[Insert Cover Picture]

Tornado Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:30 a.m. | 8:45 a.m. | Welcome and Introductions |
| 8:45 a.m. | 9:45 a.m. | Module One: Pre-Incident Information Sharing |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module One: Scenario Update  |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:05 p.m. | Module Two: Incident Response |
| 12:05 p.m. | 12:15 p.m. | Break |
| 12:15 p.m. | 1:15 p.m. | Module Three: Short-Term and Continuous Recovery |
| 1:15 p.m. | 1:45 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Tornado Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] and will focus on local, state, and federal agency integration during a tornado at [insert location].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Protection, Mitigation, Response, and Recovery [select appropriate Mission Area(s)] |
| **Capabilities** | * Community Resilience
* Economic Recovery
* Infrastructure Systems
* Intelligence and Information Sharing
* Operational Communications
* Operational Coordination
* Physical Protective Measures
* Planning
* Public Information and Warning
* Risk and Disaster Resilience Assessment
* Supply Chain Integrity and Security
* [Insert additional capabilities as necessary]
 |
| **Objectives** | 1. Examine emergency response plans and procedures before and during a tornado incident with a focus on:
	* Incident Command System (ICS) / National Incident Management System (NIMS)
	* Critical infrastructure protection
	* Public messaging protocols
2. Assess procedures for coordinating and sharing information within the organization.
3. Examine recovery protocols following a tornado with a focus on:
	* Business continuity
	* Critical infrastructure resilience
	* Supply chain integrity
4. [Insert additional objectives as necessary].
 |
| **Threat or Hazard** | Tornado |
| **Scenario** | An interactive, discussion-based exercise focused on tornados threating a community and private sector business. The scenario consists of three modules: Pre-Incident Information Sharing, Incident Response, and Short-Term and Continuous Recovery. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable.] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

|  |  |
| --- | --- |
| **Exercise Objectives** | **Capability** |
| Examine emergency response plans and procedures before and during a tornado incident with a focus on: * ICS / NIMS
* Critical infrastructure protection
* Public messaging protocols
 | * Infrastructure Systems
* Intelligence and Information Sharing
* Physical Protective Measures
* Planning
* Public Information and Warning
 |
| Assess procedures for coordinating and sharing information within the organization. | * Operational Communications
* Risk and Disaster Resilience Assessment
 |
| Examine recovery protocols following a tornado with a focus on:* Business continuity
* Critical infrastructure resilience
* Supply chain integrity
 | * Community Resilience
* Economic Recovery
* Operational Coordination
* Supply Chain Integrity and Security
 |
| [Insert additional objectives as necessary.] | * [Insert additional capabilities as necessary.]
 |

Table 1. Exercise Objectives and Associated 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** 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.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate the discussion. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Data Collectors** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Pre-Incident Information Sharing
* Module Two: Incident Response
* Module Three: Short-Term and Continuous Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate protection, mitigation, response, and recovery issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve protection, mitigation, response, and recovery efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Pre-Incident Information Sharing

## Scenario

## [Insert location]

### [Insert Month, Day, Year]: [Insert time]

The National Weather Service (NWS) has issued a severe thunderstorm watch that will be in effect for the next 24 hours in the [insert your region]. [Insert state near you] is predicted to experience the thunderstorm first, with the weather system moving quickly toward your location. Forecasters predict the severe weather conditions will include heavy rains and strong winds with the potential to cause significant damage to regional infrastructure.

## Discussion Questions

1. What sort of preparations does your organization make prior to expected severe weather?
2. How does your organization receive information about weather-related threats?
	1. Who is responsible for monitoring these threats?
3. What systems are available that can facilitate information sharing and coordination among your region and relevant stakeholders?
4. What guidance does your organization expect from local or state authorities?
5. How does the incoming storm change your organization’s security posture or operations?
	1. Is there sufficient information to warrant a change in the current normal operating status?
	2. Would any emergency operations or business continuity plans be initiated or reviewed at this time?
	3. Who would make this decision, and how would it be communicated?
	4. Are there external stakeholders who should be notified if you have enacted a change in your facility’s operating status?
6. Are there any messages or communications from your city, county, or state that your organization would be monitoring?
7. Would your organization choose to communicate with staff about this impending storm?
	1. Does your business continuity plan outline communication procedures?
	2. With whom would you communicate at this time (e.g., senior staff only, managers / supervisors, all staff, others)?
	3. If employees request to return home to prepare for the storm, does that complicate your communication methods?
	4. How would communications be disseminated? Are there any technological redundancies?
	5. Does your organization have pre-determined messaging for this kind of event?
	6. Would the impending storm warrant after-hours actions or messaging? If not, what would?
8. Would your facility or resources require increased protection, monitoring, and / or protective actions?
	1. How would that be established and conducted?
	2. What is the full scope of resources that can be leveraged for this weather event?
	3. How long would it take for your organization to set up protections?
	4. Who would set up these protections? (i.e., Would staff potentially be called in after hours to accomplish this?)
9. Does the news report come with implications specific to your location or business?

## Scenario Update

### [Insert Month, Day, Year]: [Insert time + 6 hours]

The storm develops into a powerful line of thunderstorms, damaging winds, and hail. Current conditions are conducive to tornado activity, and the NWS adjusts their notifications to include a flash flood warning and tornado watch for [insert your city] from 1:00 p.m. to 7:00 p.m.

Portions of western [insert your city] can expect storm activity to begin around 1:00 p.m. Areas east of [insert your city] can expect the most dangerous part of the storm to pass by 4:00 p.m. The storm is expected to completely pass by 7:00 p.m.

Employees within your facility begin requesting to leave early or work remotely the following day to prepare their families and homes.

## Discussion Questions

1. What actions would this updated information prompt, if any?
2. What information are you sharing within the organization?
	1. To whom will this information be disseminated, and how will it be delivered?
3. Would your organization activate ICS at this time?
	1. What would trigger ICS activation? Who will make the decision to initiate the ICS?
	2. How will the ICS structure be initiated?
	3. Who will be make up the ICS?
4. How will the ICS gather given the scenario? Are there plans to meet virtually or in an alternate location for an extended period?
5. Would management consider releasing personnel early?
	1. How would this impact business operations?
	2. How much time ahead of an event like this would be required for adequate dismissal?
	3. What is the best way for organization leadership to communicate an early dismissal to staff? What are the current protocols, expectations, and mechanisms for this instance?
	4. How would your organization handle individual requests for early release prior to a facility-wide approval?
		1. How are these early releases approved, communicated up the chain, or tracked?
6. What additional resources might be needed or are available to ensure employees are able to work from home during a storm (e.g., hotspots, checklists of materials required to be downloaded, generators, etc.)?
7. If not already done, would your organization considering activating a continuity of operations plan at this point?
	1. What are the critical operations at your organization that must continue?
	2. Are there relocation plans in case of the need for critical personnel?
	3. Who are the personnel who support the critical operations?
	4. What information from the city, county, or state might automatically trigger your organization to activate your business continuity plan?
8. What factors would impact your decision to cease operations and shut down?
9. Who notifies headquarters or any other internal stakeholders of plan activation and closure?
	1. How does this notification process occur?
10. What are the department’s priorities (e.g., continuing all actions or just critical operations, providing guidance to personnel, protecting resources or points of critical infrastructure)?
11. Are there time requirements associated with any actions or critical operations? If so, what are they?
12. What if Emergency Response Group (ERG) members cannot or refuse to act?

# Module Two: Incident Response

## Scenario

### [Insert Month, Day, Year]: [Insert time + 2 hours]

The storm has arrived, hitting the [insert vulnerable part of your region] area. Radio channels begin to report sightings of low hanging, dark clouds and a green tint in the sky.

Soon after, the local 9-1-1 call center receives tornado sighting reports and significant critical infrastructure damage in the [insert neighborhood by your facility] area. Casualties across the region are being reported. Downed trees and flooded roads hinder first responders’ ability to navigate the area and support the community. Additionally, high winds from the storm have caused widespread power outages. Your facility is among those without power.

## Discussion Questions

1. Is any staff needed at the facility throughout the storm warning and arrival?
	1. What procedures exist to keep on-site staff safe during the storm and tornados?
	2. What shelter options does your facility have for employees?
2. What response plans or procedures, if any, does your organization have for a tornado?
	1. Does this response plan include considerations for individuals on-site with functional needs?
	2. Do your shelter options account for those with functional needs?
3. At this point, what message is your organization communicating to your employees?
	1. How would your organization communicate during the storm?
	2. How would that change based on cell network availability?
4. How are your employees trained for severe weather instances that impact the workplace?
	1. How often does training take place?
5. How would your organization coordinate and conduct an evacuation or shelter-in-place?
	1. Who makes the decision to evacuate or shelter-in-place?
	2. How is this effort communicated to your staff?
	3. How are staff trained to assist individuals with access and functional needs?
6. How will this incident affect your facility’s operations?
7. What are your organization’s employee accountability protocols?
8. What mutual aid agreements (MAA) will be activated during the incident?
9. Would this severe weather incident affect the command structure?
	1. Are there alternate locations for incident command?
10. How are response operations coordinated with local, state, and federal agencies?
	1. Who is responsible for this coordination?
11. What information would be passed on to the public?
	1. Who is responsible for informing the public?
	2. How quickly is the public notified?
	3. How is this messaging coordinated across the different agencies and organizations?
12. What role would your organization have in a Joint Information Center (JIC)?
	1. Would the storm affect JIC operations?
	2. Are there alternate locations for the JIC?
	3. What communication platforms are used to communicate to facility staff?
13. Does your organization have remote access to vital records?
	1. How can vital information trapped in your facility be retrieved?

# Module Three: Short Term and Continuous Recovery

## Scenario

### [Insert Month, Day, Year]: [Insert time + 48 hours]

The storm has officially passed, and the weather event significantly impacted your local area. News footage shows a massive debris trail along the [insert major roadway] corridor, including many damaged vehicles. Other footage from around [insert your location] shows significant damage to homes and commercial buildings, and some are partially collapse. The city, county, and state enact a disaster declaration; a federal disaster declaration is being discussed.

Your [insert primary work location] operation’s site sustained moderate damage from flying debris and water damage from rain leakage through broken windows. Likewise, most businesses within your area are without power, and there is no estimate on a return to service. Cellular service is intermittent because of system damage and high call volume.

Personnel are contacting their supervisors wondering when it will be safe to return to work, and many express hesitancies towards returning to work. Many staff members, including board members and senior supervisors are caught between rebuilding their homes post-tornado and trying to support your organization. Many employee vehicles were destroyed or the roads around them are blocked, hindering their ability to commute to the facility.

## Discussion Questions

1. Now that the storms have passed, what are your organization’s priorities?
2. What triggers the next steps of your business continuity plan?
	1. Who is primarily responsible for tracking business continuity procedures, and who is responsible for deciding next steps?
	2. Is there a procedure for management to meet and discuss departmental plans for progress in the aftermath of the tornado?
3. What communication or guidance does your organization expect from local, state, or federal authorities at this point?
4. What messaging is being sent out to employees at this point?
5. Does your organization have employee accountability protocols?
	1. Does your company’s emergency action plan (EAP) outline these accountability protocols?
	2. Who is responsible for overseeing and coordinating accountability checks?
6. Who are the essential personnel needed to get the facility functioning after this incident? Are there established relocation plans for them?
7. Does your organization have an established alternate workplace or telework plans?
8. What are the options and processes to fill gaps for unavailable staff; downed technology, Wi-Fi, or cellular systems; or other required resources?
9. Does your organization have orders of succession or delegations of authority procedures?
10. Does your organization have any MAAs or memoranda of understandings (MOUs)?
	1. What would trigger these?
	2. Which groups would be available to assist first?
	3. How do local, state, or federal emergency declarations impact your recovery attempts physically or financially?
11. What contracts does your organization have with third-party site cleanup services?
	1. Can organization recover the site without outside assistance?
12. How will your organization handle notifications of deceased or severely injured staff?
13. What procedures exist following a tornado to determine if the facility is safe for employees to return to?
	1. Who will determine that the facility is safe for staff to return for item collection?
	2. What building inspectors will you bring in to determine the facility safety? What kind of delay might you anticipate because of the high demand for building inspectors following this tornado?
	3. Does your organization have an agreement with a building inspector in preparation for a tornado recovery?
		1. Who is responsible for contacting the inspector following an emergency?
	4. Does your organization have a plan for employees who need to enter the facility to retrieve personal items?
	5. If the building is deemed unsafe, where will all the recovered and / or salvaged physical items go?
14. How long will it take for your organization to be reopen and reach steady state operations?
15. What financial estimates from damage and continuity expenditures (e.g., overtime, use of alternate space, etc.) can be made at this time?
16. What plans are in place to compensate staff who are told to stay home (i.e., those that are not supporting a mission essential function [MEF])?
	1. Is there a human resources (HR) guidance document or solution?
	2. Would there be guidance provided from headquarters?
17. How will you support your personnel’s psychological needs?
	1. Are there established plans to provide counseling services to employees?

## Scenario Update

### [Insert Month, Day, Year]: [Insert time + 2 weeks]

Two weeks after the tornados hit [insert your city], cleaning crews have cleared most of the roadways of mud, debris, and trees. Although they received a significant number of injured individuals, hospitals were not overwhelmed or damaged. Most of the damage affected single-family homes and some business buildings within the [insert region of your facility]. Construction supplies and physical labor are in high demand to rebuild the city.

Your facility’s power has been restored. Thankfully, most of the facility’s damage was cosmetic, but there is one section that is semi-exposed to the elements and unsuitable for work.

Some of your staff is requesting approval to work remotely at the homes of nearby family while their homes are restored. Others are requesting bereavement because of family members passing away during the tornado or from injuries sustained during the incident.

## Discussion Questions

1. What is your organization’s current operational status?
2. What is your assessed ability to continue providing your critical operations?
3. What are your organization’s information security concerns and solutions regarding compromised access control (i.e., protecting personnel files, sensitive operating documents, money, or high-value equipment)?
4. In the long term, how will your organization fill gaps resulting from damaged equipment or staff unable to return to work?
5. What are the options to support childcare and other family needs of employees?
	1. What staffing concerns would arise if there are school closures in your area?
	2. Is your organization prepared to offer childcare assistance?
6. What are the options for providing transportation for employees to report to work?
	1. Can your organization provide transportation assistance for staff willing to work but unable to travel because of damaged vehicles or blocked roads?
7. Is your organization participating in city, county, state, or federal initiatives that might provide your company financial aid or recovery resources?
	1. Who is responsible for tracking and applying for these opportunities?
	2. If you have the capacity, will you allow staff to volunteer in the greater community’s recovery process?
	3. Is your organization part of a Community Organization Active in a Disaster (COAD)?
8. Are there outside stakeholders that will need recovery updates?
	1. What type of messaging will be sent to stakeholders, and what method of dissemination will be used?
9. What additional long-term recovery issues is your organization currently considering?
10. Does your organization have a public information officer (PIO)?
	1. What protocols exist for alerting partner organizations to an incident?
	2. Are there protocols for addressing media inquiries?
	3. How do PIOs receive information from your damaged facilities? From your leadership?
	4. Do PIOs have pre-built templates for use in this kind of emergency?
	5. Would your organization use social media to provide updates? Does your media plan include incidents like this?
	6. Have your PIOs previously collaborated with other supporting organization’s PIOs?
11. Where does your organization stand within the supply chain?
	1. Will your closure have ramifications outside of your direct clients?
	2. Who are the other organizations that might be able to fill the backlog, and how are you communicating with them?
	3. How are you communicating with clients that your closure might be impact?
12. How is your organization tracking the lessons learned and best practices that arise from your response and recovery from this incident?
	1. Would your organization share this information with other entities? How would you share this information?
13. Will the organization play any part in memorial services or funerals? How will the organization handle company-led memorial services?
14. Who will handle damage assessment and salvage of the facility?
15. Will insurance / other agency representatives be included?
16. What are the damage assessment team’s priorities and guidance?
17. Are there liabilities that you are willing to assume?

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency  |
| **COAD** | Community Organizations Active in a Disaster |
| **CTEP** | CISA Tabletop Exercise Package |
| **EAP** | Emergency Action Plan |
| **EPT** | Exercise Planning Team |
| **ERG** | Emergency Response Group |
| **HR** | Human Resources |
| **ICS** | Incident Command System |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **MAA** | Mutual Aid Agreement |
| **MEF** | Mission Essential Function |
| **MOU** | Memorandum of Understanding |
| **NIMS** | National Incident Management System |
| **NWS** | National Weather Service |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise |

