TABLETOP EXERCISE

Table of Contents

Scenario A: Pandemic (Stat-at-Home Order)

Objectives:

- To evaluate the viability of continuity plans in the event of a stay-at-home order.
- To test the department's ability to smoothly transfer to work-from-home and return-to-campus status.
- To assess the readiness of the staff and their resources.

A global pandemic occurred on Monday and a lockdown was instantly ordered.

Monday

Update 1: The media announced a stay-at-home order by the Governor starting the next day. The campus is closed, and all buildings, equipment, and supplies are inaccessible. However, you need to access your office in order to gather essential items.

- What is the notification process to your personnel and affected staff?
- What are the immediate concerns that your department has at this moment?
- Who can be contacted to give access to buildings?
- List the critical functions that need to be performed within the next 24 hours.

Tuesday

Update 2: You have received a campus-wide email that notifies everyone to stay home for an undetermined amount of time. Buildings, equipment, and supplies are still inaccessible.

- What is your work from home transition procedures?
- What are your recovery strategies when it comes gathering equipment and supplies, documents, and other necessary resources?
- Who would take the lead to ensure that confidential items are secure?
- What actions would you take to continue critical functions and deliver essential services?
- What is the supply chain impacts that the pandemic has on your department if the city of Big Rapids ends up being quarantined?
- Who would you contact for assistance in transferring your workstation and server to a different location?
- How would you provide a secure internet access outside of the campus network to home workers?

Two weeks later

Update 3**:** You received a notification stating that the lockdown has been lifted. You are advised to come back to the office in three days.

- What is your return-to-campus procedures?

- How are you going to notify your staff of the return-to-campus process?
- Who do you need to contact for assistance in transferring your workstation and server back to the original location?
- How are you documenting your return-to-campus and work-from-home strategies in your continuity plan?

Additional Questions

Which page in your continuity plan lists your emergency contact? Are they correct and current?

Do you have the minimum required office equipment ready at your alternate location? If not, do you have a process to transfer your equipment and supplies to your alternate location?

How many additional laptops, cell phones, and/or tablets does your team need for your critical functions?

How are you documenting your remote work plans in your continuity plan?

Scenario B: Tornado

Objectives:

- To evaluate the viability of continuity plans when it comes to natural disasters such as tornado, hurricanes, and earthquakes.
- To test departments' ability to recover from a tornado and smoothly return to business as usual.
- To assess department's readiness of the staff and their resources

A large tornado occurred at 12 pm on Monday. The damage is seen across campus and is impacting department's communications, access to buildings, and information technology capability.

Monday @ 12: 30 PM

Update 1: After a quick assessment of your facility, damage is visible around you, power is out, and some staff and students appear to be injured. All phones and landlines are jammed.

- What is the notification process to your management personnel and to affected staff?
- What are the immediate concerns at hand?
- Where is the nearest flashlight? Does it have batteries?
- Where is your first aid kit?
- When it is safe to evacuate, which rally point is the safest in this situation?

Tuesday @ 2:00 PM

Update 2: Media reports a severe wind of 160 MPH occurred in your area. Media strongly recommends that citizens do not drive due to unsafe roadways. The local fire department has asked for a full evacuation of the campus so that they may assess the building structure.

- How would the damage to your facility alter operations?
- What actions would you take in order to continue critical functions and deliver essential services?
- Where is your primary recovery/alternate location?
- Who would take the lead to ensure that confidential documents/items are secure?

Tuesday @ 4:00 PM

Update 3: Cell phones and landlines are working sporadically. Text messages are getting through. HR has contacted the student and staff's families letting them know that all students are safe with very minor cuts. Limited power returns.

- Who would be the person that decides if your location / department is closed for the rest of the day or beyond?

- What if employees want to leave regardless of recommendations by the emergency officials and media?

Additional Questions:

What page in your continuity plan does list your emergency contact? Are they correct and current?

Name two items in your emergency kit.

Does your building have an evacuation plan? Is it up-to-date and attached to your continuity plan?

Scenario C: Loss of personnel with unique skills

Objectives:

- To ensure that the risks of losing essential personnel with unique skills are managed.
- To evaluate your department's readiness in the event of any loss of personnel.

The HR department announced at 8:00 AM that the head of your department had passed away.

Monday @ 8:00 AM

Update 1: You discover the news upon coming to the office. You are the leadership successor of the deceased director. Therefore, you have the responsibility to notify the affected staff.

- What is the notification process to affected staff?
- How would you notify the dependencies of the potential disruption? Do you have their contact list on your continuity plan?

Monday @ 12:00 PM

Update 2: You have assessed the situation and have contacted those who are impacted by the disruption. You are required to step in as a leadership successor and perform some critical functions that the director used to perform.

- Who should you contact to obtain access to work-related confidential information that the deceased worker had access to?
- Where can you find a list of the critical functions dependencies that the deceased worker used to perform?
- How would you mitigate the risks of unmet deadlines due to personnel loss?

Tuesday @ 8:00 AM

Update 3: You realized that you are unable to perform some of the critical functions that the deceased worker was assigned of due to lack of skills.

- Have you cross-trained someone to temporarily perform the director's critical functions?
- Would you outsource/hire someone else that has the unique skills?

Scenario D: Cyber-attack

Objectives:

- Identify strengths and weakness when recovering from a campus infrastructure breakdown or failure caused by a cyber-attack.
- Assess your department's ability to communicate during such failure.

The University is a target of a malicious and complex cyber-attack using multiple vectors. The malicious actor took over and compromised all University information system and database.

Monday 10:00 AM

Update 1: Ferris IT department received calls about Banner issues. Users are unable to access it. Within a few hours, Banner is unavailable and is corrupted.

- Do you need Banner to perform your critical functions?
- What is your recovery strategies to do business as usual if Banner is down?
- What is the notification process to affected staff?
- What are your department's top critical functions at the time of this attack?

Monday 2:00 PM

Update 2: An unauthorized message is pushed out to most students and employees on the Ferris email list. The sender imitates Ferris IT department's name and states "IT Alert: On Monday morning, we were made aware of ongoing Banner issues. To fix this issue, you have to access this link we have created. Click here to access it." Once individuals click on the link, it connected the computer to a blank webpage containing malware actors which will cause their computer to crash.

- Do you have a backup for files that are stored on your department workstations?
- Do you have workarounds such as paper forms, whiteboards, etc. to continue your critical functions?
- What is your alternative communication medium if your email is down?
- Is your emergency contact up to date?

Tuesday 8:00 AM

Update 3: Ferris IT department is confident that computers affected by the malware allow malicious actors to acquire credentials from users. The hacker gained control of some of the Central Applications owned by Ferris resulting in loss of electrical power, HVAC, water, and key card access.

- Do you have an updated emergency plan attached to your continuity plan?
- Do you have a secure alternate location that is ready to use in this situation?
- How would you notify your dependency of your absence?
- How are your employees notified about the evacuation plan?
- How are students notified about classes being canceled? (If you are in Academic Affairs)

Thursday 8:00 AM

Update 4: Ferris IT department was able to block the hijacked account used to access control systems. It has been communicated that it is safe for students, faculty, and staff to return to campus. Departments are advised to return to campus if they are able to do so.

- What is your return-to-campus procedures? Are they documented in your continuity plan?
- What are the potential impacts of the attack that would cause delay in the recovery of your critical functions?

Scenario E: Connection Outage

Objectives:

- To identify the risk that weak back-ups and recovery strategies present.
- To evaluate the impact that connection outage has on supply chain, critical personnel, equipment needs, data and computer needs, and communication needs.
- To establish procedures for restoring systems.

On Monday, a connection outage occurred throughout campus. This event created a disruption in internet activities of all technology that relies on internet to function.

Monday @ 10:00 AM

Update 1: You are on your work cite when the outage happens.

- What is the impact of service disruptions?
- What is your plan to mitigate the disruptions?
- What is the notification process to affected staff, vendors, suppliers, and other dependencies?
- With whom will you need to communicate for a liaison with Network Company? Do you have their contact in your continuity plan?

Monday @ 12:00 PM

Update 2: You are informed that the disruption may continue for at least six more hours.

- Do you have an updated list of your critical functions?
- Are back-ups available to ensure the continuity of the critical functions?
- How often do perform computer security, download, and backup practices in order to secure technologies and communication networks?
- Do you have an alternate location to continue your work?
- Is everyone aware of the security measures to take while working remotely (VPN, safe network connection, etc.)?
- What is the plan for network restoration?

Tuesday @ 8:00 AM

Update 3: You are informed that connection has been restored.

- What is your department's return to business as usual protocol?
- How are you planning on documenting this disruption and the recovery strategies to your continuity plan?

INFORMATION FOR THE EXERCISE FACILITATOR (Plan Manager)

What is a Tabletop exercise? A tabletop exercise (TTX) is a discussion, a simple problem resolution exercise. A scenario or situation is presented to the participants. Using the information in your continuity plan, a discussion of the recovery process and how to resolve the issues in the scenario should be incorporated into the exercise.

Who should conduct the exercise? This exercise should be facilitated by the Plan Manager and can be conducted remotely. It could be rehearsed with FSU Department of Public Safety and the Emergency Management Team.

What if employees have questions during the exercise we can't answer? Any issues, risks, or questions identified during the discussion should be documented in action items and notated in the tabletop results document.

Participants: All participating employees should sign a tabletop participation document. Any employee does not present for the actual test discussion should be documented as not present, but will need to review this exercise and sign the roster as having reviewed the information covered.

How do I conduct this exercise?

Step 1: BEFORE THE EXERCISE

Review this entire document.

Step 2: EXERCISE DAY

- Activate your call tree before the exercise.
- Read the scenario to the group.
- Remember to document questions, any concerns, and any plan updates.

If you are unclear on any of the discussion items presented in this document, please contact the SHERM Department prior to the exercise date.