2021 Fall Exercise Series

"3rr0r 404" Information Technology Interruption

Situation Manual (SITMAN)

October 2021

EXERCISE OVERVIEW

Exercise Name	2021 Information Technology (IT) Interruption Tabletop Exercise
Exercise Dates	October 12th from 1:00 p.m. – 4:00 p.m. (Tuesday) October13th from 9:00 a.m. – 12:00 p.m. (Wednesday) October 14th from 9:00 a.m. – 12:00 p.m. (Thursday)
Scope	This table top exercise is planned for three hours at the Vinton War Memorial in Vinton, VA.
Mission Area(s)	Mitigation, Response, and Recovery
Core Capabilities	ASPR: • Health Care and Medical Response Coordination • Continuity of Healthcare Service Delivery FEMA: • Cybersecurity • Long-Term Vulnerability Reduction • Risk and Disaster Resilience Assessment
Objectives	Objective 1: Identify potential process disruptions from information systems hazards. Objective 2: Evaluate or construct emergency operation plan (EOP) annexes to address short- and long-term information systems interruptions. Objective 3: Evaluate current continuity of operations (COOP) plan with respect to an information systems interruption.
Threat or Hazard	Short- to long-term information system interruption to healthcare facilities across the Near Southwest (NSW) Region of Virginia
Scenario	Healthcare facilities located within the NSW Region encounter disruptions in information systems in expanding scenarios requiring the utilization of continuity of operations for short- to long-term system disruptions.
Sponsor	Near Southwest Preparedness Alliance (NSPA)
Participating Organizations	This tabletop exercise is designed for all NSPA members and partners to include participants from hospitals, local emergency management, public health, long-term care, home health, dialysis, hospice, behavioral health, public safety, OCME, and any other regional stakeholders. See Appendix A for full list of participants.

Points of Contact	Robert Hawkins, Executive Director, Near Southwest Preparedness Alliance, 540-562-3482, rhawkins@vaems.org James Finney, Supervisory Protective Security Advisor, Region III, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. 434-942-9269, james.finney@hq.dhs.gov

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	ASPR (HPP) Capability	FEMA Capability
Objective 1: Identify potential process disruptions from information systems hazards.	• Health Care and Medical Response Coordination • Continuity of Healthcare Service Delivery	• Supply Chain Integrity and Security • Long-Term Vulnerability Reduction • Risk and Disaster Resilience Assessment
Objective 2: Evaluate or construct emergency operation plan (EOP) annexes to address short- and long-term information systems interruptions.	• Health Care and Medical Response Coordination • Continuity of Healthcare Service Delivery	• Supply Chain Integrity and Security • Long-Term Vulnerability Reduction • Risk and Disaster Resilience Assessment
Objective 3: Evaluate current continuity of operations (COOP) plan with respect to an information systems interruption.	• Health Care and Medical Response Coordination • Continuity of Healthcare Service Delivery	• Supply Chain Integrity and Security • Long-Term Vulnerability Reduction • Risk and Disaster Resilience Assessment

Table 1. Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players**. Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.

- **Controllers**. Controllers plan and manage exercise play, set up and operate the exercise site, and act in the roles of organizations or individuals that are not playing in the exercise. Controllers direct the pace of the exercise, provide key data to players, and may prompt or initiate certain player actions to ensure exercise continuity. In addition, they issue exercise

material to players as required, monitor the exercise timeline, and supervise the safety of all exercise participants.

- **Simulators**. Simulators are control staff personnel who role play nonparticipating organizations or individuals. They most often operate out of the Simulation Cell (SimCell), but they may occasionally have face-to-face contact with players. Simulators function semi-independently under the supervision of SimCell controllers, enacting roles.
(e.g., media reporters or next of kin) in accordance with instructions provided in the Master Scenario Events List (MSEL). All simulators are ultimately accountable to the Exercise Director and Senior Controller.

- **Evaluators**. Evaluators evaluate and provide feedback on a designated functional area of the exercise. Evaluators observe and document performance against established capability targets and critical tasks, in accordance with the Exercise Evaluation Guides (EEGs).

- **Observers**. Observers visit or view selected segments of the exercise. Observers do not play in the exercise, nor do they perform any control or evaluation functions. Observers view the exercise from a designated observation area and must remain within the observation area during the exercise. Very Important Persons (VIPs) are also observers, but they frequently are grouped separately.

- **Support Staff**. The exercise support staff includes individuals who perform administrative and logistical support tasks during the exercise (e.g., registration, catering).

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation.

Assumptions

Assumptions constitute the implied factual foundation for the exercise and, as such, are assumed to be present before the exercise starts. The following assumptions apply to the exercise:

- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
- The exercise scenario is plausible, and events occur as they are presented.
- Exercise simulation contains sufficient detail to allow players to react to information and situations as they are presented as if the simulated incident were real.
- Participating agencies may need to balance exercise play with real-world emergencies. Real-world emergencies take priority.

Artificialities

During this exercise, the following artificialities apply:

- Exercise communication and coordination is limited to participating exercise organizations, venues, and the Regional Healthcare Coordination Center.

POST-EXERCISE AND EVALUATION ACTIVITIES

Debriefings

Post-exercise debriefings aim to collect sufficient relevant data to support effective evaluation and improvement planning.

Hot Wash

At the conclusion of exercise play, a facilitated Hot Wash will allow players to discuss strengths and areas for improvement, and evaluators to seek clarification regarding player actions and decision-making processes. All participants may attend; however, observers are not encouraged to attend the meeting. The Hot Wash should not exceed 30 minutes.

Participant Feedback Forms

Participant Feedback Forms provide players with the opportunity to comment candidly on exercise activities and exercise design. Participant Feedback Forms should be collected at the conclusion of the Hot Wash.

Evaluation

Exercise Evaluation Guides

EEGs assist evaluators in collecting relevant exercise observations. EEGs document exercise objectives and aligned core capabilities, capability targets, and critical tasks. Each EEG provides evaluators with information on what they should expect to see demonstrated in their functional area. The EEGs, coupled with Participant Feedback Forms and Hot Wash notes, are used to evaluate the exercise and compile the After-Action Report (AAR).

After-Action Report

The AAR summarizes key information related to evaluation. The AAR primarily focuses on the analysis of core capabilities, including capability performance, strengths, and areas for improvement. AARs also include basic exercise information, including the exercise name, type of exercise, dates, location, participating organizations, mission area(s), specific threat or hazard, a brief scenario description, and the name of the exercise sponsor and POC.

Improvement Planning

Improvement planning is the process by which the observations recorded in the AAR are resolved through development of concrete corrective actions, which are prioritized and tracked as a part of a continuous corrective action program.

After-Action Meeting

The After-Action Meeting (AAM) is a meeting held among decision- and policy-makers from the exercising organizations, as well as the Lead Evaluator and members of the Exercise Planning Team, to debrief the exercise and to review and refine the draft AAR and Improvement

Plan (IP). The AAM should be an interactive session, providing attendees the opportunity to discuss and validate the observations and corrective actions in the draft AAR/IP.

Improvement Plan

The IP identifies specific corrective actions, assigns them to responsible parties, and establishes target dates for their completion. It is created by elected and appointed officials from the organizations participating in the exercise, and discussed and validated during the AAM.

PARTICIPANT INFORMATION AND GUIDANCE

Exercise Rules

The following general rules govern exercise play:

- Real-world emergency actions take priority over exercise actions.
- Exercise players will comply with real-world emergency procedures, unless otherwise directed by the control staff.
- The entirety of this exercise occurs within the venue. No emergency communication outside of the venue should be made related to this exercise.

Players Instructions

Players should follow certain guidelines before, during, and after the exercise to ensure a safe and effective exercise.

Before the Exercise

- Review appropriate organizational plans, procedures, and exercise support documents.
- Prepare a list of the various systems or technologies that could be impacted by the indicated hazard for the exercise.

During the Exercise

- Respond to exercise events and information as if the emergency were real, unless otherwise directed by an exercise controller.
- Do not engage in personal conversations with controllers, evaluators, observers, or media personnel. If you are asked an exercise-related question, give a short, concise answer. If you are busy and cannot immediately respond, indicate that, but report back with an answer as soon as possible.
- Parts of the scenario may seem implausible. Recognize that the exercise has objectives to satisfy and may require incorporation of unrealistic aspects. Every effort has been made by the exercise's trusted agents to balance realism with safety and to create an effective learning and evaluation environment.

After the Exercise

- Participate in the Hot Wash at your venue with controllers
- Complete the Participant Feedback Form. This form allows you to comment candidly on emergency response activities and exercise effectiveness. Provide the completed form to a controller or evaluator.

EXERCISE SCHEDULE

October 12th, 2021 (Tuesday: 1:00-4:00pm)

Time	Activity
12:30 – 1:00	Registration
1:00 - 1:15	Welcome and Exercise Briefing
1:15 - 3:00	Module Discussions and Report Outs
3:10 - 4:00	Debrief & Hot Wash

October 13th, 2021 (Wednesday: 9:00am-12:00noon)

Time	Activity
8:30 - 9:00	Registration
9:00 - 9:15	Welcome and Exercise Briefing
9:15 - 11:00	Module Discussions and Report Outs
11:10 - 12:00	Debrief & Hot Wash

October 14th, 2021 (Thursday: 9:00am – 12:00pm)

Time	Activity
8:30 - 9:00	Registration
9:00 - 9:15	Welcome and Exercise Briefing
9:15 - 11:00	Module Discussions and Report Outs
11:10 - 12:00	Debrief & Hot Wash

Pre-Module Activity

Choose from the following Pre-Module Activity:

1 In person option: On the large sticky-note pads located on your table, please list all of your electronic operating systems and number them from the most vulnerable to least vulnerable. The items you identify may be specific systems, platforms, services, software or physical technical components*. Please write them large enough to be read by others in the classroom. Once you have identified a list for your table or group, place the sheet in the designated area directed by the facilitator.
2 Virtual option: Create a list with your exercise team that lists all of you electronic operating systems and number them from the most vulnerable to the least vulnerable. The items that you identify may be specific systems, platforms, services, software or physical technical components*. Items on this list will be used throughout the exercise. Please provide items in the platform of web service used for the exercise as directed by the facilitator.
You have 15 minutes to complete this assignment.

**Electronic Operation System is defined as any electronic or IT based device, equipment, systems, hardware, software, etc.*

MODULE 1

(Scenario)

On this date, at approximately 3:00 pm, you have received reports within your facility of intermittent service issues with one of the systems/platforms/services or electronic operation devices that affect the ability to deliver healthcare services to patients. Depending on your facility, and on the systems, services, software or technology identified by your team in the pre-module work, you are seeing an inability to maintain normal operations of patient care due to the interruptions. Members of your team have informed your IT support resources, which includes manufacturers of the devices or software. While they investigate the matter, you are seeing that your staff are having difficulty completing what are considered to be routine tasks which slows their workflow and has caused back-ups in the care of patients.

Discuss with your team/table the impacts to your specific organization. Utilize the questions listed below as you work through this module. Consider the additional systems identified from your pre-module work after you work through the first one.

QUESTIONS

For ALL

- Does your Emergency Operations Plan (EOP) / All-Hazards Plan / Continuity of Operations Plan (COOP) include procedures specific to information technology interruptions?
- What are your triggers for activating your Emergency Operations Plan?
- Do you initiate your EOP at this point? If so, does it include the establishment of an incident command center and its location?
- Do you have a backup system in place for this interruption? And do you utilize it at this point?
- How will an IT interruption / disruption affect your organization from an administrative standpoint? A clinical standpoint? A facilities standpoint?
- Are there any licensure or regulatory guidelines for this? And how will your organization respond in accordance with these guidelines?
- Who are you communicating with at this point (staff, patients, families, media, etc.) ? How is this communication taking place? And what information are your sharing?
- Do you have MOUs/MOAs/Vendor Contracts in place for each of these technology services when needed? How about backup Vendors? If so, who are they with?
- Are there any issues with protected personal information at this point? Do you address these in your downtime procedures if you have activated these plans?
- Have you identified your Local, Regional, and/or Statewide public or private sector partners? How and when would these individuals be notified if applicable?
- What challenges should you consider that are specific or unique to your Organization type?
-

Additional Questions for Consideration

- Do you have plans that address security concerns when these types of technology are interrupted?
- Do you have an electronic system you utilize for obtaining supplies? What plans are in place if this system is interrupted?

- Is the affected system or systems a part of a larger network? How do you address this issue on site? When do you reach out for additional assistance?

- If your Organization is a part of a health system, are you reaching out for additional resources yet? Would anyone else within the system be experiencing similar issues?

  How do staff communicate these issues/issue to the organization in a timely manner?
- Does this interruption affect your communication with other Organizations (sister organizations, vendors/supplies, community groups)?

RHCC

- What is your role and responsibility to help assist with IT issues in the region/state? What action triggers your activation?

- What backup systems are available once an IT interruption occurs at a facility?

- What information should be communicated to the RHCC in reference to an IT interruption?

- What is the process in place to share critical information across the region to all stakeholders?

MODULE 2

(Scenario 2: Regional / Expanded)

Your facility has been experiencing intermittent service outages in your identified systems for nearly 24 hours now. Your IT department has reported that the service has critical errors from an unknown source which may require extensive downtime to diagnose and repair. At 5:30 pm, the overall system for your facility, as well as other facilities within your system experience a full outage for the identified system or technology. While you have been able to leverage resources outside of your specific facility up to this point, even those are now unable to assist with use of the system or process you use to deliver healthcare using the identified technology. Meanwhile, as this situation expanded over the previous 24 hours, reports on social media have drawn the attention of the community to include media outlets. With the latest developments, your facility's ability to treat patients has been strained.

QUESTIONS

For ALL

- What are the immediate actions, concerns and priorities for…
  - Administration
  - Clinical operations
  - Facility operations

- Have you activated your EOP now? If so, describe your command structure.

- How do you include IT in your Incident Command?
- If your EOP was already activated, what is your organizational relief plan for your Incident Command Team staffing levels?
- Do you have downtime procedures for this interruption? Have these been activated?
- Are you still able to manage this interruption with your support services onsite? Or are you working with additional individuals? If so, who are they?
- Are you utilizing any MOUs/MOA's or backup systems yet? If so, is that included in your downtime procedures / policy?
- In what way does your downtime procedures address additional work flow created during this incident?
- Are there any issues with protected personal information at this point?
- Have you notified any Local, Regional, and/or Statewide public or private sector partners? If so, who?
- Do you have any security concerns at this point?
- What are your Essential Functions to maintain during this interruption?

MODULE 3

(Long-term – National/Global Issues: External System Loss)

Your facility has experienced partial restoration of systems but the intermittent nature of the service still causes rolling outages or lengthy loading times. Any augmented procedures your facility or organization have utilized to this point have caused strain within your staff and inefficiencies in your processes which directly impact healthcare delivery to your patients as well as in other areas or operations. Through state, federal and local emergency management you receive notification of large areas of service outages for multiple platforms indicating a large-scale systematic loss. The underlying cause is still unknown, though authorities are providing remediation instructions to technology companies, internet service providers and web hosts. Media begins reporting that popular websites and services cannot be accessed.

Follow Up For All

- What discussions are taking place with your command team at this point?
- Have you acquired a regional situation report?

- Has your communication changed from your previous messaging? If so, explain.
- Who are you communicating with now (internally & externally)? How is this communication taking place?
- How do you continually handle the security and safety of staff, patients and community?
- At this point you may need to be considering altering your operations. What are your alternate standards of care? (These are standards of practice if there is a significant loss due to the interruption)
- Is your Organization still operating?
    - If yes, please explain
        - Do you need additional resources to continue operations? If so, what is needed?
        - If your Organization is a part of a larger health system, how does internal sharing of resources work, and if technologically based what are alternative methods of obtaining items, information, services?
    - If not:
        - what procedures are in place for finding alternate services or placement for your patients?
        - How could you assist other Organizations if you were to close/shut down?
- How are you staying engaged in communication with your Healthcare Coalition?

For RHCC

- What information are you now sharing? And to whom?
- What is your process for collecting information to send up to state and federal agencies? Does this differ in an IT interruption?

MODULE 4

(RECOVERY)

Over the course of 3 days, services for platforms, software or technology that you have identified begin to cascade back into service. It begins with slow service in these platforms or devices and allows for restored and sometimes minimal services. State and Federal authorities continue to provide additional information to service providers about methods to reconnect to the large area network.

QUESTIONS

What steps need to take place in order to regain full facility operations? What are your immediate actions, concerns and priorities?

What challenges would you likely face as you begin restoring your facility back to normal operations?

If you only have a limited amount of service bandwidth, or limited resources to restore services, which do you identify for priority restoration?

Have you revisited your policies in regards to regulatory compliance?

Did you alter standard of care? If so, at what point will you resume your normal standards of care?

What documentation will be needed to ensure missing information during the interruption is appropriately accounted for? Example: If your billing service was impacted, how would you process/receive payments?

Who is responsible for tracking all aspects of the recovery process?

When would you close EOC?

How have you handled multiple staffing adjustments over a period of time?

How will you communicate that your operations are back to normal?

What steps can you take now to enhance these relationships in advance of an IT interruption?

FINAL QUESTIONS:

- What is the importance of providing/acquiring a regional status report?
- What steps can you take now to enhance public and private relationships in advance of a loss of critical systems to your organization?
- What role do you think the Regional Healthcare Coalition serves in regard to its efforts to assist all regional partners in these types of events?

Appendix A: Exercise Participants

To be compiled from attendance sheets at completion of exercise

Appendix B: Acronyms

Acronym	Term
AAM	After Action Meeting
AAR/IP	After Action Report / Improvement Plan
CMS	Centers for Medicare & Medicaid Services
COOP	Continuity of Operations Plan
ECO	Emergency Custody Order
EEG	Exercise Evaluation Guide
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
HVA	Hazard Vulnerability Analysis
ICS	Incident Command System
IS	Information Systems
IT	Information Technology
LTC	Long Term Care
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NSPA	Near Southwest Preparedness Alliance
OCME	Office of the Chief Medical Examiner
PACE	Program of All-Inclusive Care for the Elderly
POC	Point of Contact
RHCC	Regional Healthcare Coordination Center
SitMan	Situation Manual
TDO	Temporary Detention Order
TTX	Tabletop Exercise
VDEM	Virginia Department of Emergency Management
VDH	Virginia Department of Health
VDOT	Virginia Department of Transportation
VHASS	Virginia Healthcare Alerting and Status System

Appendix C: AAR Documentation

Instructions

Please review the following sections with information specific to your facility. This information will be used to complete your AAR for this TTX.

What was supposed to happen:

(In an ideal situation, how would your facility have handled this scenario?)

What actually occurred:

(Compared to ideal, what were you actually able to do?)

What we did well:

(Select the most important 3-5 items)

What we need to improve:

(Select the most important 3-5 items)

Plan for improvement:

(For each area of improvement from above, who will address and on what timeline?)