National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-84
Sponsored by the
Department of Homeland Security

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Recommendations of the National Institute of Standards and Technology

Tim Grance
Tamara Nolan
Kristin Burke
Rich Dudley
Gregory White
Travis Good

NIST Special Publication 800-84

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Recommendations of the National Institute of Standards and Technology

Tim Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, Travis Good

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2006

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William A. Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-84
Natl. Inst. Stand. Technol. Spec. Publ. 800-84, 97 pages (September 2006)

Acknowledgements

The authors, Tim Grance of the National Institute of Standards and Technology (NIST); Tamara Nolan, Kristin Burke, and Rich Dudley of Booz Allen Hamilton; and Dr. Gregory White and Travis Good of the University of Texas-San Antonio (UTSA); wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Joan Hash, Karen Kent, Peter Mell, Matt Scholl, Marianne Swanson, and Mark Wilson of NIST; Dick Broome, Kara Crawley, Courtney Hawkins, Munir Majdalawieh, and Zara Pyatt of Booz Allen Hamilton; and Dwayne Williams of UTSA for their keen and insightful assistance throughout the development of the document. The authors would also like to express their thanks to Glenn Fiedelholtz, Annabelle Lee, and Jeffrey Wright from the National Cyber Security Division of the Department of Homeland Security, as well as representatives from the Department of State and the MITRE Corporation, for their valuable comments and suggestions.

The National Institute of Standards and Technology would also like to express its appreciation and thanks to the Department of Homeland Security for its sponsorship and support of NIST Special Publication 800-84.

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

Organizations have information technology (IT) plans in place, such as contingency and computer security incident response plans, so that they can respond to and manage adverse situations involving IT. These plans should be maintained in a state of readiness, which should include having personnel trained to fulfill their roles and responsibilities within a plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in an operational environment specified in a plan. These three types of events can be carried out efficiently and effectively through the development and implementation of a test, training, and exercise (TT&E) program. Organizations should consider having such a program in place because tests, training, and exercises are so closely related. For example, exercises and tests offer different ways of identifying deficiencies in IT plans, procedures, and training.

This document provides guidance on designing, developing, conducting, and evaluating TT&E events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events that may affect their missions. The scope of this document is limited to TT&E events for single organizations, as opposed to large-scale events involving multiple organizations, involving internal IT operational procedures for emergencies. This document does not address TT&E for a specific type of IT plan; rather, the TT&E methodology described in this document can be applied to TT&E events built around any IT plan or around an IT emergency-handling capability that is not necessarily documented in a plan, such as computer security incident response.

As part of creating a comprehensive TT&E program, a TT&E plan should be developed that outlines the steps to be taken. The TT&E plan should define the organization's roadmap for ensuring a viable capability, and outline the organization's approach to maintaining plans, as well as enhancing and managing the capability. Enhancing emergency plans, policies, and procedures will promote more efficient utilization of capabilities in responding to cyber attacks. In addition, the TT&E plan should identify resource and budget requirements that enable organizations to achieve an effective, proven capability, and provide a schedule for conducting various types of TT&E events. Creating the TT&E program should also involve several other steps, including developing a TT&E policy, identifying roles and responsibilities, and documenting a TT&E event methodology.

The TT&E program should include several types of events to ensure the availability of a wide range of methods for validating various planning elements in the context of cyber incidents. The types of events covered in this guide are as follows:

- **Tests.**[1] Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment specified in an IT plan. For example, an organization could test if call tree cascades can be executed within prescribed time limits; another test would be removing power from a system or system component. A test is conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used. The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an IT plan. Tests often focus on recovery and backup operations; however, testing varies depending on the goal of the test and its relation to a specific IT plan.

[1] Many people use the terms "test" and "exercise" interchangeably, such as "performing testing through exercises". However, there are distinctions between the two terms. For the purpose of this document, the term "test" is reserved for testing systems or system components; it is not used to describe "exercising" plans.

- **Training.** For the purposes of this publication, training refers only to informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the IT plan. Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities, and activities that allow personnel to demonstrate their understanding of the subject matter.

- **Exercises.** An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that does not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise. There are several types of exercises, and this publication focuses on the following two types that are widely used in TT&E programs by single organizations:

  - **Tabletop Exercises.** Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

  - **Functional Exercises.** Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

Organizations should conduct TT&E events periodically; following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance; or as otherwise needed. This assists organizations in ensuring that their IT plans are reasonable, effective, and complete, and that all personnel know what their roles are in the conduct of each IT plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST Special Publication 800-53 requires Federal agencies to conduct exercises or tests for their systems' contingency plans and incident response capabilities at least annually.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Although it is important to have plans in place to help an organization respond to and manage various situations involving information technology (IT), it is equally important to maintain these plans in a state of readiness. This includes having IT personnel trained to fulfill their roles and responsibilities; having plans exercised to validate their policies and procedures; and having systems tested to ensure their operability. These three types of events can be carried out efficiently and effectively through the development and implementation of a test, training, and exercise (TT&E) program.

This publication seeks to assist organizations in designing, developing, conducting, and evaluating TT&E events in an effort to aid personnel in preparing for adverse situations involving IT. The events are designed to train personnel, exercise IT plans, and test IT systems, so that an organization can maximize its ability to prepare for, respond to, manage, and recover from disasters that may affect its mission. The guide describes the design, development, conduct, and evaluation of events for single organizations, as opposed to large-scale events that may involve multiple organizations. The TT&E methodology described in this document can be applied to TT&E events built around any type of IT-related plan, including, but not limited to, contingency plans (e.g., disaster recovery plans) and computer security incident response plans. The vocabulary related to TT&E varies across organizations; this document provides definitions of the terms most commonly used for TT&E-related activities and teams.

1.3 Audience

This document has been created for individuals responsible for their organization's TT&E program. Specifically, the document is designed to assist the IT personnel responsible for designing, developing, conducting, and/or evaluating TT&E events in fulfilling these responsibilities effectively.

1.4 Document Structure

The remainder of this document is organized into five major sections. Section 2 contains information on establishing a TT&E program. Specifically, it describes the need for a TT&E program and the steps involved in creating a TT&E program, including developing a TT&E policy; identifying roles, responsibilities, and activities; establishing an event schedule; and documenting the TT&E event methodology.

Section 3 briefly discusses the role of training in a TT&E program and how training is related to exercises and tests. Section 4 contains information on determining the need for tabletop exercises, and designing, developing, conducting, and evaluating an exercise event. This section describes the design phase in detail, including determining the topics and scope; identifying the objectives; identifying participants and training staff; and coordinating logistics. Sections 5 and 6 contain similar information for functional exercises and tests, respectively.

This document also contains several appendices. Appendices A, B, and C contain samples of the documentation associated with tabletop exercises, functional exercises, and tests, respectively. Appendix D contains a glossary, and Appendix E contains an acronym list. Appendix F identifies print and online resources that may be helpful in scoping, planning, documenting, conducting, and evaluating TT&E events. Appendix G contains an index for the publication.

2. Establishing a Test, Training, and Exercise Program

An organization's IT plans need to be maintained to sustain the organization's ability to prepare for, respond to, manage, and recover from disasters affecting its mission.[2] Common types of IT plans used for this purpose are as follows:

- Contingency plan: Recovering and reconstituting IT systems.[3] Contingency plans include continuity of operations plans, business continuity plans, and disaster recovery plans.
- Incident response plan: Reporting and managing computer security incidents.[4]

The following are the major types of events used to maintain these plans:

- **Tests.** A *test* is an evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.[5] For example, an organization could test if call tree cascades can be executed within prescribed time limits; another test would be removing power from a system or system component. The quantifiable metrics are created by developing a *test plan* that identifies the systems or components to be tested (and the components of any systems being tested) and the overall test objectives. Testing that results in components or systems malfunctioning or becoming inoperable could indicate problems in personnel training or in IT plans and procedures. Tests often focus on recovery and backup operations; however, testing varies depending on the goal of the test and its relation to a specific IT plan. Section 6 contains detailed information about testing.
- **Training.** For the purposes of this publication, *training* refers only to informing personnel of their roles and responsibilities within a particular IT plan, such as decision making, and teaching them skills related to those roles and responsibilities.[6] This prepares the personnel for participation in exercises, tests, and actual emergency situations related to the IT plan. Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities, and activities that allow personnel to demonstrate their understanding of the subject matter. Section 3 contains a brief overview of training events, which are already discussed in detail in other NIST publications.
- **Exercises.** An *exercise* is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. Exercises helps to identify gaps and inconsistencies within IT plans and procedures, as well as cases where personnel need additional training or when training needs to be changed. In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that does not involve using the actual operational environment for

---

2 Organizations also need to maintain IT capabilities, such as incident response capabilities, that are not necessarily documented in a plan. For the sake of simplicity, this guide refers to "IT plans" instead of "IT plans and capabilities".

3 Additional information on contingency plans can be found in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

4 Additional information on incident response can be found in NIST SP 800-61, *Computer Security Incident Handling Guide*.

5 The terms "test" and "exercise" are often used interchangeably. There are, however, distinctions between the two terms. For the purpose of this document, the term "test" is reserved for testing systems or system components; it is not used to describe "exercising" plans.

6 There are many types of training events not discussed in this publication. Some are discussed in detail in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and SP 800-50, *Building an Information Technology Security Awareness and Training Program*. Both publications are available for download from http://csrc.nist.gov/publications/nistpubs/index.html.

deployment of personnel. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise. There are several types of exercises, and this publication focuses on the following two types that are widely used in TT&E programs by single organizations:[7]

- **Tabletop.** *Tabletop exercises* are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources. Section 4 contains detailed information about tabletop exercises.

- **Functional.** *Functional exercises* allow personnel to validate their operational readiness for emergencies in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of an IT plan (e.g., communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner. Section 5 contains detailed information about functional exercises.

Although an organization could perform tests, training, and exercises as discrete activities without any coordination, organizations should consider having a program in place that addresses all three because they are so closely related. For example, exercises and tests offer different ways of identifying problems with IT plans, procedures, and training. An effective TT&E program should comprise a combination of training, exercise, and testing events.[8] The program should include a TT&E plan, policy, event methodology, and procedures. Using these elements should cause TT&E events to be performed more consistently and effectively, particularly reducing duplication of effort. A program should also address resource and budget requirements, and provide a schedule for conducting types of TT&E events. This section discusses the steps involved in creating a TT&E program.[9]

Regardless of the type of IT plans an organization has developed, it should have mechanisms in place to validate the plans' effectiveness and manage their maintenance. Organizations that want to establish a TT&E program should first develop a TT&E plan that outlines the steps to be taken to ensure that personnel are trained in their IT plan roles and responsibilities, IT plans are exercised to validate their

---

[7] There are many conventions for categorizing exercises. For example, some people use "tabletop exercises" to refer to discussion-based exercises in general, while other people consider "tabletop exercises" to refer to a specific type of discussion-based exercise, and use additional terms for other exercises (e.g., "seminar exercises" for exercises that combine training lectures and group discussion). Similarly, the term "functional exercise" can be thought of as a generic term for exercises involving simulated operations, or it can be thought of as a specific type of operational exercise, with other terms used for other exercise types (e.g., "command post exercise" for something very similar to a functional exercise that focuses on senior management's decision-making). The definitions used in this publication are not meant to be definitive, but rather to provide a basis for subsequent discussions of exercises in the publication. For more information on other types of exercises, see the extensive documentation provided at the Homeland Security Exercise and Evaluation Program (HSEEP) Web site, located at https://www.hseep.dhs.gov/.

[8] Although "TT&E" stands for "test, training, and exercise", the remainder of this publication typically discusses the three types of events in the sequence 1) training, 2) exercise, and 3) test because they usually occur in that order (individuals should be trained before they participate in exercises, and exercises are usually held before tests are performed).

[9] This section assumes that the individuals creating the TT&E program have already requested and obtained senior management buy-in and support.

viability; and IT components or systems are tested to validate their operability in the context of an IT plan. The TT&E plan should outline all elements of the program and ensure that information surrounding the program is documented. In addition to creating the TT&E plan, other major steps in creating a TT&E program are as follows:

- Develop a comprehensive policy
- Identify roles and responsibilities
- Establish overall schedule
- Document methodology.

These steps are described in more detail in Sections 2.1 through 2.4.

2.1 Develop Comprehensive TT&E Policy

A TT&E program should include a policy that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing components and systems. The policy forms the framework for the purpose and objectives of the program and cites applicable Federal and internal guidance. The policy further provides the framework or "rules" that govern how the organization develops and administers the TT&E events. The policy establishes a clear and consistent framework for creating all of the documentation associated with TT&E events.

Key steps for developing a TT&E policy are as follows:

- Win the support and involvement of senior management, which includes ensuring that senior managers understand the program, the resources needed to make the program successful, the benefits and need for having the program, and any potential risks involved in creating the program
- Identify all relevant planning documentation (internal and external), such as past training records; organization's policies; Federal guidance; and other practices obtained from other organizations or industry partners
- Collect all governing documentation and maintain the documentation within a central repository.

The following are suggested elements to include in a TT&E policy:

- Purpose
- Effective date
- Objectives
- Applicability and scope
- Authorities and related policies
- Roles and responsibilities of key business units and staff positions
- TT&E requirements
- TT&E review and approval

- Enforcement and compliance
- Points of contact for additional information
- Definition of terms.

Once the TT&E policy is developed, the policy statement should be updated as new guidance is applied to or impacts the program.

2.2 Identify TT&E Roles and Responsibilities

The office with primary oversight of and responsibility for a TT&E program varies based on the structure or requirements of the organization. In many organizations, it is led within the Office of the Chief Information Officer (OCIO). The TT&E program should be managed by a person or team with direct responsibility for the organization's IT planning capability. The program should have an *IT plan coordinator* who is responsible for all aspects of IT planning, including the TT&E element of maintaining the IT plans. The IT plan coordinator has overall responsibility for the IT plans, including development, implementation, and maintenance. One of the IT plan coordinator's responsibilities is to identify a *TT&E program coordinator*, who is responsible for developing a TT&E plan and coordinating events. To plan and conduct TT&E events, the TT&E program coordinator works with event design teams. Organizations might elect to purchase specialized software or obtain external support to assist in forming or staffing these teams. Sections 4 through 6 contain information on the individual design teams and the roles within each team.

2.3 Establish Overall TT&E Schedule

The TT&E plan should document the projected schedule of activities to be performed within the TT&E program. Although events should be conducted as needed, organizations should evaluate the required frequency of its events and document the frequency of each event in a TT&E schedule. For example, NIST Special Publication (SP) 800-53 requires Federal agencies to conduct exercises or tests for their systems' contingency plans and incident response capabilities at least annually. Sections 4 through 6 provide additional detail on how to evaluate an organization's specific TT&E needs.

2.4 Document TT&E Event Methodology

As part of creating a TT&E program, an organization should select and document a high-level methodology for planning and performing TT&E events. Figure 2-1 shows one commonly used methodology, which has four phases:

- **Design the event.** The TT&E program coordinator works with the plan coordinator to determine the TT&E event topic and scope based on the current needs of the organization. Examples of topics include training personnel on their specific roles and responsibilities within an IT plan, exercising response procedures, and testing a specific system. Next, the TT&E program coordinator identifies the objectives based on the topic and scope, and the personnel that should participate in the event. The TT&E program coordinator also identifies an event design team, which may consist of one person or a group of people, depending on the requirements of the event. The TT&E program coordinator oversees the event logistics, which could include document printing, room setup, meals, and audiovisual equipment.
- **Develop the event documentation.** Upon completion of the design phase, the TT&E program coordinator works with the design team on the development of the documentation to be used before, during, and after the event. The types of documentation vary for each type of event, but

examples include briefing materials, participant manuals, instructor and facilitator guides, test plans and scripts, and evaluation criteria.

- **Conduct the event.** In this phase, the event—the training, exercise, or test—is actually conducted. The details of this vary greatly by event type and scope.
- **Evaluate lessons learned from the event.** The evaluation phase is used to analyze the event and identify lessons learned, both to improve the IT plans and their execution, and to improve the TT&E process. Evaluation is performed somewhat differently by event type, as follows:
  - Training: Participants typically complete an evaluation/critique form on the success of the event and areas where enhancements can be made in terms of the personnel's knowledge of the trained subject matter. Feedback is analyzed and documented in a training analysis report, and future sessions are modified as needed.
  - Exercise or test: Participants typically engage in a facilitated debrief, also called a *hotwash*, to discuss areas that went particularly well and areas where enhancements can be made in terms of the plan's contents and/or the tested systems. Findings discussed during the debrief, observations made during the course of the event, and considerations for enhancement are documented in an after action report.

Although the details of each phase typically vary based on the type of event conducted, the same phases should be used for each event. Details pertaining to each type of event can be found within Sections 4 through 6.

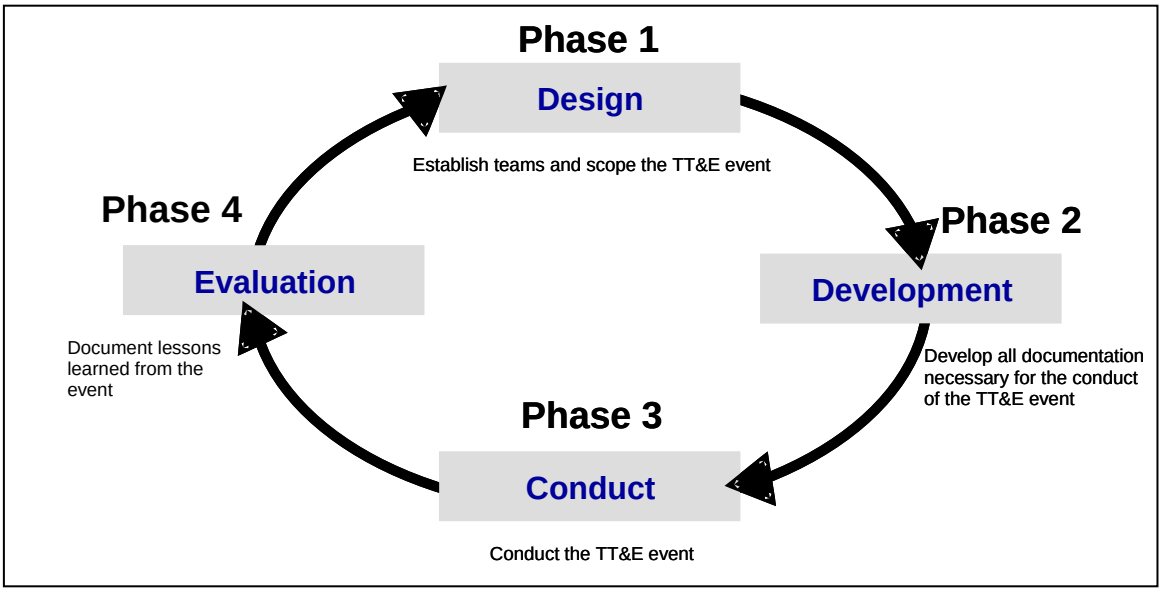

Figure 2-1. TT&E Event Methodology

2.5 Recommendations

Organizations should consider having a TT&E program that validates the effectiveness of IT plans such as contingency plans and computer security incident response plans, and manages their maintenance. The TT&E program should include a TT&E plan, policy, and event methodology. Using these elements should cause TT&E events to be performed more consistently and effectively. The TT&E plan should

outline all elements of the program and ensure that information surrounding the program is documented. In addition to creating the TT&E plan, other major steps in creating a TT&E program are as follows:

- **Develop comprehensive TT&E policy.** The policy should outline the organization's internal and external requirements associated with training personnel, exercising plans, and testing components and systems.

- **Identify TT&E roles and responsibilities.** The TT&E program should be managed by a person or team with direct responsibility for the organization's IT planning capability. The program should have a plan coordinator who is responsible for all aspects of IT planning, including the TT&E element of maintaining the IT plans. The plan coordinator has overall responsibility for the TT&E plan, including development, implementation, and maintenance. The plan coordinator should identify a TT&E program coordinator, who is responsible for developing a TT&E plan and coordinating events. Depending on the type of event conducted, the TT&E program coordinator works with one or more design teams.

- **Establish overall TT&E schedule.** The TT&E plan should document the projected schedule of activities to be performed within the TT&E program. Although events should be conducted as needed, organizations should evaluate the required frequency of its events and document the frequency of each event in a TT&E schedule.

- **Document the TT&E event methodology.** As part of creating a TT&E program, an organization should select and document a high-level methodology for planning and performing TT&E events. Although the details of each phase typically vary based on the type of event conducted, the same phases should be used for each event. One commonly used methodology has the following phases:

  - **Design.** The TT&E program coordinator works with the plan coordinator to determine the TT&E event topic and scope based on the current needs of the organization. Next, the TT&E program coordinator identifies the objectives based on the topic and scope, and the personnel that should participate in the event. The TT&E program coordinator identifies an event design team, which may consist of one person or a group of people, depending on the requirements of the event. The TT&E program coordinator also oversees the event logistics.

  - **Development**. The TT&E program coordinator works with the design team on the development of the documentation to be used before, during, and after the event. Examples include briefing materials, participant manuals, and evaluation criteria.

  - **Conduct**. In this phase, the event is conducted—the personnel are trained, the IT plans exercised, or the systems or system components tested. The details of the conduct phase vary greatly by event type.

  - **Evaluation**. This phase involves analyzing the event and identifying lessons learned, both to improve the IT plans and their execution, and to improve the TT&E process.

3. Training Sessions

Training is a continuum of learning activities that enables staff to maintain and enhance their skills and technical proficiencies and to remain current with technological advances. For the purpose of this publication, training refers only to informing participants of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to that plan.[10] Training events can be instructor-led (e.g., classroom setting, interactive online) or self-study (e.g., paper, online).

The scheduling of training events that support IT plans should be coordinated closely with the schedules of other events in a TT&E program. For example, training sessions typically precede exercises and tests. This ensures that personnel are familiar with their roles and responsibilities within a given IT plan before exercising the plan itself. Another outcome of performing training is identifying areas where additional training might be necessary.

Other NIST publications have already described training programs and events in detail. Refer to NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, and NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, for more information on training.[11]

[10] Refer to NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, for more detailed information on the benefits of training events. It is available for download from http://csrc.nist.gov/publications/nistpubs/index.html.

[11] Both publications are available for download from http://csrc.nist.gov/publications/nistpubs/index.html.

This page has been left blank intentionally.

4. Tabletop Exercises

Tabletop exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. Tabletop exercises are conducted in an informal environment, with a facilitator guiding participants through a discussion designed to meet pre-defined objectives. One or more scenarios may be discussed during a single tabletop exercise. The duration of a tabletop exercise (typically two to eight hours) varies depending on the audience, the topic being exercised, and the exercise objectives. Tabletop exercises are cost-effective tools to validate the content of IT plans, such as contingency plans and incident response plans, to ensure the plan content is viable and implementable in an emergency situation.

This section provides guidance on evaluating the need for a tabletop exercise, and designing, developing, conducting, and evaluating a tabletop exercise. The section then summarizes the key elements to consider before, during, and after the conduct of a tabletop exercise. Appendix A provides a sample tabletop exercise facilitator guide, sample participant guide, and sample after action report.

4.1 Evaluate the Need for a Tabletop Exercise and Create a Schedule

As part of the TT&E program, the program coordinator should routinely determine the need for a tabletop exercise for a particular IT plan by considering the organization's overall objectives for conducting a tabletop exercise and answering questions such as the following:

- Have the personnel who would participate in the tabletop exercise been trained on their roles and responsibilities within the plan? If the personnel have not yet been trained, the TT&E program coordinator should consider conducting a training event before the tabletop exercise so that the personnel can participate more effectively in the tabletop exercise, increasing its benefits.[12]
- When was the last time the organization conducted a tabletop exercise for the plan?
- Have recent organizational changes been made that could impact the content of the plan?
- Has new TT&E guidance been issued that could impact the content of the plan?

Organizations should conduct tabletop exercises periodically; following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance; or as otherwise needed. For each tabletop exercise, the program coordinator should choose a form of tabletop exercise that is well-suited to meeting the identified needs and objectives. The tabletop exercise schedule should be coordinated closely with the schedules of the other events of the TT&E program. The TT&E program coordinator usually ensures that tabletop exercises are scheduled within a reasonable timeframe after a training event so that the personnel participating in the tabletop exercise are recently trained in their roles and responsibilities. It is important that when an exercise is being scheduled, managers are notified and their approval obtained. Ensuring that management has agreed to an exercise is an essential step in the development of the exercise.

4.2 Design the Tabletop Exercise Event

Once the need to conduct a tabletop exercise has been established, the TT&E program coordinator should work with the tabletop exercise design team to design the event. The design phase is often the most time-consuming phase of planning a tabletop exercise. Planning is typically started at least three months

[12] Some organizations find it more cost-effective to combine a tabletop exercise with a training session that immediately precedes the tabletop exercise.

before the conduct date for large, complex exercises and at least one month in advance for less complex exercises. Sections 4.2.1 through 4.2.6 describe the major steps in the event design process.

4.2.1 Determine the Topics

The design team should determine the exercise topic based on the focus of the plan being exercised. General topics can include contingency planning and incident response; specific topics range from sustaining essential functions to managing and reporting IT security incidents. For example, disaster recovery plan exercise discussion topics would likely include the roles and responsibilities of personnel with regard to the processes and procedures associated with restoring an organization's information systems. Incident response plan exercise discussion topics would likely include processes and procedures for managing and reporting IT security incidents.

4.2.2 Determine the Scope

The scope of the tabletop exercise should be determined based on the target audience. All personnel with responsibilities under the IT plan should participate in exercises; however, senior-level teams and operational-level teams should participate in separate tabletop exercises initially because of their different levels of responsibility. Once these two groups have been exercised individually, both groups should participate in a combined exercise to validate coordination between the groups.

The exercise should apply to the roles and responsibilities of personnel within the IT plan being exercised and focus on validating that the documented roles, responsibilities, and interdependencies are accurate and current. The types of questions asked of the participants during the course of the exercise should be tailored to the level of personnel exercised. Senior-level tabletop exercises typically range from two to four hours, while operational-level tabletop exercises range from two to eight hours. To ensure that the knowledge of the roles and responsibilities identified in the plan being exercised is current, it is often effective to conduct a training session in conjunction with any tabletop exercise lasting more than four hours.

4.2.3 Identify the Objectives

The objectives of any tabletop exercise should be validating the content of the IT plan and related policies and procedures, validating participants' roles and responsibilities as documented in the plan, and validating the interdependencies documented in the plan. An additional objective for some exercises is meeting regulatory and other such requirements associated with exercising plans, such as the requirement in NIST SP 800-53 for Federal agencies to conduct exercises or tests for their systems' contingency plans at least annually.

4.2.4 Identify the Participants

Based on the topic, scope, and objectives of the exercise, the design team determines who should participate in the event. [13] The participants should be comprised of the personnel with roles and responsibilities identified in the plan to help ensure the exercise meets its stated objectives. For example, senior-level personnel should be invited to participate if the primary exercise objective is to validate the decision-making and oversight processes within the plan. If the primary objective is to validate operational procedures, operational-level personnel should be invited to the exercise. If both groups have participated in previous tabletop exercises separately, it is appropriate to conduct a combined session, where senior-level and operational-level personnel discuss individual and team roles and responsibilities

[13] Depending on the requirements that the exercise is intended to fulfill, it may be necessary to make participation mandatory for designated personnel.

and coordination requirements. Once the appropriate participants have been identified, they should receive a written invitation or announcement of the exercise as soon as possible. This is typically accomplished in the form of an e-mail or memorandum by a member of the tabletop exercise design team, but, if more appropriate, may instead be distributed by a member of management.

4.2.5 Identify the Tabletop Exercise Staff

The design team usually designates an exercise *facilitator*, who leads the discussion among the exercise participants, and a *data collector*, who records information about the actions that occur during the exercise. The facilitator and the data collector should be thoroughly familiar with the content of the IT plan being exercised and with the exercise objectives. The facilitator and data collector should meet before the event to discuss the details surrounding the exercise, including its scope and objectives. At this time, the facilitator and the data collector review the results from previous tabletop exercises, if applicable, to heighten their awareness of potential issues before the event.

4.2.6 Coordinate the Logistics

One person on the design team should typically be responsible for coordinating the exercise event's logistics. The logistics coordinator usually begins to do this at least one month before the conduct of the tabletop exercise. The checklist in Table 4-1 can be used as a starting point by the logistics coordinator to ensure the necessary tasks are completed.

Table 4-1. Sample Logistics Checklist for Tabletop Exercise Events

Logistics	Target Date	Completed
Select a date for exercise conduct		
Reserve a conference room that will accommodate all participants		
Determine the need for audio/visual equipment		
Reserve audio/visual equipment, if applicable		
Identify the facilitator and data collector		
Identify participants		
Invite participants		
Coordinate the development of the facilitator guide and participant guides		
Arrange for the printing of name tents		
Ensure conference room is available in sufficient time before the exercise to perform setup		
Arrange for refreshments, if appropriate		
Copy all files as a backup onto a CD-ROM, USB flash drive, or other removable media		

4.3 Develop the Tabletop Exercise Material

Once the event is designed, the design team should assign roles and responsibilities to its members to develop the tabletop exercise material. Tabletop exercises typically include the following documentation:

- **Briefing.** A briefing is created for the participants; it includes an agenda and logistics information.

- **Facilitator Guide.** The facilitator guide includes the following:
  - The purpose for conducting the exercise
  - The exercise's scope and objectives
  - The exercise's *scenario*, which is a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives
  - A list of questions regarding the scenario that address the exercise objectives[14]
  - A copy of the IT plan being exercised.

  The types of questions documented in the facilitator guide should be tailored to the participants. For example, if senior-level personnel are the participants, the questions should be of a more general, high-level nature and focus on decision-making and oversight, which are consistent with their roles and responsibilities within the plan. If operational personnel are the participants, the questions should typically be focused on specific procedures and processes that are followed to carry out roles and responsibilities.
- **Participant Guide.** The participant guide includes the same information as the facilitator guide without the list of questions. Participant guides contain a modified, shorter list of questions to orient participants to the types of issues that may be discussed during the exercise.
- **After Action Report.** An after action report is developed after the exercise event; it contains information based on pre-identified evaluation criteria. The criteria should be developed before the exercise to ensure data collectors know what type of information to capture during the exercise and, ultimately, document in the after action report. Evaluation criteria are based on the exercise objectives and provide a means to evaluate how well exercise objectives were met and identify areas where additional exercises might be necessary. After action reports are discussed in more detail in Section 4.5.

Sample tabletop exercise documentation is located in Appendix A.

A common misconception is that scenarios must be very detailed to be effective. Actually, it is often more effective to develop a short, concise scenario. During tabletop exercises with long, detailed scenarios, participants often spend more time dissecting the scenario and discussing its content than they spend on meeting the objectives of the exercise. If a detailed scenario is desired, a trusted agent with detailed knowledge of the plan and all the procedures documented within the plan should aid in the development of the scenario to ensure accuracy. In addition, the facilitator should have the ability to redirect the participants' focus from the scenario to the objectives, should they begin focusing too much on the content of the scenario.

4.4 Conduct the Tabletop Exercise

Tabletop exercises are usually conducted in a classroom-type setting. This permits a facilitator to address each individual or the participants as a group while facilitating the exercise. This also fosters communication among the participants, as does placing a name tent on the table for each participant

[14] Samples of exercise scenarios and related lists of questions are available from NIST SP 800-61, *Computer Security Incident Handling Guide*, and NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*. Both publications are available from http://csrc.nist.gov/publications/nistpubs/.

before the start of the exercise. This is particularly important if participants and teams work within different operational areas of the organization. Participants are usually not seated with their teammates to encourage independent thought processes and provide exposure to other operational areas. A copy of the participant guide should be placed with each name tent.[15]

At the start of the exercise, the facilitator welcomes the participants to the event and request that the participants introduce themselves by name and give a general description of their roles within the organization. The facilitator then projects the briefing and discusses the scope of the exercise and logistics information. The facilitator then walks participants through the scenario and kicks off the discussion with one of the discussion questions documented in the facilitator guide, designed to prompt decision-making or coordination among participants.[16] Following the kickoff, the discussion occurs naturally among participants based on the scenario and the objectives. The facilitator may inject periodic questions from the facilitator guide. If the discussion does not occur naturally, the facilitator should prompt discussion by asking additional questions from the facilitator guide until all objectives are met. During the course of the exercise, the data collector should record observations to be included in the after action report.

Immediately following the facilitated discussion, the facilitator and data collector should conduct an exercise debrief, often referred to as a hotwash. During the debrief, the facilitator asks participants in which areas they felt they excelled, in which areas they could use additional training, and which areas of the plan should be updated.

4.5 Evaluate the Tabletop Exercise

The comments that surface during the debrief, along with lessons learned documented by the data collector during the exercise, should be captured in the after action report. The introduction to the after action report should describe background information about the exercise such as purpose, objectives, participants, and the scenario. The after action report should also contain documented observations made by the facilitator and data collector during the exercise and recommendations for enhancing the IT plan that was exercised.

Following the development of the after action report, the plan coordinator might assign action items to select personnel to update the IT plan being exercised. The plan coordinator should then update the plan, if appropriate, by implementing recommendations made in the after action report. It may also be necessary to brief certain managers on the results of the exercise, update other security-related documents, and perform other actions based on the exercise.

4.6 Summary

Tabletop exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. Tabletop exercises are conducted in an informal environment, with a facilitator guiding participants through a discussion designed to meet

[15] Although participants typically receive the participant guides the day of the exercise, the exercise design team may elect to deliver copies of the guide to participants in advance to provide them the opportunity to familiarize themselves with the exercise topic. If the guides are sent in advance, it is often most effective to do so approximately one week before the exercise. If they are sent too far in advance, the content may be forgotten. If the guides are sent too close to the event, participants might not have an opportunity to read them.

[16] If the tabletop exercise is combined with a training event, the trainer begins the session by providing participants with an overview of the plan and their individual and team roles and responsibilities within the plan. The facilitator then administers hands-on activities before the scenario discussion that prompt participants to work though problems and identify solutions in a discussion-based, team environment.

pre-defined objectives. One commonly used methodology for planning and performing tabletop exercise events has the following phases:

- **Design.** The TT&E program coordinator works with a tabletop exercise design team to design the event. The design phase is often the most time-consuming, and planning for exercises typically starts at least one month in advance (three months for large, complex exercises). The major steps in the event design process are as follows:
  - Determine the exercise topic based on the focus of the plan being exercised
  - Determine the exercise scope based on the target audience
  - Identify the objectives of the exercise
  - Identify the individuals that should participate in the exercise and invite them to the event
  - Identify the staff for the exercise, including a facilitator and a data collector
  - Coordinate the logistics for the exercise event.
- **Development.** The design team creates the documentation to be used before, during, and after the exercise event. Typical documentation includes a briefing, a facilitator guide, a participant guide, and an after action report.
- **Conduct.** In this phase, the IT plan is actually exercised. Tabletop exercises are usually conducted in a classroom-type setting. The facilitator provides a briefing to the participants, then walks them through the scenario and initiates a group discussion using a question from the facilitator guide. As the discussion continues, the facilitator may inject additional questions periodically. The data collector documents issues to be included in the after action report. Immediately following the facilitated discussion, the facilitator and data collector conduct an exercise debrief, in which they ask the participants in which areas they excel, in which areas they could use additional training, and which areas of the IT plan should be updated.
- **Evaluation.** The comments from the debrief, along with lessons learned during the exercise, should be captured in an after action report. The report should include background information about the exercise, documented observations made by the facilitator and data collector, and recommendations for enhancing the IT plan that was exercised. Outcomes of the evaluation could include updating the IT plan or other security-related documents, briefing managers on the results, and performing other actions.

5. Functional Exercises

Functional exercises allow personnel with operational responsibilities to validate their IT plans and their operational readiness for emergencies by performing their duties in a simulated operational environment. Activities for a functional exercise are scenario-driven, such as a particular building's IT systems becoming unavailable in the simulated environment and the participants then learning that the building is on fire. Additional situations are often simulated during the course of the exercise. Functional exercises are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of an IT plan (e.g., communications, emergency notifications, IT equipment set-up). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. The duration of functional exercises typically lasts from between several hours to several days, depending on the event's objectives and the complexity of the plan being exercised.

This section provides guidance on evaluating the need for a functional exercise, and designing, developing, conducting, and evaluating a functional exercise. The section then summarizes the key elements to consider before, during, and after the conduct of a functional exercise. Appendix B provides functional exercises samples, including a scenario, a tracking form, and an after action report.

5.1 Evaluate the Need for a Functional Exercise and Create a Schedule

As part of the TT&E program, the program coordinator should routinely determine the need for a functional exercise for a particular IT plan by considering the organization's overall objectives for conducting a functional exercise and answering questions such as the following:

- Have the personnel who would participate in the functional exercise been trained on their roles and responsibilities within the plan? Have tabletop exercises for the plan been held on which potential functional exercises could build? If the personnel have not yet been trained, or initial tabletop exercises have not been held, the TT&E program coordinator should consider first conducting a training event and a tabletop exercise before the functional exercise so that the personnel can participate more effectively in the functional exercise, increasing its benefits.
- When was the last time the organization conducted a functional exercise for the plan?
- Have recent organizational changes impacted the contents of the plan?
- Has new TT&E guidance been issued that could impact the contents of the plan?

Organizations should conduct functional exercises periodically; following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance; or as otherwise needed. It is usually best to ensure adequate staff training and tabletop exercises have taken place before engaging in a functional exercise. The functional exercise schedule should be coordinated closely with the schedules of the other events of the TT&E program. The TT&E program coordinator usually ensures that functional exercises are scheduled within a reasonable timeframe after a tabletop exercise event. It is important that when an exercise is being scheduled, that managers are notified and their approval obtained. Ensuring that management has agreed to an exercise is an essential step in the development of the exercise.

5.2 Design the Functional Exercise Event

Once the need to conduct a functional exercise has been established, the TT&E program coordinator should work with the functional exercise design team to design the functional exercise event. The team is comprised of personnel who are familiar with the plan's content and can facilitate the exercise design

process. The design phase of a functional exercise is usually started at least a few months before the desired conduct date, depending on the complexity of the exercise. Sections 5.2.1 through 5.2.6 describe the major steps in the event design process.

5.2.1 Determine the Topic

The design team should determine the overarching objectives for exercising the IT plan (e.g., as part of a strategic long-term plan, in response to ad hoc requirements). These broad objectives represent the topic areas that will be addressed in the exercise. The topic areas chosen will depend on whether the exercise will address the full plan or specific aspects of the plan. Topic areas addressing the full plan could include (but are not limited to) validating the plan's procedures, evaluating an organization's ability to implement the plan, and assessing interdependencies of organizations and personnel responsible for carrying out the plan. Examples of topic areas that are more narrowly focused on specific aspects of the plan are assessing the plan's alert and notification process, validating personnel responsibilities associated with the operational phase of the plan, and evaluating the processes involved in resuming normal operations.

5.2.2 Determine the Scope

The scope of the functional exercise should be determined based on which portions of the IT plan (or all of it) should be exercised.[17] If only portions of the plan are to be exercised, the design team should consider examining a specific phase of plan implementation, such as activation, operation, or reconstitution, or specific functions.

When determining the scope of a functional exercise, the design team should clearly identify the specific element or elements of the IT plan that will be assessed and consider the types of participants necessary to carry out the exercise. Ultimately, a robust TT&E program ensures that all elements of a plan are exercised; however, the emphasis of initial functional exercises is often placed on operational-level team roles and responsibilities. As an organization's TT&E program matures, senior-level participants can also engage in functional exercises to fully validate decision-making aspects of the plan.

5.2.3 Identify the Objectives

The objectives of any functional exercise should be validating the content of the IT plan, validating participants' roles and responsibilities as documented in the plan, validating the interdependencies documented in the plan, and providing an opportunity for participants to get hands-on practice in executing their functions. An additional objective for some exercises is meeting regulatory and other such requirements associated with exercising plans, such as the requirement in NIST SP 800-53 for Federal agencies to conduct exercises or tests for their systems' contingency plans at least annually. Specific objectives should be documented and clearly articulated to exercise participants.

5.2.4 Identify the Participants

Based on the topic, scope, and objectives of the exercise, the design team determines who should participate in the event.[18] The participants should be comprised of the personnel with roles and responsibilities under the plan that will be needed to help ensure the exercise meets its stated objectives. For example, senior-level personnel should be invited to participate if the primary exercise objective is to validate the decision-making and oversight processes within the plan. If the primary objective is to

[17] A comprehensive exercise of an entire IT plan is sometimes known as a *full-scale exercise*.

[18] Depending on the requirements that the exercise is intended to fulfill, it may be necessary to make participation mandatory for designated personnel.

validate operational procedures, operational-level personnel should be invited to the exercise. Finally, if the primary objective is to validate the full-scale readiness of a plan, both senior-level personnel and operational-level personnel should participate. Once the appropriate participants have been identified, they should receive a written invitation or announcement of the exercise as soon as possible. This is typically accomplished in the form of an e-mail or memorandum by a member of the functional exercise design team, but, if more appropriate, may instead be distributed by a member of management.

5.2.5 Identify the Functional Exercise Staff

The design team usually designates an *exercise director*, who is responsible for all aspects of the exercise, including staffing, development, conduct, and logistics. The exercise director designates one or more *controllers*, who monitor, manage, and control exercise activity; *data collectors*, who record information about the actions that occur during the exercise; and *simulators*, who simulate or otherwise represent non-participating individuals and organizations whose input is necessary to the flow of the exercise. The controllers, data collectors, and simulators should be thoroughly familiar with the content of the IT plan being exercised and with the exercise objectives.

The exercise director, controllers, data collectors, and simulators should meet before the event to discuss the details surrounding the exercise, including its scope and objectives. At this time, the exercise director, controllers, data collectors, and simulators review the results from previous tabletop and functional exercises, if applicable, to heighten their awareness of potential issues before the event.

5.2.6 Coordinate the Logistics

One or more members of the design team should typically be responsible for coordinating the exercise event's logistics. The logistics coordinator(s) typically begin to do this approximately three months before the conduct of the functional exercise. The checklist in Table 5-1 can be used as a starting point by the logistics coordinator(s) to ensure the necessary tasks are completed.

Table 5-1. Sample Logistics Checklist for Functional Exercise Events

Logistics	Target Date	Completed
Select a date for exercise conduct		
Make arrangements with facility manager(s) at the facilities at which the exercise is conducted		
Identify the controllers, data collectors, and simulators		
Identify participants		
Invite participants		
Coordinate the development of controller, data collector, simulator, and participant books		
Arrange for the printing of name tags for controllers, data collectors, and simulators to ensure they are readily recognizable during the exercise		
Arrange for transportation and billeting, if applicable		
Ensure that appropriate equipment is available and properly configured to function at exercise site(s)		
Arrange for refreshments, if appropriate		
Create a supplies checklist to include items such as power strips, extension cords, markers, and tape for the control cell		
Copy all files as a backup onto a CD-ROM, USB flash drive, or other removable media		

5.3 Develop the Functional Exercise Material

Once the event is designed, the exercise director should assign roles and responsibilities to the team to develop the functional exercise material. Functional exercises typically include the following documentation:

- **Briefings.** Briefings and/or briefing books are usually created for participants and the exercise staff; briefings may be conducted in person or through read-ahead packages. Depending on the nature of the exercise, a single briefing might be presented approximately one week before the exercise, or multiple briefings might be presented in the weeks and months before the exercise, with the final briefing typically occurring a week or more before the exercise. The briefings document any information pertaining to the scope and objectives of the exercise, rules of engagement, and administrative aspects of the event. In addition, briefings are conducted to provide the exercise staff with information pertaining to management aspects of the event, the level of activities that are simulated, and the level of activities that are directed by player action.

- **Scenario.** The scenario is designed to add realism to the exercise by providing participants with situations that will inspire responses that help participants achieve exercise objectives. The scenario chosen should be crafted to adequately address the broad topic areas and specific objectives selected in the design phase. In addition, exercise developers should ensure the scenario does not stray outside the scope of the exercise. Exercise scenarios may be crafted to explore worst-case situations; however, it is often useful to develop scenarios that cause participants to respond to topical issues they are apt to encounter in the real world. For example, an exercise of an IT contingency plan for an organization that is prone to disruptions from natural disasters may consider a scenario involving a significant power outage caused by a hurricane. A narrative scenario is documented and typically distributed to participants via handouts or an oral presentation on the day of the exercise.

- **Master Scenario Events List (MSEL).** The MSEL is a chronologically sequenced outline of the simulated events and key event descriptions that participants will be asked to respond to during the course of exercise play. It also contains a list of expected actions resulting from the events and objectives that should be met based on the events. The MSEL regulates simulated events by coordinating the actions of participants and defining the schedule of events. The MSEL should be planned carefully to ensure that key events lead to the achievement of exercise objectives and that all participants remain active throughout the duration of the event. The MSEL is for exercise development and management purposes only.

- **Message Injects.** A message inject, also known as an implementer or an event inject, is a pre-scripted message that will be provided to participants during the course of an exercise. An example of a message inject is "The vehicle transporting the backup tapes to the restoration site is in a traffic jam, and is expected to arrive 3 hours later than originally scheduled." Message injects can be provided in many forms, including e-mails, letters, memoranda, telephone calls, and radio call scripts. Each message inject contains information designed to supplement the scenario and prompt additional actions. They expand on the outline of key events portrayed in the MSEL; therefore, each MSEL entry may have multiple injects associated with it. The intent of each inject is in concert with the storyline of the overall scenario and MSEL, and prompts a player to take an action that will ultimately lead to achievement of an exercise objective(s). Each inject includes the time at which the message will be injected, to whom it will go, from whom the message will come, the means by which it will be delivered (e.g., fax, phone, e-mail), and the actual text of the message. The number of injects selected should be designed to keep participants adequately occupied but should not be so many that participants will become

overwhelmed. Therefore, the number of injects selected will vary based on the duration of the exercise.

- **Message Inject Tracking Form.** Message inject tracking forms contain the inject numbers, scheduled times for the messages to be injected into the exercise, actual times that the messages were injected, summaries of the message, and any comments for the individuals injecting the messages.[19]

- **Controller, Data Collector, and Simulator Books.** These books contain all information relevant to the exercise staff. Each controller, data collector, and simulator typically receives a book the day of the exercise (or the day of the briefing, if deemed appropriate) containing information pertinent to their roles during the exercise. The books contain the exercise scenario, MSEL, and injects.

- **After Action Report.** An after action report is developed after the exercise event; it contains information based on pre-identified evaluation criteria. Another important aspect of the development phase is determining and documenting exercise evaluation criteria that will be used by data collectors during the conduct of the event. Evaluation criteria are closely tied to the exercise objectives to help data collectors know what type of information to capture during the exercise and ultimately document in an after action report. Once evaluation criteria have been developed, it is often helpful to create forms or other tools that will aid in the data collection process. Such forms instruct data collectors of specific player actions to look for and serve as a roadmap that is used in determining whether specific exercise objectives were met, how they were met, what improvements may need to be made to the plan that is being exercised, and where additional exercises might be necessary. After action reports are discussed in more detail in Section 5.5.

Sample functional exercise documentation is located in Appendix B.

In addition to the members of the design team discussed previously, functional exercise material development might require assistance from other individuals. For example, a trusted agent who has detailed knowledge of the IT plan and the associated procedures could aid in the development of the scenario, MSEL, and message injects to ensure accuracy. As described in Section 4.3, it is often most effective to have a short, concise scenario so that participants do not focus on critiquing the scenario itself.

5.4 Conduct the Functional Exercise

Functional exercises are typically conducted in real or near-real time and prompt participants to carry out their roles and responsibilities as realistically as possible. A functional exercise is often initiated by a telephone call or other appropriate means, alerting selected personnel of the implementation or activation of a specific IT plan. This alert prompts further notification of all personnel who would be notified via the means identified in the plan. Once the notification process is completed, participants are expected to carry out operational or decision-making activities documented in the plan. Depending on the scope of the exercise, activities could range from implementing notification procedures to deploying to an alternate site to mobilizing resources, including staff and equipment. The exercise scope dictates whether deployments or mobilizations are simulated or if they actually occur. Regardless of location, the participants should carry out the activities as they would according to the plan being exercised. Participants should be informed of any exercise artificialities during the participant briefing.

[19] Message injects and message inject tracking forms are sometimes included within the MSEL documentation.

Controllers, data collectors, and simulators should be pre-positioned at the location where the exercise takes place. Controllers form a *control cell*—a central location for exercise coordination, typically in a separate area from the exercise participants—from which the controllers introduce the scenario and message injects to participants. Controllers administer the exercise by referring to the message inject tracking form and MSEL to ensure the exercise remains on schedule and within scope.

Data collectors directly observe player actions during the exercise. They refer to the evaluation criteria and any other evaluation forms that the data collection team may create to aid their efforts. Simulators assume the roles of various internal and external entities that are not participating in the event, such as other government organizations, private citizens, or law enforcement. Information provided by simulators should be delivered in accordance with how it would be provided by the organization(s) being simulated. They coordinate closely with the controllers and exercise director to ensure their responses are consistent with the MSEL. Simulators may be collocated with controllers or assemble a response cell in a separate room. During the course of exercise, the exercise director, controllers, data collectors, and simulators should remain in constant contact with each other to ensure that the exercise remains coordinated and on schedule.

The exercise director announces when the exercise concludes. Typically, this occurs when the time allocated for the exercise has ended, or earlier if all objectives have been met or the MSEL and injects have been fully played out. In cases where a real-world emergency occurs, it is the exercise director's responsibility to call an immediate end to the event. Following the conclusion of exercise play, the exercise director, controllers, and data collectors should conduct an exercise debrief with participants, often referred to as a hotwash. The exercise director leads the hotwash and requests feedback from participants, controllers, simulators, and data collectors. Immediately following the exercise, the controllers, data collectors, simulators, and participants should be asked to provide the exercise director with their notes or any forms completed during the course of the exercise and the hotwash session.

5.5 Evaluate the Functional Exercise

During the evaluation phase, the exercise director relies on the design team or other specified staff to develop the after action report that documents findings and recommendations from the functional exercise. Exercise notes, forms, and other material created during the course of exercise play and during the hotwash are the basis of the after action report. The introduction to the after action report should document background information about the exercise such as the scope, objectives, and scenario. The after action report should also document observations made by the exercise staff and participants during the exercise and recommendations for enhancing the IT plan that was exercised. The after action report should also include a list of exercise participants and may provide information from any participant surveys that were distributed during the hotwash to solicit feedback.

Following the development of the after action report, the plan coordinator might assign action items to select personnel in an effort to update the IT plan being exercised. The plan coordinator should then update the plan, if appropriate, by implementing recommendations made in the after action report. It may also be necessary to brief certain managers on the results of the exercise, update other security-related documents, and perform other actions based on the exercise.

5.6 Summary

Functional exercises allow personnel with operational responsibilities to validate their IT plans and their operational readiness for emergencies in a simulated operational environment. Activities for a functional exercise are scenario-driven, such as a particular building's IT systems becoming unavailable in the simulated environment and the participants then learning that the building is on fire. Additional situations

are often simulated during the course of the exercise. Functional exercises are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of an IT plan. Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.

One commonly used methodology for planning and performing functional exercises has the following phases:

- **Design.** The TT&E program coordinator works with a functional exercise design team to design the event. The design phase is usually started three to six months in advance of the event. The major steps in the event design process are as follows:
  - Determine the exercise topic based on the overarching objectives for exercising the IT plan
  - Determine the exercise scope based on which portions of the IT plan should be exercised
  - Identify the objectives of the exercise
  - Identify the individuals that should participate in the exercise and invite them to the event
  - Identify the staff for the exercise, including an exercise director and one or more controllers, data collectors, and simulators
  - Coordinate the logistics for the exercise event.
- **Development.** The design team creates the documentation to be used before, during, and after the exercise event. Typical documentation includes briefings for participants and exercise staff; a scenario; a master scenario events list (MSEL); message injects and a message inject tracking form; an after action report; and controller, data collector, and simulator books.
- **Conduct.** Functional exercises are typically conducted in real or near-real time and prompt participants to carry out their roles and responsibilities as realistically as possible. A functional exercise is often initiated by a telephone call or other appropriate means, alerting selected personnel of the implementation or activation of a specific IT plan. Participants are expected to carry out operational or decision-making activities documented in the plan. The exercise controllers administer the exercise, including introducing the scenario and message injects to participants. Data collectors directly observe player actions during the exercise. Simulators assume the roles of entities that are not participating in the event, such as external organizations or private citizens. The exercise director announces the conclusion of the exercise. Immediately following the exercise play, the exercise director, controllers, and data collectors conduct an exercise debrief with the participants, requesting feedback from everyone present.
- **Evaluation.** The comments from the debrief, along with lessons learned during the exercise, should be captured in an after action report. The report should include background information about the exercise, documented observations made by the exercise staff, and recommendations for enhancing the IT plan that was exercised. Outcomes of the evaluation could include updating the IT plan or other security-related documents, briefing managers on the results, and performing other actions.

This page has been left blank intentionally.

6. 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 (e.g., operating system, application, pager, Blackberry) that are identified as critical in an IT plan.[20] Tests can take several forms, including the following:

- **Component testing** is testing individual hardware or software components, or groups of related components. A component test also might test processes and procedures that are part of any of the organization's IT plans. The testing of hardware or software components at the conclusion of their development should also be conducted, but this is not within the scope of this document. Component testing in this document is concerned with individual components already operational that are critical to the effective operation of the organization that they should be regularly tested.
- **System testing** is testing complete systems to evaluate each system's compliance with specified requirements. A system test should also include an examination of any processes or procedures related to the system being tested.
- **Comprehensive testing** is testing all systems and components that support an IT plan. These tests generally involve multiple components and systems and may become quite extensive in their scope. An example of a comprehensive test is confirming that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.

A test is conducted in as close to an operational environment as possible, which means that the test should be conducted in a manner that resembles the everyday work environment in which the system or component is found. If feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used. Tests can potentially be disruptive to an organization's operations, so tests are sometimes performed on systems that mimic the actual operational systems, especially if there is not strong confidence that the tests will be completely successful.

This section provides guidance on evaluating the need for testing; creating a test plan; and designing, developing, conducting, and evaluating a test. The section then summarizes the key elements to consider during a test and after conducting a test. Appendix C provides test documentation examples, including a test plan, a test briefing, test validation and evaluation worksheets, and an after action report.

6.1 Evaluate the Need for a Test and Create a Schedule

As part of the TT&E program, the program coordinator should routinely determine the need for a test by considering the organization's overall objectives for conducting a test and answering questions such as the following:

- Is the system or component to be tested installed and ready for operational use?
- Are the processes and procedures for the system or component established?
- Have the personnel been trained on the use of the system or component? Was the training effective?

[20] The testing described in this publication should not be confused with testing performed in support of system certification and accreditation (C&A) efforts. Testing for C&A focuses on the security of systems under normal conditions, whereas TT&E test events focus on the functionality of systems under adverse conditions as defined in IT plans, such as contingency plans and incident response plans. Although the requirements of C&A and TT&E test events are usually quite different, in some cases it might reduce duplication of efforts to have a single testing event that encompasses both the C&A and the TT&E sets of requirements.

- Are there requirements (e.g., compliance efforts, regulations) that mandate certain tests be performed on a specific schedule or frequency, such as compliance with NIST SP 800-53?

- When was the last time that this component, system, or group of components and systems was tested? Have there been any significant changes or updates since the completion of the last test?

Tests are usually conducted after personnel have been trained on the use of the systems or components being tested and before the systems or components become operational, to ensure they do not adversely affect the security posture or other operational aspects of the organization. If personnel have not yet been trained, system testing should be delayed until the training has been completed. After operational use has begun, periodic testing should be conducted to ensure the continued proper and secure use of the systems or components. Comprehensive tests should also be scheduled periodically to ensure that the IT plans are reasonable, effective, and complete, and that personnel know what their roles and responsibilities are in the conduct of the plans. High personnel turnover might necessitate more frequent testing to maintain the level of preparedness the organization requires.

The scheduling of tests should also consider factors such as available resources and the potential impact on the organization. It is important that when a test is being scheduled, that senior managers are notified and the potential impact on operations assessed to determine the best time to conduct the test. For example, conducting a test that might affect the operations of the organization might not be wise during known peak operational periods. Although scheduling comprehensive tests when many employees are on vacation or on holiday breaks might have a minimal impact on operations, it also could limit the number of available personnel. Ensuring that senior leadership in the organization has agreed to the test, especially for comprehensive tests, is an essential step in the development of the test.

Testing schedules might also be affected by factors external to the organization itself. For example, compliance and regulatory issues might dictate that certain tests be performed on a periodic basis. Another example is environmental and safety issues; a test requiring that staff relocate operations from one facility to another might be better accomplished when the weather is not unpredictable so that employees do not have to travel under extreme conditions, such as a blizzard.

6.2 Design the Test Event

Once the need to conduct a test has been established, the TT&E program coordinator should create a test design team[21] to design each specific test. Several factors can have a significant bearing on the design of the test, including the level of the test (component, system, or comprehensive), the organizational entities involved, and the scope of the test. These factors can affect the lead time required to develop the test, the level of complexity for the test, and the length of time the test will take. At an early stage in the design process, the personnel who will participate in the test should be identified and the senior managers for these affected areas should be contacted. Sections 6.2.1 through 6.2.6 describe the major steps in the event design process.

6.2.1 Determine the Scope

The scope of the test should be determined based on current system or security requirements and any potential compliance or regulatory requirements. The scope of the test is directly shaped by the type of test. Component tests are more focused and generally involve fewer individuals and organizational entities. System tests are broader in scope and include more personnel and multiple components.

[21] The test design team should include a team leader and subject matter experts for each of the areas to be tested; they should develop the content of the test cooperatively.

Comprehensive tests involve much larger portions of the organization, potentially all personnel, and require more extensive coordination and planning.

6.2.2 Identify the Objectives

The design 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. Where possible, the expected results or outcomes should be expressed in an objective and measurable manner, with subjective measurements being minimized. The results should be quantifiable and repeatable to the extent reasonably possible.

Tests are often performed as part of standard operational activities, such as restoring a backup, moving a server from one room to another, upgrading or patching operating systems or applications, or changing hardware components (e.g., swapping hard drives, replacing a failed power supply). Combining tests with operational activities is generally more efficient than performing them separately and is also less likely to negatively impact operations.

Other examples of common tests are activating call tree cascades and determining if they can be executed within prescribed time limits, and removing power from a system or system component.

6.2.3 Determine the Testing Tools

The design team should specify the assessment tools and procedures needed to accomplish the test. The specific tools needed may vary greatly depending upon the scope of the test. Tools might range from specialized software or hardware tools (e.g., network sniffers, vulnerability scanners) to measurement and recording devices (e.g., stopwatches, cameras, video recorders) to checklists used to measure adherence to defined processes and procedures. Tools might also include items needed by the test team for logistical support (e.g., radios, cell phones, badges).

6.2.4 Identify the Participants

The participants in a test vary based on the scope of the test to be performed. Participation in testing events can be thought of in two levels:

- The first level of participant consists of the individuals who are operating the components or systems being tested.
- The second level of participant consists of those individuals who are not directly involved in the test, but who might be impacted by the test or related activities. For example, if the test included an evacuation drill, the involved participants would be all personnel who were forced to evacuate, while affected individuals would include those individuals who might be trying to contact the evacuated people but could not reach them because they were not in their offices.

The design team should attempt to identify both levels of participants, although for larger tests the affected individuals might have to be identified in groups instead of individually. Individuals in the first level of participants should be notified well in advance of the test through an e-mail or memorandum. Individuals and groups in the second level of participants should be notified before the test occurs; examples of this include an announcement to the participants of possible disruptions to the systems being tested and a message on a help desk phone number stating that disruptions may occur to the systems being tested between certain hours.

6.2.5 Identify the Test Staff

The design team usually designates a *test director*, who is responsible for all aspects of the test, including staffing, development, conduct, logistics, and oversight of the design team. The test director designates one or more data collectors, who monitor and record the results of the test. The test director and data collectors should meet before the event to discuss the details surrounding the test, including its scope and objectives. At this time, the test director and data collectors review the results from previous exercises and tests, if applicable, to heighten their awareness of potential issues before the event.

The design team also often includes one or more individuals that are subject matter experts in the areas being tested. These individuals can help develop the test plan and identify the necessary testing tools. Because they are aware of the details of the test, these individuals should not be participants in the test; instead, they can be test observers, facilitators, data collectors, or controllers.

6.2.6 Coordinate the Logistics

The design team should begin to coordinate the logistical support far enough in advance to ensure the successful completion of the test. The time required for coordination also depends on the scope, and typically varies from a month in advance for component testing to several months for a comprehensive test of components and systems for a large IT plan such as a disaster recovery plan or incident response plan. The checklist in Table 6-1 contains examples of possible logistics actions that might need to be performed. Although specific logistical elements are identified during the test design phase, it is imperative that the required list of logistical components be updated frequently, especially after the test is fully developed.

Table 6-1. Sample Logistics Checklist for Test Events

Logistics	Target Date	Completed
Select a date for conducting 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		
Reserve audio/visual and recording equipment, if applicable		
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 test documents and files as a backup onto a CD-ROM, USB flash drive, 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 of the test to be performed, if necessary		
Review procedures to terminate the test, should operational issues necessitate it		

6.3 Develop the Test Material

Once the event is designed, the design team needs to create test documentation. The magnitude of this work depends on the scope of the test. This documentation could include the following:

- **Briefings.** For larger system or comprehensive tests, an initial meeting may be used to signal the start of the event. Specific briefings to senior management and to the managers of others that might be affected by the test need to be developed to provide an understanding of what the test will comprise and why it is important.
- **Test Guide.** This document outlines the basic steps involved in conducting a test and includes a list of the participants. It should also include a list of all individuals and groups who might be affected by the test, and discuss procedures for early termination of the test should events necessitate this action. This guide provides an overall examination of what will occur during the test.
- **Test Plans.** For each specific test to be performed, a test plan needs to be developed that outlines the specific steps that will be performed. Each step should include a list of required logistical items and delineate the expected outcome or response from this step. The procedures for early test termination should be repeated in this documentation, because the evaluators or the people conducting the test should be using the documentation during the test. A list of emergency contact numbers (including cell phone and pager numbers) should also be included.
- **After Action Report.** An after action report is developed after the test is completed. It should contain the results of each individual test as well as an overall synopsis of the test activities. Corrective actions and recommendations are one element of this report. For larger tests, an executive summary for senior management should also be created that provides a synopsis of the test, the results of the test, and the recommendations for improvement.

When developing a comprehensive test for an IT plan, there might be significant overlap with what would occur when developing a functional exercise for the same plan. In fact, many comprehensive tests have test plans that include materials similar to those used for functional exercises, including a scenario, an MSEL, and message injects. For example, during a test, participants may be told that a particular backup tape has failed, a certain server is unusable, or a road to the backup facility is closed. The key difference between a functional exercise and a test is that a test is conducted in an operational environment whenever possible, and it is designed to validate the actual effectiveness of both the processes and procedures for system recovery and restoration outlined in the plan, as well as the training that has been conducted, to ensure personnel understand their responsibilities and know how to react in a given situation.

6.4 Conduct the Test

The locations for tests vary based on the type of test being conducted and the test's scope. For example, a small component test could be conducted in a single office, while a comprehensive test of components and systems for an IT plan could involve many different parts of an organization in various locations.

Safety and security are two elements that should be maintained during any test. The organization's operational systems and networks need to be protected so that they do not sustain damage. The core function or mission of the organization should not be disrupted to the extent that the organization can no longer function and provide the services that it was created to provide. For these reasons, the test director should monitor all tests closely. At any sign of a possible catastrophic disruption, or in the event that the

safety of an individual is at stake or the security of the organization or its data is in question, the test director and any member of the test team should have the ability to terminate the test immediately.

Following the conclusion of the test, the test director and data collectors should conduct an informal test debrief with participants, often referred to as a hotwash. The test director leads the hotwash and requests feedback from the participants and data collectors. Immediately following the test, the data collectors and participants should be asked to provide the test director with their notes or any forms completed during the course of the test and the hotwash session.

6.5 Evaluate the Test

During the evaluation phase, a member of the design team or another selected staff member should develop an after action report that determines how well the tested systems or components functioned. The introduction to the after action report should document background information about the test such as the scope, objectives, and tests. The after action report should also document observations made by the test team during the test and recommendations for enhancing the IT plan that had its components or systems tested, along with associated procedures and components. The after action report should also include a list of test participants and may provide information from any participant surveys that were distributed during the hotwash to solicit feedback.

The after action report typically takes a few days to prepare. In the event that critical lapses in security or safety are noted, the test director should not wait until the final report is created to notify management. An informal report should be generated immediately with any critical changes that should be made, with the full report following in a reasonable amount of time. A formal debrief is sometimes conducted after a test so that the test director, plan coordinator, and other management staff can discuss the results of the test. Stakeholders typically review the report and may provide suggestions for minor wording changes, such as strengthening a recommendation to ensure that its importance is clear.

Following the development of the after action report, the plan coordinator might assign action items to select personnel to update the IT plan that had its components or systems tested. The plan coordinator should then update the plan, if appropriate, by implementing recommendations made in the after action report. It may also be necessary to brief additional managers on the results of the test, update other security-related documents, and perform other actions based on the test.

6.6 Summary

Tests are evaluation tools that use quantifiable metrics or expected outcomes to validate the operability of one or more IT systems or system components that are identified as critical in an IT plan. Tests can take several forms, including component testing (testing individual hardware or software components, or groups of related components), system testing (testing complete systems), and comprehensive testing (testing all systems and components that support an IT plan). A test is conducted in as close to an operational environment as possible, which means that the test should be conducted in a manner that resembles the everyday work environment in which the system or component is found. If possible, an actual test of the components or systems used to conduct daily operations for the organization should be used. Tests can potentially be disruptive to an organization's operations, so tests are sometimes performed on systems that mimic the actual operational systems, especially if there is not strong confidence that the tests will be completely successful.

One commonly used methodology for planning and performing test events has the following phases:

- **Design.** The TT&E program coordinator works with a test design team to design the event. Several factors can affect the design of the test, including the form (component, system, or comprehensive), the organizational entities involved, and the scope of the test. The major steps in the event design process are as follows:
  - Determine the test scope based on current system or security requirements and any potential compliance or regulatory requirements
  - Identify the objectives of the test
  - Determine which assessment tools and procedures are needed to accomplish the test
  - Identify the individuals that should participate in the test and notify them of when it will occur
  - Identify the staff for the test, including a test director and one or more data collectors
  - Coordinate the logistics for the test event.
- **Development.** The design team creates the documentation to be used before, during, and after the test event. Typical documentation includes briefings, a test guide, test plans, and an after action report. For some tests, especially comprehensive tests, materials similar to those used for functional exercises, such as a scenario, MSEL, and message injects may also be needed.
- **Conduct.** The locations for tests vary based on the type of test being conducted and the test's scope. For example, a small component test could be conducted in a single office, while a comprehensive test of components and systems for an IT plan could involve many different parts of an organization in various locations. During a test, the mission of the organization should not be disrupted to the extent that the organization can no longer function and provide the services that it was created to provide. The test director should monitor all tests closely, and if there is any sign of a possible catastrophic disruption, or the safety of an individual is at stake or the security of the organization or its data is in question, the test director and any other member of the test staff should have the ability to terminate the test immediately. After the test concludes, the test director and data collectors should conduct an informal test debrief, requesting feedback from everyone present.
- **Evaluation.** The comments from the debrief, along with lessons learned during the test, should be captured in an after action report. The report should include background information about the test, documented observations made by the test staff, and recommendations for enhancing the IT plan that had its components or systems tested. Outcomes of the evaluation could include updating the IT plan or other security-related documents, briefing managers on the results, and performing other actions.

This page has been left blank intentionally.

Appendix A—Sample Tabletop Exercise Documentation

Appendix A provides the following sample documentation:

- Tabletop Exercise Facilitator Guide
- Tabletop Exercise Participant Guide
- Tabletop Exercise After action report.

This sample documentation is designed to be used as a template by those responsible for designing and developing tabletop exercise documentation. In addition to the documentation described in this appendix, a briefing containing the agenda and logistics information should be developed and projected at the beginning of the exercise.

A.1 Sample Tabletop Exercise Facilitator Guide

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

FACILITATOR GUIDE

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

In an effort to validate *[insert organization name] [insert name of plan being exercised*[22]*], [insert organization name]* will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the *[insert plan name]*. This discussion-based exercise will be a *[insert number of hours]*-hour event that will begin at *[insert start time]* and will last until *[insert end time]*.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at *[insert organization name]* following an event causing the outage of mission critical systems that are housed in the *[insert facility name]*. This exercise is designed to improve the readiness of the *[insert organization name]* and help validate existing *[insert plan name]* procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the recovery of mission critical systems at the *[insert facility name]*. To achieve the exercise's stated objectives, discussion will focus on the following *[insert facility name]* contingency planning elements:

- What would be done to recover each class of system (e.g., Messaging, Web) at the [*insert facility name*]?
- How will system recovery be accomplished and what is the priority/optimal chronology of restoration?
- What is the time required for restoration and how can this be optimized?
- What are the expected results and action items that will assist system teams and improve readiness after the exercise?

Participants may choose to bring back-up reference material that will aid in answering the above questions.

SAMPLE CONCEPT OF OPERATIONS

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions they would take in response to an emergency situation. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting the *[insert facility name]*. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives. The facilitator may choose to inject modifications to the scenario to further stimulate discussion. Participants will also be encouraged to ask one another questions.

[22] This example illustrates an IT contingency planning tabletop exercise.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility
- Validate the accuracy of recovery procedures documented in the *[insert plan name]*
- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE SCENARIO

At *[insert time]* on *[insert date]*, an electrical fire in the *[insert facility name]* caused extensive damage and the termination of operations in the data center. The *[insert plan name]* was fully activated in response to this incident, and operations will be conducted at the *[insert alternate facility name]* for the foreseeable future. *[Insert organization name]* employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the *[insert facility name]*, Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the *[insert alternate facility name]*.

SAMPLE FACILITATOR QUESTIONS

The following questions are designed to be used by the facilitator to guide the discussion and ensure the pre-defined objectives are met; depending on the flow of the exercise, the facilitator may elect to use these questions or other questions to ensure participants meet the objectives through the discussion:

1. Who has authority to activate the *[insert plan name]*?
2. If the plan were activated, what level of staffing should be available at the *[insert facility name]*?
3. How would you be notified of plan activation and by whom?
4. What are the roles and responsibilities of the team at the *[insert facility name]*?
5. How would the transfer of operations have occurred if critical personnel were injured in the fire and could not report to the *[insert facility name]*?
6. Are IT recovery procedures fully documented? Are they accurate? Should additional procedures be documented in the contingency plan?

- Can recovery procedures be completed within the timeframe dictated in the *[insert plan name]*?
- What are the steps to reconstitute operations at *[insert facility name]?*

SAMPLE DEBRIEF/HOTWASH QUESTIONS

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants.

- Are there any other issues you would like to discuss that were not raised?
- What are the strengths of the contingency plan? What areas require closer examination?
- Was the exercise beneficial? Did it help prepare you for follow-on testing?
- What did you gain from the exercise?
- How can we improve future exercises and tests?

A.2 Sample Tabletop Exercise Participant Guide

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

PARTICIPANT GUIDE

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

In an effort to validate *[insert organization name] [insert name of plan being exercised*[23]*], [insert organization name]* will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the *[insert plan name]*. This discussion-based exercise will be a *[insert number of hours]*-hour event that will begin at *[insert start time]* and will last until *[insert end time]*.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at *[insert organization name]* following an event causing the outage of mission critical systems that are housed in the *[insert facility name]*. This exercise is designed to improve the readiness of the *[insert organization name]* and help validate existing *[insert plan name]* procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the recovery of mission critical systems at the *[insert facility name]*. To achieve the exercise's stated objectives, discussion will focus on the following *[insert facility name]* contingency planning elements:

- What would be done to recover each class of system (e.g., Messaging, Web) at the *[insert facility name]*?
- How will system recovery be accomplished and what is the priority/optimal chronology of restoration?
- What is the time required for restoration and how can this be optimized?
- What are the expected results and action items that will assist system teams and improve readiness after the exercise?

Participants may choose to bring back-up reference material that will aid in answering the above questions.

SAMPLE CONCEPT OF OPERATIONS

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions they would take in response to an emergency situation. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting the *[insert facility name]*. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility

[23] This example illustrates an IT contingency planning tabletop exercise.

- Validate the accuracy of recovery procedures documented in the *[insert plan name]*
- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE SCENARIO

At *[insert time]* on *[insert date]*, an electrical fire in the *[insert facility name]* caused extensive damage and the termination of operations in the data center. The *[insert plan name]* was fully activated in response to this incident, and operations will be conducted at the *[insert alternate facility name]* for the foreseeable future. *[Insert organization name]* employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the *[insert facility name]*, Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the *[insert alternate facility name]*.

SAMPLE PARTICIPANT QUESTIONS

The following questions sample questions that might appear in the Participant Guide.

1. Who has authority to activate the *[insert plan name]*?
2. How would you be notified of plan activation and by whom?
3. Are IT recovery procedures fully documented? Can recovery procedures be completed within the timeframe dictated in the *[insert plan name]*?

SAMPLE DEBRIEF/HOTWASH QUESTIONS

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants.

- Are there any other issues you would like to discuss that were not raised?
- What are the strengths of the contingency plan? What areas require closer examination?
- Was the exercise beneficial? Did it help prepare you for follow-on testing?
- What did you gain from the exercise?
- How can we improve future exercises and tests?

A.3 Sample Tabletop Exercise After Action Report

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

AFTER ACTION REPORT

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

On *[insert date]*, *[insert organization name]* participated in *[insert duration of exercise]*-hour tabletop exercise designed to validate their understanding of the *[insert plan name]*.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility
- Validate the accuracy of recovery procedures documented in the [insert plan name]
- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE DISCUSSION FINDINGS

The *[insert exercise name]* provided information on *[insert relevant information]*. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event and topics, to be included in the after action report. *A sample evaluation form can be found on page C-16.*

The discussion findings from the exercise along with any necessary recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the exercise, participants left with a heightened awareness of *[insert relevant information]*.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

Observation 1. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Example Observations and Recommendations:

Observation 1. Communications

A plan identifying standardized systems for communicating with contingency plan members does not exist.

Recommendations

- The organization should consider developing a communications plan that establishes standardized communications requirements, addresses how and where backup communication systems will be positioned, and describes procedures for personnel to access backup communication systems.
- The organization should identify redundant communications systems to ensure that essential personnel can be contacted in the event of an emergency. Redundant communications systems may consist of home telephones, cellular telephones, laptop computers, and other communications systems.

Observation 2. Flyaway Kits

Essential personnel have not been issued flyaway kits, containing personal items and/or those items needed to perform their operations, to carry to relocation facilities in the event of an emergency.

Recommendation

- The agency should examine the possibility of developing flyaway kits and distributing them in advance to personnel who would relocate during an emergency. In addition to personal items that personnel might need if deployed for an extended period of time, flyaway kits should contain flash drives, diskettes or CD-ROMs with information needed for essential personnel to carry out their essential functions.

SAMPLE EVALUATION FORM

Please take a moment to fill out the evaluation form.

INSERT NAME OF EVENT

Exercise Evaluation Form

INSERT DATE

Please take a few moments to answer the following questions about the exercise.

NAME _____

1). Did you have available to you all of the information and resources needed to fulfill your responsibilities?

2). Did you feel that there was an adequate level of training to support the response effort at the relocation site?

3). Was the structure of the exercise realistic?

4). Please provide comments regarding what you believe worked and didn't work during the exercise.

5). Do you believe you are sufficiently prepared to conduct extended emergency operations from the relocation facility? *Please Circle One*

Not Prepared ***Slightly Prepared*** ***Prepared*** ***Extremely Prepared***

6.) Please rate the overall exercise. *Please Circle One*

Needs Improvement ***Fair*** ***Good*** ***Very Good***

SAMPLE EVALUATION RESULTS

Following the *[insert tabletop exercise name]*, on *[insert date]*, participants were given an evaluation form on which to record their impressions of the exercise. These forms allowed participants to rate presentations on a numerical scale and to provide additional comments for consideration in the after action report. Refer to Exhibit 1 for more detailed information regarding the participants' responses. *Each exhibit will reflect the evaluation forms for each individual event. If evaluation forms have a point scale, either a pie chart or bar graph will be depicted.*

The questions covered whether participants thought additional issues should have been raised; whether participants thought the exercise was beneficial; what participants gained from the exercise; and what can be done to improve future exercises. *[Insert percentage]* of the participants completed the evaluation.

In response to the question regarding whether participants thought additional issues should have been raised, nearly *[Insert percentage]* of those who completed the evaluation indicated that all relevant issues were addressed. Other comments were *[insert relevant information]*.

In response to the question regarding whether participants thought the exercise was beneficial, *[Insert percentage]* of those who completed the evaluation indicated that the exercise was beneficial. Comments ranged from *[insert relevant information (i.e., "good start" to "extremely beneficial.")]*.

In response to the question about what participants gained from the exercise, nearly *[Insert percentage]* of those who completed the evaluation form remarked *[insert relevant information]*.

EXHIBIT: PARTICIPANT RESPONSES

What are your thoughts on the exercise?	What did you gain from the exercise?
■ *[Insert comments]*	■ *[Insert comments]*
■	■
■	■
■	■

Overall, the feedback from the *[insert tabletop exercise name]* was *[insert relevant information]*.

This page has been left blank intentionally.

Appendix B—Sample Functional Exercise Documentation

Appendix B provides the following sample documentation:

- Scenario
- Master Scenario Events List (MSEL)
- Message Inject
- Message Inject Tracking Form
- After Action Report.

This sample documentation is designed to be used as a template by those responsible for designing and developing functional exercise documentation. In addition to the documentation described in this appendix, a briefing containing the agenda and logistics information should be developed and presented at the beginning of the exercise.

B.1 Sample Functional Exercise Scenario

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

SCENARIO

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The scenario is developed by the functional exercise team during the Development Phase. Scenario documentation may include a brief Scenario Background designed to provide participants a sense of the world/local situation in the weeks or months before the start of the exercise. This information will be provided to participants in briefings before the exercise or at the beginning of the exercise event. The scenario itself portrays the events that will occur during the conduct of the event. These events will also become a part of the Master Scenario Events List and will be introduced into exercise play in the form of Injects.

SAMPLE SCENARIO BACKGROUND

D-Day Minus 20

International tensions have dramatically risen overseas involving strategic interests of the United States. Despite attempts to resolve disputes diplomatically, troops from hostile countries deploy and appear poised to make a major military incursion against nations allied to the United States. U.S. intelligence agencies also detect documented attempts by hostile nations to destabilize the governments and economies of allies, which would have an adverse impact on U.S. military and economic interests in the region.

D-Day Minus 10

As tensions continued to build, hostile entities undertake small-scale military operations against allied and U.S. interests overseas. A U.S. reconnaissance plane is shot down and the bodies of the dead crew are displayed on television. An emergency Cabinet meeting is called and it is decided that the U.S. military will deploy to the region to protect allied governments and U.S. interests. It is anticipated that an initial operational capability to defend U.S. interests will not be complete until next month.

D-Day Minus 5

In response to the U.S. declaration to send troops and materiel to the region, hostile nations vow to take whatever actions are necessary to "strike a vicious blow against the American imperialists." They state that any war that the U.S. provokes will also be fought on the American homeland. U.S. intelligence agencies soon detect an increase of cyber attacks against U.S. and threats to carry out terrorist attacks against the U.S. government. Intelligence also indicates that hostile foreign interests within the U.S. are increasingly active and terrorist cells in other countries have been activated to potentially carry out attacks against the U.S., both overseas and within U.S. borders. U.S. government officials suspect that the hostile nations hope to weaken U.S. public support and impede the military's capability to deploy by engaging in actions that might include the use of weapons of mass destruction and cyberterrorism. Nevertheless, the U.S. military continues to deploy to the region.

SAMPLE SCENARIO

D-Day

0900: The United States Computer Emergency Readiness Team (US-CERT) issues an alert indicating the presence of what is thought to be an advanced computer worm. US-CERT estimates that the worm has already infected over 500,000 computers worldwide in only 2 hours, prompting the center to warn that the worm's spread has the potential to disrupt business and personal use of the Internet for applications such as electronic commerce, e-mail, and entertainment. U.S. intelligence agencies link the worm's release as a response to U.S. military deployments and fear the attack may have been designed specifically to disrupt communications between agencies supporting the military deployment.

Intrusions into numerous Federal Web sites have been reported in recent hours. Hackers, who government officials believe to be associated with hostile nations, have successfully compromised the security of various U.S. Government information systems. Anti-government vandalism has also been reported on numerous department and agency Web sites.

[*Insert organization/data center name*] is currently in the process of responding to the effects of the worm and defending against further electronic intrusions.

1000: As a result of credible threats of imminent terrorism and the fear that ongoing electronic intrusions against Federal information systems may be part of a concerted information warfare attack, the Department of Homeland Security (DHS) raises the Homeland Security Advisory System threat condition from an Orange "High" to a Red "Severe" risk of terrorist attack.

1200: A freight train pulling numerous tanker cars passes slowly through the center of the city. Some of the tankers are carrying methyl isocyanate (MIC), a highly explosive chemical used in the production of pesticides. As the train passes the [*insert name of organization's facility*], one of the tanker cars erupts in a violent explosion. The blast collapses a portion of the building and results in power outages in the immediate vicinity. Many personnel in the [*insert name of organization's facility*] are killed or injured.

The [i*nsert data center name*] survived the blast and emergency power was engaged for critical IT systems. Several data center personnel had recently left the center for lunch and their well-being is unknown at this time. Management has directed that the data center implement contingency plans and relocate to their alternate computing facility. In addition to restoring essential data center operations at the alternate facility, management indicates that defending [i*nsert organization name*] from further electronic intrusions remains a priority.

D-Day Plus 1

1000: Intelligence and law enforcement agencies continue to track numerous threats against the United States. The Federal Bureau of Investigation (FBI) notifies Government agencies of documented threats of further attacks against Federal departments and agencies throughout the United States. One such notice to [i*nsert organization name*] includes a report of possible terrorist surveillance activities outside the organization's alternate computing facility. As a result, management directs that data center personnel explore options to move operations to a backup alternate facility in the event that the threat is found to be credible.

B.2 Sample Functional Exercise Master Scenario Events List

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

MASTER SCENARIO EVENTS LIST (MSEL)

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The Master Scenario Events List (MSEL) is created by the functional exercise team during the Development Phase. The MSEL lists key scenario events, expected Injects that will build on the key events, and the objectives of the each MSEL item. Controllers, simulators, and data collectors will refer to the MSEL throughout the Conduct Phase of the exercise to ensure the exercise remains on track.

Master Scenario Events List			
Event #	**MSEL Key Event Description**	**Expected Actions Resulting from MSEL Event**	**Objectives**
1	***Example*** The [*insert organization name*] experiences electronic intrusions on critical information systems.	***Example*** Supporting Injects: Day 1, 0900 - 1700 ■ Activate cyber incident response team ■ Implement Cyber Intrusion Response Plan ■ Notify and coordinate with customers and other stakeholders ■ Take actions to clean infected systems	***Example*** ■ Familiarize staff with responsibilities under Cyber Intrusion Response Plan ■ Validate Cyber Intrusion Response Plan ■ Coordinate with Federal cyber entities, customers, and key stakeholders
2	***Example*** The Homeland Security Advisory System threat level has been raised from an Orange "High" to a Red "Severe" risk of terrorist attack.	***Example*** Supporting Injects: Day 1, 1000 - 1200 ■ Activate emergency response teams ■ Initiate backup procedures for all mission critical IT systems ■ Relocate essential personnel to alternate facilities ■ Coordinate with the White House and other departments and agencies to inform them of decision to relocate operations	***Example*** ■ Familiarize staff with emergency activation and notification procedures ■ Validate IT contingency plans and procedures ■ Validate relocation plans and procedures ■ Validate coordination and communications processes with key stakeholders
3	***Example*** A large explosion occurs outside the Office Building.	***Example*** Supporting Injects: Day 1, 1200-1700 ■ All commercial power to building has been cut ■ The site reports that some data communications links have failed ■ Facility managers report the building cannot be repaired	***Example*** ■ Validate IT contingency plans and procedures ■ Identify whether additional contingency plans need to be developed ■ Examine plans to restore data center operations
4	***Example*** Possible threat of terrorism to alternate facility.	***Example*** Supporting Injects: Day 2, 1000-1200 ■ Explore options if alternate facility is disabled ■ Prioritize IT system recovery	***Example*** ■ Identify whether additional contingency plans should be developed for alternate facility

B.3 Sample Functional Exercise Injects

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

INJECTS

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

Injects are created by the functional exercise team during the Development Phase. These messages are introduced by Controllers during the Conduct Phase and are provided to exercise participants via the means shown on the Inject form. In the case of the Sample Inject provide below, a Controller would play the role of the Chief Information Officer and would call the Team Chief to provide information and request follow-on action. Expected actions by the Team Chief or other exercise participants are documented in the "Notes to Control/Response Cell" at the bottom of this form to aid controllers, simulators, or data collectors in anticipating what actions will result from the Inject.

****EXERCISE**EXERCISE**EXERCISE**EXERCISE****

[Insert Name of Exercise]
Implementers for *[Insert Date]*

EXAMPLE

#15 – [*Insert inject title*] **(i.e., Development of Disaster Recovery Strategies for Alternate Facility)**

Inject Date/Time: [*Insert date/time*] **(i.e., Day 2, 1045)**

From: [*Insert by whom the message is delivered*] **(i.e., Chief Information Officer)**

To: [*Insert for whom the message is intended*] **(i.e., Team Chief)**

Inject Means: [*Insert the means by which the message is delivered*] **(i.e., Phone Call)]**

[*Insert message text*]

Example

Now that we know the magnitude of the damage to the Building and our data center there, it is apparent that we will be operating out of the alternate facility (AF) for the foreseeable future. Given the continued threat of terrorist attacks, we need to develop contingency plans in the event of a major outage affecting the AF. What is our strategy to ensure continuity of mission critical systems at the AF? Which systems and applications are prioritized for recovery? How long will it take to develop a viable backup for those systems?

Note to Control/Response Cell:

[*Insert any type of information that the Control/Response Cell may need to consider to track, evaluate, or respond to exercise players*]

Example

Expect the AF Team Chief to consult the AF Contingency Plan and coordinate with appropriate system and application engineers to develop a recovery strategy.

B.4 Sample Functional Exercise Inject Tracking Form

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

INJECT TRACKING FORM

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

Portions of the Inject Tracking Form are developed by the functional exercise team during the Development Phase, and additional information is filled in by Controllers during the Conduct Phase. In the sample below, ***BOLDED*** *text would have been created during the Development Phase and ITALICIZED text would have added to the form by Controllers during the Conduct Phase. The purpose of the form is to provide Controllers with a "play book" that states which injects are provided to participants at each given time. The form is then used by Controllers to document the time at which an Inject is introduced and a summary of activities taken by participants in response to the Inject.*

Inject Tracking Form				
Inject #	**Scheduled Inject Time**	**Actual Inject Time**	**Inject Summary**	**Comments**
Example **1**	*Example* **0900**	*Example* *0901*	*Example* **Malicious Computer Worm Denial-Of-Service Attacks**	*Example* *Injected by Director to Chief. Chief assigned immediate action to Network Administrator. Administrator took appropriate actions and informed management and customer advocate. Administrator continued to monitor developments for remainder of exercise.*
Example **2**	*Example* **1015**	*Example* *1018*	*Example* **Situation Reporting Schedule to Leadership**	*Example* *Injected by Director to Chief. Chief assigned action to Operations Officer at 1020, who logged and posted schedule for all of team per standard operating procedures.*
Example **3**	*Example* **1025**		*Example* **Call to White House**	
Example **4**	*Example* **1200**		*Example* **Large Explosion Outside Office Building**	

B.5 Sample Functional Exercise After Action Report

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

AFTER ACTION REPORT

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The After Action Report is developed by Data Collectors during the Evaluation Phase. The After Action Report provides relevant background information about the event, scope of the exercise, objectives, scenario, and key findings and recommendations. In addition, the After Action Report lists the event's participants and may provide relevant information from surveys completed by participants at the conclusion of the exercise.

SAMPLE TABLE OF CONTENTS

[Insert table of contents]

SAMPLE INTRODUCTION

On *[insert date]*, *[insert organization name]* participated in *[insert duration of exercise]* functional exercise designed to validate their understanding of the Cyber Intrusion Response Plan and the Alternate Facility Contingency Plan. *[Insert any other additional background information about the exercise that is relevant for the after action report.]*

SAMPLE SCOPE

The exercise was designed to examine the *[insert organization's name]* ability to respond to a concerted cyber attack campaign from the alternate computing facility. The event examined all aspects of the activation, operation, and reconstitution phases of both the Cyber Intrusion Response Plan and the Alternate Facility Contingency Plan. All personnel with operational responsibilities under the two plans participated in the event. Senior level decision-makers were not exercised in the exercise; however, a second exercise focused on management activities is planned in the coming months.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate Cyber Intrusion Response Plan and Alternate Facility Contingency Plan
- Identify interdependencies, overlaps, and inconsistencies between the two plans
- Validate the team's ability to recover IT operations at alternate facility
- Familiarize staff with their responsibilities under the plans
- Validate the accuracy of recovery procedures documented in the plans
- Coordinate with Federal cyber entities, customers, and key stakeholders
- Identify areas of the plans that need to be revised
- Identify whether additional contingency plans need to be developed.

SAMPLE SCENARIO

[Insert scenario or high-level overview of the scenario.]

SAMPLE EXERCISE FINDINGS

The *[insert exercise name]* provided information on *[insert relevant information]*. An important benefit of the exercise was the opportunity for participants to receive hands-on training in responding to an emergency from the alternate facility. In addition, the exercise provided participants with an opportunity to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event, to be included in the after action report. *[A sample evaluation form can be found on page B-17.]*

Findings from the exercise and recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the exercise, participants left with a heightened awareness of *[insert relevant information]*.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

Observation 1. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Example Observations and Recommendations:

Observation 1. Communications

A plan identifying standardized systems for communicating with contingency plan members does not exist.

Recommendations

- The *[insert organization name]* should consider developing a communications plan that establishes standardized communications requirements, addresses how and where backup communication systems will be positioned, and describes procedures for personnel to access backup communication systems.
- The *[insert organization name]* should identify redundant communications systems to ensure that essential personnel can be contacted in the event of an emergency. Redundant communications systems may consist of home telephones, cellular telephones, laptop computers, and other communications systems.

Observation 2. Flyaway Kits

Essential personnel have not been issued flyaway kits, containing personal items and/or those items needed to perform their operations, to carry to relocation facilities in the event of an emergency.

Recommendation

- The *[insert organization name]* should examine the possibility of developing flyaway kits and distributing them in advance to personnel who would relocate during an emergency. In addition to personal items that personnel might need if deployed for an extended period of time, flyaway kits should contain flash drives, diskettes or CD-ROMs with information needed for essential personnel to carry out their essential functions.

SAMPLE EVALUATION FORM

Please take a moment to fill out the evaluation form.

INSERT NAME OF EVENT

Exercise Evaluation Form

INSERT DATE

Please take a few moments to answer the following questions about the exercise.

NAME _____

1). Did you have available to you all of the information and resources needed to fulfill your responsibilities?

2). Did you feel that there was an adequate level of training to support the response effort at the relocation site?

3). Was the structure of the exercise realistic?

4). Please provide comments regarding what you believe worked and didn't work during the exercise.

5). Do you believe you are sufficiently prepared to conduct extended emergency operations from the relocation facility? *Please Circle One*

Not Prepared ***Slightly Prepared*** ***Prepared*** ***Extremely Prepared***

6.) Please rate the overall exercise. *Please Circle One*

Needs Improvement ***Fair*** ***Good*** ***Very Good***

SAMPLE EVALUATION RESULTS

Following the *[insert functional exercise name]*, on *[insert date(s)]*, participants were given an evaluation form on which to record their impressions of the exercise. These forms allowed participants to rate presentations on a numerical scale and to provide additional comments for consideration in the after action report. Refer to Exhibit 1 for more detailed information regarding the participants' responses. *[Each exhibit will reflect the evaluation forms for each individual event. If evaluation forms have a point scale, either a pie chart or bar graph will be depicted.]*

The questions covered whether participants thought additional issues should have been raised; whether participants thought the exercise was beneficial; what participants gained from the exercise; and what can be done to improve future exercises. *[Insert percentage]* of the participants completed the evaluation.

In response to the question regarding whether participants thought additional issues should have been raised, nearly *[insert percentage]* of those who completed the evaluation indicated that all relevant issues were addressed. Other comments were *[insert relevant information]*.

In response to the question regarding whether participants thought the exercise was beneficial, *[insert percentage]* of those who completed the evaluation indicated that the exercise was beneficial. Comments ranged from *[insert relevant information (i.e., "good start" to "extremely beneficial.")]*.

In response to the question about what participants gained from the exercise, nearly *[insert percentage]* of those who completed the evaluation form remarked *[insert relevant information]*.

EXHIBIT 1: PARTICIPANT RESPONSES

What are your thoughts on the exercise?	What did you gain from the exercise?
■ *[Insert comments]*	■ *[Insert comments]*
■	■
■	■
■	■

Overall, the feedback from the *[insert functional exercise name]* was *[insert relevant information]*.

Appendix C—Sample Test Documentation

Appendix C provides the following sample documentation for three types of tests (component, system, and comprehensive):

- Test Structure Description
- Test Plan
- Test Briefing for Participants
- Test Inject or Action
- Test Validation Worksheet
- Test Evaluation Worksheet
- Test After Action Report.

This sample documentation is designed to be used as a template by those responsible for designing and developing test documentation.

C.1 Sample Component Test Documentation

An example of a component test is the occasional test of the nation's Emergency Alert System, formerly known as the Emergency Broadcast Network.[24] During such a test, the equipment is tested, and a tone and announcement associated with an emergency are broadcasted on the radio or television. Although the test does not involve a simulated emergency with responders, the message tests a specific component of the system.

SAMPLE COMPONENT TEST PLAN

[Insert test type or name]

Component Test Plan

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Broadcast System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Test Details: *[Insert test details]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

Test Main Point of Contact: *[Insert test main point of contact]*

Test Approval Grantor: *[Insert test approval grantor]*

[24] For more information on the Emergency Alert System, visit http://www.fcc.gov/eb/eas/.

SAMPLE COMPONENT TEST BRIEFING FOR PARTICIPANTS

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component]* for *[organization or policy]* will be tested. Participants will be expected to perform the following tasks:

- *[Insert task]*
- *[Insert task]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

If you have any questions, please contact *[insert point of contact]*.

SAMPLE COMPONENT TEST INJECT OR ACTION

Initiate the Emergency Alert System, which will perform the following functions:

- Discontinue normal programming.
- Broadcast the following message: *"This is a test. This station [optional—insert station call sign] is conducting a test of the Emergency Broadcast System. This is only a test."*
- Transmit the two-tone attention signal from the EBS encoder.
- Broadcast the following message: *"This is a test of the Emergency Alert System. The broadcasters of your area in voluntary cooperation with the Federal, state and local authorities have developed this system to keep you informed in the event of an emergency. If this had been an actual emergency, [optional—stations may mention the types of emergencies likely to occur in their area] the Attention Signal you just heard would have been followed by official information, news or instructions. This station [optional—insert station call sign] serves the [insert operational area name] area. This concludes this test of the Emergency Alert System."*

SAMPLE COMPONENT TEST VALIDATION

A test of a component requires validation criteria to determine whether the component or system functioned as intended. Test validation should include the metrics by which the success of the component or system will be measured. It should also detail the expected outcome; in this case, the two-tone attention signal and message should be heard clearly.

SAMPLE COMPONENT TEST VALIDATION WORKSHEET

[Insert test type or name]

Component Test Validation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Broadcast System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Validation Methodology: *[Insert validation methodology]*

Was the test able to be validated? *[Insert answer]*

Comments: *[Insert comments]*

Were there any aspects of the test that could not be validated? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SAMPLE COMPONENT TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the system test and associated components and processes performed adequately. Possible improvements and recommendations are an important part of the evaluation process.

SAMPLE COMPONENT TEST EVALUATION WORKSHEET

[Insert test type or name]

Component Test Evaluation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Alert System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Were the test objectives met? *[Insert answer]*

Comments: *[Insert comments]*

Test details: *[Insert test details]*

Was testing criterion adequate? *[Insert answer]*

Comments: *[Insert comments]*

Could the testing criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Was the test validation criterion adequate? *[Insert answer]*

Could the test validation criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Did the test perform as expected? *[Insert answer]*

Comments: *[Insert comments]*

Were there any failures during the test? *[Insert answer]*

Did the failure cause the test to fail? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

COMPONENT TEST AFTER ACTION REPORT

The component test after action report should consist of the following components:

- General findings, often in the form of an executive summary
- Specific findings

- Supporting data.

COMPONENT TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the test. It might consist of a statement along the lines of the following:

> The component test provided an excellent opportunity for participants to test the *[insert relevant information]*. As a result of this component test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

COMPONENT TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1.** ***[Insert general topic area]***
>
> *[Insert observation]*
>
> **Recommendations**
>
> *[Insert recommendations]*
>
> **Observation 2.** ***[Insert general topic area]***
>
> *[Insert observation]*
>
> **Recommendations**
>
> *[Insert recommendations]*

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These are often included as attachments with a brief explanation of how they were gathered.

C.2 Sample System Test Documentation

An example of a system test is the testing of an organization's data backup and restoration system and procedures. During such a test, all aspects of the data backup equipment and personnel procedures for archiving and restoring data are tested.

SAMPLE SYSTEM TEST STRUCTURE:

System Test: Data Backup and Restoration

- Test data backup procedure
- Test data backup equipment
- Test data backup integrity verification procedures
- Test local data storage procedures
- Test local data retrieval procedures
- Test offsite data storage procedures
- Test offsite data retrieval procedures
- Test data restoration for UNIX systems
- Test data restoration for Microsoft Systems
- Test data restoration for network systems
- Test data restoration for other systems.

SAMPLE SYSTEM TEST PLAN

[Insert test type or name]

System Test Plan

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: *[Insert test objectives]*

Test Details: *[Insert test details]*

Test Components:

- *[Insert component]*
- *[Insert component]*
- *[Insert component]*

System Test Component 1: *[Insert component]*[25]

- **Component Test Participants:** *[Insert participants]*
- **Component Test Validation Staff:** *[Insert validation staff]*
- **Component Test Evaluation Staff:** *[Insert evaluation staff]*
- **Component Test Cancellation Procedures:** *[Insert test cancellation procedures]*
- **Component Test Main Point of Contact:** *[Insert test main point of contact]*
- **Component Test Approval Grantor:** *[Insert test approval grantor]*

System Test Main Point of Contact: *[Insert system test main point of contact]*

System Test Approval Grantor: *[Insert system test approval grantor]*

SAMPLE SYSTEM TEST BRIEFING FOR PARTICIPANTS

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component or system]* for *[department or policy]* will be tested. Each of the following components will be tested:

- *[Insert component]*. Date: *[insert date]*. Time: *[insert time]* to *[insert time]*.
- *[Insert component]*. Date: *[insert date]*. Time: *[insert time]* to *[insert time]*.

[insert component] Component Test in *[insert system]* System Test[26]

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component]* for *[department or policy]* will be tested. Participants will be expected to perform the following tasks:

- *[Insert task]*
- *[Insert task]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

If you have any questions, please contact *[insert point of contact]*.

[25] Repeat this sub-section as needed for each component test within the system test.
[26] Repeat this sub-section as needed for each component test within the system test.

SAMPLE SYSTEM TEST VALIDATION

A test of any system requires methods and criteria to evaluate whether the system test and associated component tests or processes worked as intended. Test validation should include the metrics by which the success of the component or process will be measured and detail the expected outcome. System test validation can be determined by the validation of each individual component test objectives and validation.

In this example, validation for this system test should verify the backup procedures' accuracy and equipment functionality for backing up data for its associated type of systems; verify data integrity checking; validate local and offsite data storage and retrieval procedures; and verify system restoration function as expected for each associated type of system.

SAMPLE SYSTEM TEST VALIDATION WORKSHEET

[Insert test type or name]

System Test Validation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Test Objectives: The objectives of this test are as follows:

- *[Insert objective]*
- *[Insert objective]*

Test Components: *[Insert test components]*

Validation Methodology: *[Insert validation methodology]*

Was the test able to be validated? *[Insert answer]*

Comments: *[Insert comments]*

Were there any components of the test that could not be validated? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SAMPLE SYSTEM TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the system test and associated components and processes performed adequately. Possible improvements and recommendations are an important part of the evaluation process.

SAMPLE SYSTEM TEST EVALUATION WORKSHEET

[Insert test type or name]

System Test Evaluation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Components: *[Insert test components]*

Test Objectives: The objectives of this test are as follows:

- *[Insert objective]*
- *[Insert objective]*

Were the test objectives met? *[Insert answer]*

Comments: *[Insert comments]*

Test details: *[Insert test details]*

Was testing criterion adequate? *[Insert answer]*

Comments: *[Insert comments]*

Could the testing criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Was the test validation criterion adequate? *[Insert answer]*

Could the test validation criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Did the test perform as expected? *[Insert answer]*

Comments: *[Insert comments]*

Did any test components fail? *[Insert answer]*

Did the failure cause the test to fail? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SYSTEM TEST AFTER ACTION REPORT

A system test after action report should consist of the following components:

- General findings, often in the form of an executive summary
- Specific findings
- Supporting data.

SYSTEM TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the system test. It might consist of a statement along the lines of the following:

> The system test provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

SYSTEM TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1. [Insert general topic area]**
>
> *[Insert observation]*
>
> **Recommendations**

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These are often included as attachments with a brief explanation of how they were gathered. For example, individual component testing forms might be attached as supporting data.

C.3 Sample Comprehensive Test Documentation

An example of a comprehensive test is the testing of all the systems and components comprising an organization's business continuity plan. During such a test, all the equipment, processes, and procedures for each system and associated components are tested as a comprehensive unit.

SAMPLE COMPREHENSIVE TEST PLAN OVERVIEW

Because a comprehensive test plan is specifically designed around an organization's security, business continuity, or other plans, it is not practical to provide a full sample of the test documents. However, this section provides a plan overview that outlines the systems and component tests as part of the comprehensive plan. The forms in Appendices C.1 and C.2 for component and system testing can be used to form individual parts of the comprehensive test.

SAMPLE COMPREHENSIVE TEST STRUCTURE

Comprehensive Tests are comprised of several System Tests which in turn are comprised of several Component Tests. The following is an example of the structure of one branch of a comprehensive test.

Comprehensive Test: Business Continuity Plan

- **System Test:** Data Backup and Restoration
  - **Component Test:** Test data backup procedure
  - **Component Test:** Test data backup equipment
  - **Component Test:** Test data backup integrity verification procedures
  - **Component Test:** Test local data storage procedures
  - **Component Test:** Test local data retrieval procedures
  - **Component Test:** Test offsite data storage procedures
  - **Component Test:** Test offsite data retrieval procedures
  - **Component Test:** Test data restoration for UNIX systems
  - **Component Test:** Test data restoration for Microsoft systems
  - **Component Test:** Test data restoration for network systems
  - **Component Test:** Test data restoration for other systems
  - **Component Test:** Identify any delays, failures, or areas of improvement.

SAMPLE COMPREHENSIVE TEST PLAN

[Insert test type or name]

Comprehensive Test Plan

Dates of Testing: *[Insert date]* to *[insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: *[Insert test objectives]*

Test Details: *[Insert test details]*

Systems to be Tested:

- *[Insert system test]*
- *[Insert system test]*
- *[Insert system test]*

System 1: *[Insert system test]*[27]

System 1 Component Tests:

- *[Insert component test item]*
- *[Insert component test item]*
- *[Insert component test item]*

Component Test 1: *[Insert component]*[28]

- Component Test Participants: *[Insert participants]*
- Component Test Validation Staff: *[Insert validation staff]*
- Component Test Evaluation Staff: *[Insert evaluation staff]*
- Component Test Cancellation Procedures: *[Insert test cancellation procedures]*
- Component Test Main Point of Contact: *[Insert test main point of contact]*
- Component Test Approval Grantor: *[Insert test approval grantor]*

Comprehensive Test Cancellation Procedures: *[Insert test cancellation procedures]*

Comprehensive Test Main Point of Contact: *[Insert test main point of contact]*

Comprehensive Test Approval Grantor: *[Insert test approval grantor]*

[27] Repeat this sub-section as needed for each system test within the comprehensive test.
[28] Repeat this sub-section as needed for each component test within each system test.

SAMPLE COMPREHENSIVE TEST VALIDATION

A comprehensive test of many systems and system components requires a method and criteria to evaluate whether the component or process worked as intended. Because a comprehensive test is a compilation of many system and component tests, the validation can be determined from the validation of the system and component, and evaluated as a whole.

Comprehensive test validation should include the metrics by which the success of the component or process will be measured. It should detail the expected outcome.

SAMPLE COMPREHENSIVE TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the comprehensive test and its associated system and component tests performed adequately. Because a comprehensive test is a compilation of system and component tests, the comprehensive test will be determined from the evaluations of the individual system and, and then evaluated as a whole. Possible improvements and recommendations are an important part of the evaluation process.

COMPREHENSIVE TEST AFTER ACTION REPORT

A comprehensive test after action report should consist of the following components:

- General findings, often in the form of an executive summary
- Specific findings
- Supporting data.

COMPREHENSIVE TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the test. It might consist of a statement along the lines of the following:

> The test provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

COMPREHENSIVE TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1. *[Insert general topic area]***
>
> *[Insert observation]*

Recommendations

[Insert recommendations]

Observation 2. *[Insert general topic area]*

[Insert observation]

Recommendations

[Insert recommendations]

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These will often be included as attachments with a brief explanation of how they were gathered.

Appendix D—Glossary

Appendix D contains definitions for selected terms in this publication.

After Action Report: A document containing findings and recommendations from an exercise or a test.

Component Test: A test of individual hardware and software components or groups of related components.

Comprehensive Test: A test of all systems and components that support a particular IT plan, such as a contingency plan or computer security incident response plan.

Control Cell: A central location for exercise coordination, typically in a separate area from the exercise participants.

Controller: A functional exercise staff member who monitors, manages, and controls exercise activity to meet established objectives.

Data Collector: A person who records information about actions that occur during an exercise or test.

Exercise: A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.

Exercise Briefing: Material that is presented to participants during an exercise to outline the exercise's agenda, objectives, scenario, and other relevant information.

Exercise Director: A person responsible for all aspects of an exercise, including staffing, development, conduct, and logistics.

Facilitator Guide: A document for an exercise facilitator that includes the material the facilitator needs for the exercise, such as the exercise's purpose, scope, objectives, and scenario; a list of questions regarding the scenario that address the exercise's objectives; and a copy of the IT plan being exercised.

Facilitator: A person that leads a discussion among exercise participants.

Functional Exercise: An exercise that allows personnel with operational responsibilities to validate their IT plans and their operational readiness for emergencies in a simulated operational environment.

Hotwash: A debrief conducted immediately after an exercise or test with the staff and participants.

Master Scenario Events List (MSEL): A chronologically sequenced outline of the simulated events and key event descriptions that participants will be asked to respond to during an exercise.

Message Inject: A pre-scripted message that will be given to participants during the course of an exercise.

Participant Guide: An exercise document that typically contains the exercise's purpose, scope, objectives, and scenario, and a copy of the IT plan being exercised

Plan Coordinator: A person responsible for all aspects of IT planning, including the TT&E element of maintaining the IT plans. The plan coordinator has overall responsibility for the IT plans, including development, implementation, and maintenance.

Scenario: A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.

Simulators: A functional exercise staff member who simulates or represents non-participating individuals or organizations whose input or participation is necessary to the flow of the exercise.

System Test: A test performed on a complete system to evaluate its compliance with specified requirements.

Tabletop Exercise: A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Test: An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.

Test Director: A person responsible for all aspects of a test, including staffing, development, conduct, and logistics.

Test Guide: A document that outlines the basic steps involved in conducting a test and includes a list of the participants, a list of individuals and groups who might be affected by the test, and procedures for early termination of the test.

Test Plan: A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.

Test, Training, and Exercise (TT&E) Event: An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IT plan and implement solutions before an adverse situation occurs.

Test, Training, and Exercise (TT&E) Plan: A plan that outlines the steps to be taken to ensure that personnel are trained in their IT plan roles and responsibilities, IT plans are exercised to validate their viability, and IT components or systems are tested to validate their operability in the context of an IT plan.

Test, Training, and Exercise (TT&E) Policy: A policy that outlines an organization's internal and external requirements associated with training personnel, exercising IT plans, and testing IT components and systems.

Test, Training, and Exercise (TT&E) Program: A means for ensuring that personnel are trained in their IT plan roles and responsibilities; IT plans are exercised to validate their viability; and IT components or systems are tested to validate their operability.

Test, Training, and Exercise (TT&E) Program Coordinator: A person who is responsible for developing a TT&E plan and coordinating TT&E events.

Training: Informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities.

This page has been left blank intentionally.

Appendix E—Acronyms

Selected acronyms used in the guide are defined below.

AF	Alternate Facility
CD	Compact Disk
CIO	Chief Information Officer
COOP	Continuity of Operations
FISMA	Federal Information Security Management Act
FPC	Federal Preparedness Circular
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITL	Information Technology Laboratory
MSEL	Master Scenario Events List
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
SP	Special Publication
TT&E	Test, Training, and Exercise
UTSA	University of Texas-San Antonio

This page has been left blank intentionally.

Appendix F—Print and Online Resources

Appendix F identifies print and online resources that may be helpful to the reader in scoping, planning, documenting, conducting, and evaluating IT exercises.

- Federal Emergency Management Agency, Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004. http://www.fema.gov/pdf/library/fpc65_0604.pdf
- Federal Information Security Management Act of 2002, *Public Law 107-347*, December 2002. http://csrc.nist.gov/policies/FISMA-final.pdf
- Homeland Security Exercise and Evaluation Program, May 2004. http://www.ojp.usdoj.gov/odp/docs/HSEEPv3.pdf
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, February 8, 1996. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government*, October 21, 1998. http://www.fas.org/irp/offdocs/pdd/index.html

This page has been left blank intentionally.

Appendix G—Index