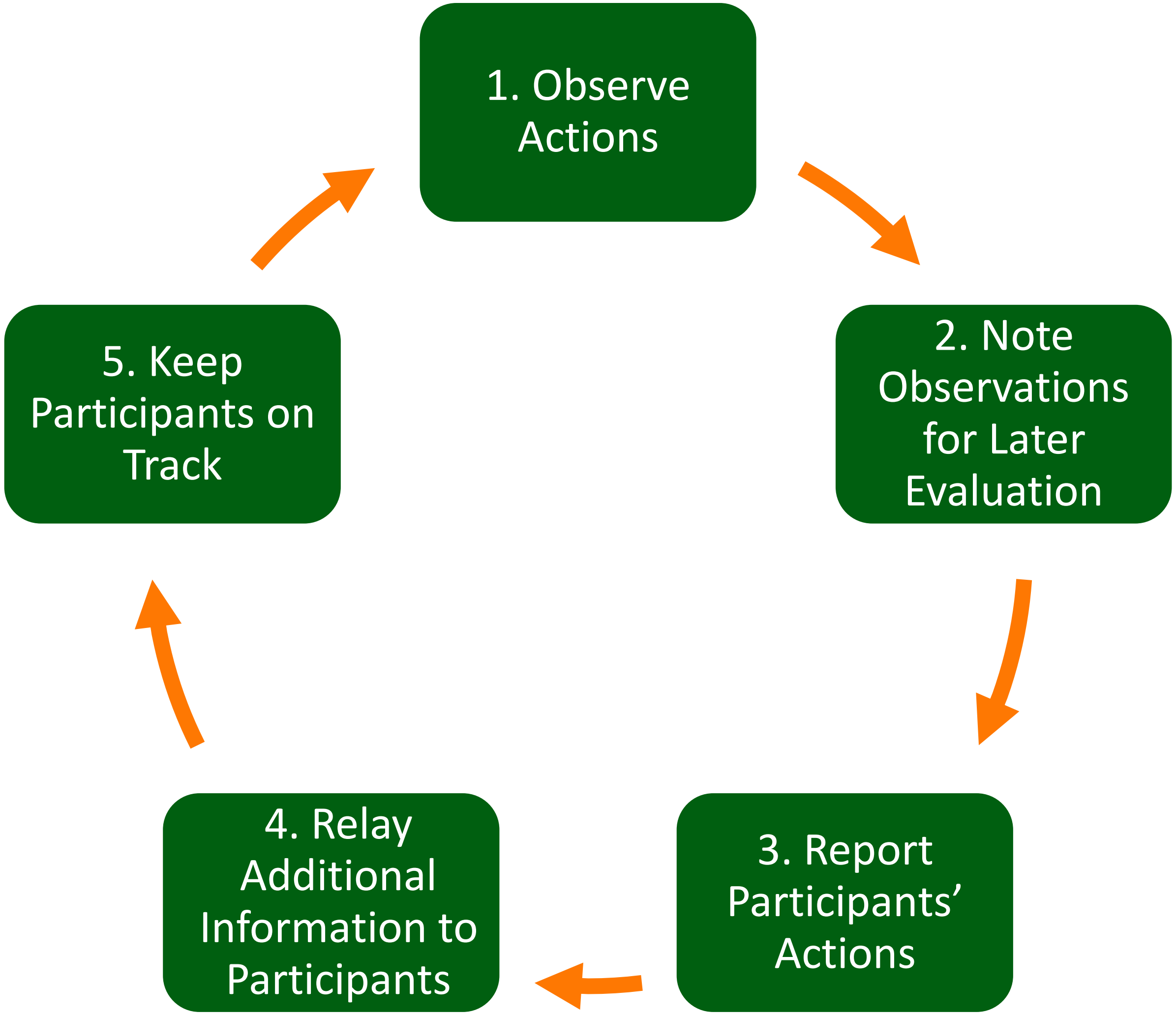
PHASE 4: EVALUATE

Document lessons learned from the event

Roles Involved in Exercises

- *Executive sponsor*
- *Program coordinator and core planning team*
- *Exercise facilitators*
- *Data collectors*
- Participants
  - **Players**
  - **Observers**
  - **VIPs**

Exercise Facilitator Process



1. Observe Actions

2. Note Observations for Later Evaluation

3. Report Participants’ Actions

4. Relay Additional Information to Participants

5. Keep Participants on Track

Module 3: Establishing Exercise Audiences and Objectives

- At the end of this module, you will be able to:
  - Define the factors in developing exercise priorities
  - Determine how to establish the training audience and scope for an exercise, based on a needs analysis

Three Pillars of Exercise Creation

- **Training audience**
- **Objectives**
- Modalities

Determine Your Audience

- Determine how to establish the audience and scope for the exercise:
  - What are the strategic issues and priorities for the organization and what will satisfy these needs?
  - Is person or team with direct responsibility for the organization’s IT planning capability on board with this course of action?
  - Conduct a needs assessment

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: Who is the audience for the exercise? Who can benefit the most? Who has the most to improve? What roles will staff play?

Possible outcomes: Audience better established; staff performance evaluated so exercise program can grow skills in all parts of the organization; facilitators and data collector roles established

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: What will the exercise program look like? What is its scope? What are its overall objectives? What legal, regulatory, and compliance objectives need to be taken into account?

Possible outcomes: An exercise program with scope and objectives fitting the needs of the organization

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: Why embark on an exercise program? What can the organization gain from doing so? What does it risk?

Possible outcomes: Clear reasons for implementing the exercise program; a sense of organizational benefit and risk management issues and considerations; primary metric definition

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: Where will the exercise take place? Onsite or away from the usual office setting? Who is responsible for coordinating site setup?

Possible outcomes: A site booked for the exercise and one person responsible for coordinating the site setup

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: Will the exercise take place on a particular day or two away from usual work? Or over a week for a portion of each work day?

Possible outcomes: The exercise set on the calendar, with deadlines and responsibilities taken into consideration

Needs Assessment

Category	Questions	Possible outcomes
Who		
What		
Why		
Where		
When		
How		

Questions: What are the logistics for putting the exercise together? What needs to happen organizationally to support the exercise coming together?

Possible outcomes: Logistics set for the exercise

Tools To Support Exercise Priorities

- Support tools to help exercise programs succeed:
  - Spreadsheet programs
  - Data-collection tools
  - Communications monitoring and analysis tools
  - Evaluation tools
  - Cyber ranges and virtual environments

Module 4: Deciding on the Exercise Type

- By the end of this module, you will be able to:
  - Identify the two main types of exercises
  - Determine how different types of exercises fit with different organizational needs
  - Establish the role of testing in exercise creation
- 3 pilars
  - Training audience
  - Objectives
  - **Modalities**

Types of Exercises

- **Discussion-Based Exercises:** Familiarize players with plans, policies, agreements, and procedures, with focus on strategic, policy-oriented issues.
- **Operations-Based Exercises:** Validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps

1 - Exercises

Discussion-based exercises include:

- Seminars
- Workshops
- Tabletop exercises (TTXs)
- Games

2017Geneva, FIRST WS on IR for Policy makers. Image S. Droz

Seminars (1)

- Orient participants to authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas
- Valuable for entities that are developing or making major changes to existing plans or procedures
- Helpful when attempting to assess or gain awareness of the capabilities of interagency or inter-organizational operations

Workshops (2)

- Similar to seminars, but participant interaction is increased, and the focus is placed on achieving or building a product
- Products emerging from a workshop can include procedures, plans, agreements
- Should have clearly defined objectives, products, or goals, and should focus on a specific issue

Tabletop Exercises (3)

- **A tabletop exercise (TTX) is intended to generate discussion of various issues surrounding a hypothetical, simulated emergency**
  - To enhance general awareness, validate plans and procedures, rehearse concepts
  - To assess the types of systems needed to guide incident response
- Aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions
- Issues discussed in depth, collaboratively examining areas of concern and solving problems
- All participants should be **encouraged to contribute** to the discussion and be reminded that they are making decisions in a no-fault environment

Tabletop Exercises (3)

TTXs can range from basic to complex:

- Basic TTX: the scenario is presented and remains constant - describes an emergency and brings participants up to the simulated present time
- More advanced TTX: play advances as players receive pre-scripted messages, or injects, that alter the original scenario

Games (4)

- Simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedures designed to depict an actual or hypothetical situation
- Explore the consequences of player decisions and actions
- Useful for validating plans and procedures or evaluating resource requirements
- During game play, decision-making may be either slow and deliberate or rapid and more stressful, depending on the exercise design and objectives

2 - Operations-Based Exercises

- Operations-based exercises include:
  - Drills
  - Functional exercises (FEs)
  - Full-scale exercises (FSEs)

Drills (1)

- Coordinated, supervised activity usually employed to validate a specific function or capability in a single agency or organization
- Commonly used to provide training on new equipment, validate procedures, or practice and maintain current skills
- Can be used to determine whether plans can be executed as designed, to assess whether more training is required, or to reinforce best practices
- For every drill, clearly defined plans, procedures, and protocols need to be in place

Functional Exercises (2)

- Functional exercises (FEs) are designed to validate and evaluate capabilities, multiple functions and/or sub-functions, or interdependent groups of functions
- Typically focused on exercising plans, policies, procedures, and staff members involved in management, direction, command, and control functions
- Events are projected through an exercise scenario in a realistic, real-time environment with movement of personnel and equipment usually simulated
- Decide whether to use fictitious or real entities in your exercises

Full-Scale Exercises (3)

- Full-scale exercises (FSEs) are typically the most complex and resource-intensive type of exercise
- Involve multiple agencies, organizations, and/or jurisdictions and validate many facets of preparedness
- Often include many players operating under cooperative systems
- Events are projected through an exercise scenario with event updates that drive activity at the operational level in a real-time, stressful environment that is intended to mirror a real incident
- Simulates reality by presenting complex and realistic problems that require critical thinking, rapid problem solving, and effective responses by trained personnel
- The level of support needed to conduct an FSE is high

Tests

- Tests are evaluation tools that use quantifiable metrics or expected outcomes to validate the operability of one or more IT systems or system components identified as critical in an IT plan
- Tests can take several forms:
  - Component testing of hardware or software components
  - System testing of complete systems to evaluate each system's compliance with specified requirements
  - Comprehensive testing of all systems and components that support an IT plan

Tests: Results and Outcomes

- The core planning team team should define the tests that will be conducted and specify the expected results or outcomes
- The test plan could consist of a series of smaller individual tests each designed to examine a part of the component, system, or group of components and systems being tested
- The objectives for each test should be to measure, check, or verify whether the component, system, or group of components and systems satisfies its intended purpose and functions adequately
- Examples include restoring a backup, moving a server from one room to another, upgrading or patching operating systems or applications, and more

Tests: Results and Outcomes

Specialized testing tools might include:

- Specialized software or hardware tools (e.g., network sniffers, vulnerability scanners)
- Measurement and recording devices (e.g., stopwatches, cameras, video recorders)
- Checklists used to measure adherence to defined processes and procedures
- Items needed by the test team for logistical support (e.g., radios, cell phones, badges)

Module 5: Coordinating Exercise Logistics

By the end of this module, you will be able to:

- Map your exercise program to the four segments of the exercise life cycle
- Put together a logistics plan for the exercise program

Exercise Life Cycle

Identifying

Organizer

- Identify the measures and groups to test
- Choose the exercise type, size, geographic scope
- Choose high-level scenario options
- Identify key stakeholders

Planning

Organizer

- Acquire financial resources

Organizer & Planners

- Select appropriate location
- Set a schedule
- Conduct meeting to introduce subject and build consensus
- Creative realistic scenario
- Assign roles
- Set objectives for evaluation

Planners

- Train monitors, moderator, others, to perform their duties during the exercise
- Invite desired observers
- Decide on a media policy
- Notify media, if relevant

Conducting

Planners

- Ensure all role-players are prepared for their duties
- Train participants

Moderator/Director

- Execute the scenario and injects as guided by moderator/director

Monitors

- Observe participants and note actions/decisions
- Report back to the moderator/director

Participants

- Simulate procedures

All

- Support evaluation process through questionnaires or other tasks

Evaluating

All

- Complete questionnaires and debriefings
- Evaluators
- Collect required information
- Prepare evaluation for individual stakeholders
- Prepare evaluation for all stakeholders
- Prepare public document for media and public
- Present group evaluation and recommendations to stakeholders
- Follow up individually if desired
- Follow up over time to encourage implementation of recommendations

1. Identifying the Exercise

In this segment, the core planning team identifies a need for an exercise

Identifying

Organizer

- Identify the measures and groups to test
- Choose the exercise type, size, geographic scope
- Choose high-level scenario options
- Identify key stakeholders

2. Planning the Exercise

In this segment, the core planning team drives the planning process

Planning

Organizer

- Acquire financial resources

Organizer & Planners

- Select appropriate location
- Set a schedule
- Conduct meeting to introduce subject and build consensus
- Creative realistic scenario
- Assign roles
- Set objectives for evaluation

Planners

- Train monitors, moderator, others, to perform their duties during the exercise
- Invite desired observers
- Decide on a media policy
- Notify media, if relevant

3. Executing the Exercise

In this segment, the exercise itself takes place

Conducting

Planners

- Ensure all role-players are prepared for their duties
- Train participants

Moderator/Director

- Execute the scenario and injects as guided by moderator/director

Monitors

- Observe participants and note actions/decisions
- Report back to the moderator/director

Participants

- Simulate procedures

All

- Support evaluation process through questionnaires or other tasks

4. Evaluating the Exercise

After the exercise itself, the core planning team conducts an evaluation

Evaluating

All

- Complete questionnaires and debriefings

- Evaluators

- Collect required information

- Prepare evaluation for individual stakeholders

- Prepare evaluation for all stakeholders

- Prepare public document for media and public

- Present group evaluation and recommendations to stakeholders

- Follow up individually if desired

- Follow up over time to encourage implementation of recommendations

Exercise Life Cycle

Identifying

Organizer

- Identify the measures and groups to test
- Choose the exercise type, size, geographic scope
- Choose high-level scenario options
- Identify key stakeholders

Planning

Organizer

- Acquire financial resources

Organizer & Planners

- Select appropriate location
- Set a schedule
- Conduct meeting to introduce subject and build consensus
- Creative realistic scenario
- Assign roles
- Set objectives for evaluation

Planners

- Train monitors, moderator, others, to perform their duties during the exercise
- Invite desired observers
- Decide on a media policy
- Notify media, if relevant

Conducting

Planners

- Ensure all role-players are prepared for their duties
- Train participants

Moderator/Director

- Execute the scenario and injects as guided by moderator/director

Monitors

- Observe participants and note actions/decisions
- Report back to the moderator/director

Participants

- Simulate procedures

All

- Support evaluation process through questionnaires or other tasks

Evaluating

All

- Complete questionnaires and debriefings
- Evaluators
- Collect required information
- Prepare evaluation for individual stakeholders
- Prepare evaluation for all stakeholders
- Prepare public document for media and public
- Present group evaluation and recommendations to stakeholders
- Follow up individually if desired
- Follow up over time to encourage implementation of recommendations

Coordinate the Logistics

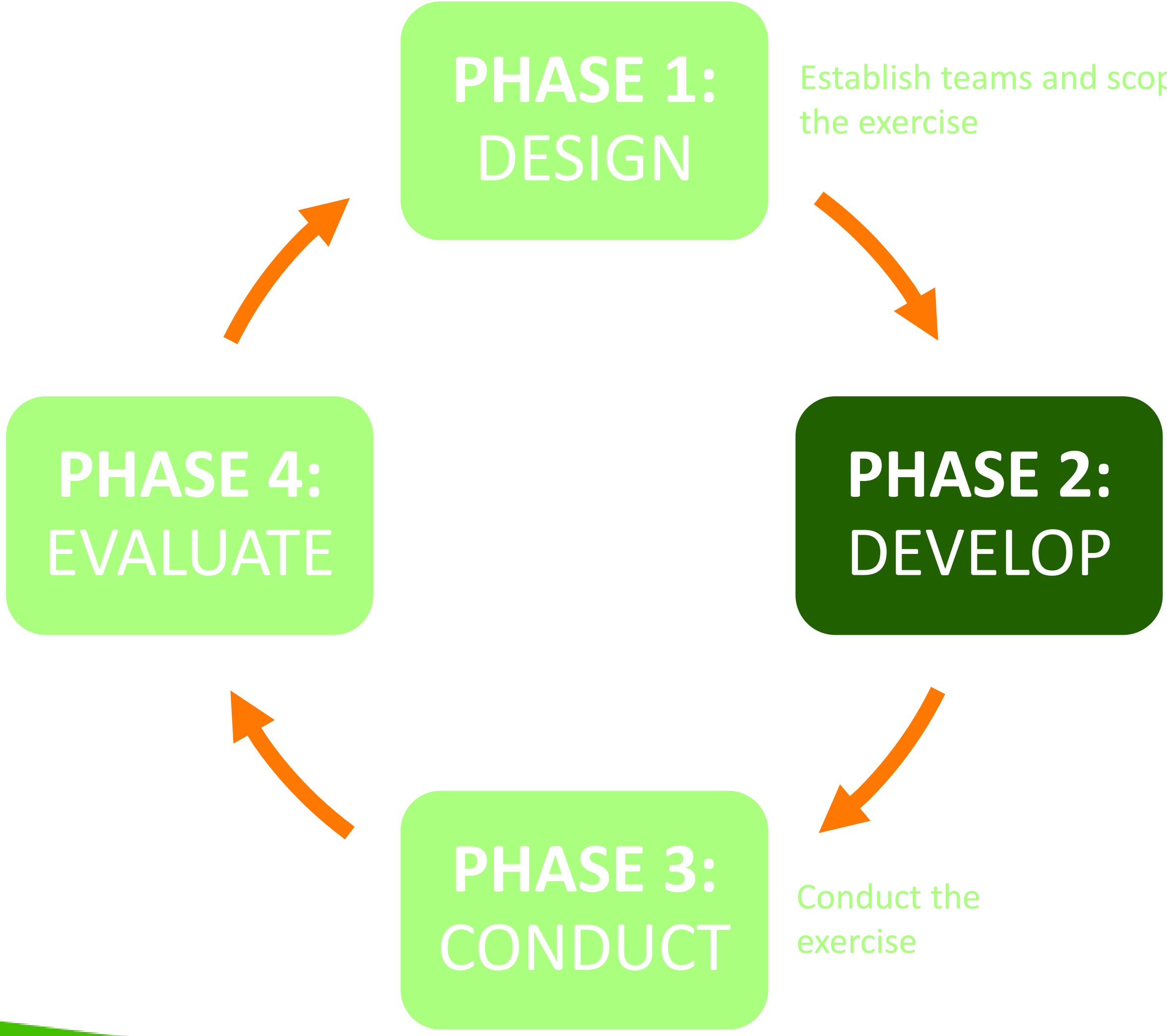
Checklist of possible logistics actions for the exercise

Logistics	Target Date	Completed
Select a date for conduction the test		
Identify each individual component that will be tested		
Identify participants		
Invite core participants to an organizational meeting		
Coordinate the development of the test plan and other required documentation		
Reserve a conference room that accommodates all participants		
Ensure conference room is available at least one day before the conference to perform setup		
Determine the need for audio/visual and recording equipment		
Arrange for refreshments, if appropriate		
Create a supplies checklist to include required testing tools, measurement and recording devices, and items such as nametags/nametag holders, clipboards, and pens		
Copy all text documents and files as a backup onto a CD-ROM, USB flash device or other removable media		
Validate the correct operation of testing equipment and ensure evaluators know how to operate the test equipment		
Conduct a dry-run/walk through the test to be performed, if necessary		
Review procedures to terminate the test, should operational issues necessitate it		

Module 6: Setting Up Exercise Scenarios, Assets, and Documents

- By the end of this module, you will be able to:
  - Establish the importance of simulations in creating a strong exercise
  - Identify the various assets and documents that support a strong exercise program

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation
of the exercise

PHASE 3: CONDUCT

Conduct the exercise

PHASE 4: EVALUATE

Document lessons learned from the event

Scenario

- A simulated sequence of events designed for the exercise
- Can be written as a narrative or depicted by an event timeline
- Provides the backdrop that drives participant discussion. Or background information about the incident catalysts
- Should be realistic, plausible, and challenging;
  - however, not so complicated that it overwhelms players
- Measure the resilience of your organization and its capacity for recovery from an incident

Scenario

A scenario consists of **three** basic elements:

1. The **general context** or comprehensive story
2. The **required conditions** that will allow players to demonstrate proficiency and competency in conducting critical tasks, demonstrating core capabilities, and meeting objectives
3. The **technical details** necessary to accurately depict scenario conditions and events

- The scenario should facilitate assessment of exercise objectives and core capabilities
- Avoid use of real names of terrorist groups or sensitive venues

Threat or Hazard

- The first step in designing a scenario is determining the type of threat or hazard on which the exercise will focus
- The core planning team should choose a threat or hazard that best assesses the objectives and core capabilities on which the exercise will focus
- Emphasize the core preparedness capabilities of your organization

Modeling and Simulation

Modeling and simulation can bring versatility, cost savings,
and fidelity to exercises:

- **Model:** representation of a system at a point in time or space intended to expand an understanding of the real system
- **Simulation:** method of implementing the performance of a model, or combination of models, over time

Advantages of Modeling and Simulation

- Modeling and simulation support decision-making processes by providing human and/or computer feedback to players during exercise play, thus dynamically representing the impact of their decisions
- Modeling and simulation can also be applied in situations where enacting a real-life situation is not practical or safe

Using the Best Scenarios and Storylines

- Identify how to use the best scenarios and storylines in an exercise:
    - Background scenario
    - Main actors (including threats)
    - Storylines
    - Media

Key Exercise Assets and Documents

Document Title	Exercise Type	Distribution Audience
Exercise Design Document	Seminar (optional), Workshop (optional), TTX, Game	All participants
Facilitator Guide	Seminar (optional), Workshop (optional), TTX, Game	Facilitators
Multimedia Presentation	Seminar (optional), Workshop (optional), TTX, Game	All participants
Exercise Plan (ExPlan)	Drill, FE, FSE	Players and observers
Player Handouts	Drill, FE, FSE	Players and observers
Extent of Play Agreement (XPA)	FE, FSE	Exercise planning team
Waiver Forms	TTX, Game, Drill, FE, FSE	Players and observers
Surveys and Instructor Debriefs	All exercises	All participants

1 - Exercise Design Document

- An Exercise Design Document, also called the **Situation Manual** (SitMan) provides the textual background for a facilitated exercise
- The Exercise Design Document generally includes:
  - Exercise scope, objectives, and core capabilities
  - Exercise assumptions and artificialities
  - Instructions for exercise participants
  - Exercise structure (module order)
  - Exercise scenario background
  - Discussion questions and key issues
  - Schedule of events

Exercise Design Document

- Introduction provides an overview of the exercise as well as an exercise agenda
- Scenario may be divided up into distinct, chronologically sequenced modules
- Each module is followed by discussion questions, usually divided by organization or discipline, derived from the exercise objectives and associated core capabilities, capability targets, and critical tasks documented in each survey

2 - Facilitator Guide

- A Facilitator Guide is designed to help facilitators manage a discussion-based exercise
- Usually outlines instructions and key issues for discussion during the event and provides background information to help the facilitator answer questions from participants or players
- May also include an evaluation section that provides evaluation staff members with guidance and instructions on evaluation or observation methodology

3 - Multimedia Presentation

- Multimedia presentations are often used to illustrate the general scenario for participants and support the Exercise Design Document
- Divided into distinct, chronologically segmented modules that, when combined, create the entire scenario
- This presentation typically contains, at a minimum, the following information:
  - Introduction
  - Exercise scope, objectives, and core capabilities
  - Exercise play rules and administrative information
  - Modules that describe the scenario

4 - Exercise Plan

- Exercise Plans (**ExPlans**) are general information documents that help operations-based exercises run smoothly by **providing participants with a synopsis of the exercise**
  - Published and distributed to the participating organizations following development of most of the critical elements of the exercise
  - ExPlans assign activities and responsibilities for exercise planning, conduct, and evaluation but does not contain detailed scenario information

Exercise Plan

- An ExPlan typically contains:
  - Exercise scope, objectives, and core capabilities
  - Participant roles and responsibilities
  - Rules of conduct
  - Safety issues
  - Logistics
  - Security and access information about the exercise site
  - Communications information
  - Duration, date, and time of exercise
  - Maps and directions

5 - Player Handouts

- Provides key information to exercise players
- Can supplement the Exercise Design Document or ExPlan by providing a quick-reference guide to logistics, agenda or schedule, and key contact data

6 - Extent of Play Agreements

- Extent of Play Agreements (**XPAs**) can be used to define the organizations participating in the exercise as well as their extent of play
- Formed between exercise participants and the exercise sponsor, and can be vital to the planning of an exercise

7 - Waiver Forms

- Each participant should receive a waiver form prior to the exercise
- Waives liability for all exercise planners and participants.
- If the exercise requires volunteers younger than 18-years-old, parents or legal guardians must sign their waiver forms

8 - Surveys and Instructor Debriefs

- Intended to help evaluators collect relevant exercise observations
- Aligned to objectives, and document the related core capability, capability targets, and critical tasks.
- Provides evaluators with information on what they should expect to see demonstrated or hear discussed
- Participants may receive a Participant Feedback Form that asks for input regarding observed strengths and areas for improvement that players identified during the exercise

Surveys and Instructor Debriefs

- At a minimum, the questions on the Participant Feedback Form solicit:
  - Strengths and areas for improvement pertaining to the implementation of participating agencies and organizations' policies, plans, and SOPs
  - Impressions about exercise conduct and logistics
- Information collected from feedback forms contributes to the issues, observations, recommendations, and corrective actions
- Feedback forms can be supplemented by the conduct of a Hot Wash immediately following the exercise

9 - Option: Controller and Evaluator Handbook

- The Controller and Evaluator (C/E) Handbook describes the roles and responsibilities of exercise controllers and evaluators and the procedures they should follow
- Distributed to only those individuals designated as controllers or evaluators to supplement the ExPlan or as a standalone document
- Usually contains:
  - Assignments, roles, and responsibilities of group or individual controllers and evaluators
  - Detailed scenario information
  - Exercise safety plan
  - Controller communications plan (e.g., a phone list, a call-down tree, instructions for the use of radio channels)
  - Evaluation instructions
- The Controller portion of the C/E Handbook provides guidelines for control and simulation support and establishes a management structure for these activities

10 - Option: Information Packets

- One option is to provide packets immediately prior to an exercise that contain key information from the C/E Handbook and additional information specific to the functional area in which the given controller or evaluator will be working.
- Packets could contain:
  - Essential C/E Handbook information
  - Ground truth document, detailing key elements of the exercise scenario
  - Injects and events for each responsible controller and evaluator
  - Surveys and debriefs
  - Maps and directions

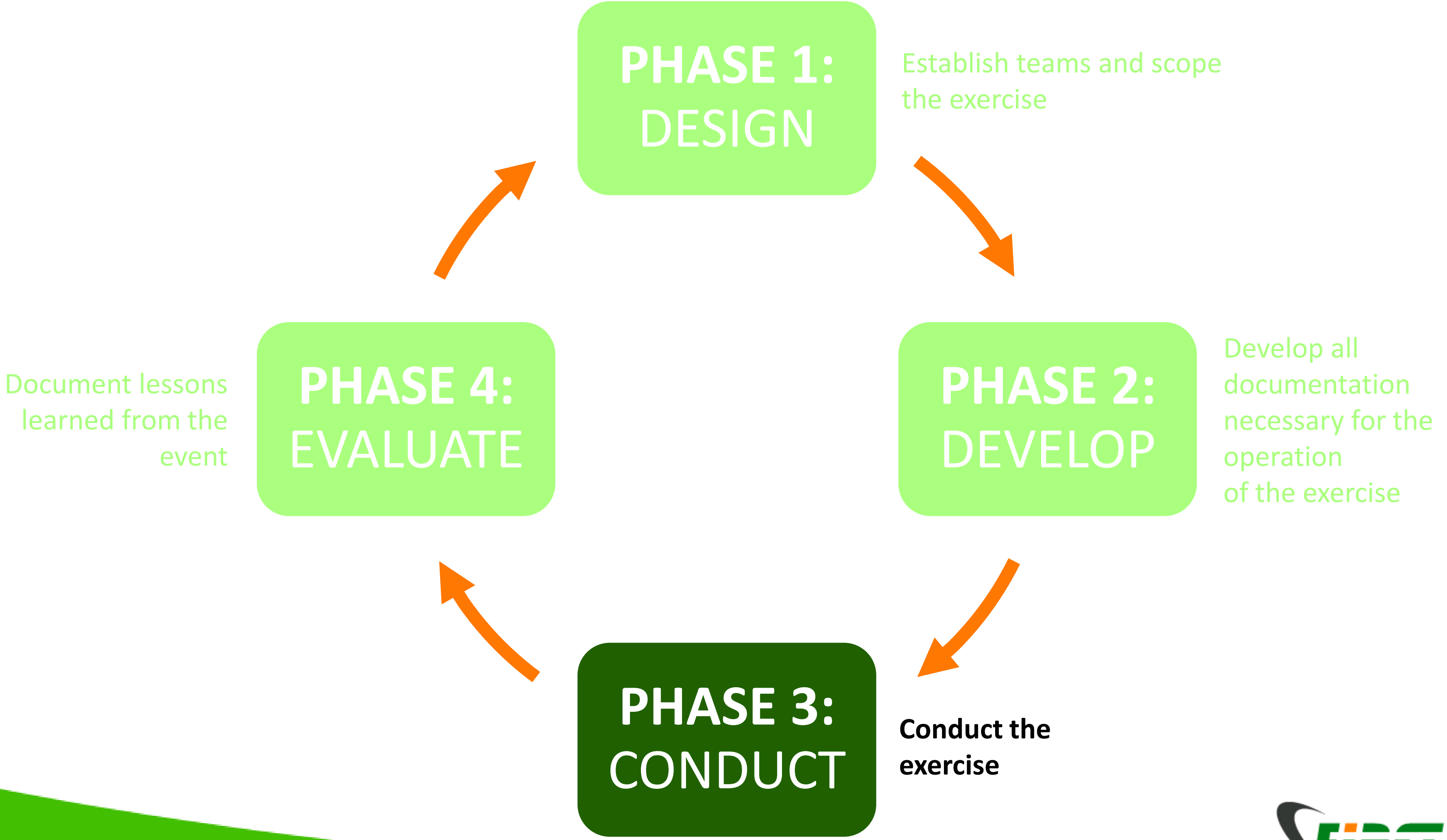
11 - Option: Weapons and Safety Policy

- Exercises, where applicable, can employ a written weapon and safety policy that is in accordance with applicable state or local laws and regulations
- Exercise sponsors should coordinate the application of this policy with the appropriate safety and/or legal departments as necessary

Module 7: Conducting an Exercise

- By the end of this module, you will be able to:
  - Establish useful communication strategies for conducting an exercise
  - Decide how best to leverage the various assets and documents to keep an exercise moving
  - Ascertain the best ways to wrap up and debrief various stakeholders in an exercise

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation of the exercise

PHASE 3: CONDUCT

Conduct the exercise

PHASE 4: EVALUATE

Document lessons learned from the event

Communication Methods - During an Exercise

- A **communications** strategy:
  - Methodology to communicate during the exercise
  - Which communications types will be used and by whom
  - Multiple organization types are represented as well as varying training requirements
- Where the communications technologies are used to manage the exercise, there should be separate channels for participation in, and management of, the exercise

Communication Methods - During an Exercise

- The core planning team should nominate separate individuals to monitor the exercise management communications and develop a contingency plan
- The communications strategy should be tested along with other testing protocols prior to the exercise
- Protocols should be defined to allow participants to notify the exercise project team if it is necessary to terminate the exercise

Preparation

Prior to conducting the exercise, the core planning team must deliver the necessary exercise materials and equipment:

- Exercise Design Documents or other written materials
- Multimedia presentation
- Appropriate A/V equipment
- Table tents for each table
- Name tents for each participant
- Badges identifying the role of each exercise participant
- Sign-in sheets
- Surveys and Participant Feedback Forms

Briefings

- Held before an exercise, briefings educate participants about their roles and responsibilities
- By scheduling separate briefings for all roles, core planning team members can ensure the right feedback goes to the right people
  - Executive sponsor briefings
  - Exercise facilitator and data collector briefings
  - Participant briefings
  - Observer briefings

Use Case: Conduct Discussion-Based Exercises

There are usually four facets of discussion-based exercises:

1. Multimedia presentation
2. Facilitated discussion
3. Moderated discussion
4. Exercise data collection

1- Multimedia Presentation

- Starts with brief remarks by representatives from the core planning team or sponsoring organization, and/or elected and appointed officials from the governing jurisdiction
- After the opening remarks, the presentation moves into a brief introductory and explanatory phase led by a facilitator
- Attendees are introduced to any other stakeholders; given background on the exercise process; and advised about their individual roles and responsibilities
- The facilitator presents the multimedia briefing and leads the discussion

2 - Facilitated Discussion

- Facilitated group discussions can occur in a plenary session or in breakout groups, which are typically organized by discipline or agency/organization
- A facilitator is responsible for keeping the discussion focused on the exercise objectives and making sure all issues are explored within the time allotted
- A good facilitator should possess:
  - Strong skills in keeping group discussions moving
  - Functional area expertise or experience
  - Awareness of appropriate plans and procedures
  - The ability to listen well and summarize player discussions

3 - Moderated Discussion

- Moderated discussions generally follow breakout discussions
- A representative from each group presents all participants with summarized results from a group's facilitated discussion
- At the end of the moderated discussion period, the facilitator opens the floor for questions
- Time for moderated discussion is generally scheduled at the end of each module, with another longer period for each at the conclusion of the exercise

4 - Exercise Data Collection

During discussion-based exercises, facilitators help collect useful data by keeping discussions focused on exercise objectives, core capabilities, capability targets, and critical tasks.

Use Case: Conduct Operations-Based Exercises

- Prior to the start of the exercise, rules for exercise play should be disseminated to all participants to establish the parameters that they must follow during the exercise
- Exercise areas for operations-based exercises should be clearly defined, and all exercise operations should take place within these designated areas
- To prevent confusion with real-world communications or accidental deployment of resources, all communications must be clearly identified as exercise-related

Control

- During exercise play, data collectors or monitors closely monitor exercise play to ensure a safe and effective exercise
- In all operations-based exercises, it is critical that all facilitators and data collectors take appropriate actions to ensure a safe and secure exercise environment
- These actions may involve monitoring conditions that impact player and/or actor safety, such as heat stress and other health issues

Exercise Data Collection

- During the exercise, each data collector or monitor should record both quantitative and qualitative data for capabilities, capability targets, and critical tasks, as assigned by the facilitator or program coordinator
- During operations-based exercises, data collectors should be strategically pre-positioned in locations at which they can gather useful data

Contingency Process

- The core planning team should maintain a contingency process to halt, postpone, or cancel an exercise as necessary
- Should the operation of the exercise put at risk any efforts to respond to real-world events or should real-world events hinder the operation of the exercise, the program coordinator and core planning team should convene, in coordination with other stakeholders, to determine the appropriate course of action
- Following decision on a final course of action, the program coordinator should communicate that course of action to all key stakeholders through all relevant communications mechanisms.

Scenario Injects

- During the course of the exercise, the scenario needs to be managed and adapted in response to the actions of participants and pre-planned injects of new information
- The moderator requires incoming information for all of the participants, relayed by the monitors located on site with each team of participants
- As the facilitator determines the changes required, he or she will communicate them to participants
- Many of the injects will be planned in advance and are designed to simulate the way a real incident would unfold
- Many exercises simulate media reports as one way to inject new developments

Wrap-Up Activities

Thorough exercise wrap-up:

- Debriefings
- Player Hot Wash
- Facilitator Debriefing

1 - Debriefings

- Immediately following the exercise, a short debriefing should be conducted with core planning team members to ascertain the levels of satisfaction with the exercise, discuss any issues or concerns, and propose improvements
- Data collectors should collect exercise attendance lists, provide copies to the exercise program manager, collect Participant Feedback Forms, and develop debriefing notes.

2 - Player Hot Wash

- A **Hot Wash** provides an opportunity for exercise participants to discuss exercise strengths and areas for improvement immediately following an exercise
- Should be led by an experienced facilitator who can ensure that the discussion remains brief and constructive
- For operations-based exercises, a Hot Wash should be conducted for each functional area by that area’s controller or evaluator immediately following an exercise

3 - Facilitator Debriefing

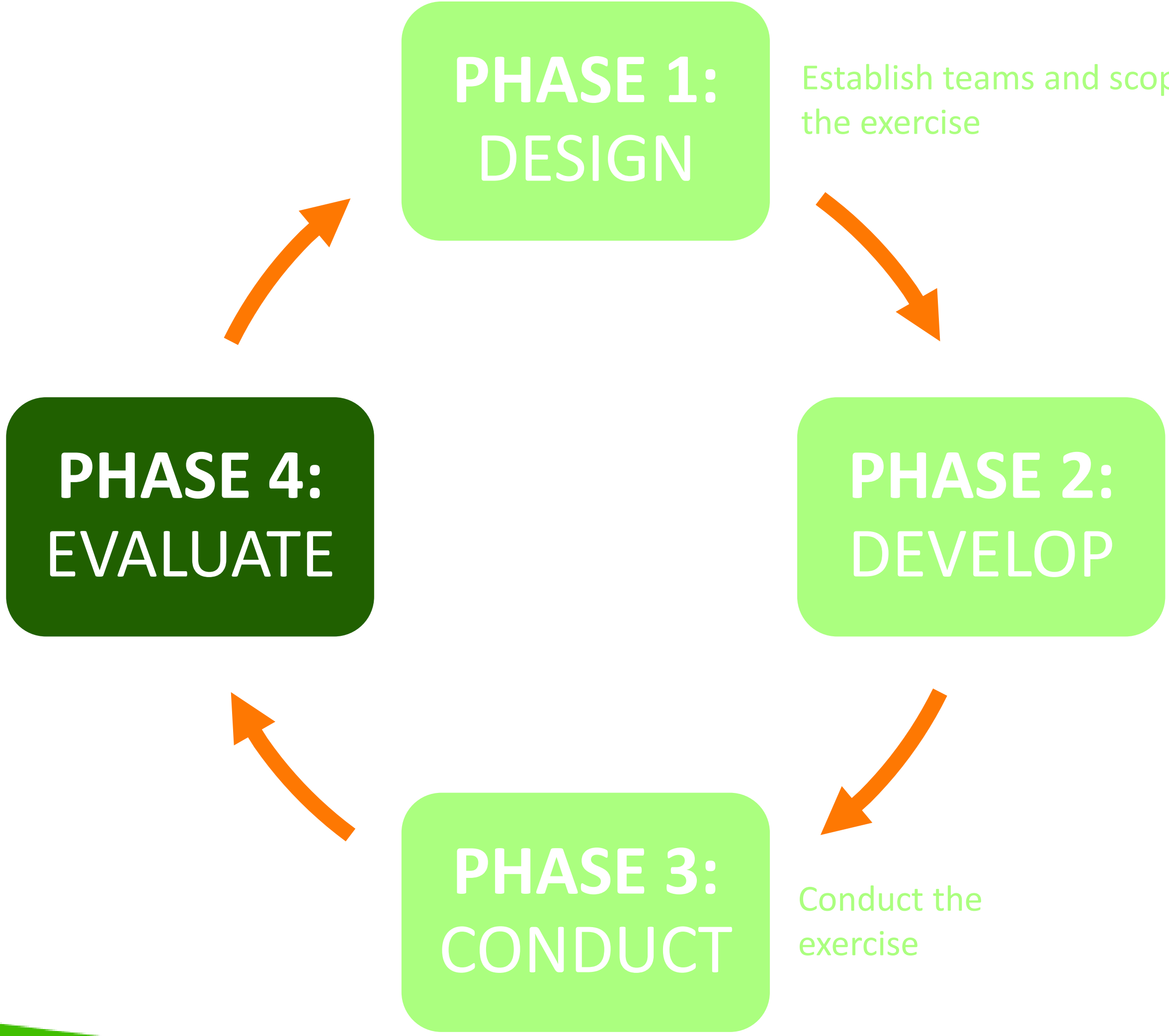
- The **Facilitator Debriefing** provides a forum for functional area controllers and evaluators to review the exercise
- The exercise program manager facilitates this debriefing, which provides each facilitator with an opportunity to provide an overview of the functional area they observed and to discuss both strengths and areas for improvement
- During the debriefing, controllers and evaluators complete and submit their Participant Feedback Forms.
- Similarly, for discussion-based exercises, a Facilitator/Data Collector Debriefing is held to review exercise operation

Module 8: Evaluating an Exercise

By the end of this module, you will be able to:

- Plan the right kind of evaluation for your exercise program
- Communicate evaluation information at appropriate levels for stakeholders
- Measure the success of your exercise program

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation of the exercise

PHASE 3: CONDUCT

Conduct the exercise

PHASE 4: EVALUATE

Document lessons learned from the event

Evaluation

- Upon completion of the exercise, the program manager should ensure that the exercise is effectively and usefully evaluated
- This process is sometimes given insufficient attention, but it is very important, as it is the process that draws conclusions and recommendations for improving resilience plans and ensuring that stakeholders act on these points

Evaluation Process

- The evaluation process is designed to enable all involved to learn lessons from the exercise
- Include observations about areas for improvement within individual organizations and their processes, as well as observations about interdependencies, ways to improve cooperation across organizations, and lessons in various other areas
- The evaluation process should aim to identify these lessons and must be designed in advance to collect the necessary information

Evaluation Process

- The objectives of the evaluation must be clear in advance.
- Objectives may include:
  - The major obstacles to success of the continuity plans tested
  - Skills required for successful implementation
  - Interdependencies and weak links in the chains of communications, coordination, and decisions among participants;
  - Developing recommendations to improve in these areas
  - Other exercise objectives
- Make objectives SMART:
  - Specific, Measurable, Attainable, Relevant, Time-Bound

After-Action Review

- Ensures that lessons are learned, interdependencies identified, and that these are communicated effectively back to participants for them to take action
- Should be done fairly quickly after the exercise
- During the planning phase, the evaluation measures and process will have been specified in detail, and the stakeholders will now need to follow through with those plans
- Should be as inclusive as the planning and execution were to ensure comprehensive insight into challenges experienced, procedures followed, interdependencies, lessons learned, corrections needed, and more

After-Action Review

- The evaluation process and outcomes must be handled delicately to protect sensitive information
- Don’t embarrass participants or lay blame
- Ensure a high level of commitment to the evaluation process

Planning Ahead on Evaluation

- The evaluation process must be planned in advance of the exercise
- The evaluation process should be inclusive
- Avoid blaming individual participants or stakeholders and keep the conclusions and recommendations constructive

Evaluations: Sources of Information

Evaluations are usually prepared using several different materials:

- Reports from the data collectors or monitors
- Questionnaires completed by data collectors or monitors at interim stages during and after the exercise
- Questionnaires completed by participants during and after the exercise
- Hot washes with participants after each main section of the exercise
- Debriefing sessions/workshops held with participants, data collectors, and facilitators after the exercise;
- Questionnaires and reports submitted by participant organizations
- Possibly also technical results from tools

Evaluations: Sources of Information

For your evaluations, remember to:

- Seek information for evaluation from many sources
- Obtain this information at interim periods during the exercise as well as after completion
- Prepare the materials and the plan for obtaining this information in advance

Evaluations: Reports

- Most evaluation processes focus on and culminate in one
  or more evaluation reports
- To cope with the issues of sensitive information, evaluation reports need to be carefully worded, avoid blame, and probably be issued in different versions. For example:
  - Individual report
  - Consensus report
  - Public report

Tips for Reports

- **Prepare separate reports for separate audiences**, tailoring each to the type and amount of information required
- Ensure that sensitive information is only revealed to the company to which it pertains, if necessary at all

Follow-Up Process

- Consider the evaluation activities as a useful process, rather than as a means of producing a report
- Focus on the process itself, rather than only the result
- Participants and stakeholders will have grown motivated to see the exercise and to learn the results
- Once the exercise is completed, it is possible to retain the core planning team for evaluation, discussion of results, discussion of key challenges or problems experienced, and so on
- Obtaining the evaluation report is an important goal, but planners should also ensure continuing collaboration and developing consensus

Follow-Up Process

Ongoing collaboration can also be extended in other ways.
For example:

- Establish a committee of stakeholders to prepare the evaluation over a period of time, including a series of meetings and discussions
- Hold additional follow-up meetings to review progress in implementing recommendations, or to continue discussing specific challenges or action plans
- Have individual follow-up steps with stakeholders to address particular issues or needed improvements

Follow-up Tips

- Leverage the evaluation process as a means to generate consensus about next steps the sector stakeholders need to take, and to generate interest and commitment to taking those steps
- Roll over exercise evaluation quickly into planning for the next exercise, in order to maintain momentum and build on the skills and commitment generated in the previous one
- Consider ways to extend collaboration in other ways, through ongoing committees, meetings, or forums to discuss the challenges identified

Media After the Exercise

- You may want to include in the evaluation process a public report on the exercise
- This report should not identify the detailed findings but should include a higher level summary of the objectives, participating sectors, broad benefits of the exercise, and related high-level information

Measuring Success

The success of an exercise can be measured using two different metrics:

1. Whether the exercise achieves the objectives
2. The effectiveness of the exercise processes

Measuring Success

Specific factors are easier to measure. Options for measurement tools include:

- Questionnaires to gauge changed views of specific issues and measure an exercise's effectiveness
- Repeat testing to compare results to see whether improvement occurs
- Individual follow-up to ensure that participants address
  any revealed weaknesses in their continuity plans

Measuring Success

- A general follow-up on lessons learned and action plans may reveal specific areas for improvement
- Program managers can ensure that a separate evaluation document is prepared that focuses on lessons learned
- Log lessons from each exercise, collecting them as a set of good practices for internal use

Tips for Measuring Success

- Conduct surveys of stakeholders over time to measure changed perception of various issues
- Test repeatedly for certain key areas to measure improvement
- Follow-up with stakeholders (as a group or individually) to encourage follow-through with needed improvements
- Include questions in the evaluation process that reveal views on the effectiveness of the exercise processes
- Prepare a separate evaluation of the exercise processes, to help guide future exercise processes

Olivier CALEFF on behalf of FIRST

October 2021 - online

Copyright

FIRST.Org is name under which Forum of Incident Response and Security Teams, Inc. conducts business.

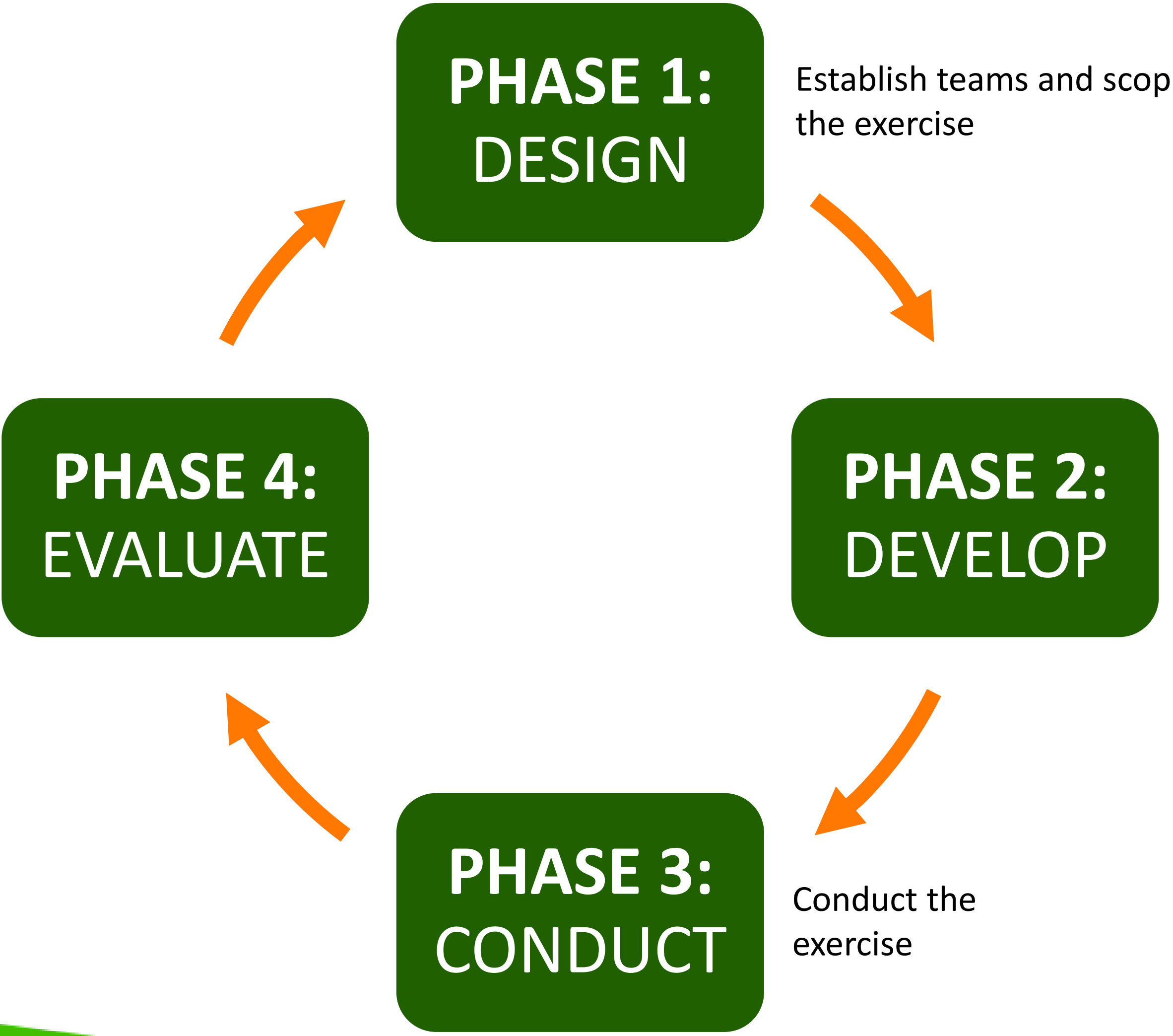
FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Module 9: Exercise Creation Lab / Wrap-up

At the end of this lab, you will be able to:

- Work through the various considerations in creating an exercise
- Define more clearly how roles work in creating exercise programs
- Identify real-world issues that occur when developing an exercise

Exercise Creation Process



PHASE 1: DESIGN

Establish teams and scope the exercise

PHASE 2: DEVELOP

Develop all documentation necessary for the operation of the exercise

PHASE 3: CONDUCT

Conduct the exercise

PHASE 4: EVALUATE

Document lessons learned from the event

Lab: Tabletop Exercise

- You will be assigned roles to develop a tabletop exercise (TTE)
- The task will have 4 phases, one for each phase in the Exercise Creation Process
- The task is mainly a group discussion and you will do individual and sub-group work

Lab: Materials Needed

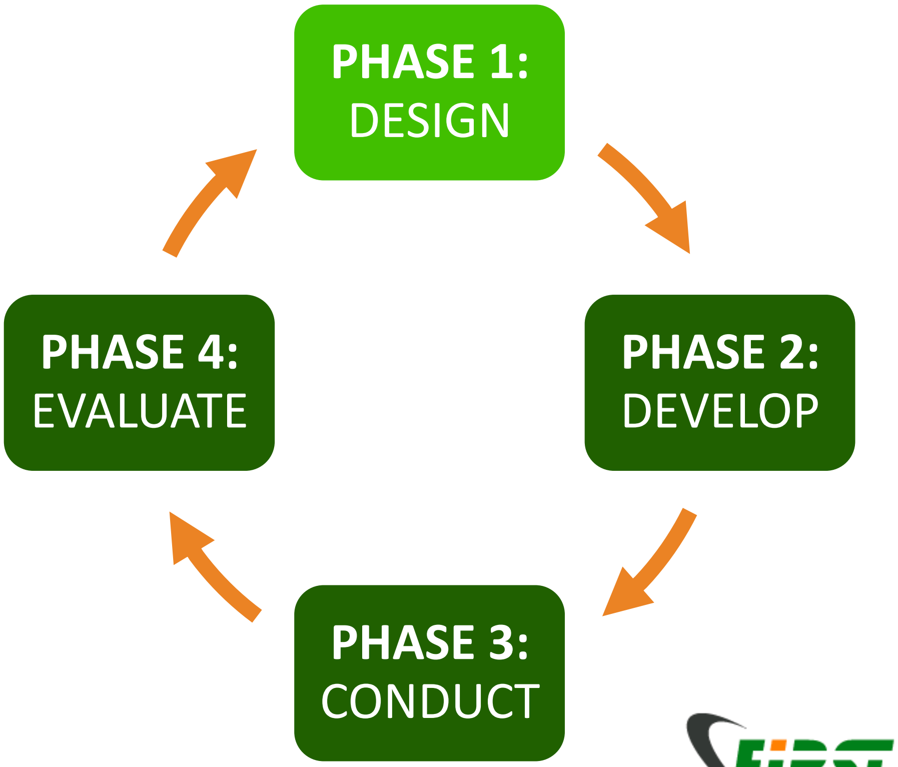
- **Establish basic parameters to start the discussion:**
  - An evaluation of the training audience
  - Pre-selected exercise objectives
  - Constraints

Lab: Phase 1: Design, Planning

You will be assigned a role:

- Program Coordinator
- Core Planning Team
- Technical Planner
- Exercise Facilitators
- Data Collectors

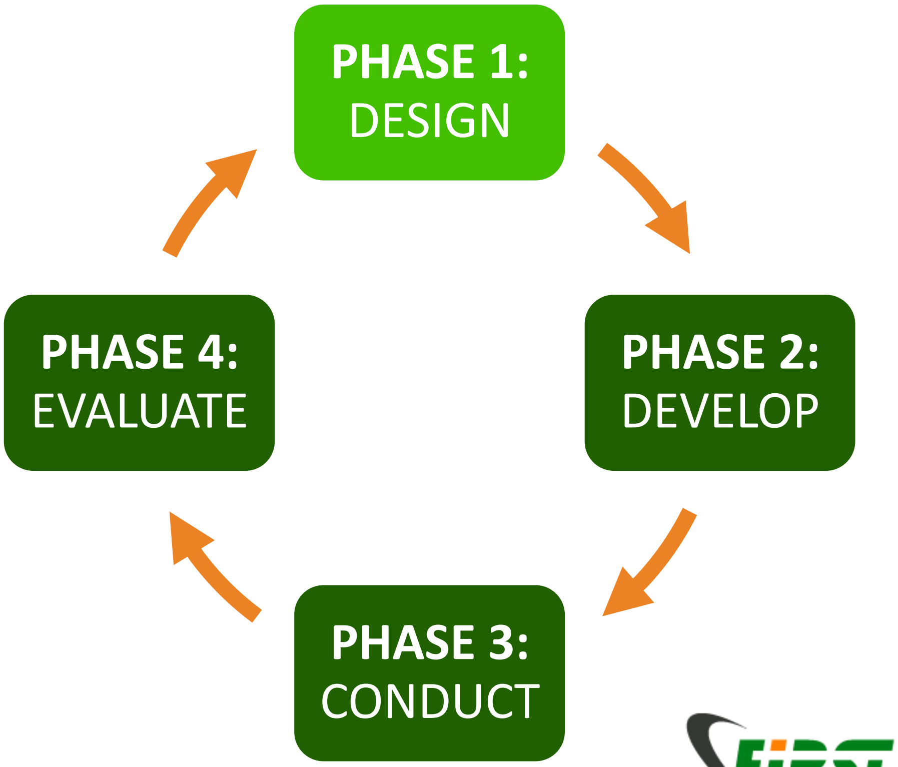
Exercise Creation Process



Lab: Phase 1: Design, Planning

Parameters for the exercise

Exercise Creation Process

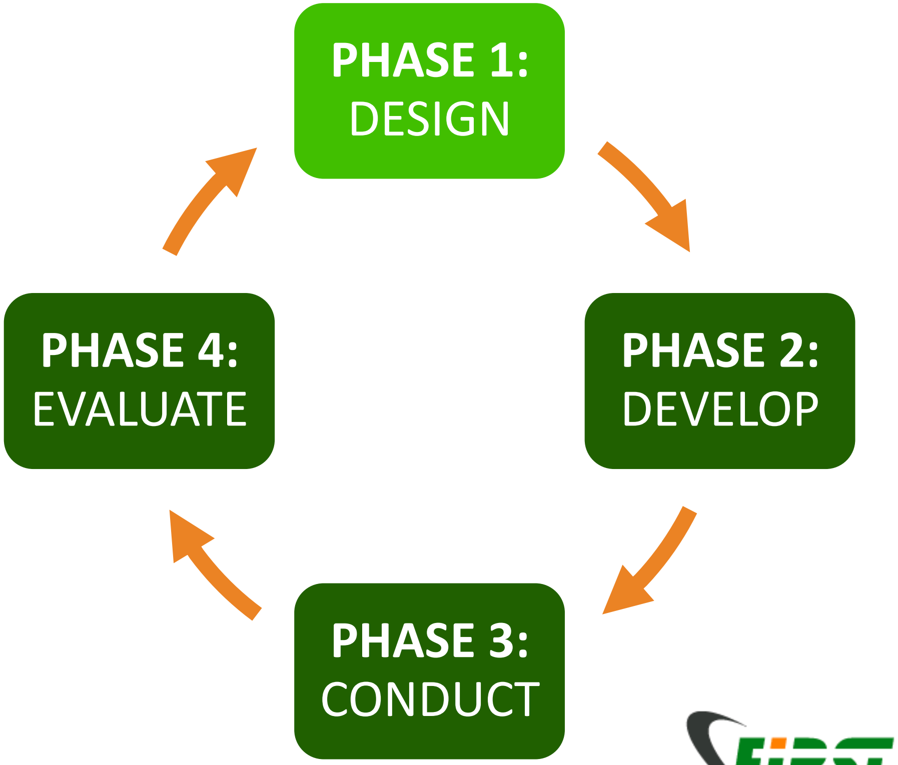


Lab: Phase 1: Design, Needs Assessment

Questions to evaluate:

- Who?
- What?
- Why?
- Where?
- When?
- How?

Exercise Creation Process



PHASE 1: DESIGN

PHASE 2: DEVELOP

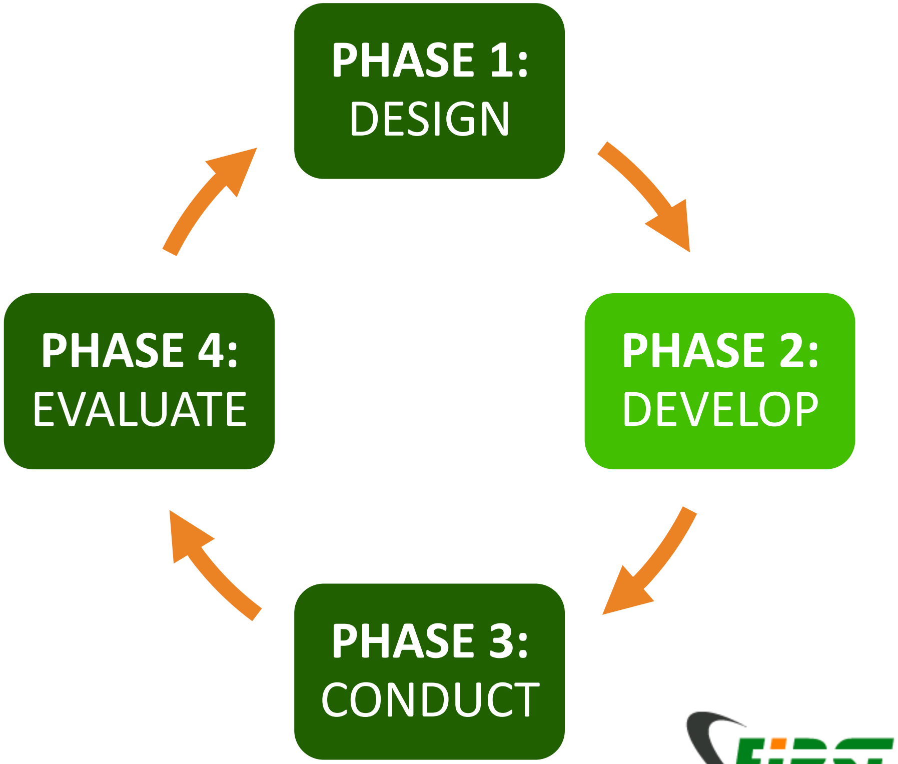
PHASE 3: CONDUCT

PHASE 4: EVALUATE

Lab: Phase 2: Develop

1. Set the exercise objectives and modalities
2. Define the scenario and storylines
3. Review exercise objectives and modalities
4. Fully develop scenario and storylines

Exercise Creation Process


PHASE 1: DESIGN

PHASE 2: DEVELOP

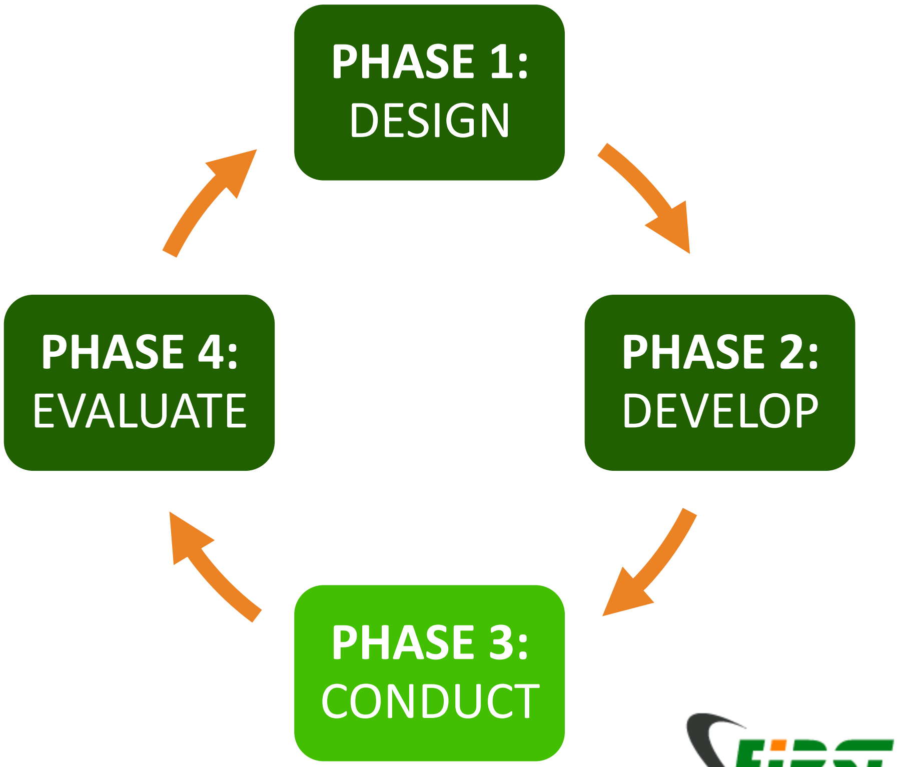
PHASE 3: CONDUCT

PHASE 4: EVALUATE

Lab: Phase 3: Conduct

Start the exercise!

Exercise Creation Process



PHASE 1: DESIGN

PHASE 2: DEVELOP

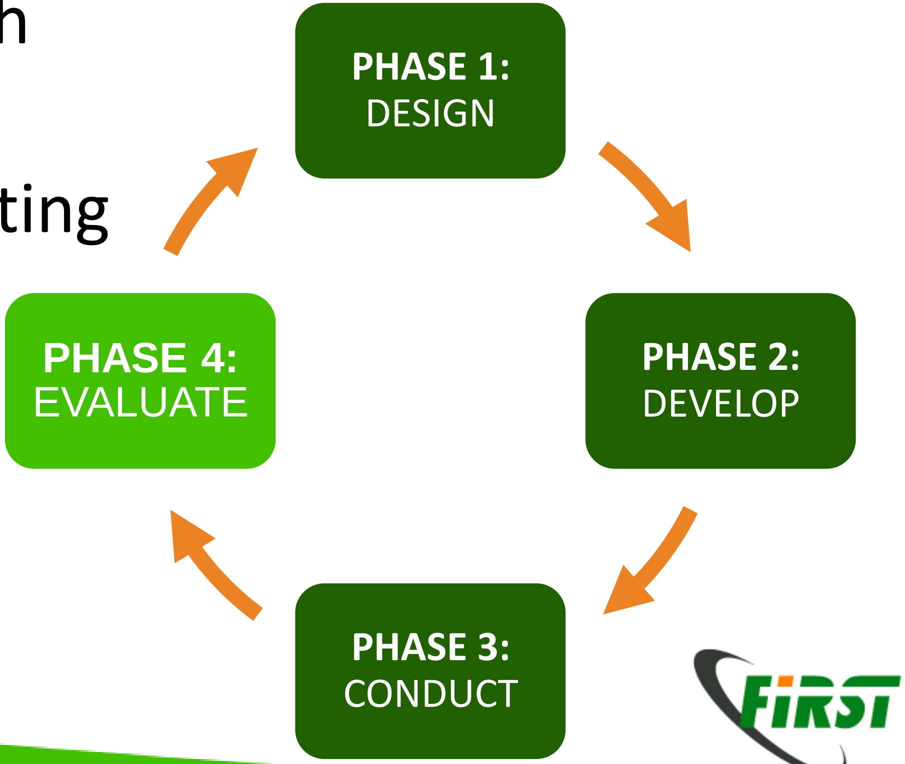
PHASE 3: CONDUCT

PHASE 4: EVALUATE

Lab: Phase 4: Evaluate

- How did exercise development go?
- What were some challenges and how did you overcome them?
- How did you work through any communication issues?
- What did you learn in putting together an exercise?
- What would you do differently in your organization?

Exercise Creation Process



PHASE 1: DESIGN

PHASE 2: DEVELOP

PHASE 3: CONDUCT

PHASE 4: EVALUATE

Conducting Exercises to Improve Incident Response
ITU-D 2021 Global CyberDrill

Olivier CALEFF on behalf of FIRST

October 11th, 2021 - online