



Establishing a Successful Testing, Training and Exercise (TT&E) Program

A Functional Handbook

Final rev 2.0

May 28, 2010

Developed for Business Continuity and Security
Professionals

Dedication

Leadership is about trust, agility and clarity. Companies that accelerate are those that can adapt quickly and lead with a crisp, clear vision about the path to success. Setting the course for this new leadership starts by example.

In this handbook, we highlight different approaches that leverage people and technology to solve business problems, coupled with trust, communication and clarity. I invite you to consider the suggestions presented as a means to facilitate a mix of lecture and breakout table discussions that identify how to establish and operate your own Testing, Training and Exercise (TT&E) program. The development of your program starts with personnel awareness (awareness in your program, awareness of its intent and the continued awareness of its very existence). When we fall into routine and become comfortable with back office planning and development, we lose the attention of our audience. It is through subtle continued reminders of the program through posters, emails, and even pandemic signs near wash stations that people are reminded that we exist to protect them and the organization and that we all share a role in that function, from the office cleaning crew, to reception to the account teams and through to the executives. By hiring us, they showed their support. Now it is up to us to remind them what we bring. This is what adds up to successful initiatives within an organization.

This handbook represents the combined contribution of the following members:

- Ashley Fimiano, CGI Federal
- Doroden Gully, CGI Federal
- Cary Jasgur, CGI Federal
- David Johnson, CGI US Tier 1
- Frank Slater, CGI Ottawa
- Mark Spreitzer, CGI Federal

We dedicate this book to all of those individuals that have influenced our personal and professional lives and offer this collection of thoughts to the community of business continuity and security professionals as a means to accelerate their education using our collective experience.

“Building awareness, training and exercising programs takes creativity and passion. The partnership that led to developing this handbook shaped by the CGI Federal and CGI Ottawa Business Continuity teams is a fine example of how practical education and training needs can drive initiatives that further our Thought Leadership program outreach efforts.”

- Mark Spreitzer

For more information:

Mark Spreitzer, CBCP
Director, Business Continuity
CGI Federal Enterprise Security Practice
mark.spreitzer@cgi.com
(212) 612-3611

Table of Contents

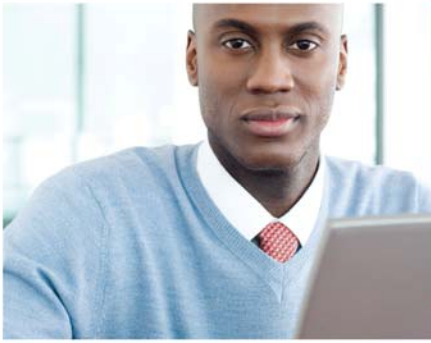
1	Introduction	1-1
2	Precursors to a TT&E Program.....	2-1
2.1	Understanding the Organization.....	2-3
2.2	Determining Business Continuity Management Strategies	2-3
2.3	Develop and Implementing the BCM Response	2-4
2.4	Plan Exercise, Maintenance and Review	2-5
3	Plan Exercise, Maintenance and Review	3-1
4	PDCA Applied to BCMS	4-1
5	Developing Employee Awareness	5-1
6	Awareness Strategies	6-1
7	Campaign in Motion	7-1
8	Components of a Successful TT &E Program	8-1
8.1	Develop Comprehensive TT&E Policy	8-2
8.2	Identify TT&E Roles and Responsibilities	8-2
8.3	Establish Overall TT&E Schedule	8-2
8.4	Document the TT&E Event Methodology	8-3
9	TT&E Strategies.....	9-1
9.1	Training vs. Awareness	9-1
9.1.1	Awareness.....	9-1
9.1.2	Training	9-1
9.2	Testing vs. Exercising	9-2
9.2.1	Testing.....	9-2
9.2.2	Exercising.....	9-2
9.2.3	Exercises.....	9-3
10	Exercise Methodology.....	10-1
11	Steps for Exercise Planning	11-1
11.1	Exercise Types.....	11-1
11.1.1	Discussion-Based Exercises	11-1
11.1.2	Operations-Based Exercises.....	11-3
11.2	Step by Step Process for Planning an Exercise.....	11-4
11.2.1	Step One	11-5
11.2.2	Step Two	11-5
11.2.3	Step Three.....	11-5

11.2.4	Step Four.....	11-6
11.2.5	Step Five	11-6
11.2.6	Step Six	11-6
11.2.7	Step Seven.....	11-7
11.2.8	Step Eight.....	11-9
11.2.9	Step Nine.....	11-10
12	Appendix A: Glossary of Terms	12-1
13	Appendix B: External References	13-1
14	Appendix C: Exercise Sign Sheet Template	14-1
15	Appendix D: Discussion Based Exercise Scenario Template	15-1
16	Appendix E: Discussion Based Exercise Results Template	16-1
17	Appendix F: Participant Feedback Form Template	17-1
18	Appendix G: Evacuation Drill Checklist Template	18-1
19	Appendix H: After Action Report Template (HSEEP).....	19-1

List of Exhibits

Exhibit 1-1: Employee on the Run	1-1
Exhibit 2-1: Business Continuity Management (BCM) Lifecycle	2-1
Exhibit 3-1: Contingency-Related Plan Relationships.....	3-1
Exhibit 3-2: The Business Continuity Plan	3-2
Exhibit 4-1: Plan, Do, Check, Act Cycle (PDCA) applied to BCM Systems Processes	4-1
Exhibit 8-1: TT&E Methodolgy	8-1
Exhibit 10-1: Exercise Program Management	10-1
Exhibit 11-1: Exercise Types, Discussion vs. Operations Based.....	11-1
Exhibit 11-2: Disaster Recovery Plan	11-4
Exhibit 11-3: Exercise Type, with Participant Listing	11-7

This page intentionally left blank.



_experience the commitment™



Business Continuity Solutions

COMPANY PROFILE

A focus on the fundamentals

- 30+ years of long-term growth with 26,000 professionals in 100+ offices
- 9.0/10 satisfaction score from 2,000 annual client interviews
- Rigorous project monitoring resulting in 95% on-time, on-budget delivery
- Committed to world-class service levels with over 98% exceeded or met
- NYSE: GIB — TSX: GIB.A

End-to-end services

- Business process services
- Systems integration and consulting
- Technology and application management
- Complementary portfolio of proprietary software

Focused industry expertise

- Government and healthcare
- Financial services
- Telecommunications and Utilities
- Retail and distribution
- Manufacturing, including oil and gas

Statistics verified as of June 2009.

CGI helps clients manage risk and achieve operational resiliency through business continuity (BC) programs based on risk management principles, client organization policy, and regulatory guidelines.

An enterprise approach to risk management

More than ever, managing risk is at the core of success. Unanticipated business interruptions can devastate the enterprise. It has become a top priority to safeguard reputation and provide for the continuity of operations to meet financial objectives, regulatory compliance, and consumer and citizen expectations.

CGI works with organizations to define the level of contingency planning required based on their internal risk profile to reduce the likelihood and impact of both manmade and natural threats to their operations.

The CGI Business Continuity Management approach and methodology supports the identification, assessment and development of your organizations policies and procedures for addressing operational risk should it materialize. It includes a proper response, communication, assessment, execution, monitoring and reporting activities.

Reduce your risk of business disruption

CGI's consulting expertise extends to all aspects of BC planning across the enterprise value chain. Our approach includes the balancing of risk vs. controls to achieve the continuity of your business operations, recovery of the supporting your technological infrastructure, and the stability of your operational environment to resume and sustain activities.

CGI's engagement framework emphasizes acquiring an in-depth knowledge of each organization's culture and unique needs. CGI's approach also fosters accountability among an organization's leaders and the managers responsible for critical business processes. Personnel at all levels of the organization are included in the planning process to ensure a sound and practical plan.

Your partner of choice

CGI offers a proven track record of delivering a full suite of risk management services and solutions that meet various international standards and guidelines. CGI enhances the value proposition of our services through thought leadership and industry expertise. CGI consultants are industry practice influencers, serving as professional practice board chairs, authoring various articles and white papers, and presenting at industry conferences.

Our services

Our comprehensive BC offerings assist in hardening your critical business functions and supporting applications and data to provide fast, reliable customer service anytime, anywhere. Our experts analyze, recommend and assist the implementation of reliable strategies and solutions to satisfy operational requirements and accommodate growing business needs.

Offerings include:

- Business continuity (BC) and disaster recovery (DR) planning
- Contingency strategy and emergency/disaster response solutions
- Continuity of operations planning (COOP) and critical infrastructure protection (CIP) planning
- Pandemic response planning
- Risk assessment (RA) and business impact analysis (BIA)
- Crisis management and communications response planning
- Awareness, testing, training and exercise (TT&E) programs
- Business continuity program management

Related services include:

- Risk management
- Information security
- Compliance
- IT service management

Client benefits

CGI offers more than 30 years of BC planning experience across a wide range of organizations in various sectors, including government, energy, finance, manufacturing and not-for-profit.

Key benefits our clients achieve include:

- Protection of key assets and their value
- Preservation of important trust relationships with client and partners
- Balanced legislative and regulatory compliance
- Managed investments
- Increased service quality
- Focused holistic, enterprise-wide approach
- Tested and proven methodologies
- Balanced enterprise risk management

OUR APPROACH

CGI's BC objective is to assess, design, develop and implement *security solutions* for our clients that securely manage and integrate disparate security solutions, on multiple levels, across the entire spectrum of an enterprise.

Accreditations/certifications

- CGI actively supports consultants' pursuit of professional industry certifications
- Certification examples include CBCP, PMP, CISSP, CISM, CISA & ITIL® - Practitioner and Service Manager

Frameworks, standards and compliance control

- Repeatable, customizable process and extensive use of templates built around flexibility
- Methodology based on private and public sector frameworks and best practices (examples: CMMi, FISMA, ISO & ITIL®)
- Recommendations driven by the value and priority of the organization's core business processes instead of focusing exclusively on the technology components

Contact us at info@cgi.com for more information on CGI's information security solutions and services.

Preface

This Business Continuity Management (BCM), Testing, Training and Exercise (TT&E) Handbook is designed to provide information and procedures to assist in the awareness planning and the conducting of a successful testing, training and exercise program. This workshop provides attendees with tools needed to setup or enhance their existing program based on various public standards.

This handbook introduces you to the principles, concepts, and terminology needed to establish a successful testing, training and exercise program – wherever you are across the United States, and, with few modifications for changes in legislation, etc, anywhere in the world.

The material covered in the BCM Testing Training and Exercise Handbook draws upon material from the BCM Process Model Overview, Exercise Design Life Cycle, best practices and standards of the American & International communities. The utilization of various methodologies when implementing a BCM Testing, Training, Exercise and Awareness Program is essential to the overall success of the program. There are currently several business continuity standards and best practices defined by the industry's common body of knowledge; however, BS25999, the British Standard, is closest to an international standard.

This page intentionally left blank.

1 Introduction

Organizations use contingency and incident response plans to respond to and manage adverse situations. A Test, Training, and Exercise (TT&E) Program is a means for ensuring that personnel are trained in their execution of plan roles and responsibilities, plans are exercised to validate their viability and components or systems are tested to validate their operability.

Program elements:

- **Tests** – Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises with quantifiable metrics focused on system or automated processes.
- **Training** – Training refers to informing and teaching personnel of their roles and responsibilities related to those roles and responsibilities, thereby preparing them for participation in exercises, tests and actual emergencies.
- **Exercise** – A people focused activity designed to execute plans and evaluate the individual and/or organization performance against approved standards or objectives.

Creating a successful TT&E program is vital to ensuring that an organization is prepared to respond to an interruption. A TT&E program rounds out your BCM Program. The program should include several types of TT&E events to ensure the availability of a wide range of methods for validating various planning elements in the context of business interruptions.

This handbook provides a tutorial walk through the process of establishing a TT&E program, as well as developing a TT&E policy, defining roles and responsibilities and documenting a TT&E event methodology.

Exhibit 1-1: Employee on the Run



This page intentionally left blank.

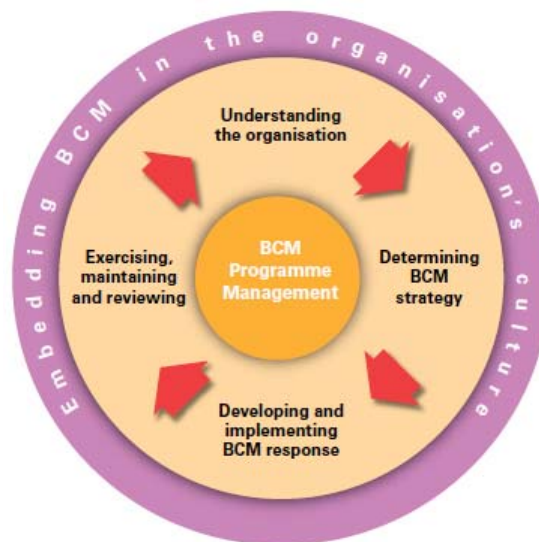
2 Precursors to a TT&E Program

Business Continuity Management (BCM) is:

- “A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.”¹
- Business continuity management is ensuring the continuity or uninterrupted provision of operations and services. BCM is an ongoing process with several different but complementary elements, including disaster recovery, business recovery, business resumption, contingency planning, and crisis management.
- Business Continuity is a management process that provides a framework to ensure the resilience of your business to any eventuality, to help ensure continuity of service to your key customers and the protection of your brand and reputation. It provides a basis for planning to ensure your long-term survivability following a disruptive event.

Exhibit 2-1 illustrates the BCM lifecycle. Each element of the BCM lifecycle contributes to a different level of understanding and awareness, bringing in differing and disparate audiences from all levels across the organization. The lifecycle facilitates creating a deeper level of understanding than that achieved by broader and more generic campaigns by structuring direct input into the deliverables and relating deeper insight into the components of the program’s intent. This should assist in managing expectations both in the capability of your BCM program, what is important and achievable, and in the organizations ability to respond to an event².

Exhibit 2-1: Business Continuity Management (BCM) Lifecycle



Reference: BS25999-1, 2006

¹ Source: Business Continuity Institute & BS:25999

² Business Continuity Journal, Vol.3, Issue 3

Organizations cannot possibly prepare for every scenario but the more extensive planning and preparation, the better prepared the organization is to react to the unexpected. A robust Business Continuity (BC) plan documents the steps implemented, the resources needed and the procedures required before, during and after the crisis.

An effective BCM program establishes the organization's approach to business continuity by identifying the program restraints (scope); the goals objectives (policy), assigning BCM responsibilities (governance structure/oversight committee), overall project management and the identification of deliverables outcomes (plan documentation). An effective BCM program framework offers the following:

- Increased levels of employee readiness to ensure the safety of personnel and an organized organizational response
- Compliance with applicable regulatory requirements and fiduciary responsibilities to avoid potential penalties and litigation
- Prioritized recovery of the organization's business processes to achieve optimal allocation of resources focused on protecting revenue and containing costs; including the identification and the impact of potential loss to critical business functions and processes in order to resume and recover in timely manner.
- Customized response strategies focused on high probability scenarios that ensure the efficient and effective allocation of the organization's BCM budget
- A well-planned emergency response, incident response and crisis communications framework designed to address internal and external requirements
- Minimized revenue loss and brand reputation by maintaining viable recovery strategies and plans that safeguard assets and liabilities
- Awareness of third party/vendor continuity plans to ensure uninterrupted service and protection of assets
- Continuity of operations through exercise, maintenance and review
- Tools for senior leadership executives to predict operational impact of business disruptions

Achieving organizational buy-in (top down and bottom up), as well as, visible and continued support by Executive-level management towards a BCM program is not an easy task. Embedding a successful BCM culture involves influencing values, beliefs and behaviors. It is critical everyone within the organization develop a positive attitude of preservation (self and organizational) in order to create a strong BCM program. The organization must instill BCM as a core value within the organization by ensuring that all stakeholders have a complete understanding of roles, responsibilities and tasks. Adopting this change management approach ensures the BCM culture becomes an integral part of the organization's strategic and day-to-day operations.

2.1 Understanding the Organization

Discussions held and questions asked during the Business Impact Analysis (BIA) process enable the organization to see what the up and downstream activities are as well as the benefits to the overall BCM program. The BIA is the foundation on which to build an organization-wide BCM Program. Identifying the impacts of disruptive events helps to measure and report on the possible effects associated with changes or disruptions to critical business functions, process and services. The purpose of BIA is to ease and improve decision making while reducing errors. The risk analysis process is a technique utilized to help an organization assess and identify potential threats that may jeopardize various business functions or departments within the organization. The RA process helps to define the preventive measures needed to reduce the probability of the impacts from occurring and identify countermeasures to successfully deal with these constraints when they develop.

- What is BC Policy and BC Program Management?
- What are your key business functions /objectives of the organization?
- How are business objectives achieved?
- Have you identified Mission Critical Activities (MCA)?
- Who is involved (internally and externally) in the delivery of product and services?

2.2 Determining Business Continuity Management Strategies

It is important to bring awareness and communicate the potential impacts and threats to the organization to executive level management. Utilize the business impact and risk assessment to facilitate engaging executive level management to develop the appropriate continuity strategies. BCM strategy discussions are likely to take place with those who are responsible for the organization's wider objectives and budget once the strategies are determined.

- Business Impact Analysis (BIA) – How Detailed?
- Recovery Time Objectives (RTO) – How Fast?
- Recovery Point Objectives (RPO) – How Much?

BCM strategies include:

- Implementing alternative operating procedures after an interruption to maintain or resume the organizations internal or external business functions
- Protection of vulnerabilities and failure points in business critical processes identified in the risk analysis
- Recovery time objective for each mission critical business activity
- Interdependencies of services, business processes, data and technologies
- Resource requirements

2.3 Develop and Implementing the BCM Response

Depending on the size of your organization, the development and delivery of your incident management and business continuity plans will involve other groups, teams or committees. The identification of appropriate incident management teams across your will include some people who have not been directly involved in any of the preceding components of the business continuity lifecycle and, again, when continuity plans are developed for individual business units.

Plans include:

- Business Continuity Plan
- Crisis Management Plan
- Emergency Response Plan
- Incident Management Plan

Embedding BCM in the Organization's Culture

A key element in developing a successful BCM culture within the organization is the preparation and delivery of a program to create corporate awareness and enhance the skills knowledge and experience required to implement, maintain, manage and execute business continuity management.

"An awareness, training, testing and exercise program is crucial in that it is the vehicle for disseminating information which users, including managers, need in order to do their jobs."³

TT&E teams and plans are by far the best ways of directly embedding business continuity in the culture. "Making these events visible increases awareness and understanding of those not directly involved, additionally it shows that your organization takes business continuity seriously. Internal or independent auditors are another group that could be actively engaged to assist in the delivery of your BCM program. They are capable of bringing different viewpoints and weight to the issues you may be facing. An added benefit is they can assist in raising awareness of the BCM Program to others within the organization and ultimately can raise issues up to the highest levels."⁴

Awareness of the importance of business continuity management to the organization and its business priorities is fundamental to embedding a successful BCM culture. Testing, Training and Exercising are valuable techniques utilized within the organization to motivate and increase employee understanding and overall awareness of the BCM program and policies.

³ NIST 800 Series (USA): NIST.gov

⁴ Andy Mason, Business Continuity Journal, Vol.3, Issue 3

The single most important tool in developing, implementing and maintaining an ongoing business continuity program is the education, testing, training and awareness of ALL employees in the organization. Business continuity must be an integral part of the orientation process, or the policy and procedure manual and of the employee handbook.

- Develop General Employee Awareness:
 - By assessing current level of awareness within your organization
- Embed into Organization's culture through:
 - Awareness
 - Training
 - Testing
 - Exercising

2.4 Plan Exercise, Maintenance and Review

Learning is a continuum: it starts with awareness, builds to training, enhances through testing and exercising. Effective plan testing requires a continuum of drills and exercises from simulations and walk-through, to full-scale operational exercises.

Employees tend to practice a tuning-out process called acclimation. Employees will selectively ignore a stimulus (i.e. BCM attention-getter) if it is used repeatedly. Assimilation is a process whereby an individual incorporates new experiences into an existing behavior pattern. The average employee needs repeated exposure to gain understanding. The BCM program awareness delivery must be continuous, creative and motivational, with the objective of focusing and incorporating BCM within the employee's day-to-day decision-making.

When was the last time you saw posters on the wall reminding employees about business continuity?

This page intentionally left blank.

3 Plan Exercise, Maintenance and Review

According to the National Institute of Science and Technology (NIST) Special Publication (SP) 800-34 revision one (rev.1), continuity and contingency planning are critical components of emergency management and organizational resilience. Continuity planning and contingency planning are often confused in their use. Continuity planning normally applies to the business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. Contingency planning normally applies to information systems, and provides the steps needed to recover the operation of information systems at an existing or new location in an emergency. Exhibit 3-1 illustrates the NIST defined relationship between contingency related plans.

Periodic and regular testing of Contingency Plans and Continuity of Support Plans, per NIST guidance, ensures that the procedures, processes and systems that comprise the plans are viable and effective. The BC / Disaster Recovery Coordinator audit review and test the recovery plans annually.

Exhibit 3-1: Contingency-Related Plan Relationships⁵



Below are a few examples of Continuity plans:

- **Business Continuity Plan (BCP)** – The BCP focuses on sustaining an organization’s business functions during and after a business disruption. An example of a business function may be an organization’s payroll process or customer service process. Business continuity plans address the business processes within a single business unit or the entire organization. In certain circumstances, a BCP will work in conjunction with the Continuity of Operations

⁵ NIST Special Publication 800-34 Rev.1 (Draft)

Plan, allowing additional processes to come online as resources or time allow. Keep in mind, the BCP may not address the organization's long-term recovery of business processes.

- **Continuity of Operations Plan (COOP)** – COOP focuses on restoring an organization's mission-essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Minor threats or disruptions that do not require relocation to an alternate site are generally not part of a COOP plan.

Standard elements of a COOP plan include:

- Program Plans and Procedures
- Continuity Communications
- Risk Management
- Vital Records Management
- Budgeting and Acquisition of Resources
- Human Capital
- Essential Functions
- Test, Training, and Exercise
- Order of Succession, Devolution, Delegation of Authority, Reconstitution and Continuity Facilities

COOP plans are mandated for organizations by HSPD –20/NSPD-51, National Continuity Policy and FCD 1 & 2, Federal Executive Branch National Continuity Program and Requirements. Federal directives distinguish COOP plans as a specific type of plan that is not to be confused with Information System Contingency Plans, Disaster Recovery Plans or BCPs. Nongovernment agencies typically use BCPs rather than COOP plans to address business processes

Exhibit 3-2: The Business Continuity Plan ⁶



⁶ CallCenterComics.com, Cartoon #112, 2009

- **Crisis Communications Plan (CCP)** – A crisis communication plan documents the standard procedures for internal and external communications in the event of a disruption. The crisis communications plan designates specific individuals as the only authority representing the organization for answering questions from or providing information to the public regarding emergency response.
- **Critical Infrastructure Protection Plan (CIP)** – Critical Infrastructure and Key Resources are those components of the national infrastructure that deemed so vital that their loss would have a debilitating effect of the safety, security, economy and/or health of the United States.⁷ A CIP is a set of policies and procedures that serve to protect and recover these national assets and mitigate risks and vulnerabilities. CIPs define the roles and responsibilities for protection, develops partnerships and information sharing relationships, implement the risk management framework defined in the National Infrastructure Protection Plan (NIPP) for CIKR assets, and integrate federal, state and local emergency preparedness, protection, and resiliency of critical infrastructure.
- **Cyber Incident Response Plan (CIRP)** – The Cyber Incident Response Plan establishes procedures to address cyber attacks against an organization’s information system(s). The design of these procedures is to enable security personnel to identify, mitigate and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software or data (e.g., malicious logic, such as a virus, worm or Trojan horse). This plan may be included among the appendices of the BCP.
- **Disaster Recovery Plan (DRP)** – The DRP applies to a major, usually physical disruption to service that denies access to the primary facility for an extended period. The DRP is an information system-focused plan designed to restore operability of the target system, application and database or computer facility at an alternate site after an emergency. A DRP may support a BCP or COOP plan by recovering supporting systems for essential functions and processes at an alternate location.
- **Information System Contingency Plan (ISCP)** – An ISCP provides established procedures for the assessment and recovery of a system following a disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. The ISCP differs from a DRP primarily in that the information system contingency plan procedures outline the recovery of the system regardless of site or location. The activation of an ISCP occurs either at the system’s current location or at an alternate site. In contrast, a DRP is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DRP has successfully transferred an information system site to an alternate site, each affected system would then use its respective information system contingency plan to restore, recover, test systems and put them into operation.

⁷ For more information on Critical Infrastructure and Key Resources (CIKR), refer to the Department of Homeland Security’s *National Infrastructure Protection Plan 2009*

- **Occupant Emergency Plan (OEP)** – The OEP outlines first response procedures for occupants of a facility in the event of an incident or threat to the health and safety of personnel, the environment or property. Events may include a fire, bomb threat, chemical release, domestic violence in the workplace, or a medical emergency. The OEP may also address shelter-in-place procedures for events requiring personnel to stay inside the building rather than evacuate; which addresses the facility level, specific to the geographic location and structural design of the building.

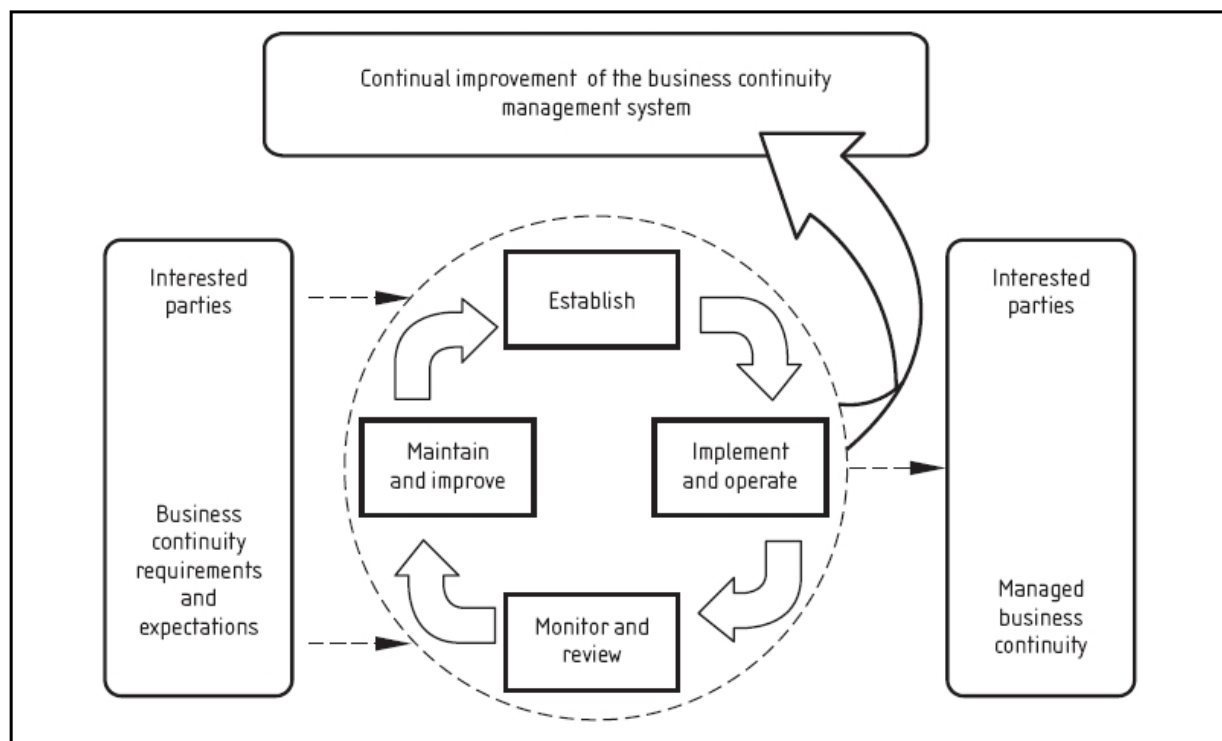
4 PDCA Applied to BCMS

One of the goals of any management standard is that of continuous improvement. BS25999-2:2007 utilizes the PDCA (Plan-Do-Check-Act) cycle for developing, implementing and improving the effectiveness of an organization's Business Continuity Management System (BCMS). A BCM policy is required that demonstrates clear management commitment and details the scope and objectives of the BCMS.

The British Standard BS 25999 features an approach to coordinating elements of a BC program. The approach is consistent with the International Organization for Standardization (ISO). ASIS document and the British Standards Institution (BSI) authored BS 25999. The ASIS document endorses the Plan-Do-Check Act (PDCA) model found in BS 25999 and many ISO standards. PDCA weaves decision making into the fabric of an organization's overall operational and business practices. PDCA makes the organization more efficient and better able to meet important challenges by providing a set of problem identification and problem-solving tools that can be implemented by an organization in many different ways, depending on its unique activities and needs.

Exhibit 4-1 shows how to apply the PDCA cycle to every element of the BCM life cycle as set out in BS 25999-2:2007. Utilizing the PCDA cycle will ensure business continuity is established and continuously managed within an organization.

Exhibit 4-1: Plan, Do, Check, Act Cycle (PDCA) applied to BCM Systems Processes



Plan (Establish and Manage the BCMS)

Establish policy, objectives, targets, controls, processes and procedures relevant to managing risk and improving business continuity to deliver results in accordance with overall policies and objectives.

- Obtain Top Management commitment
- Assign departmental business continuity roles and responsibilities
- Conduct a Business Impact Analysis (BIA) and Risk Assessment (RA)

Do (Implement and Operate BCMS)

Put plans into action. Implement and operate the business continuity policy, controls, processes and procedures.

- Understand the Organization
- Determine the BCM strategy
- Develop and Implement a BCM response
- Exercise, Maintain and Review the BCM plans

Check (Monitor and Review the BCMS)

Monitor and review performance against business continuity objectives and policy.

- Test the plan
- Audit the plan

Act (Maintain and Improve the BCMS)

Maintain and improve the BCMS by taking preventative and corrective actions to ensure continuous improvement.

- Improve the business continuity plan

The work of Walter Stewart who developed statistical process control in the US during the 1930s and from the 1950s onwards by quality management authority, W. Edwards Deming, serves as the basis for the Plan Do Check Act methodology.

5 Developing Employee Awareness

BC is a key component of an organization's risk management program. Most often, employees are unaware of the existence of the program, or their role within the business continuity effort. Employees must be knowledgeable of BC plans and processes. It is critical for all employees to be aware of the program role and responsibilities applicable to them. For example, building evacuation, employee accountability and crisis communications are all important topics that all employees should understand. In order to implement a coordinated BC effort during a crisis, everyone must be aware of these processes prior to the event occurring:

- **Awareness** –In awareness activities, the learner is a recipient of information. Awareness implies knowledge obtained through one's own perceptions or by means of information. Awareness involves guiding and motivating people on appropriate behaviors. Awareness is the passing of informative.
- **Training** – Training is a vehicle for awareness. Participants take an active role and engage in activities meant to help them learn and apply the concepts and skills introduced. Training helps people develop specific skills.

Support for awareness and training starts with Executive - level management. Their buy-in and backing is an essential part of the planning process. Management needs to understand their responsibilities, required level of involvement, scope and importance as well as, required resources. Weekly briefings and reports ensure you are keeping Management engaged and committed to the planning process.

Support for awareness training starts with a full understanding of the BCM planning process at the executive management-level and the individual staff level. Executive level 'buy-in' and 'sign-off' of a clearly defined and documented BCM awareness program should facilitate an organizational-wide understanding of overall BCM strategy , in particular awareness and why business continuity management is critical to the employees individual roles and responsibilities within BCM process.

Initial awareness and training requirements does not end with Executive-level management. The BCM planning process involves every member of the organization, including stakeholders. Awareness training for all employees should include an overview of the BCM planning process, program objectives.

Building knowledge and skills to enhance job performance is all very well but has little value unless people actually use the knowledge and skills when they get back to work. Achieving this is the crux of an effective TT&E awareness program. An effective awareness program directly correlates to the ability to recover effectively and in a timely manner.⁸

It is imperative each person in your organization understand why business continuity is important. Each employee should understand the impact—both personal and organizational—of not following or adhering to the business continuity best practices, as defined in policies, standards and guidelines.

⁸ Yardis, Susan. *Designing a Business Continuity Training Program to Maximize Value and Minimize Cost*. White Paper retrieved from <http://www.continuitycentral.com/bctrainingandawareness.pdf>.

This page intentionally left blank.

6 Awareness Strategies

Awareness, training and exercising take creativity and passion. Learning achieved through a single awareness activity tends to be short-term, immediate and specific. For example, if a learning objective is “to facilitate the increased use of effective password protection among employees,” an awareness activity might be the use of reminder stickers for computer keyboards.⁹

If you are not sure how to get started, begin by sending out a survey or training needs assessment (TNA). Information received from the survey provides a good baseline and helps an organization determine where the gaps are in communicating important information about the business continuity management program (be sure to include executive-level management).

Questions should be relevant to your organization and could include:

- What is the workaround when the facility is unavailable?
- Are your crisis communication plans in place?
- Do you know what to do during an emergency?
- Do you know the location of the nearest stair exit, alternate stair exit(s) and the direct route to each exit?
- Do you know where to gather upon exiting the building?

“Business Continuity Educated” employees are very rare, unless they just experienced a business interruption or participated directly in well-planned exercise. As a result, employee training and awareness is an area for improvement during internal audit reviews. The Business Continuity Institute (BCI) gives some great ideas and methods to increase internal business continuity awareness.¹⁰

What does business continuity mean to YOU?

1. **Give them something physical:** Wallet cards are a great way to give employees a physical item that continuously reminds them of key business continuity information. Wallet cards contain information such as key numbers and tools to use in the case of emergency. Other great ideas include magnets, desk mats or even emergency bags with key supplies.
2. **Get the word out online:** In addition to the organization’s intranet, new tools allow business continuity professionals to develop online training materials for use by thousands of employees in an on demand environment. An organization has an opportunity to custom design training materials to meet their specific needs. These tools can also provide the ability to develop an awareness “quiz” as a method of measuring awareness or compliance.
3. **Involve employees during drills and inspections:** Fire drill evacuations are a great time to provide employees with additional information on disaster preparedness, emergency response and business continuity. Taking advantage of their free time as they mill about the parking lot. Your audience is already thinking about emergency response and business continuity. **Note:** This is a good time to review fire and bomb procedures. These are most visible and easily remembered by staff

⁹ Noticebored.com - www.noticebored.com/blog/2009/03/revised-nist-awareness-standard.html

¹⁰ <http://www.usfst.com/article/Take-your-continuity-program-to-the-next-level/>

Your campaign strategy should include¹¹:

- Basic information such as why the program is being developed (if this is a first for your organization)
- The importance of business continuity planning and disaster recovery, and definitions of key terms so everyone in the organization is speaking the same language
- Organizational information that includes who in your organization is involved in business continuity planning / disaster recovery activities
- What your organization is doing to protect itself from various events, and your organization's emergency response procedures
- Employee information including how an event may affect employees, what to do before/during/after an event, who to contact, where to go, how to deal with the media
- Information on external entities such as information about the Red Cross, Federal Emergency Management Association, local emergency management offices and local fire/police
- Communication plan / materials

Examples of Business Continuity (BC) awareness activities include:

- Employee Orientation:
 - Make “disaster preparedness” a part of new employee orientation and ensure that all employees receive the training
- Events, such as a business continuity day:
 - Encourage your business groups to include Business Continuity Management as an agenda item during their staff meeting this week
 - Encourage your business groups to circulate and update their contact lists/call trees, etc.;
- Promotional/specialty trinkets with motivational slogan
- Media:
 - A business continuity reminder banner on computer screens, which comes up when a user logs on
 - Business continuity awareness video tapes
- Printed materials:
 - Host quizzes to enhance Business Continuity awareness across your organization
 - Cross-word puzzles, posters or flyers
- Include articles in your corporate newsletters and/or on your intranet website:
 - Reserve a 15 minute slot during management briefings

¹¹ Lynne Miller, Keane, Inc., <http://www.continuitycentral.com/feature067.htm>

Create and display posters within the building or even holding a contest to enhance awareness in your organization. Lunch and learn sessions are a great way to allow employees to come and go as their schedules permit. Make sure to always give each employee a "take-away" e.g., pamphlet or laminated card with important information.

This page intentionally left blank.

7 Campaign in Motion

The level of understanding that employees receive from any Business Continuity Management (BCM) awareness program determines the overall success of that program.

Employees often respond to an event according to the training received. By using an ongoing process of testing, training and exercising, organizations have a greater assurance that their employees understand their roles and responsibilities in an emergency and act accordingly.

The following represents several key concepts essential to developing an emergency preparedness training and exercise program for your organization.

- Provide “disaster preparedness” as part of new employee orientation and ensure that all employees receive the training
- Provide refresher training on disaster preparedness for all staff on a routine basis, depending on the roles and responsibilities of a particular group of employees, additional training may be required
- Exercise all portions of your organization’s emergency management plan, in accordance with the training and exercise schedule described in the plan
- Use a variety of training and exercise approaches, including discussion-based tabletop exercises and operations-based drills
- Conduct exercises that include representatives from the fire department, local law enforcement, the local health department, the emergency management office, the Red Cross and other service providers
- Exercise all vendor and mutual aid agreements identified in your plan to be sure of their continued viability, particularly evacuation transportation agreements, receiving facility agreements, and energy/generator agreements
- Evaluate all training and exercise activities using the information to make improvements to your emergency management plan and training and exercise schedule
- Develop relationships with your local emergency management office and health department and participate in training and exercise opportunities they might sponsor

This page intentionally left blank.

8 Components of a Successful TT &E Program

The TT&E methodology development process is comprised of four phases, with a continuous improvement loop. The TT&E program should include a TT&E plan, policy and event methodology. The continuous improvement loop identifies areas to continually improve, modify, and implement exercises of various scales and scope every six to nine months. Conducting TT&Es becomes an ongoing process.

The TT&E plan should outline and document all elements of the program. In addition to creating the TT&E plan, other major steps in creating a TT&E program are as follows:

- Develop a Comprehensive TT&E Policy
- Identify TT&E Roles and Responsibilities
- Establish Overall TT&E Schedule
- Document TT&E Event Methodology

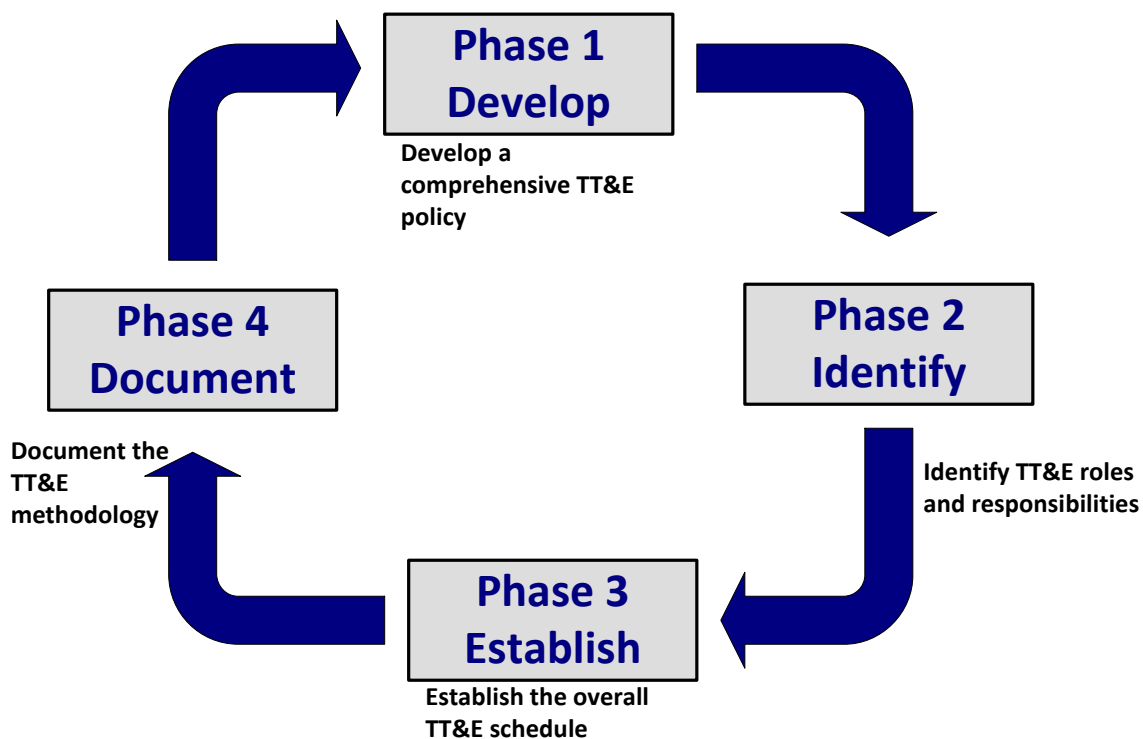


Exhibit 8-1: TT&E Methodology

8.1 Develop Comprehensive TT&E Policy

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

Establish BUY IN - An organization must be committed to the program!

- Win the support and involvement of Executive level leadership
 - They must see the value
- Identify relevant documentation (internal and external)
- Collect and maintain the documentation within a central repository
- Obtain commitment from each department and each business unit involved
- Secure participation by decision makers and managers

Continued buy-in rests with you. It is through continued education, awareness and value added activities that resources follow you as a leader.

8.2 Identify TT&E Roles and Responsibilities

The TT&E program should have a plan coordinator who is responsible for all aspects of program planning. 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.

- The TT&E program should be managed by a person or team with direct responsibility for the organization's continuity planning or disaster recovery planning
- The program should have an plan coordinator who has overall responsibility for the continuity plans

8.3 Establish Overall TT&E Schedule

The TT&E plan should document the projected schedule of activities performed within the TT&E program. Organizations should evaluate the required frequency of events and document each event in a TT&E schedule.

- Adhere to BCM mandated practices for exercise program management, design, development and conduct the exercise to meet compliance needs where applicable
- Incorporate exercise participant roles & responsibilities
- Take into account training needs, establish the need for additional training and incorporate events into the schedule

8.4 Document the TT&E Event Methodology

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, use the same phases for each event. One commonly used methodology has the following phases (for more detail see Section 10 - Exercise Methodology):

- **Design** – Determining the event topic and scope based on the current needs of the organization. Identify the objectives based on the topic and scope, and the personnel that should participate in the event. Oversee the event logistics.
- **Develop** – Working on the development of the documentation (i.e. briefing materials, participant manuals and evaluation criteria) used before, during and after the event.
- **Conduct** – Training employees and exercising plans or testing the application, database, systems or system components.
- **Evaluation** – Analyzing the event and identifying lessons learned to improve the BC/DR plans and their execution, and the overall TT&E process.

NIST SP 800-53 rev.3 requires federal agencies to conduct exercises or tests for their systems' contingency plans and incident response capabilities at least annually.

This page intentionally left blank.

9 TT&E Strategies

No matter how well designed a plan may be, it is only as good as the performance of the participants. The purpose of testing, training and exercising is to get people to perform instinctively, with the precision that a live disaster requires. In order to achieve this purpose, the participants must first know the plan.

A well-rounded TT&E program may consist of:

- Testing (Component, System, Comprehensive)
 - You will be testing and validating your plans, policies, procedures, training, equipment, and inter-organizational agreements
- Training (Instructor-led, Self study)
 - Train personnel in roles and responsibilities – as supported by your plans and procedures
 - Identify gaps in resources and training, and identify areas for improvement
- Exercising (Discussion-Based, Operation Based)
 - Exercises enhance teamwork and encourage the interaction and cooperation required when a real emergency occurs

Testing, training and exercise programs address the gap between current performance and ideal performance within your contingency plans.

9.1 Training vs. Awareness

The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are borne from the awareness foundation.

9.1.1 Awareness

A Business Continuity awareness program has the challenge to change behavior or to reinforce successful continuity practices. Awareness relies on reaching broad audiences with attractive packaging techniques. The purpose of an awareness program is to raise the level of awareness of an employee's role before, during and after an event. By making employees more aware and involving them, you are making employees "lifeguards" for business functions and company assets, as well as their own assets. Another user for a Business Continuity awareness program is to establish a baseline of your organization's awareness against which to measure the effectiveness of awareness efforts and to garner ongoing management support.

9.1.2 Training

Training refers to activities undertaken to educate personnel in their roles and responsibilities within a particular plan and teaching them skills related to those roles and responsibilities. Thereby, preparing them for participation in exercises, tests and actual emergencies related to the

plan. Training provides guidance on how the staff is educated on relevant details of the plan. Additionally, it allows for successful communication of the plan to the organization as a whole, while addressing current and incoming staff.

Steps for the successful and effective Business Continuity plan implementation include:

- Briefing all resources on the contents of the BCP including education on their individual roles and responsibilities
- Training resources with direct responsibilities on the tasks they are required to perform, and educated on the functions of other teams

9.2 Testing vs. Exercising

Discussions within the business continuity community have occurred regarding the testing and exercising of plans and the best methods to achieve both. Some planners contend that you "test the plan" and "exercise the personnel." However, the true test of this statement is in the results received from the very act of properly educating personnel in their roles and responsibilities so they can properly respond should a business disruption or event occur.

The successful exercising of a plan and the personnel is set to accomplish two goals:

- Assure the plan is complete and up to date
- Develop confidence in the responders, and to assure they are prepared

9.2.1 Testing

It is important to emphasize and manage the possible negative connotation of the term "test." A test is the means by which the presence, quality or genuineness of anything is determined. This may conjure images of personal evaluation and the possibility of failure, which can be counterproductive to the goal of developing, maintaining and refining a BCM program. The term test can be an unnecessary distraction from the goal of developing the capability to deal with disruptive events in an orderly, efficient and effective manner. A "test" in the business continuity world does not indicate a "pass or fail" situation. To counter this perception, it is necessary to stress that the goal of testing is to provide validation and improvement of the program and plan and not to the individuals' and teams' roles and performance. 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) as identified as critical resources in a continuity plan.

9.2.2 Exercising

An exercise is a simulation of an emergency designated to validate the viability of one or more aspects of a plan. Exercises should be developed and scheduled in order to achieve and maintain high levels of competence and readiness. While exercises are time and resource consuming, they are the best method for validating a plan. Consider the following tools when planning an exercise:

- Player Handbook
- Drill Guide & Scenario Development
- Realistic Scenarios/Simulations
- Exercise Checklist
- Corrective Action Log
- Participant Feedback Form

We only learn so much by reading:

- Training programs and plans cover over 95% of the information required for emergency response
- Unless someone is forced into a course of action under the stress of a simulated emergency situation, the plans may not be as effective in a real situation

A well-designed and well-executed TT&E program is the most effective means of bringing awareness, including the following:

- Assessing and validating whether policies, contingency plans and procedures are working
- Improving individual performance, organizational communication, and coordination between teams
- Increasing employee awareness through training by clarifying roles and responsibilities
- Measuring performance and identifying resource gaps that may be present
- Identify opportunities for improvement prior to an actual event or disaster
- Satisfying regulatory requirements
- The importance for a company-wide business continuity / disaster recovery program
- The company commitment to business continuity planning and disaster recovery

9.2.3 Exercises

Exercises are an essential component of the overall TT&E program. Exercising is critical in the development and maintenance of contingency plans. Exercises are the primary tool for Validation, Testing and Training.

Exercises ARE:

- Scenario-based approaches to learning
- A practical and cost cost-effective way for organizations to prepare for real emergency response and recovery situations
- A method of improving program awareness and support
- A means of increasing personnel confidence in the program, while increasing the reliability of the plan
- Where true learning occurs

Exercises ARE NOT:

- A plan walkthrough
- A classroom-based training presentation

Remember:

- An exercise must have a clearly defined scope
- An exercise must be practical and cost effective
- An exercise must not pose a risk to the organization
- An exercise has to ensure confidence in the program and its associated plans

Exercise Program Management

Effective TT&E Programs have pre-determined, clearly defined goals and objectives that provide criteria for measuring success. Building an effective Exercise Management Program is a multi-departmental effort that includes:

- Cost of the program
- Analysis of what you are capable of doing
- Setting realistic goals for the organization
- Development of a short term and a long term plan
- Scheduling the task involved
- Developing a series of messages to keep staff involved informed and up-to-date as your program moves through the various phases

10 Exercise Methodology

The National Incident Management System (NIMS) defines the preparedness cycle as “planning, training, equipping, exercising, evaluating and taking action to correct and mitigate.” Exercise project management is a component of exercise program management used to carry out the activities needed to execute an individual exercise. Exercise project management involves five phases, known as the exercise cycle. Exercises conducted in accordance with the phases of the exercise cycle lead to tangible preparedness improvements. Exhibit 10-1 illustrates the five phases of the exercise cycle.

Exhibit 10-1: Exercise Program Management¹²



The following phases must be adhered to in order to provide for an effective exercise:

1. Exercise Foundation

- Create a base of support (i.e., establish buy-in from Executive Management)
- Review current plans (Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan, Occupant Emergency Plan, Disaster Recovery Plan)
- Assess capability to conduct an exercise
- Assess the cost and liabilities associated with conducting the exercise
- Develop a project management timeline and establish milestones
- Identify an exercise planning or design team

¹² This image represents the ongoing process of Exercise Program Management and includes: Improvement Planning, Foundation, Design and Development, Conduct, and Evaluation. HSEEP, vol.II, Exercise Planning and Conduct.pdf

Building on the exercise foundation, the design and development process focuses on:

2. Exercise Development

- Exercise Plan
- Control Plan
- Evaluation Plan
- Player Handbook

3. Exercise Design

- Establish the purpose, scope and objectives of the exercise
- Assess the need
- Define the scope
- Write a purpose statement
- Define the objectives of the exercise
- Design the scenario
- Coordinate Logistic
- Establish an evaluation and improvement methodology
- Develop documentation

4. Conduct

After the design and development steps are complete, the exercise takes place. The conduct phase describes the process for executing the TT&E on the actual day and outlines recommended logistical and support requirements for a successful exercise

- Setup
- Schedule planning conferences and briefings
- Distribution of initial material (Agenda, Objectives, Assumptions, Plans, Session evaluation)
- Circulate attendance sheet for everyone to sign
- Discuss Agenda, Objectives, and Assumptions
- Discuss Ground Rules, Time-lining, and Roles
- Distribution of scenario

5. **Evaluation**

Document lessons learned from the event:

- Formal exercise evaluation
- After Action Report (AAR) that identifies strengths and areas for improvement

6. **Improvement Planning**

The corrective actions identified in the evaluation phase are:

- Assign with due dates, to responsible parties
- Track to implementation
- Validate during subsequent exercises

This page intentionally left blank.

11 Steps for Exercise Planning

Considered the following types of testing, training and exercise methodologies when a developing a program. Each methodology offers different rewards for the overall enhancement of business continuity awareness within your organization. Exercising and Testing methods vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives and benefits.

Prime Tenant

Any exercise, drill or test that you develop should not place the organization at risk. It should be practical, cost-effective, and appropriate to the organization.

11.1 Exercise Types

There are two basic types of exercises

- Discussion Based
- Operations Based

Exhibit 11-1 provides an example of how progression planning activities and training events enable your organization to progress to increased incident response capability. View the graphic the way you would view a stairwell. Progressing up the steps in a planned manner enables you and your stakeholders to progress to the next level with a secure footing.

Exhibit 11-1: Exercise Types, Discussion vs. Operations Based



11.1.1 Discussion-Based Exercises

Discussion-based exercises familiarize participants with existing plans, policies and procedures. Discussion-based exercises typically focus on strategic, policy-oriented issues. Facilitators and/or presenters usually lead the discussion, keeping participants on track toward meeting exercise objectives.

- **Orientations** – An orientation is the most basic type of exercise. Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP. Conduct orientations when new procedures or people enter the workplace.

Orientations are:

- Discussions about the BCP in a conference room or small group setting
- Individual and team training
- Clarification and highlighting of critical plan elements

- **Seminars** – A seminar is an informal discussion that introduces participants to new or updated plans, policies or procedures. Seminars provide a good starting point for entities that are developing or making major changes to their plans and procedures. Provide overview of new or current plans, resources, strategies, concepts or ideas. Seminars are also a good method for informing and training staff on changes to the facility's emergency management plan.

- **Workshops** – After seminars, workshops represent the second tier of exercises in the Homeland Security Exercise & Evaluation Program (HSEEP) building-block approach. They differ from seminars in two important respects: participant interaction is increased, and the focus is on achieving or building a product (such as a draft plan or policy). Workshops often work in conjunction with exercise development to determine objectives, develop scenarios and define evaluation criteria. Workshops can also be successful in the production of new standard operating procedures (SOPs), emergency operations plans (EOPs), Mutual Aid Agreements (MAAs), multi-year plans, or improvement plans. To be effective, workshops must be highly focused on a specific issue with a clearly defined goal or outcome. Achieve specific goal or build product (e.g., exercise objectives, SOPs, policies, plans).

- **Tabletops** – A tabletop exercise (TTX) is a great way to get business continuity plans off the written page without the interruption of a full-scale drill. A tabletop Exercise is a discussion-based exercise where key participants meet in an informal setting or in breakout groups to discuss their roles and responsibilities during a particular incident. The purpose of a tabletop exercise is to stimulate discussion of various issues regarding a hypothetical situation. Another use of a tabletop exercise is to assess plans, policies and procedures or to assess types of systems needed to guide the prevention of, response to, or recovery from a defined incident. Facilitating understanding of concepts, identifying strengths and shortfalls, and achieving changes in the approach to a particular situation are additional uses of a tabletop exercise.

A single tabletop exercise can involve one or more scenarios. The duration of a tabletop exercise (typically two to eight hours) varies depending on the audience, the scenario 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.

Tabletop exercise attributes include:

- Cost-effective
- Low-stress
- Discussions guided by trained facilitator(s)

- Keeps participants on track
- Encourage discussion which captures plan strengths and identifies weaknesses
- Allow exercise participants fulfill their normal day to day roles
- Realistic scenarios that are shaped and limited in scope to meet specific objectives
- Limits: Specific recovery procedures are not actually tested

11.1.2 Operations-Based Exercises

Operations-based exercises serve as validation for the plans, policies, agreements, and procedures solidified in discussion-based exercises. Operations-based exercises include drills, functional exercises (FEs), and full-scale exercises (FSEs). They can clarify roles and responsibilities, identify gaps in resources needed to implement plans and procedures, and improve individual and team performance.

- **Structured Walk-Through** – An exercise in which team members physically implement the business continuity plans, and, verbally review each step to assess its effectiveness, identify enhancements, constraints and deficiencies. Structured walk-through exercises require more time and resources than a tabletop exercise.
- **Drills** – A drill is a coordinated, supervised activity usually employed to validate a single, specific operation or function in a single organizational entity, such as a department. Providing training on new equipment, development or validation of new policies or procedures, or the practice and maintenance of current skills are some uses for a Drill exercise. Drills can help identify particular personnel issues such as people who are unable to walk down stairs or have particular disabilities or anxieties and require assistance during emergencies.

Drill exercise attributes include:

- Narrow focus, measured against established standards
 - Immediate feedback
 - Realistic environment
 - Performance in isolation
- **Functional** – Functional Exercise simulates the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful, time-constrained environment. Response- and recovery-focused functional exercises generally concentrate on exercising the plans, policies, procedures and personnel. Movement of personnel and equipment is simulated.

The functional exercise simulates a crisis in the most realistic manner possible short of moving your staff to the recovery center. Participants practice their response in a realistic method based on the facilitator's scenario or leading questions. Participants validate the following information: call out lists, access to computer hardware or software, policies or procedures. The actions occur in real time and generate real consequences. Functional Exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment.

Functional exercise attributes include:

- Expensive in terms of time and resources expended
- A Limit: Technical competencies may not be tested
- **Full-scale** – The full-scale exercise is the most complex type of exercise. Full-scale exercises can be multi-jurisdictional, multi-organizational exercises that validate many facets of disaster recovery preparedness. They focus on implementing and analyzing the plans, policies, procedures, and cooperative agreements developed in discussion-based exercises and honed in previous, smaller, operations-based exercises. In full-scale exercises, the reality of operations in multiple functional areas presents complex and realistic problems that require critical thinking, rapid problem solving and effective responses by trained personnel. During full-scale exercises, events proceed through a scripted exercise scenario with built-in flexibility, which allow updates to drive activity. Full-scale exercises proceed in real time, creating a stressful, time-constrained environment that closely mirrors real events. The level of support needed to conduct a full-scale exercise is greater than that needed during other types of exercises. During a full-scale exercise, personnel and resources operate from an alternate location.

This replicates the crisis to the smallest detail. Participants in a full-scale exercise are those who hold a critical role in the successful recovery of business operations. It differs from a functional exercise because the full-scale exercise focuses on the operation where the functional exercise focuses on specific processes or procedures. Typically, those operations that have the highest exposure require a full-scale exercise.

11.2 Step by Step Process for Planning an Exercise

This section discusses steps for developing and conducting an exercise for your facility. Included are basic steps to developing a tabletop exercise as well as sample scenario/injects and corresponding exercise goals and objectives. The Homeland Security Exercise and Evaluation (HSEEP) website is a good source to assist with exercise planning activities (https://hseep.dhs.gov/pages/1001_About.aspx - and click on “About HSEEP” for a quick overview of exercise and evaluation concepts and terminology).

Exhibit 11-2: Disaster Recovery Plan¹³



¹³ Dilbert 2002 (Calendar) by Scott Adams

11.2.1 Step One

Synchronize exercise with plan and training programs.

- Determine which business continuity, disaster recovery or emergency management plan or capability or training competency that you want to exercise and evaluate
- Distribute the plan and ask that samples from the intended audience review it and provide feedback before considering the type of exercise you want to conduct. This determines the depth and scope of the training event.
- Does the plan or parts of the plan require first time or refresher training?
- Drills are very useful as intermediate exercises to validate specific training proficiency standards
- Utilize existing tools to develop the exercise basis

11.2.2 Step Two

Determine scenario in developing exercise objectives. The topic can be anything from a simple, single-task activity or process involving a few people to a complex, multi-tasked activity involving multiple departments and organizations.

- Employee roles and responsibilities during an emergency
- Building evacuation procedures
- Bomb Threats
- The location of fire extinguishers and how to use them
- Organization's crisis communication plan
- Talking to the media in emergency events
- Significant structural damage to a section of the facility
- Violent resident, family member, staff member or other guest/visitor

11.2.3 Step Three

Determine the type of exercise to meet objectives. Build exercises to correspond with the topic's objectives, plans and/or training programs for evaluation.

11.2.4 Step Four

Determine exercise cost.

- Seminars, workshops, and drills are low cost exercise options
- Tabletop exercises with multiple objectives and scenarios and functional exercises may require additional outside support
- Personnel time has a cost. Downtime costs include lost productivity. Focus how much volunteer time you need from the resources involved. Communicating time estimates helps help reduce anxiety about participating in future events.
- Review your tools and intended use when evaluating costs. Review past experiences. How much time was needed to use them? How effective they were and how much care and feeding was required to make them effective?
- Costs may change from past experiences. Establish if you need additional resources to support tools used during the exercise or if budget may be on target based on history.
- Leave everything up for discussion. Documentation styles may be visually effective but if they take too much time to use and it detracts form your activity, look for a simpler way.

11.2.5 Step Five

Set the exercise date

- Identify and organize the planning team
- Reserve a meeting space for the planning team
- Schedule planning meetings
- Identify the type, scope, objectives, and purpose of the exercise
- Assign responsibility to planning team members
- Create supporting handouts as needed
- Take care of administrative tasks, such as creating attendee sign-in sheets, ordering refreshments, etc.
- Notify exercise participants of exercise date
- Invite observers as well external partners as needed

11.2.6 Step Six

Assemble the exercise planning team. The most important factor for a successful exercise is organizing a skilled and experienced exercise planning team. The exercise planning team oversees, and is responsible for, exercise foundation, design, development, conduct and evaluation.

Functions of the planning team include:

- A team leader directs and coordinates all exercise planning activities. He or she assigns exercise activities and responsibilities, provides guidance, establishes timelines, and monitors the development process
- A subject matter expert (SME) provides technical or functional expertise used to develop the scenario and potentially serve as evaluators during the conduct of the exercise
- Someone assumes responsibility for compiling and developing all exercise documentation. This team member collects and reviews policies, plans, and procedures for the exercise
- A team member serves a logistical function, providing or arranging for the supplies, materials, facilities, and services that enable the exercise to function smoothly without outside interference or disruption
- The exercise requires administrative support throughout development. This team member coordinates schedules for the planning team, participating partners and agencies, and registers exercise participants on the day of the exercise
- Follows the Incident Command Structure (ICS) - Planning, Operations, Logistics, and Administration

11.2.7 Step Seven

Identify the exercise staffing roles. Exhibit 11-3 identifies anticipated participation for different exercise types. Depending on the type of exercise, identify the individuals filling these roles well before the day of the exercise. You do not want surprises. Surprises create anxiety and loose participation.

Surprises are not a principle of war. They can be tactical, but never strategic.

Exhibit 11-3: Exercise Type, with Participant Listing

Exercise Type	Actor	Controller	Evaluator	Facilitator	Observer	Player/ Participant	Safety Officer	Scribe/ Recorder	Simulator	Timekeeper
Seminars			X	X	X	X		X		
Workshops			X	X	X	X		X		
Tabletop			X	X	X	X		X		X
Games / Orientations			X	X	X	X		X		
Structured Walk-Through			X	X	X	X		X		
Drill			X	X	X	X		X		
Functional Exercises	X	X	X	X	X	X	X	X	X	
Full-scale Exercises	X	X	X	X	X	X	X	X	X	

Exercise Participants Roles & Responsibilities

- **Actors** – Actors simulate specific roles, such as disaster casualty victims, adding realism to an exercise (often called “walking dead”).
- **Controller** – The controller introduces artificial stimuli at the direction of the facilitator. These employees observe the players during the "play" of the exercise and ensure they stay properly focused on the assigned tasks. For tabletop exercises, use the title of “facilitator” rather than “controller.”
 - Acts as an extension of the facilitator
 - Introduce artificial stimuli at the direction of the facilitator
 - Makes decisions in the event of unanticipated actions or resource requirements
 - Helps eliminate safety and property damage issues by maintaining order as well as tracking and aiding actions of participants
- **Evaluator** - The selection criterion for evaluators largely depends on the experience they have in the functional areas utilized during the exercise. Evaluators have a passive role in the exercise and should only record the actions/decisions of players; they should not interfere with exercise flow. Evaluators often use formal forms to record observations and make notes, which contribute greatly to the exercise After-Action Report. For large and complex operations-based exercises, appoint an experienced Chief Evaluator to lead the evaluation team.
- **Facilitator (Lead Controller)** – During a discussion-based exercise, the facilitator is responsible for ensuring that participant discussions remain focused on the exercise objectives. He or she ensures the proper exploration of all issues that may arise during the exercise.
 - Possesses overall knowledge of the scenario
 - Supervises the exercise, monitors sequence of events, adjusts pace, and controls timeline
 - Introduces action messages
 - Provides exercise oversight
 - Arranges a tabletop exercise, (TTX), conducts, schedules and follows-up on the TTX.
 - Commences and orchestrates all activities related to a tabletop exercise, but does not provide advice or solutions during the exercise
- **Observers** – Observers may request to view all or selected portions of exercise play. Observers may include corporate representatives, sister facility administration, or other invitees. Observers must not participate in exercise play or in exercise evaluation and control functions. Observer comments are a vital part in capturing the entire exercise experience.
 - Strategically positioned to observe and document performance
 - Knowledgeable about the subject matter or function evaluated
 - Evaluate the actions of the participants and, the effectiveness of the Business Continuity Plan
- **Players/Participants** – Players are members of the organization(s) being evaluated; they have an active role in responding to an incident by either discussing (in a discussion-based

exercise) or performing (in an operations-based exercise) their regular roles and responsibilities. These employees respond to the simulated emergency and attempt to solve the simulated problems portrayed in the scenario. Players usually perform the same duties as during a real emergency.

- Assume crisis roles and perform actual or simulated activities commensurate with the type of exercise and scenario used
- **Safety Officer** – During an operations-based drill or functional exercise, he or she looks out for the safety of all exercise participants and must have no other duties. The Safety Officer briefs participants on any safety concerns before the start of the exercise.
- **Scribes/Recorders** – Scribes are responsible for recording information related to the tabletop exercise (TTX).
 - Accurate time lining of recovery activities
 - Accurate documentation of responses during the lessons learned round table exercises.
 - Record tabletop exercise proceedings
 - Issue “roadblocks” as or when required
 - Capture issues as they arise
 - Record corrective actions and responsible group/department
 - Deliver Exercise Communication Forms between team tables
 - Assist in creating the Post - Exercise Report
- **Simulator** – The simulator adds realism to the scenario; acts as victim, adversary, media member and any other extra role. The simulator may portray private citizens, agencies, companies and organizations, as they would normally interact with participants.
- **Timekeeper** – The timekeeper is responsible for keeping track of the time during the administration of a tabletop exercise (TTX). These duties relate to the time estimates shown on the agenda, and to the accurate time lining of recovery activities as recorded by the scribe.

11.2.8 Step Eight

Identify External Exercise Participants. Determine the outside partners or organizations that need to be involved in the exercise. Depending on the objectives and scope of the exercise, here is a list of potential external partners to consider when building an exercise team:

- Law Enforcement Representatives
- Fire and Rescue
- Local Hotel
- Utility Managers, especially the local electricity provider
- Generator Supplier or Manufacturer
- Transportation Provider
- Management Company

The listing of outside partners and organizations above is not mandatory. Examine the context of the plan. All partners that have a part in your plan should have a part in exercise planning even if their particular part will not be included this time. If the purpose of the exercise seminar or workshop is to develop a plan, consider all who will be potentially included when the plan is completed. Be inclusive rather than exclusive.

11.2.9 Step Nine

Hot Wash / Evaluation / After Action Report (AAR)

- **Hot Wash** – Immediately following the exercise, the controller leads a hot wash and allows players to provide immediate feedback. This enables the controller and evaluators to capture information about events while they are still fresh in the players' minds. The hot wash is an opportunity to ascertain the level of satisfaction with the exercise, identify issues or concerns and propose areas for improvement.

Players complete and submit their Participant Feedback Forms during the hot wash. All evaluators take notes during play and hot washes for later compilation with other observations from their functional areas. Information captured from Participant Feedback Forms becomes a feeder to the AAR.

- Review of immediate activities
- Identification of good/best practices
- Identification of areas needing improvement
- Post exercise review process
- **Evaluation/Evaluation Plan** – The evaluation phase for all exercises includes a formal exercise evaluation, an integrated analysis, and an AAR that identifies strengths and areas for improvement observed during the exercise. Areas for improvement identified help to develop the corrective actions tracked throughout the improvement-planning phase.
- **Improvement Planning** – During improvement planning, the corrective actions identified in the evaluation phase are assigned, with due dates, to responsible parties; tracked to implementation; and then validated during subsequent exercises.
- **After Action Report (AAR)** – After execution of an exercise, an evaluation team produces an After Action Report. The AAR defines the specific corrective actions taken to remedy issues observed during exercise evaluation. An AAR assigns all corrective actions to a responsible person or organization, and includes incremental benchmarks and deadlines for completion. The AAR Provides accountability for corrective action implementation

Exhibit 11-3: Exercise Methodology Lifecycle



This page intentionally left blank.

12 Appendix A: Glossary of Terms

Term	Definition
After Action Report (AAR)	“An After Action Report (AAR) is the final product of an exercise. The AAR/IP has two components: an AAR, which captures observations and recommendations based on the exercise objectives as associated with the capabilities and tasks; and an IP, which identifies specific corrective actions, assigns them to responsible parties, and establishes targets for their completion.” (FEMA, About HSEEP, 2008)
Best Practices	Documented strategies or methods used by high performing organizations to achieve successful outcomes for particular services, processes or products. Distinct from ‘good’ or ‘promising’ ideas, best practices deliver consistent, predictable results that can be implemented across organizations to improve performance.
Benchmark	Recognized standards against which to compare or measure performance of a service, process or product. Benchmarking involves continuous comparison to industry leaders or the “best in class,” and adapting best practices to improve results and performance.
Business Continuity	A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.
Business Continuity Management (BCM)	Business Continuity Management (BCM) defined as a “holistic management process that identifies potential risks that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and value creating activities.” (DRJ online glossary)
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe an organization’s recovery steps during and after a significant disruption.
Business Continuity Management (BCM)	An ongoing process supported by senior management and funded to ensure that the necessary steps taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing and maintenance.
Business Impact Analysis (BIA)	A management level financial analysis that identifies the impacts of losing an organization’s resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide reliable data upon which to base decisions on mitigation, recovery and business continuity strategies.
Contingency Plan (CP)	A predefined collection of procedures and documentation designed to assist an organization to respond to any of a set of disasters, disruptions or emergencies. A contingency plan should contain and describe sufficient management thought and preplanning such that any employee can implement specific direction guidance of management in an emergency, whether or not the manager is present.
Continuity	An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event

Term	Definition
Continuity of Operations (COOP)	An effort within individual agencies to ensure they can continue to perform their Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.
Crisis Management	Intervention and coordination by individuals or teams before, during and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.
Crisis Management Team	A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.
Critical Function	Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization
Disaster	An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths; The interval when the organization decides to divert from normal business practices and exercises its disaster recovery plan signified by the moving from primary to remote processing.
Disaster Recovery (DR)	Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.
Emergency	An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability
Evaluation/ Evaluation Plan	The Evaluation Plan helps exercise evaluators understand their roles and responsibilities in exercise data collection and evaluation in order to conduct an effective analysis of the exercise and produce a comprehensive AAR (FEMA, HSEEP Glossary, 2008).
Event	Any occurrence that may lead to a business continuity incident
Exercise	An activity performed for the purpose of training and conditioning team members and personnel in appropriate crisis responses with the goal of achieving maximum performance. Exercises can be used for: testing and validating policies, plans, procedures, training, equipment, and inter-agency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement.
Foundation	A foundation is the premise or set of assumptions used to lay the rules for the planned event. Foundation activities including creating a base support (i.e., establish buy-in from the appropriate entities and/or senior officials), developing an exercise planning timeline with milestones, selecting participants for an exercise planning team, and scheduling planning conferences. Project management skills are essential during the foundation phase of the exercise process.

Term	Definition
Full-Scale Exercise	A full-scale exercise simulates responses required to respond to the broad impact of a disaster event. Full-scale exercises could simulate an emergency event and may involve emergency response functions. It could require full deployment of equipment and personnel. Actors could include fire, law enforcement, emergency management and other agencies, organizations and local businesses as identified in the scenario.
Functional Exercise	A functional exercise is a type of exercise that involves training using the capabilities performed during normal production activity in a controlled environment. These events may include business processes, technology, partners, supply chain activities, etc as part of the service or product produced. This exercise focuses on the coordination of multiple functions or organizations and ideally utilizes an Emergency Operations Center. The Functional Exercise strives for realism, short of actual deployment of equipment and personnel.
Hot Wash	An informal debriefing held immediately following an exercise among exercise players from each functional area. Capturing exercise feedback regarding improvements/issues while fresh in the participants' minds is the primary purpose of a hot wash discussion.
Occupant Emergency Plan (OEP)	A short-term emergency response program that establishes procedures for safeguarding lives and property
Plan	A plan is a proposed or intended method of getting from one set of circumstances to another. One user for a plan is to move from the present situation towards the achievement of one or more objectives or goals.
Program	A group of related initiatives managed in a coordinated way, to obtain a level of control and benefits that would not be possible from the individual management of the initiatives. Programs may include elements of related work outside the scope of the discrete initiatives in the program.
Recovery	The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following an interruption or disaster.
Recovery Point Objective (RPO)	The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization and describes the acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively affecting the organization's mission or business processes.
Risk Assessment (RA)	The Risk Assessment is a process of identifying the internal and external threats and vulnerabilities as risks to an organization. It sets probability of event and facilitates balancing controls necessary to manage the risk using controls. Risk analysis often involves evaluating the cost for controls and level of risk the organization is willing to accept as part of business operations strategy.
Simulation Exercise	A test in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises are performed under conditions as close as practicable to "real world" conditions.

Term	Definition
Tabletop Exercise	A test method (in a stress-free environment) that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.
Testing	Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in plans.
Test, Training, and Exercise (TT&E) Program	Measures to ensure that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity situation
Scope	Predefined areas of operation for which a disaster recovery plan is developed.
Structured Walk-Through Test	Team members walk through the plan to identify and correct weaknesses.

13 Appendix B: External References

- ANSI / NFPA 1600:2007: Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association <http://www.nfpa.org>
- BCI Good Practice Guidelines Section 5 & 6, British Standard 25999 Parts 1 and 2 www.thebci.org
- BS 25777:2008 – Information and Communication Technology Continuity Management <http://www.bsigroup.com>
- BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information <http://www.bsigroup.com>
- Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS, International <http://www.asisonline.org/guidelines/guidelines.htm>
- Department of Homeland Security, Federal Emergency Management Agency; Homeland Security Exercise and Evaluation Program (HSEEP), Policy and Guidance Volumes I-III http://hseep.dhs.gov/pages/1001_HSEEP7.aspx
- Disaster Recovery Institute International (DRII – USA) - Professional Practices <http://www.drii.org/professionalprac/index.php>
- Disaster Recovery Journal (DRJ – USA) - Generally Accepted Business Continuity Practices <http://www.drj.com/GAP/gap.pdf>
- Federal Continuity Directive -1; Federal Executive Branch National Continuity Program and Requirements <http://www.fema.gov/pdf/about/offices/fcd1.pdf>
- FEMA 141: Emergency Management Guide for Business and Industry. FEMA, <http://www.fema.gov/pdf/library/bizindst.pdf>
- Federal Emergency Management Agency (FEMA), IS-139 Exercise Design
- HB 221:2004 Business Continuity Management (Australia) <http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB221-2004.PDF>
- HB 292 /293:2006 Business Continuity Management Handbooks (Australia) <http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB293-2006.pdf>
- NIST 800 Series (USA) <http://csrc.nist.gov/publications/PubsSPs.html>
- Strohl Systems (SunGard), Consultant's Corner: Best Practices for Conducting a Functional Exercise <http://www.mcombs.utexas.edu/dept/irom/bba/risk/rmi/arnold/DOWNLOADS/newletter0701.pdf>

This page intentionally left blank.

14 Appendix C: Exercise Sign Sheet Template

Exercise Sign-in Sheet

[Date]

(PLEASE PRINT CLEARLY)

NAME	AGENCY/DEPARTMENT	PHONE/FAX	E-MAIL

This page intentionally left blank.

15 Appendix D: Discussion Based Exercise Scenario Template

<SYSTEM NAME> Discussion Based Exercise Scenario Brief

<DATE>

Moderated by <FACILITATOR NAME>

Introduction

In an effort to validate the <DIVISION> <SYSTEM NAME> Contingency Plan, <DIVISION> will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the <SYSTEM NAME> Contingency Plan. This discussion-based exercise will be a two (2) hour event that will begin at <START TIME> and will last until <END TIME>.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at <DIVISION> following an event causing the outage of mission critical systems that are housed in the <PRIMARY LOCATON>, located in <PHYSICAL LOCATION>. This exercise is designed to improve the readiness of the <ORGANIZATION> and help validate existing <SYSTEM NAME> Contingency Plan procedures.

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 <PRIMARY LOCATION>. A facilitator will help guide discussion by asking questions designed to address the exercise’s objectives.

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 <SYSTEM NAME> Contingency Plan

Identify areas of the contingency plan that need revision.

Agenda

Date: <DATE>

Location: <LOCATION>

09:00 – 09:15 Welcoming Remarks and Introductions

09:15 – 09:30 Exercise Briefing

09:30 – 10:30 Scenario Discussion

10:30 – 11:00 Debrief / Hot wash

Scenario

At <START TIME> on <DATE>, an <SCENARIO> in the <PRIMARY LOCATION> caused extensive damage and the termination of operations in the data center. The <SYSTEM NAME> Contingency Plan was fully activated in response to this incident, and operations will be conducted at the <ALTERNATE LOCATION> for the foreseeable future. <DIVISION> employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the <PRIMARY LOCATION>, Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the <ALTERNATE LOCATION>.

Assumptions

For the purpose of this exercise, we will assume that the above mentioned scenario did not have an adverse effect on any other system located in the <PRIMARY LOCATION> data center. Only the servers and equipment directly related to <SYSTEM NAME> were affected.

Participant Questions

Who has authority to activate the <SYSTEM NAME> Contingency Plan?

How would you be notified of plan activation and by whom?

Are the IT recovery procedures fully documented?

Can recovery procedures be completed within the timeframe dictated in the <SYSTEM NAME> Contingency Plan?

Debrief / Hot Wash 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?

This page intentionally left blank.

16 Appendix E: Discussion Based Exercise Results Template

IT Security Contingency Plan (ITCP)
DISCUSSION-BASED EXERCISE RESULTS
<SYSTEM NAME>
Prepared by:
<FACILITATOR NAME>
Date: <DATE>

Introduction

The follow results represent the discussion-based exercise that was performed on <DATE>. The table below captures the simulated activities performed, the responsible party(s), expected results and actual results. Refer to the after action report for a complete description of what occurred, lessons learned and activities for improvement.

This discussion-based exercise results cover the following systems only: <SYSTEM NAME>

DISCUSSION-BASED EXERCISE TEST RESULTS			
Scenario: <SCENARIO>			
Notification/Activation Phase			
Simulated Activities	Responsible Party	Expected Results	Actual Results
Recovery Phase			
Simulated Activities	Responsible Party	Expected Results	Actual Results
Return to Normal Operations Phase			
Simulated Activities	Responsible Party	Expected Results	Actual Results

This page intentionally left blank.

17 Appendix F: Participant Feedback Form Template

PARTICIPANT FEEDBACK FORM

Exercise Name: [Exercise Name]

Exercise Date: [Date]

Participant Name: _____ Title: _____

Agency: _____ Role: ____ Player ____ Observer
____ Facilitator ____ Evaluator

Part I – Recommendations and Action Steps

7. Based on discussions today and the tasks identified, list the top three issues and/or areas that need improvement.

8. Identify the action steps that taken to address the issues identified above. For each action step, indicate if it is a high, medium or low priority.

9. Describe the action steps that should be taken in your area of responsibility. Who should be assigned responsibility for each action item?

10. List the policies, plans and procedures that should be reviewed, revised or developed. Indicate the priority level for each.

Part II – Exercise Design and Conduct

11. What is your assessment of the exercise design and conduct?

Please rate, on a scale of 1 to 5, your overall assessment of the exercise relative to the statements provided below, with one indicating strong disagreement with the statement and five indicating strong agreement.

	Assessment Factor	Rating of Satisfaction with Exercise				
		Strongly Disagree				Strongly Agree
a.	The exercise was well structured and organized.	1	2	3	4	5
b.	The exercise scenario was plausible and realistic.	1	2	3	4	5
c.	The multimedia presentation helped the participants understand and become engaged in the scenario.	1	2	3	4	5
d.	The facilitator(s) was knowledgeable about the material, kept the exercise on target and was sensitive to group dynamics.	1	2	3	4	5
e.	The Situation Manual used during the exercise was a valuable tool throughout the exercise.	1	2	3	4	5
f.	Participation in the exercise was appropriate for someone in my position.	1	2	3	4	5
g.	The participants included the right people in terms of level and mix of disciplines.	1	2	3	4	5

12. What changes would you make to improve this exercise?

Please provide any recommendations on how this exercise or future exercises could be improved or enhanced.

This page intentionally left blank.

18 Appendix G: Evacuation Drill Checklist Template

Evacuation Drill Checklist				
Facility Name:			Facility Location:	
Prepared By:		Date Prepared:		Time:
Title & Contact Information:				
Part One: Drill				
Date of evacuation drill:		Time of evacuation drill:		
Building or floors involved in drill:				
Scope of evacuation drill:	Full building evacuation Floors or areas evacuated or relocated			
Time evacuation signal sounded:				
Time floor or area evacuated:				
Elapsed time:				
Part Two: Evacuation Team Performances				
Did floor monitor(s) take charge and direct persons to exits?	Yes	No	Not Observed	
Comments:				
Did deputy floor warden connect with floor warden and divide tasks?	Yes	No	Not Observed	
Comments:				
Did stairwell monitors report to stairwells?	Yes	No	Not Observed	
Comments:				
Did elevator monitor report to the elevators?	Yes	No	Not Observed	
Comments:				
Did searchers check restrooms, storage rooms, and other areas?	Yes	No	Not Observed	
Comments:				

Did elevator monitor report to the elevators?	Yes	No	Not Observed
Comments:			
Did searchers check restrooms, storage rooms, and other areas?	Yes	No	Not Observed
Comments:			
Was the evacuation team wearing identification hats, vests or insignia?	Yes	No	Not Observed
Comments:			
Did floor monitor check stairwells before allowing persons to enter?	Yes	No	Not Observed
Comments:			
Was the control of traffic into stairwells orderly; were proper instructions given?	Yes	No	Not Observed
Comments:			
Were persons with disabilities partnered with a “buddy” and directed to areas of refuge or rescue assistance?	Yes	No	Not Observed

Part Three: Building and Systems

Was the evacuation signal audible throughout the floor?	Yes	No	Not Observed
Comments:			
Were instructions clear and easily understood by occupants on the floor?	Yes	No	Not Observed
Comments:			
Were any exits, access corridors or stairwells obstructed; were any exits signs obstructed or not illuminated?	Yes	No	Not Observed
Comments:			
Were any doors blocked open?	Yes	No	Not Observed
Comments:			
Did building systems perform as intended (HVAC shutdown, stairwell doors unlock, stairwell pressurization fans start)?	Yes	No	Not Observed
Comments:			

Part Four: Occupant Actions	
Did building occupants respond immediately to the evacuation signal?	Yes No Not Observed
Comments:	
Did building occupants follow instructions of the evacuation team?	Yes No Not Observed
Comments:	
Were occupants orderly and reasonably quiet during the evacuation drill?	Yes No Not Observed
Comments:	
Was any occupant unfamiliar with the location of the exits?	Yes No Not Observed
Comments:	
Did all occupants on the floor participate in the drill?	Yes No Not Observed
Comments:	
Did occupants evacuate to the proper floor or assembly area as instructed?	Yes No Not Observed
Comments:	
Recommended Actions:	
Comments:	

This page intentionally left blank.

19 Appendix H: After Action Report Template (HSEEP)

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)**

[Full Exercise Name]

[Exercise Name Continued]

[Note: For After Action Report/Improvement Plan (AAR/IP) Example:

Text found in this document that is highlighted and bracketed is included to provide instruction or to indicate a location to input text.

All text that is not highlighted is to be included in the final version of the AAR/IP.]

[Full Exercise Name]

[Exercise Dates]

AFTER ACTION REPORT/IMPROVEMENT PLAN

[Publication Date]

[On the cover page, insert additional graphics such as logos, pictures and background colors as desired. The word “Draft” should be included before the phrase “After Action Report/Improvement Plan” on the cover page and in the header/footer of all versions except the final AAR/IP.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]****[Exercise Name Continued]****Handling Instructions**

13. The title of this document is [complete and formal title of document].
14. The information gathered in this AAR/IP is classified as [For Official Use Only (FOUO)] and should be handled as sensitive information not to be disclosed. This document should be safeguarded, handled, transmitted and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from [agency] is prohibited.
15. At a minimum, the attached materials will be disseminated only on a need-to-know basis and when unattended, will be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.
16. Points of Contact: [List all points of contact.]

[Federal POC:]

Name

Title

Agency

Street Address

City, State ZIP

xxx-xxx-xxxx (office)

xxx-xxx-xxxx (cell)

e-mail

[Exercise Director:]

Name

Title

Agency

Street Address

City, State ZIP

xxx-xxx-xxxx (office)

xxx-xxx-xxxx (cell)

e-mail

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)**

[Full Exercise Name]

[Exercise Name Continued]

Contents

Administrative Handling Instructions	1
Contents	3
Executive Summary	5
Section 1: Exercise Overview	[p]
Exercise Details.....	[p]
Exercise Planning Team Leadership.....	[p]
Participating Organizations	[p]
Section 2: Exercise Design Summary	[p]
Exercise Purpose and Design	[p]
Capabilities and Activities Identified for Demonstration	[p]
Scenario Summary	[p]
Planned Simulations.....	[p]
Section 3: Analysis of Capabilities	[p]
[Capability 1]	[p]
[Capability 2]	[p]
[Capability 3]	[p]
Section 4: Conclusion	[p]
Appendix A: Improvement Plan.....	[p]
Appendix B: Lessons Learned [Optional]	[p]
Appendix C: Participant Feedback Summary [Optional]	[p]
Appendix D: Exercise Events Summary Table [Optional]	[p]
Appendix E: Performance Ratings [Optional].....	[p]
Appendix F: Acronyms.....	[p]

[If an AAR contains graphics, figures or tables, they should be numbered and listed in the Contents section (e.g. Figure 1, Table 1, etc.).

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]****[Exercise Name Continued]****Executive Summary**

[When writing the Executive Summary, keep in mind that this section may be the only part of the AAR/IP that some people will read. Introduce this section by stating the full name of the exercise and providing a brief overview of the exercise. This brief overview should discuss why the exercise was conducted; the exercise objectives; and what Target Capabilities List (TCL) capabilities, activities, and scenario(s) were used to achieve those objectives. All of these areas will be discussed in more detail in the subsequent chapters of the AAR/IP. In addition, the Executive Summary may be used to summarize any high-level observations that cut across multiple capabilities.]

The [agency or jurisdiction] [scenario type] [exercise type] exercise [exercise name] was developed to test [agency or jurisdiction]'s [Capability 1], [Capability 2], and [Capability 3] capabilities. The exercise planning team was composed of numerous and diverse agencies, including [list of agencies participating in planning team]. The exercise planning team discussed [include a brief overview of the major issues encountered, discussed, and resolved during the exercise planning process. Topics to address in this section could include the length of the planning process, the reasoning behind the planning team's choice of objectives to exercise, etc.]

Based on the exercise planning team's deliberations, the following objectives were developed for [exercise name]:

- Objective 1: [Insert 1 sentence description of the exercise objective]
- Objective 2: [Insert 1 sentence description of the exercise objective]
- Objective 3: [Insert 1 sentence description of the exercise objective]

The purpose of this report is to analyze exercise results, identify strengths to be maintained and built upon, identify potential areas for further improvement, and support development of corrective actions.

[In general, the major strengths and primary areas for improvement should be limited to three each to ensure the Executive Summary is high-level and concise.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]
[Exercise Name Continued]****Major Strengths**

The major strengths identified during this exercise are as follows:

- [Use complete sentences to describe each major strength.]
- [Additional major strength]
- [Additional major strength]

Primary Areas for Improvement

Throughout the exercise, several opportunities for improvement in [jurisdiction/organization name]'s ability to respond to the incident were identified. The primary areas for improvement, including recommendations, are as follows:

[Use complete sentences to state each primary area for improvement and its associated key recommendation(s).]

[Additional key recommendation]

[Additional key recommendation]

[End this section by describing the overall exercise as successful or unsuccessful, and briefly state the areas in which subsequent exercises conducted by these jurisdictions and/or organizations should focus.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]****[Exercise Name Continued]****Section 1: Exercise Overview**

[Information in the Exercise Overview should be “structured data”—written as a list rather than in paragraph form—in order to facilitate preparation of other parts of the AAR/IP, maintain consistency within AAR/IPs, and facilitate the analysis of AAR/IPs for program reporting.]

Exercise Details**Exercise Name**

[Insert formal name of exercise, which should match the name in the header.]

Type of Exercise

[Insert the type of exercise as described in Homeland Security Exercise Evaluation Program Volume I (e.g. seminar, workshop, drill, game, tabletop, functional exercise, or full-scale exercise.)]

Exercise Start Date

[Insert the month, day, and year that the exercise began.]

Exercise End Date

[Insert the month, day, and year that the exercise ended.]

Duration

[Insert the total length of the exercise, in day or hours, as appropriate.]

Location

[Insert all applicable information regarding the specific location of the exercise; including any city, State, Federal region, international country, or military installation.]

Sponsor

[Insert the name of the Federal agency or agencies that sponsored the exercise, as well as any co-sponsors if applicable. Also, list any applicable points of contacts.]

Program

[Insert the name of the program (e.g. Fiscal Year 2007 State Homeland Security Grant Program) from which exercise funding originated.]

[Protective Marking]**Homeland Security Exercise and Evaluation Program (HSEEP)****After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]
[Exercise Name Continued]****Mission**

[Insert the appropriate mission areas of the exercise (e.g. Prevent, Protect, Response, and/or Recovery).]

Capabilities

[Insert a list of the target capabilities addressed within the exercise.]

Scenario Type

[Name the exercise scenario type (e.g. chemical release).]

Exercise Planning Team

[The name of each member of the planning team leadership should be listed along with his or her role in the exercise, organizational affiliation, job title, mailing address, phone number and e-mail address.]

Participating Organizations

[Insert a list of the individual participating organizations or agencies, including Federal, State, Tribal, non-governmental organizations (NGOs), local and international agencies and contract support companies as applicable.]

Number of Participants

[Insert a list of the total number of each of the following exercise participants, as applicable:

- Players
- Controllers
- Evaluators
- Facilitators
- Observers
- Victim Role Players]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]
[Exercise Name Continued]****Section 2: Exercise Design Summary**

[The Exercise Design Summary is intended to provide a summary of the exercise design process.]

Exercise Purpose and Design

[This section should be a brief (one-to-two paragraph) summation of why the exercise was conducted and what the exercise participants hoped to learn. It should also include a brief history of how the exercise was organized, designed, funded, etc.]

Exercise Objectives, Capabilities and Activities

[The purpose of this section is to list exercise objectives and align them with associated capabilities from the Target Capabilities List (TCL). For each TCL capability, there is an Exercise Evaluation Guide (EEG), which lists specific activities, which must be performed to demonstrate a capability. In addition to TCL capabilities, the EEG activities relevant to each objective should also be included in this section. Begin this section with the following text.]

Capabilities-based planning allows for exercise planning teams to develop exercise objectives and observe exercise outcomes through a framework of specific action items that were derived from the Target Capabilities List (TCL). The capabilities listed below form the foundation for the organization of all objectives and observations in this exercise. Additionally, each capability is linked to several corresponding activities and tasks to provide additional detail.

Based upon the identified exercise objectives below, the exercise planning team has decided to demonstrate the following capabilities during this exercise:

Objective 1: [Insert a one sentence description of each objective].

[Capability Title]: [Activity 1]; [Activity 2]; and [Activity 3].

[Capability Title]: [Activity 1]; [Activity 2]; and [Activity 3].

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]
[Exercise Name Continued]****Scenario Summary**

[For an operations-based exercise, this section should summarize the scenario or situation initially presented to players, subsequent key events introduced into play, and the time in which these events occurred. For a discussion-based exercise, this section should outline the scenario used and/or modules presented to participants.]

Section 3: Analysis of Capabilities

This section of the report reviews the performance of the exercised capabilities, activities and tasks. In this section, observations are organized by capability and associated activities. The capabilities linked to the exercise objectives of [full exercise name] are listed below, followed by corresponding activities. Each activity is followed by related observations, which include references, analysis and recommendations.

[The format for Chapter 3, as described above, represents the preferred order for analysis of exercise observations. However, observations that are crosscutting and do not apply to one specific activity within the capability should be listed first, directly under the capability summary. Below the crosscutting observations, you may then present the complete list of activities, which apply to the observation.]

Capability 1: [Capability Name]

Capability Summary: [Include a detailed overview of the capability, drawn from the TCL capability description, and a description of how the capability was performed during an operations-based exercise or addressed during a discussion-based exercise. The exact length of this summary will depend on the scope of the exercise.]

Activity 1.1: [Using the EEGs, identify the activity to which the observation(s) below pertain.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]
[Exercise Name Continued]****Observation 1.1:**

[Begin this section with a heading indicating whether the observation is a “Strength” or an “Area for Improvement.” A strength is an observed action, behavior, procedure, and/or practice that is worthy of recognition and special notice. Areas for improvement are those areas in which the evaluator observed that a necessary task was not performed or that a task was performed with notable problems. Following this heading, insert a short, complete sentence that describes the general observation.]

References:

[List relevant plans, policies, procedures, laws, and/or regulations, or sections of these plans, policies, procedures, laws and/or regulations. If no references apply to the observation, it is acceptable to simply list “N/A” or “Not Applicable.”]

[Name of the task and the applicable plans, policies, procedures, laws, and/or regulations and 1-2 sentences describing their relation to the task]

[Name of the task and the applicable plans, policies, procedures, laws, and/or regulations and 1-2 sentences describing their relation to the task]

[Name of the task and the applicable plans, policies, procedures, laws, and/or regulations and 1-2 sentences describing their relation to the task]

Analysis:

[The analysis section should be the most detailed section of Chapter 3. Include a description of the behavior or actions at the core of the observation, as well as a brief description of what happened and the consequence(s) (positive or negative) of the action or behavior. If an action was performed successfully, include any relevant innovative approaches utilized by the exercise participants. If an action was not performed adequately, the root-causes contributing to the shortcoming must be identified.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)
After Action Report/Improvement Plan **[Full Exercise Name]**
(AAR/IP) **[Exercise Name Continued]**

Recommendations:

[Insert recommendations to address identified areas for improvement, based on the judgment and experience of the evaluation team. If the observation was identified as strength, without corresponding recommendations, insert “None.”]

17. [Complete description of recommendation]
18. [Complete description of recommendation]
19. [Complete description of recommendation]

[Continue to add additional observations, references, analyses and recommendations for each capability as necessary. Maintain numbering convention to allow for easy reference.]

Section 4: Conclusion

[This section is a conclusion for the entire document. It provides an overall summary to the report. It should include the demonstrated capabilities, lessons learned, major recommendations and a summary of what steps should be taken to ensure that the concluding results will help to further refine plans, policies, procedures and training for this type of incident.]

Subheadings are not necessary and the level of detail in this section does not need to be as comprehensive as that in the Executive Summary.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

After Action Report/Improvement Plan (AAR/IP)

[Full Exercise Name]
[Exercise Name Continued]

Appendix A: Improvement Plan

This IP has been developed specifically for [identify the State, county, jurisdiction, etc., as applicable] as a result of [full exercise name] conducted on [date of exercise]. These recommendations draw on both the After Action Report and the After Action Conference. [The IP should include the key recommendations and corrective actions identified in Chapter 3: Analysis of Capabilities, the After Action Conference, and the EEGs. The IP has been formatted to align with the Corrective Action Program System.]

Capability	Observation Title	Recommendation	Corrective Action Description	Capability Element	Primary Responsible Agency	Agency POC	Start Date	Completion Date
[Capability 1: Capability Name]	1. Observation 1	1.1 Insert Recommendation 1	1.1.1 Insert Corrective Action 1	Planning	State X EMA	EMA Director	Dec 1, 2006	Sep 1, 2007
			1.1.2 Insert Corrective Action 2	Planning	State X EMS System	EMS System Director	Dec 1, 2006	Feb 1, 2007
		1.2 Insert Recommendation 2	1.2.1 Insert Corrective Action 1	Training	State X EMA	EMA Director	Dec 1, 2006	Jan 1, 2007
			1.2.2 Insert Corrective Action 2	Systems/ Equipment	State X EMA	EMA Director	Dec 1, 2006	Mar 15, 2007
	2. Observation 2	2.1 Insert Recommendation 1	2.1.1 Insert Corrective Action 1	Planning	State X EMS System	EMS System Director	Dec 1, 2006	Jan 15, 2007
			2.1.2 Insert Corrective Action 2	Systems/ Equipment	State X EMA	EMA Director	Dec 1, 2006	Jan 1, 2007

Table A.1 Improvement Plan Matrix

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

**After Action Report/Improvement Plan
(AAR/IP)****[Full Exercise Name]****[Exercise Name Continued]****Appendix B: Lessons Learned**

While the After Action Report/Improvement Plan includes recommendations, which support development of specific post-exercise corrective actions, exercises may also reveal lessons learned which could be shared with the broader homeland security audience. Federal Emergency Management Agency (FEMA) maintains the Lessons Learned Information Sharing (LLIS.gov) system as a means of sharing post-exercise lessons learned with the emergency response community. This appendix provides jurisdictions and organizations with an opportunity to nominate lessons learned from exercises for sharing on LLIS.gov.

For reference, the following are the categories and definitions used in LLIS.gov:

- **Lesson Learned:** Knowledge and experience, positive or negative, derived from actual incidents, such as the 9/11 attacks and Hurricane Katrina, as well as those derived from observations and historical study of operations, training, and exercises.
- **Best Practices:** Exemplary, peer-validated techniques, procedures, good ideas, or solutions that work and are solidly grounded in actual operations, training, and exercise experience.
- **Good Stories:** Exemplary, but non-peer-validated, initiatives (implemented by various jurisdictions) that have shown success in their specific environments and that may provide useful information to other communities and organizations.
- **Practice Note:** A brief description of innovative practices, procedures, methods, programs, or tactics that an organization uses to adapt to changing conditions or to overcome an obstacle or challenge.

Exercise Lessons Learned

[Insert an account of any observations nominated for inclusion in the DHS LLIS.gov system. If there are not any nominations, a simple statement to that effect should be included here.]

[Protective Marking]

Homeland Security Exercise and Evaluation Program (HSEEP)

After Action Report/Improvement Plan (AAR/IP) [Full Exercise Name]
[Exercise Name Continued]

Appendix C: Exercise Events Summary Table

[In formulating its analysis, the evaluation team may assemble a timeline of key exercise events. While it is not necessary to include this timeline in the main body of the AAR/IP, the evaluation team may find value in including it as an appendix. If so, this section should summarize what actually happened during the exercise in a timeline table format. Focus of this section is on what inputs were actually presented to the players and what actions the players took during the exercise. Successful development of this section is aided by the design, development, and planning actions of the exercise design team. Prior to the exercise, the exercise design team should have developed a timeline of anticipated key events.]

An example of the format for the Exercise Events Summary Table is presented below.]

Table C1: Exercise Events Summary

Date	Time	Scenario Event, Simulated Player Inject, Player Action	Event/Action
02/20/06	0900	Scenario Event	Explosion and injuries reported at subway station 13
02/20/06	0902	Player Action	Subway services stopped in accordance with protocols; notifications started
02/20/06	0915	Player Action	Evacuation ordered for planning zone 2A
02/20/06	0940	Simulated Player Inject	Traffic at a standstill on major egress route 1 reported to players (Response generated issue because personnel to staff traffic control points were not deployed)

This page intentionally left blank.