

# AUDIT REPORT

## *Disaster Preparedness & Continuity* Information Technology 2022-2 - June 2022



### **Internal Audit Department**

City of Fort Smith, Arkansas  
Tracey Shockley, CFE, CCA  
Internal Audit Director

## Our Mission

We deliver independent, transparent, and professional audits in order to safeguard and improve the public's investment in the City of Fort Smith. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.

---

## BACKGROUND

### **What Is Disaster Preparedness? What is Continuity Information Technology?**

Disaster preparedness consists of a set of measures undertaken to better respond and cope with the immediate aftermath of a disaster, whether it be human-made or caused by natural hazards. The objective is to reduce loss of life and livelihoods.

Disasters can occur naturally, (e.g. tornadoes, hurricanes, earthquakes, floods, fires, or drought) or be human caused (e.g. mass shootings, chemical spills, or terrorist attacks). Preparing for responding to, and recovering from disasters and traumatic events is essential to the behavioral health of the City. With increasing population growth, rapid urbanisation, climate change, environmental degradation and widespread poverty, a growing number of people and assets are exposed to disasters.

Improved practice and response mechanisms save lives and strengthen the City's ability to reduce the impact of disasters. Understanding the occurrence and frequency of natural hazards, as well as the risks, vulnerabilities and potential impact on the community and its assets, help to improve preparedness.

Disaster preparedness typically focuses on continuity of operations planning (COOP), which ensures that essential operations can continue during an emergency situation or be resumed as quickly as possible after an emergency event. Continuity planning and preparation for Information Technology is a holistic approach to managing technology systems in the event of a major disruption/disaster.

One important tool for establishing robust COOP strategies is the disaster preparedness cycle, which outlines each important step of the recovery process.

### **Elements of an Effective Policy and Procedure**

1. Mitigation – involves taking action to prevent or reduce the effects of a disaster. This can include reinforcing buildings against wind damage, improving drainage and permanent barriers in flood-prone areas, or installing cybersecurity software to protect against digital threats.
  2. Prevention and preparedness – planning, training, and live drills are necessary tools in disaster preparedness. Training materials must be developed that explain what to do during a disaster, when to enact a plan, and more so that each member of the City is ready to support recovery efforts. Preparedness can also include an audit of vulnerabilities within the City that may leave it open to accidentail or intentional disasters.
  3. Response – during the response phase, disaster preparedness departments lead the implementation of their prevention and COOP strategies. Because operations are not functioning normally during disaster response, it's important that all team members are aware of their responsibilities, know where to go for accurate information, and understand how to communicate with each other and
-

- the public, if needed.
4. Recovery – begins after the disaster has ended. While normal business operations resume as much as possible, restoration efforts like rebuilding damaged structures and addressing long-term needs are also underway. During this stage, disaster preparedness the departments will examine what happened to create new mitigation strategies that better protect against similar events in the future.
  5. Continuity Phases – planning, tests, training and exercises; evaluation; and corrective action plans. These processes ensure consistency across all continuity plans/programs. It helps maintain resiliency, in responding quickly to an interruption. Saves money, time and the City's reputation.

## **Conclusion**

The objective of our audit was to evaluate the City's Disaster Preparedness and Continuity plan process. The City Administrator and the Interim ITS Department Head did not assist in providing even minimal information necessary for progressing with this audit. Additionally, the Interim ITS Department Head would not respond to meeting request or emails from Internal Audit.

The City and ITS should consider the following if it does not have it established in their plans:

- Continuity of operations (COOP) plans which are designed to help departments prevent or minimize interruptions of critical business functions and return to normal operations quickly after a disaster. (This was prepared by ITS and is still in draft form. Last update and finalization plan is not known)
  - The plans need to recognize the potential disaster and recognize the duration that could be system-wide loss of power and water, and regional impact. The City needs to be prepared for unexpected events with potentially high impacts.
  - The plan should include adequate resources, including staffing and supplies to respond to each complex type of disaster. The staff should be trained in each of the identified disasters to ensure they meet requirements. The plan should be able to meet the needs for staff. Such as food, lodging, minimal dress, and possible child care.
  - All Departments should create continuity of operations (COOP) plans. This important because it enables departments to continue operating effectively in the case of a disaster.
  - The plan should include how to assist with reaching vulnerable populations before, during and/or after a disaster. Engage with community organizations to assist in educating and reaching vulnerable populations before, during and after a disaster. The City can leverage these relationships to ensure people who need assistance the most have access to information and resources.
  - All departments and personnel should have training in the different areas of disaster several times a year.
  - The data backups should be tested at least quarterly, preferably after each data backup to ensure that the City can be up and operational after a disaster.
-