MAINTAINING EFFECTIVE INFORMATION TECHNOLOGY (IT) SECURITY THROUGH TEST, TRAINING, AND EXERCISE PROGRAMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

To maintain an effective information security program, organizations need plans for responding to adverse situations that could affect the confidentiality, integrity, and availability of their information and information technology (IT) systems. Plans such as contingency and computer security incident response plans must be maintained in a state of readiness to handle potentially harmful events. Staff members should be trained to carry out their responsibilities. Systems and system components should be tested to ensure proper operation when adverse events occur, and plans should be exercised to validate their effectiveness. Organizations are better able to maintain this state of readiness if they establish test, training, and exercise (TT&E) programs, and if they use the tests and exercises to identify deficiencies in their IT plans, procedures, and training.

The National Institute of Standards and Technology (NIST) Information Technology Laboratory has developed guidance to help organizations design, develop, conduct, and evaluate TT&E activities. A recently published guide details how organizations can prepare for, respond to, manage, and recover from adverse events, which could disrupt operations and interfere with the conduct of the organization's business. The guide focuses on TT&E actions that individual organizations can manage within their overall IT planning or within their emergency-handling capabilities for IT.

NIST Special Publication (SP) 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities: Recommendations of the National Institute of Standards and Technology*, was written by Tim Grance of NIST, Tamara Nolan, Kristin Burke, and Rich Dudley of Booz Allen Hamilton, and Gregory White and Travis Good of the University of Texas-San Antonio. The publication of the guide was supported by the Department of Homeland Security (DHS).

The guide discusses the need for establishing a TT&E program and the steps involved in creating the TT&E program. In addition, the guide discusses the role of training in a TT&E program and the relationship of training to exercises and tests. Two types of exercises are detailed: tabletop exercises and functional exercises. The section on tabletop exercises helps organizations determine their need for these exercises and advises how to design, develop, conduct, and evaluate the exercises. The section on the design phase of developing these exercises helps users to determine the topics and scope of the exercises, to identify the objectives, to identify participants and training staff, and to coordinate logistics. Other sections contain similar information for functional exercises and for tests.

Included in the appendices are samples of the documentation associated with tabletop exercises, functional exercises, and tests. Also in the appendices are a glossary of terms used, an acronym list, and a listing of print and online resources that may be helpful in establishing and managing a TT&E program.

The TT&E guide is available on NIST's web pages at:

http://csrc.nist.gov/publications/nistpubs/index.html.

Establishing a Test, Training, and Exercise Program

Organizations should maintain their IT plans so that they will be prepared to manage and recover from adverse events that could disrupt their operations. Contingency and computer security incident response plans, which are part of the organization's IT planning framework, are examples of plans that address recovery from adverse events. A TT&E program contributes to the effective maintenance of all IT plans through the following activities:

* **Tests** – evaluation tools that use quantifiable metrics to validate the operability of a system or system component in an operational environment as specified in an IT plan. Tests could include activities such as checking if call tree cascades can be executed within prescribed time limits or removing power from a system or system component. Quantifiable metrics can be collected when these activities are performed. The organization should develop a test plan to identify the systems or components to be 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 can be conducted to accomplish other goals, depending upon the specific IT plan.

* **Training** – advising 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. These training activities prepare staff members for participation in exercises, tests, and actual emergency situations related to the IT plan. Staff members are trained on their roles and responsibilities before an exercise or test event. Discussions at these training events enable staff members to demonstrate their understanding of the subject matter.

* **Exercises** – simulations of an emergency designed to validate the viability of one or more aspects of an IT plan. Exercises help 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. The responses may be executed in a simulated operational environment or through other means of validating responses that do not involve using the actual operational environment for deployment of personnel.

Exercises are scenario-driven; for example, an exercise might be concerned with a power failure in one of the organization's data centers or a fire that causes certain systems to be damaged. Often exercises provide for the presentation of more than one adverse situation. Two types of exercises are discussed in the guide:

- **Tabletop exercises**, which are discussion-based exercises enabling personnel to 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. The questions initiate 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,** which 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, such as communications, emergency notifications, or IT equipment setup. Functional exercises vary in complexity and scope, and range from the validation of specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff members to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

The TT&E Plan

Organizations should develop TT&E plans that outline all of the elements of the TT&E program and all of the steps that need to be taken to carry out the program. 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 will enable the organization to achieve an effective, proven capability, and should provide a schedule for conducting various types of TT&E events.

Steps in Developing a TT&E Program

In addition to developing their TT&E plans, organizations should take the following steps to create a TT&E program:

* **Develop a comprehensive policy.** The comprehensive policy should outline the organization's internal and external requirements that are associated with training personnel, exercising plans, and testing components and systems. The policy also provides an overall framework for an explanation of the purpose and objectives of the program; references for applicable federal and internal guidance; the rules that govern

how the organization develops and administers the TT&E events; and requirements for the documentation associated with TT&E events.

* **Identify roles and responsibilities.** The TT&E program should be managed by a person or team with direct responsibility for the organization's IT planning functions. In many federal organizations, these functions are carried out by the Office of the Chief Information Officer (OCIO). An IT plan coordinator should be designated to be responsible for all aspects of IT planning, including development, implementation, and maintenance. The plan coordinator should have responsibility for the TT&E element of maintaining the IT plans and should identify a TT&E program coordinator, who is responsible for developing a TT&E plan and coordinating events. The TT&E program coordinator works with event design teams in planning and conducting TT&E events. Organizations may decide to procure specialized software or obtain external support to assist in forming or staffing these teams.

* **Establish an overall 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 SP 800-53 requires federal agencies to conduct exercises or tests for their systems' contingency plans and incident response capabilities at least annually. The testing activities discussed in the guide are not the same as the testing activities performed for system certification and accreditation (C&A). C&A activities are associated with the security of systems under normal conditions. Although the requirements of C&A and TT&E test events are usually different, organizations may wish to avoid duplication of efforts and conduct a single testing event that encompasses requirements that are common to both C&A and TT&E.

* **Document methodology.** In creating a TT&E program, an organization should select and document a high-level methodology for planning and performing TT&E events. The methodology includes four basic phases, which should be used for each event.

  - **Design the event.** The TT&E program coordinator works with the IT 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 who 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 providing needed documents, having the room set up, and arranging for 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 could include briefing materials, participant manuals, instructor and facilitator guides, test plans and scripts, and evaluation criteria.

- **Conduct the event.** In this phase, the training, exercise, or test event is conducted. The details of this phase may vary greatly depending upon 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. Participants in training events can be asked to complete an evaluation form, and their comments can be analyzed and documented in a training analysis report. Future training sessions may then be modified as needed. Participants in exercises or tests can discuss in a follow-up debriefing session those activities that went particularly well and those that they think should be modified or enhanced. Findings discussed during the debriefing sessions, observations made during the course of the event, and considerations for enhancement are documented in an after action report.

NIST Recommendations for TT&E Programs

Organizations should develop TT&E programs that combine training, exercise, and testing activities. These activities are closely related, but offer different ways of identifying problems with IT plans and procedures.

The TT&E program should include a TT&E plan, policy, event methodology, and procedures. It should address resource and budget requirements, and provide a schedule for conducting types of TT&E events.

The TT&E plan should document the projected schedule of activities to be performed within the TT&E program. TT&E events should be conducted periodically, following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance.

TT&E events should be conducted as needed, and organizations should evaluate the required frequency of its events and document the frequency of each event in a TT&E schedule. 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.

More Information

Other NIST publications that support test, training, and exercise processes include:

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, presents a framework for meeting the organization's requirements to provide IT security training that is appropriate for current and future computing environments.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, assists organizations in developing security plans that summarize the security requirements for each information system and identify the security controls in place or planned for meeting the requirements.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides instructions, recommendations, and considerations for federal government IT contingency planning.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, assists organizations in providing IT users with training on security policies, procedures, and techniques, including the security controls that are available to protect information and systems.

NIST SP 800-53, *Minimum Security Controls for Federal Information Systems*, provides guidance in selecting, specifying, and tailoring security controls that will provide an appropriate level of security, based on the organization's assessments of risk to its information and systems. The controls are administrative, operational, and technical safeguards that are selected, based on the security categorization of the information and systems.

NIST SP 800-61, *Computer Security Incident Handling Guide*, discusses how to organize a security incident response capability and how to handle incidents including denial of service, malicious code, unauthorized access, and inappropriate use of systems.

NIST publications assist organizations in planning and implementing a comprehensive approach to IT security. For information about NIST standards and guidelines that are referenced in the test, training, and exercise guide, as well as other security-related publications, see NIST's web page:

http://csrc.nist.gov/publications/index.html.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.