**Name of Organization**

**Incident Response Tabletop Exercise Examples**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Number** | **Revision Date** | **Summary of Changes Made** | **Changed By** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization), Incident Response Tabletop Exercise Procedures document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

Table of Contents

[Introduction and Purpose 5](#_Toc87021180)

[Objectives 5](#_Toc87021181)

[Formats 5](#_Toc87021182)

[General Recommendations 6](#_Toc87021183)

[Scenarios: 15-minutes Table Top Exercises 8](#_Toc87021184)

[Full Table Top Exercise – Example 1 13](#_Toc87021185)

[Module 1: Communications and Decision-Making 16](#_Toc87021186)

[Module 2: Resources, Logistics and Communications 18](#_Toc87021187)

[Appendix B: Participant Observer Evaluation 20](#_Toc87021188)

# Introduction and Purpose

Tabletop exercises are used for training and practicing execution of Cyber Security Incident Response at sites containing one or more Low Impact incidents. The exercise is not intended to fulfill all requirements of National Institute of Standards and Technology (NIST), National Incident Management System (NIMS), and other governance regulations for (Name of Organization), or test with High-Impact or Medium-Impact incidents.

The purpose of Incident Response Tabletop Exercise Procedures is to test and enforce processes that will be followed during an emergency event or the execution of the (Name of Organization) Incident Response Plan (“the Plan”). Furthermore, Tabletop Exercises are designed to assist the (Name of Organization) Incident Commander, Cybersecurity Incident Response Team (CIRT), Incident Handling Team (IHT), Human Resources function, and Business Continuity Members concerning all possible incidents.

This document is designed to guide/assist the organization and key personnel such as the Incident Commander, CIRT Team Internal Communications, Human Resources, and Business Continuity representatives in the event of an emergency or crisis situation.

# Objectives

* Exercise the organization’s Incident Response Plan
  + Must trigger NIST definition of a Cyber Security Incident
* Evaluate compliance of the organization’s Incident Response Plan with NIST and NIMS
  + Must have identification, classification, and response for the Cyber Security Incident
  + Must determine if the Cyber Security Incident is a Reportable Cyber Security Incident

# Formats

Tabletop Exercise

* Tabletop exercises involve a collaboration of all participants to work through the cyber security incident responses.
* Tabletop exercises are akin to playing a game with all cards face-up on the table. Each participant is aware of all information available.
* Tabletop exercises are used to validate the overall process and train each participant in their role while exposing them to other roles.

Expedited Paper Drill

* Expedited paper drills attempt to simulate a security event response with high fidelity (reproduction of the event that is faithful to the original) in a compressed timeframe.
* Participants only have access to a certain level of information which is updated with ‘injections’ of extra information as the exercise proceeds, and through interaction with other participants
* This kind of exercise can highlight problems with communication between teams, problems with the process, and misunderstandings of individuals. This kind of exercise can also “get stuck” and may require planners to adapt if participants respond unexpectedly.

Format Recommendation

* From a process perspective, organizations should start with an initial Tabletop Exercise that can be used to validate incident response Plan maturity. Once one or more exercises or actual executions have exhibited repeatable, robust responses to events, an Expedited Paper Drill should be considered to “stress test” groups and individuals.

# General Recommendations

Exercise the (Name of Organization) Incident Response Plan

* The chosen incident should trigger NIST definition of a Cyber Security Incident and fall into Priority 1-3

Evaluate compliance of the (Name of Organization) Incident Response Plan with NIST and NIMS,

* Must have identification, classification, and response for the Cyber Security Incident
* Must determine if the Cyber Security Incident is a Reportable Cyber Security Incident

Conduct Tabletop Exercise

* Involve a collaboration of all participants
* Must work though each step of the incident responses
* Validate the individual and overall process, end-to-end
* Train each participant in their role while exposing them to other roles

Expedited Paper Drills

* Simulate a security event response with high fidelity in a compressed timeframe
* Participants only have access to a certain level of information which is updated with ‘injections’ of extra information as the exercise proceeds
* The information is shared through interactions with the other participants
* Identify problems with communication between teams
* Identify problems with processes
* Identify misunderstanding between individuals

Scenario Tabletop Exercise

* Conduct an exercise for each type of incident (see scenarios below)
* Brief individuals, but do not provide all details
* Provide guidance throughout the evolution of the training scenario
* A User’s role is to report any suspicious events or potential incidents
* Emphasize individual’s responsibilities during training

CIRT Teams

* Must participate in the exercise
* Should relay suspicious events
* Serve as Users during exercise
* Should discover physical signs related to Cyber Security Incidents
* Should always be incorporated into a response for example:
  + When physical presence is required
  + Observing status lights
  + Disconnecting cables
  + Evaluating security perimeter integrity

(Name of Organization) Incident Commander

* Should plan the exercise
* Provide an employee to participate in each exercise as a System Administrator

Scheduler (Incident Commander)

* Should allow execution and review to be performed in one hour
* Should allow execution and review of Paper Drill to be performed in two hours
* Should schedule at the minimum twelve (12) exercises annually

Participation

* CIRT Team Members
* Other required Staff Members including Incident Handling Team
* Other Department Representatives

Recommendations

* Ensure exercises do not interfere with normal work-related duties
* Ensure all participating personnel get a chance to contribute
* Keep training realistic
* Keep agenda introduction between 5 – 10 minutes
* Keep agenda scenarios between 15 – 30 minutes
* Conduct After Action (AA) and Lessons Learned
* Keep AA between 1 - 20 minutes
* Update Procedures
* Update GAP Analysis
* Keep Paper Drill between 1 – 2 hours

# Scenarios: 15-minutes Table Top Exercises

Training is a critical step in being prepared to respond to real cybersecurity incidents. A quick and easy way to help prepare your team is to hold short 15-minute table top exercises every month. Here are a few of the important questions you may want to ask while holding a tabletop exercise:

* Do you have a Cybersecurity Incident Response Plan?
* Do you have compliance requirements you must adhere to?
* Who should be notified internally in your organization in the event of an incident? External to your organization?
* Do you have a backup point-of-contact for key roles in your organization? (For example, who do you contact if the Incident Commander who handles cybersecurity issues is sick or unavailable?)
* What are the resources available to your team?
* Who do you contact to get more resources? (For example: consultation, equipment, additional cybersecurity professionals or any other third parties.)

Here are some tabletop exercise examples to use:

Example 1:

An employee casually remarks about how generous it is of state officials to provide the handful of USB drives on the conference room table, embossed with the State logo. After making some inquiries you find there is no state program to provide USB drives to employees. Further investigation subsequently found an unspecified password-stealing keylogger. The spyware was designed to upload stolen usernames and passwords to a server under the control of hackers.

Example 2:

Your agency has received various complaints about slow Internet access and that your

web site is inaccessible. After further investigation, it is determined that your agency is a victim of a DNS amplification attack which is currently overwhelming your DNS server and network bandwidth. An overwhelming large number of Internet spoofed IP addresses are involved in the attack.

Example 3:

Have one or two people from your agency visit the following two Chinese websites. These sites

are both recommended by our federal partners as safe for browsing.

www.ustc.edu.cn (University of Science and Technology of China)

http://en.ustc.edu.cn (English site of the University)

Have the team identify which logs would be needed to trace this activity through the network

from end (desktop) to end. Wait one to two weeks, and request these logs identifying this traffic from the appropriate administrative operations sources.

Example 4:

The news is reporting that a major chemical plant, located 2 miles away, has had a significant

toxic chemical leak. There is a chemical “cloud” and your office building is in the path of the

plume. Additionally, the news has reported that a number of people at the factory have died. Authorities have directed everyone to remain where they are and not go outside. Issues for discussion:

1. Can you shut down the HVAC or air intake system?

2. Who is responsible for shutting the system down?

3. How many people would leave the building in spite of the direction to stay in place?

4. How will your operation continue with so many people leaving?

You are now into the next business day and the authorities have signaled the all clear. The

chemical accident was not caused by terrorists. Those who sheltered in place are now leaving to go home to get some sleep, food and shower.

How will you sustain your operations with so many people out of the office?

Example 5:

An epidemic starts killing people in Australia. The medical community fears that the disease will spread to other continents. Anyone who has been in Australia in the past three weeks could be a carrier. As a precautionary measure, employees who have traveled to Australia within the past three weeks have been asked not to return to work until they see a doctor. Additionally, security is screening every visitor to see if they have been to Australia in the past three weeks.

Example 6:

A few people in the region are diagnosed with the disease and absentee rates at local schools rises. Employees start calling in sick, but it’s not clear if they are ill or afraid to go out in public. Enough people are absent that the organization struggles to maintain the IT infrastructure (applications, networks, and computers).

Example 7:

Your agency has received a phone call indicating that you will experience a Telephony Denial of

Service (TDoS) attack beginning in two days unless you pay $30,000 to a specified foreign bank

with details of how to transfer the funds. The payment is to be received by 12pm local time or the attack will proceed as planned.

Example 8:

Your organization’s social media website is compromised. Through public news outlets, an international terrorist group calling themselves the “Rebellion Cyber Forces” has displayed outrage against American politics. They have publicly claimed the successful cyber-attacks on various government organizations. You learn that your organization’s official social media accounts have been compromised and someone is sending out notifications through your social media website to your public claiming that your organization has been compromised by the rebellion cyber forces.

Example 9:

You receive news that one of your employees has accidently disclosed sensitive personally identifiable information (PII) records for over 200 clients and personnel. This occurred when they accidentally emailed a document that had not been properly scrubbed to a contractor. The employee had been recently trained on the handling of PII by your privacy and/or security staff.

Example 10:

One of your organization’s internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive. You have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data in the cloud provider’s infrastructure may have been compromised.

Example 11:

Numerous sensitive internal documents are found on the Internet. Thorough network checks review no evidence of a compromise, but it appears that the multi-function printer/copier is connected to an external facing IP. All documents found on the Internet are known to have been printed or copied on this machine. The machine was not originally connected to the Internet. It is now connected to the Internet through a Cat5 cable

Example 12:

An employee calls to ask for the password for the Wi-Fi network, indicating they would like to use it on their personal cell phone so they can check Facebook on their lunch break. You don’t have a Wi-Fi network. A scan of the building indicates there are 4 Wi-Fi networks, clearly originating from within government space and broadcasting a variety of names that suggest people are using them for work purposes. How do you respond?

Injection: In the course of follow-up to this report it is found that all 4 devices are plugged into your hard-wired network. Two have logging enabled and show that they are being used by employees for official work purposes.

Example 13:

Malware containing a backdoor is discovered on the surveillance cameras used in sensitive locations, including the conference room used by senior executives. It was determined that the cameras were active during several meetings, including one with team managers during contract negotiations.

Example 14:

A routine financial audit reveals that several people receiving paychecks are not, and have never been, on payroll. A system review indicates they were added to the payroll approximately one month prior, at the same time, via a computer in the payroll department. How do you proceed?

Inject: You confirm the computer in the payroll department was used to make the additions. Approximately two weeks prior to the addition of the new personnel, there was a physical break-in to the payroll department in which several laptops without sensitive data were taken.

OPTIONAL injection: Further review indicates that all employees are paying a new “fee” of $20 each paycheck and that money is being siphoned to an offshore bank account.

Example 15:

A severe vulnerability has been identified in a common open-source application that is used to securely transmit information. This common application provides communication security for application such as web email, instant messaging, and some virtual private networks.

Example 16:

The browser deployed on all machines in your organization has a significant zero-day vulnerability which is actively being exploited. You have already identified 10 machines that are compromised as a result of this exploit and the help desk call volume continues to increase abnormally due to this problem. There is currently no vendor patch or vendor workaround. A patch is anticipated to be issued in one week.

Example 17:

You have been notified that a device, which appears to control an aspect of building management (such as a water valve or HVAC), is found to be accessible from the Internet. This device was discovered by a trusted third party who provided you with device’s live IP address and claims that the device does not require any authentication to access.

Example 18:

An executive from your organization has been requested to speak at an international symposium hosted in the beautiful country of Fictionia. You are aware of the customs policy regarding loss of physical control and out of site “inspection” of computers, smart phones, and other technologies conducted by the country of “Fictionia” in addition to previous incidents of espionage emanating from the government of Fictionia. Regardless, the executive is adamant about attending and is requesting to bring a work laptop.

Example 19:

Cyber security has become a big topic of interest for the leadership of your organization. They

have vocalized the intention of not only expanding current awareness efforts targeting

employees, but also the community during October Cyber Security Awareness Month. How do

you proceed in developing a holistic, yet cost effective security awareness program?

Example 20:

You have been notified via a trusted third party that one of your websites has been compromised and is hosting a propaganda video by a hacktivist group which supports violent political activity.

In addition, the hacktivist group is also publicly announcing that your organization is supporting

their efforts and are providing a link to the compromised website through social media sites such as Twitter and Facebook. While you have removed the offending website and patched the exploited vulnerability, you are receiving calls and queries from media regarding your organization’s support of the hacktivist’s violent political ideology.

Example 21:

Upon review of your logs, several of your organization’s internet facing assets are being scanned. After investigation, the scans are originating from what seems to be a legitimate private cyber security company.

Example 22:

The private company acknowledges the scans but refuses to disclose any information such as who ordered the scans due to a non-disclosure agreement (NDA). The scans from the same source continue to scan other external facing assets and the private company still refuses to disclose any information.

Example 23:

You have been notified that your organization may be targeted through spear phishing emails

and social engineering phone calls.

# Full Table Top Exercise – Example 1

Goal

The Goal of the Incident Response Table Top Exercise (TTX) is to ensure that the organizations policies and procedures are effective, collaborative, and comprehensive in setting forth sound preparation, mitigation, response, and recovery measures. The output from this TTX will be used to update the relevant Incident Response Procedures, communications list and, provide additional training where needed.

Purpose

The purpose of this exercise is to provide participants an opportunity to evaluate current response concepts, communications, crisis management and capabilities for a response to a presumed failure of its IT systems, catastrophic and/or widespread inability to deliver critical business operations with the use of IT infrastructure and assets. The exercise will provide Players with an opportunity to evaluate current emergency response and incident management concepts, communications, and capabilities for responding to an impact of the organization Information Technology systems. Player feedback will be used to update relevant procedures and documentation.

Scope

This exercise will allow participants to discuss the issues and response requirements for an impact to organization’s Information Technology systems. The exercise will lead participants in discussions about the organizational communications and response impacting the systems. The denial of service to the systems will impact the ability to route any phone calls and communicate with any IT systems managed by the organization. Through the decisions necessary to invoke the Incident Response Plan and respond to the denial of services and begin planning considerations for improved business resumption response and recovery of IT services.

Exercise Objectives

The Exercise design objectives to achieve the goal are predicated on the event of an Information Technology denial of service by Ransomware, causing the organization’s systems to fail. Particular attention should be focused on improving understanding of a response concept, identifying opportunities or problems, and/or achieving a change in attitude. The exercise will focus on the following design objectives selected by the exercise planning team:

Topical areas for objectives include, but are not limited to, the following:

* Public, Governmental, Vendor, other Customers and Internal Communications
* Supporting Service Restoration
* Information Sharing
* Supporting Recovery
* Situational Awareness
* Supporting Crisis Response

Objectives of the TTX:

Exercise internal and external communications of the event.

* How communications will be handled between internal and external
* How communications will be handled internally.
  + Leadership Management (local, regional and national)
  + Organizations Staff members
* How communication will be handled with other support vendors.
* External communications to the media.
* Communications to customers and third parties/suppliers.
* How communications will be handled between Organization and regional/national agencies

Organization’s response

* Initial response to the event
* Support actions and containment of the ransomware.
* Information sharing between organizations and other affected providers.
* How the will information be shared with the other organizations and will Legal need to be involved.
* Coordination between organization and support vendors. i.e., network vendor, ISP, etc.
* What are the succession plans for the response team - If needed.

Walk through any legal issues that may arise.

* The scenario outlined above are dependent upon a collaborative effort between organization leadership and ISP adding a blend of response and coordinated activities addressing the denial of service.

Participants

* Players: respond to the situation presented based on expert knowledge of response procedures, current policies, plans, procedures, and insights derived from training.
* Observers: support the group in developing responses to the situation during the discussion; however, they are not participants in the moderated discussion period.
* Facilitator/s: provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key planning Committee members may also assist with facilitation as subject matter experts (SMEs) during the tabletop exercise.

Exercise Structure

This will be a facilitated tabletop exercise. Players will participate in the following two distinct modules:

* Module 1: Communications and Decision-making
* Module 2: Resources, Communications and Logistics

Each module begins with an update that summarizes the key events occurring within that time period. Following the updates, participants review the situation and engage in facilitated discussions of appropriate response issues.

Following these discussions, participants then enter into a facilitated discussion in which a response and synopsis will be discussed based on the scenario.

Schedule of Events

|  |  |
| --- | --- |
| 2:00 PM | Participant Briefing / Start Exercise |
| 2:15 PM | Module 1 |
| 3:00 PM | Module 2 |
| 3:45 PM | Additional Discussion |
| 4:00 PM | Adjourn |
| TBD | After-Action Review |

Exercise Guidelines

* This is an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
* Respond based on your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from training.
* This is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.

Assumptions and Artificialities

In any exercise a number of assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

* The scenario is plausible, and events occur as they are presented/injected.
* There is no “hidden agenda”, nor any trick questions.
* All players receive information at the same time.
* The players may assume that their Internet Service Provider is aware of the Denial-of-Service attack
* Facilitator/s will introduce and set the scenario, inject statuses and situational updates to focus on participant discussions and responses.

# Module 1: Communications and Decision-Making

The Scenario: CYBER ATTACK

Foreign Actors, wanting a ransom of 1 million dollars have determined that shutting down Organization’s systems would suite their purpose. They do their research and determine all supporting providers involved that support the organizations system. Ransomware has been propagated from one of the affected ISPs and the organization has possibly been affected by Ransomware on one of their servers and the 2 data centers hosting their infrastructure.

Assumptions:

* All systemic components of the organizations systems including Hardware systems and application servers, communication routers, disk data storage sub-systems, Operating Systems, and backup systems are supported at the “Location 1” and “Location 2” data centers.
* Calls have been successfully routed to the organization.
* All components of the organizations systems are configured in a High Availability (HA) failover configuration.
* All data backups are stored and current between the 2 data centers.
* Recovery may be needed to recover the organizations systems at the current site or fail over to the secondary site.
* All organizations personnel are available at this time

Key Issues

* At this time, we only know of one organization being affected by ransomware.
* We do not know if other/similar organizations are also a target.
* We still do not have all the details, as information we have is not complete and slow to come in.

Questions

Based on the information provided, participate in the discussion concerning the issues relative to the potential impact on services.

Identify any additional requirements, critical issues, decisions, and/or questions that should be addressed at this time.

Discuss if any, what communications should be prepared with information we have.

The following questions are provided as suggested general subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question in this section.

Decision-Making

* What is the immediate response and what are planning considerations at this time for the organization?
* What are the priorities?
* Is this an incident to activate the Incident Commander and deploy the Incident Handling Team?
* List what preparation steps should be taken.
* What information is required to make an informed decision?
* What communications need to be sent? And who will provide those communication?
* Communications between the organization and regional centers?
* Communications internally?
* Communication with other organization support vendors?
* Communications external to the media?
* Communications to other customers?
* Communications between organization and regional ISPs?
* When is it appropriate to invoke the Incident Response Plan?

Resources

* What resources are readily available for this event?
* List resources that will be needed
* What resources are required if data needs to be recovered?
* What resources may be needed from other areas within the region? (i.e., third parties, ISPs, regional emergency/incident offices?)
* What resources, if any, are needed from external sources?
* What response workstreams within existing teams will need to be setup for the response?

Communication

* What is the key message/s, at this time and who would be sending to the internal team, public, vendors, customers, business partners and government officials at this time?

# Module 2: Resources, Logistics and Communications

It has been two hours since the first organization has been infected with Ransomware. The decision has been made to:

* Security scans have already begun in both support data centers.
* Prepare for containment and isolation.
* Notify support team/vendors/external IR teams of possible ransomware.
* Prepare communications to be released in the event of ransomware being found

Key Issues

* We only have information regarding 1 server being affected - no other information has come in.
* We have no additional information from regional offices
* We don’t know if ransomware has affected our support data centers and other assets

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 1. Identify any additional requirements, critical issues, decisions, and/or questions that should be addressed at this time.

The following questions are provided as suggested general subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question in this section.

* How does the option of restoring a system from backup influence your decisions? Describe the changes?
* What is the impact to the organization and services that need to be provided?
* Are there appropriate procedures in place to ensure an alternate capability exists to continue call routing commitments?

Communications

* What levels of communication are necessary to; internal, business partners, customers, Government officials and other organization/regional centers - if any?

Discovery / Isolation

* Once the ransomware has been contained, how are the systems synchronized to the accommodate the downtime?
* What procedures are in place for immediate procurement for software, hardware, professional services or additional data center space?
* What communications would need to be sent and to whom?

# Appendix B: Participant Observer Evaluation

Exercise Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Exercise Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Participant Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Player: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Observer: \_\_\_\_\_\_\_\_\_\_\_

Part I – Recommendations and Action Steps

1. Based on discussions today and the tasks identified, list the top 3 issues and/or areas that need improvement.

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

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

1. 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

1. 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 1 indicating strong disagreement with the statement and 5 indicating strong agreement.*

|  |  | Rating of Satisfaction with Exercise | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Assessment Factor | | *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 facilitator(s) was knowledgeable about the material, kept the exercise on target, and was sensitive to group dynamics. | | | 1 | 2 | | 3 | 4 | | 5 |
|  |  | | |  |  | |  |  | |  |
| d. | The Situation Manual used during the exercise was a valuable tool throughout the exercise. | | | 1 | 2 | | 3 | 4 | | 5 |
|  |  | | |  |  | |  |  | |  |
| e. | Participation in the exercise was appropriate for someone in my position. | | | 1 | 2 | | 3 | 4 | | 5 |
|  |  | | |  |  | |  |  | |  |
| f. | The participants included the right people in terms of level and mix of organization’s operational areas. | | | 1 | 2 | | 3 | 4 | | 5 |
|  |  | | |  |  | |  |  | |  |

2. 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.*