ERS®
EMPLOYEES RETIREMENT SYSTEM OF TEXAS

Continuity of Operations (COOP) Audit

#2022-03

August 23, 2023

ERS Internal Audit Division

From the Director:

Internal Audit has completed its audit over Continuity of Operations (COOP). Based on the audit scope areas reviewed, internal controls require improvement and only partially address significant risks related to continuity of mission essential functions including: .

1) Scope of current Business Impact Analysis (BIA) should be narrowed to allow for a more detailed assessment and response to event level disruptions. (Significant)

Other matters deemed less significant were communicated with management directly. We thank the Enterprise Planning Office and Information Systems Division for their courtesy and cooperation extended to us during the review.

Sincerely,

Anthony Chavez

Anthony Chavez, CIA, CGAP, CRMA

Director, Internal Audit Division

Table of Contents

Objectives and Summary Results

The objective of a Continuity of Operations Plan (COOP) is to ensure that an organization can continue to serve its customers, maintain its operations, and fulfill its mission even during and after a disruptive event.
- Federal Emergency Management Agency

Audit Objective: To determine if processes and procedures are in place to ensure essential services continue to be provided in the event of a disruption.

Overall Results: Controls are in place to ensure continuity of mission essential functions in event of disruption, however, improvements are needed over business analysis to provide greater detailed mitigation and response strategies. **(Satisfactory)**

SCOPE AREA	SUB-OBJECTIVES		RESULTS/RATING
COOP Development	• Do Mission Essential Functions align with key ERS deliverables? • Are critical applications aligned to Mission Essential Functions? • Are prioritizations of applications, recovery times and data backups aligned with Continuity Plan objectives?	Satisfactory	• COOP is reviewed and approved biannually. • COOP periodically submitted to State Office of Risk Management for periodic review. • COOP addresses key operational elements including essential records retrieval and devolution of control & leadership. • *See Appendix A*
COOP Maintenance	• Is the plan reviewed at a frequency and methodology that aligns with best practices and agency objectives? • Is the plan communicated to key stakeholders to enable efficient activation and execution of the plan in the event of disruption?	Needs Improvement	• Business Impact Analysis needs improvement. *See Observation #1.*

Audit Rating Legend:

Exemplary - Effective, sustainable process

Satisfactory - Internal controls effective and working as intended

Needs Improvement - Internal controls partially effective

Unsatisfactory - Entire control framework in need of repair

Continuity of Operations Background

The goal of a Continuity of Operations Plan (COOP) is to ensure citizens continue to receive essential services/goods in the event of a disaster. A COOP is intended to ensure readiness and preparedness to avert or withstand any disaster or disruption to essential functions when it occurs. To assist in developing and maintaining a strong COOP Federal guidance recommends performing the following:

Continuity of Operations Plan: Each state agency shall work with the State Office of Risk Management to develop an agency -level continuity of operations plan that outlines procedures to keep the agency operational in case of disruptions to production, finance, administration, or other essential operations. The plan must include detailed information regarding resumption of essential services after a catastrophe *(Texas Labor Code 412.054)*

a) Entity-wide Risk Assessment to identify essential functions

b) Business Process Analysis (BPA) to describe process flow including identification of key systems and personnel over essential functions.

c) Business Impact Analysis (BIA) to identify specific threats and hazards (i.e. ransomware, natural disaster) related to key processes that may disrupt the delivery of specific services/goods and develop mitigation/recovery strategies.

MISSION ESSENTIAL FUNCTIONS (MEFs)

A COOP is not intended or designed to ensure all ERS services continue in the event of a disaster. Rather only those services identified as both impactful and urgent particularly as it relates to health and safety. Although no regulatory timeline for "urgent" exists, generally it is measured in hours/days vs. weeks. ERS current target of resumption of service is < 72 hours.

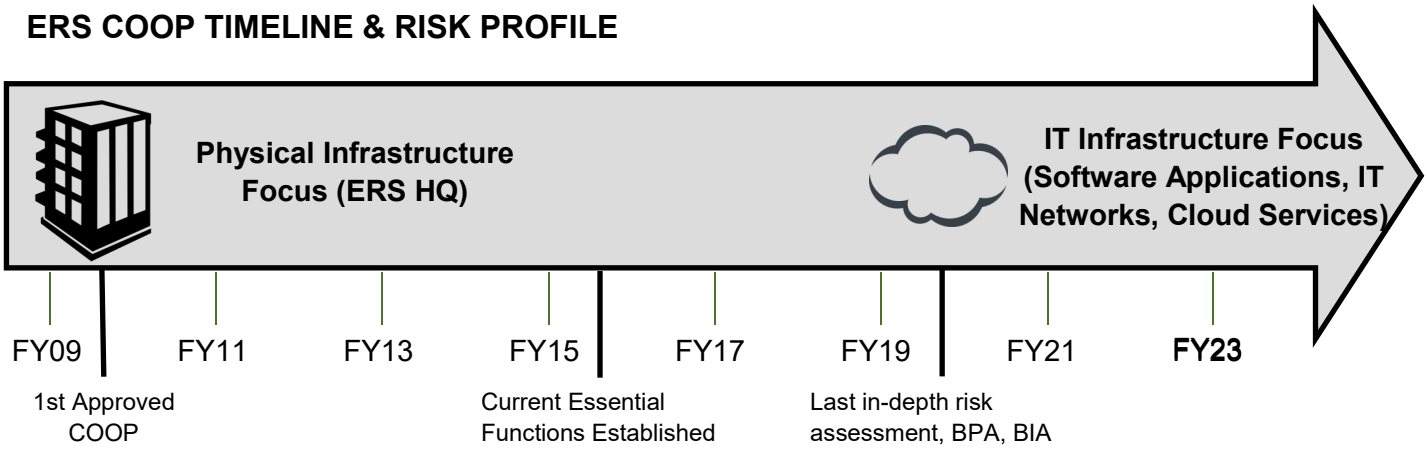
The State of Texas has established essential functions to preserve continuity of government. ERS MEFs do not directly support performance of Texas Essential Functions and ERS is lower risk from a statewide perspective. Currently ERS has identified four (4) MEFs with two (2) that directly impact services/benefits to ERS members, two (2) related to vendor reimbursement and one (1) for internal investment activities.

State of Texas Essential Functions*
(Continuity of Government)

- Maintain continuity of government (critical government leadership elements/key office succession)
- Provide visible leadership
- Defend Texas Constitution
- Maintain effective relationships with neighbors/partners**
- Maintain law and order
- Ensure availability of emergency services
- Maintain economic stability **
- Ensure availability of critical services (health, safety, welfare, critical infrastructure)

**Texas State Office of Risk Management Continuity Policy Directive*
*** Functions indirectly supported by ERS as determined by ERS Internal Audit*

ERS COOP TIMELINE & RISK PROFILE



Observation 1: Scope of current Business Impact Analysis (BIA) should be narrowed to allow for a more detailed assessment and response to event-level disruptions. (Significant)

Program Risk	• Member services and benefits unable to be provided for extended period.
Inherent Risk	• Multiple types of threats and hazards that could potentially disrupt services • Service delivery may cross multiple divisions and/or multiple business IT applications • External partners may assist in service delivery • Severity of disruption may vary based on timing of event (i.e. beginning or end of month) • Identify threats/disruptions may never occur.
Background	• A Business Impact Analysis (BIA) for COOP assists organizations in identifying specific threats and hazards (i.e. ransomware, natural disaster) that may disrupt the delivery of specific services/goods. • Analysis of threats/hazards should be specific to key process components (people, information systems, external partners) used to deliver services (essential functions).

Control Observations	• The current BIA incorporates a broader entity-level risks that encompass the entire organization rather than addressing the event-specific risks related to delivering key services (essential functions).
	• **Failure to identify unique characteristics associated with each event, limited the effectiveness of the risk management process including mitigation and response.**
	• Specifically, the following conditions were identified:
	  ◦ Mitigation plans for some essential functions prioritized communicating to ERS members that services would not be available rather than plans to return operations to normal including alternative methods of delivery.
	  ◦ Ransomware testing was not fully developed and did not account for event-specific scenarios. The last ransomware test performed in January 2020 did not include threats to information system components that directly support delivery of essential services. In addition estimated time for recovery (after triage) was one (1) hour. Although recovery time is dependent on severity of ransomware, ransomware trend reports note recovery typically takes days/ weeks, not hours.
	  ◦ Review of key external partners (vendors) disaster recovery results did not assess/incorporate recovery time for downed software applications with ERS recovery time objectives.

Recommendation	The Enterprise Planning Office should implement the following: • Incorporate an event-level impact analysis on key components of mission essential processes • Evaluate recovery time objectives to ensure capabilities align with acceptable timelines for both internal and external resources • Recovery strategies should include detailed action plans to restore operations
Management Action Plan	*Management Response:* Management agrees with observation that Business Impact Analysis should be improved to better align with event risk. *Management Action Plan:* Management will adjust its business impact analysis to provided a more focused assessment on event risk. In addition the following specific actions will be taken to address detailed observations noted. • Management agrees with the need to prioritize restoration of essential services for ERS members and retirees in the event of a service disruption. Management will work with the impacted business and support areas to develop action plans to restore essential services first, while also communicating the disruption in services to ERS members and retirees. • Management acknowledges the previous ransomware test exercise focused on impacts to certain network drives and did not specifically address disruptions to mission essential services that impact ERS members and retirees. Management will work with Information Systems and other impacted staff to create ransomware test exercises with threats to applications or systems that directly support mission essential services. • Management acknowledges that recovery time objectives (RTOs) vary across the critical applications that support essential functions. Management will review the current RTOs for critical applications with Information Systems staff to more appropriately align the internal RTO with the RTO stated in the vendor's current contract. Management will also coordinate with Information Systems and other impacted divisions on the order in which certain applications will be restored in the event of a disruption to essential functions. Responsible Position: Director of Enterprise Planning Office Implementation Date: January 31, 2024

Scope and Methodology

We performed this audit in accordance with the FY23 annual audit plan. Internal control activities reviewed include those in place during the last in-depth risk assessment (FY20) up to the time of audit fieldwork testing which ended June 2023.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

A defined set of control objectives was utilized to focus on operational goals for the identified scope. The Committee of Sponsoring Organizations of the Treadway Commission Internal Control Integrated Framework was the basis for internal control assessment. Our Internal Audit opinion is an assessment of the condition of the overall control environment based on the effectiveness of internal control activities through the audit period and the degree to which defined control objectives are being met. Our Internal Audit opinion is not a guarantee of operational effectiveness or regulatory compliance, particularly in areas not included in the scope of this audit.

This audit included a review of internal controls considered relevant to audit objectives including review of statutes, policies and procedures, interviews with management and staff, data analysis, and testing procedures.

Related Audits

- Disaster Recovery Audit (Report #2022-06)

Appendix A - Control Framework

Risk:	ERS COOP does not align with ERS Leadership's goals and expectations
Key Control:	ERS Continuity of Operations Plan (COOP) is reviewed and approved bi-annually by ERS Executive Director

Risk:	COOP is incomplete and does not fully address all required elements.
Key Control:	COOP submitted to State Office of Risk Management for periodic review to gain feedback on compliance with FEMA guidance