# *Office of Internal Audit*

## *COOP Plan Audit*

February 6, 2019

Reviewed and approved by Yikchau Sze, OIA Director

Yikchau Sze

Electronically Signed 2/7/2019

| Board | Mtg Date | Item # |
|---|---|---|
| AUD | 3.21.19 | 4A |

## Executive Summary

We have completed an audit of the Department of Employee Trust Fund's (ETF) Continuity of Operations Plan (COOP or "the Plan"). This audit was conducted to address continuity of operations risks identified in the 2017-2019 Biennial Audit Plan. An effective COOP Plan is necessary to ensure ETF can resume essential business services under all threats and conditions. Essential business services are those that must be recovered within 30 days of Plan activation.

The COOP function at ETF primarily resides in the Secretary's Office, with the Agency Continuity Manager, Deputy Agency Continuity Manager, and Assistant Agency Continuity Manager. As *COOP Implementation Team Directors*, these individuals are responsible for the overall development and oversight of ETF's COOP Plan.

The following table illustrates our assessment of ETF's COOP Plan, given the scope of our audit:

| Audit Scope | Process Description | Assessment |
|---|---|---|
| COOP Governance | ETF has a defined governance structure directly supported by the Secretary's Office. The COOP Implementation Team Directors involve key stakeholders in decision making and meet regularly with key stakeholders and subject matter experts to address emerging issues and provide oversight. | Low risk exposure.<br>Could be further strengthened by integrating COOP into ETF's strategic and operational plans. |
| Business Impact Analysis & Essential Business Services Identification | ETF conducted a business impact analysis in 2012 to initially identify ETF's essential business services. The COOP Plan was formally reviewed in 2013 and 2018. | Medium risk exposure.<br>Could be strengthened by requiring division/office management review of all essential business services, including any updates and revisions to Sustainable Planner content. |

| Audit Scope | Process Description | Assessment |
|---|---|---|
| COOP Plan Development | ETF has developed an evolving and adaptable COOP Plan and continues to develop workable solutions to Department of Administration (DOA) requirements, using available facility and Information Technology (IT) services.<br>ETF has developed a practical Work from Home (WFH) Plan. | High risk exposure.<br>To reduce risk, ETF should develop a comprehensive IT Disaster Recovery Plan that is integrated with enterprise COOP planning efforts, for all critical IT services. |
| COOP Plan Maintenance | ETF has a documented Plan, including Call Trees and other Plan resources that require frequent revisions. The Plan is maintained electronically in the Sustainable Planner software and in other locations. | Low risk exposure.<br>Could be strengthened by ensuring the Plan is complete, current, and strategically organized for easy access and maintenance. |
| COOP Plan Testing | ETF has conducted annual testing exercises on functions such as the Call Center, messaging capabilities, and tourniquet training. After-Action Reports were prepared after each exercise. These reports summarize the event, participants and follow-up action items. | Medium risk exposure.<br>Could be strengthened by implementing a systematic way of testing to ensure adequate coverage of essential business services to ensure that COOP Implementation Team and Recovery Team Members are adequately prepared, trained, and confident in their recovery plan efforts. |

## Background

ETF's COOP Plan is part of a statewide governmental preparedness initiative. The DOA State Continuity of Government (COG) Director issued a *COOP Guidance Directive*, dated April 17, 2018, documenting the continuity requirements for DOA and executive agencies. These guidelines are based on Federal Emergency Management Agency (FEMA) best practices issued by the Department of Homeland Security in a *Continuity Guidance Circular,* dated February 2018.

Examples of agency requirements included in the DOA *COOP Guidance Directive* are:

- Establish and maintain a Business Continuity Plan and an Information Technology Disaster Recovery Plan that comports with FEMA guidance and DOA COOP/COG plans and procedures;
- Utilize Sustainable Planner continuity software as a system of record in developing and/or updating COOP/COG plans; and
- Conduct a yearly COOP/COG exercise under the supervision of DOA's COG Director and develop a multi-year training and exercise plan.

The Directive further outlines additional requirements for DOA and executive agencies to achieve the COOP/COG goals.

### DOA Roles and Responsibilities and Impacts on ETF

The DOA COG Director is responsible for issuing COOP requirements and guidance to executive agencies, and for serving as a resource to agencies in their planning and testing efforts. DOA also serves as a key business partner and service provider for ETF facility and IT related services.

*Facility Services*

A FEMA best practice is to identify an alternate location that is not the primary operating facility, where an organization can continue or resume essential services. Upon Plan activation, DOA indicated it would partner with agencies to identify an alternate location to resume operations.

Prior to ETF's move to the Hill Farms State Office Building (HFSOB), ETF worked extensively with the Department of Transportation (DOT) to secure a pre-determined alternate location. The HFSOB no longer serves as a viable alternate location. DOA's current guidance is for agencies not to make advance alternate site agreements of their own, but to rely on DOA to determine a suitable alternate location post-disaster. However, ETF has partnered with the DOA Bureau of Publishing and Distribution (BPAD) to secure an alternate location for the Supply & Mail Services Section and Record and Imaging services only. A formal cooperative agreement has been finalized and is awaiting approval from BPAD. Although this is a mitigating control, it is limited in the scope of essential business services that it covers.

To further mitigate the risk of not having a full pre-determined alternate location, the COOP Implementation Team Directors and IT Director have developed a WFH Plan that is currently being piloted. The WFH Plan is designed to provide all Recovery Team Members with a COOP assigned laptop that will remain at home. Participants are required to work from home at least one day every two weeks to test the login and system access procedures for effectiveness. They also must adhere to ETF's formal WFH policy. Additionally, ETF will house a small inventory of ETF laptops in a DOA building for staff to access upon Plan activation. Although the WFH Plan is still in a pilot stage, it appears to be practical and well thought out.

*IT Services*
The DOA, Division of Enterprise Technology (DOA-DET) serves as the enterprise IT service provider for mainframe, STAR (the State's enterprise accounting system), email, file, print, and other essential IT system operations. Consequently, the DOA-DETs continuity planning significantly impacts ETF's ability to resume operations. ETF has several essential systems with recovery time objectives (RTO) of less than one hour hosted on the DOA-DET mainframe, including the Wisconsin Employee Benefit System (WEBS) and Benefit Payment System (BPS). WEBS records retirement activity for all Member annuity accounts, and BPS tracks all Member annuity payment activity. The resumption of STAR and email services for ETF also have an RTO of less than one hour.

On October 10, 2018, DOA-DET held an *Information Technology Disaster Recovery Enterprise Exercise*. The exercises tested the primary data center electrical power and back-up generation failures, with a purpose of supporting COOP/COG requirements from the technology service perspective. The DOA-DET issued an After-Action Report/Improvement Plan, published November 19, 2018, identifying improvement actions that, until fully implemented by DOA-DET, could significantly impact ETF's ability to resume essential business services, such as:

- "Develop on-going IT Disaster Recovery training plan.
- DOA-COOP/COG and DOA-DET to provide consultation and collaboration with user agencies to review agency performance expectations, reset priorities as necessary, and complete Disaster Recovery plans at the application level and association infrastructure. These plans are to include dependencies and interfaces with other applications and systems.
- Identify a management process to resolve in advance potential cross-agency application recovery prioritization conflicts.
- Provide a replicated data copy for disaster recovery purposes in Milwaukee data center of the configuration management database that operates at Femrite primary data center so that in the event of a disaster affecting the primary data center this tool for management services may be recovered quickly."

## ETF Roles and Responsibilities

*Plan Governance Structure*
ETF is responsible for appointing an Agency Continuity Manager and identifying COOP Assigned Staff responsible for resuming Plan operations. Although the COOP Plan and governance structure continually evolves, the current COOP Assigned Staff include the COOP Policy Team, the COOP Implementation Team, and Recovery Teams.

| COOP Policy Team | |
|---|---|
| **Members** | **Responsibilities** |
| • Secretary<br>• Deputy Secretary<br>• Assistant Deputy Secretary/Agency Continuity Manager<br>• Chief Legal Counsel | • Approve recovery strategies<br>• Declare an emergency and activate the Plan or portions of the Plan<br>• Make policy decisions on human resource issues<br>• Approve media communications<br>• Evaluate the expected duration of the emergency<br>• Participate in and approve reconstitution plans |
| **COOP Implementation Team** | |
| **Members** | **Responsibilities** |
| • COOP Implementation Team Directors:<br>○ Agency Continuity Manager<br>○ Deputy Agency Continuity Manager<br>○ Assistant Agency Continuity Manager<br>• Information Technology Team<br>• Facilities Team<br>• Telecom Team<br>• Budget/Procurement Team<br>• Communications Team | • Knowledgeable of COOP Plan contents.<br>• Meet monthly to determine preparedness priorities, develop work plans and review COOP Policy<br>• Ensure the development and maintenance of COOP Plan, including familiarity with accessing Sustainable Planner for COOP purposes<br>• Ensure Recovery Teams are adequately trained; conduct required testing and exercises.<br>• Manage and direct the team's Plan implementation<br>• Recommend policy directions to the Policy team<br>• Activate and de-activate recovery teams<br>• Assess and determine priorities<br>• Manage agency resources<br>• Authorize internal communications |

| Recovery Team Members | |
|---|---|
| **Members** | **Responsibilities** |
| *Call Tree Leads/Back-ups:*<br>• Division of Management Services<br>• Division of Retirement Services<br>• Division of Trust Finance<br>• Office of Communications | • Participate in identifying essential business services, including the recovery time objectives, and any resources, records, supporting steps/tasks and assigned recovery teams<br>• Use Call Trees to contact Recovery Team Members<br>• Recovery of assigned service following the procedures set forth in the Plan<br>• Participate in WFH Plan and abide by policy expectations |
| *All Other COOP Assigned Staff* | • Recovery of assigned service following the procedures set forth in the Plan<br>• Participate in WFH Plan and abide by policy expectations |

*Essential Business Services*
A FEMA best practice and DOA requirement is to conduct a business impact analysis to identify an organization’s essential services, or functions that must be recovered within 30 days of Plan activation. ETF conducted a business impact analysis in 2012 to identify their essential business services and facilitated formal updates to them in 2013 and 2018.

The COOP Implementation Team Directors define the planning, maintenance, annual testing and training requirements surrounding the essential business services for ETF. The Deputy Agency Continuity Manager largely facilitates the implementation of these requirements. Division/office management, in conjunction with Recovery Team Members, is responsible for identifying program specific essential business services, documenting them in Sustainable Planner, and reviewing and updating them periodically.

*Plan Documentation*
ETF is required to use Sustainable Planner, a DOA-hosted system, to document its identified and prioritized essential business services, along with the dependencies, workflows and resources supporting them. ETF also uses a COOP SharePoint site and a restricted folder on the shared drive to maintain some Plan documentation. While Sustainable Planner can be accessed by select COOP Assigned Staff only, the COOP SharePoint site is accessible to all ETF employees, and access to the restricted folder is

restricted to COOP Implementation Team Directors and other management. The COOP Implementation Team Directors are in the process of developing a strategy on where Plan documentation should be maintained for each of these sites.

ETF is using RAVE, a DOA-hosted emergency alert system, to communicate COOP messages to all ETF employees. Call Trees document the communication structure for COOP Assigned Staff.

*Review and Testing of Plan*
A FEMA best practice and DOA requirement is to conduct an annual review and test of the Plan, including IT systems. The formal review of identified essential business services in 2013 and 2018, included varying levels of division/office management review of the Recovery Team's Plans. ETF has not developed a formal IT Disaster Recovery Plan or strategy for resumption of its critical IT Systems.

Historically, the COOP Implementation Team Directors have planned annual testing exercises with input from the DOA COG Director. Going forward, the COOP Implementation Team Directors intend to adopt a multi-year, risk-based testing approach.

## Audit Objective and Scope

Our audit was conducted in conformance with the International Standards for Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.

The audit objective was to provide assurance that ETF's essential business services are functional during an event that disrupts ETF's normal operations, and to identify actions to enhance the effectiveness of the COOP Plan.

The scope of our audit included the following areas of the Plan:

- COOP governance;
- Business impact analysis;
- Essential business services identification; and
- Development, maintenance and testing of the Plan.

The scope of our audit excluded emergency management.

We used the DOA *COOP Guidance Directive* and FEMA best practices as the reference framework for our audit.

### Results and Recommendations

## Positive Results

We found ETF has an effective COOP control environment, such as a defined governance structure directly supported by the Secretary's Office; competent COOP Implementation Team Directors that are knowledgeable in COOP best practices, well trained, and dedicated to continually improve ETF's Plan; and knowledgeable Recovery Teams that know how to perform their essential business services. Additionally, ETF was able to overcome challenges presented by certain DOA requirements, and limitations on certain DOA-provided services. For example, ETF has developed a practical WFH Plan to respond to DOA's guidance, which prevents ETF from providing advanced notice of an alternate location to recover all essential business services.

## Findings, Recommendations and Management Responses:

| **Finding** | **Risk/Effect** |
|---|---|
| 1. ***IT Disaster Recovery Planning***<br>We found ETF has not developed a formal IT Disaster Recovery Plan or a strategy for resumption of its critical IT Systems.<br>As stated in the Background section, ETF relies on DOA-DET for mainframe, STAR, email, file, and print services. The results from the recently completed IT Disaster Recovery Enterprise Exercise heightened the need for ETF to assess the assurances provided by DOA-DET and determine how to develop disaster recovery capability that can ensure critical IT systems can be resumed to support ETF essential business services, upon Plan activation. | Without a comprehensive IT Disaster Recovery Plan and strategy, ETF's critical IT systems may not be fully recovered, which may delay or prevent the Recovery Team's ability to resume ETF's essential business services. |
| **Recommendation**<br>The COOP Implementation Team Directors, as the owner of the COOP Plan, should ensure ETF has a comprehensive IT disaster recovery strategy that is integrated with enterprise COOP Planning efforts for all critical ETF and DOA-DET provided IT services, and develop a process to document and implement the IT Disaster Recovery Plan. | |
| **Management Response**<br>Management agrees. The Bureau of Information Technology Services (BITS) has outlined a process for documenting and implementing ETF's IT Disaster Recovery Plan that will include:<br>• Finalized plan and procedure documentation for the COOP WFH Plan<br>• Recommendations for a more robust alternative to the current DET solution for back-up of business applications | |

- Documentation of DET- and ETF-specific recovery responsibilities
- A draft agreement for DET to secure an IT-focused alternate site, network set-up plan, and all other necessary DET services needed to recover agency headquarters

**Responsible Staff:** BITS Chief Information Officer, COOP Implementation Team Directors

**Completion Date:** December 31, 2019

| **Finding** | **Risk/Effect** |
|---|---|
| ***2. COOP Plan Annual Review and Systematic Testing***<br>A DOA requirement is to conduct an annual review of identified essential business services, and an annual DOA-facilitated exercise addressing one of the agency's essential business services. While Sustainable Planner documentation continues to be developed, a systematic review of the existing Plan content, which includes identified essential business services, can still be performed. We found although the latest formal review was performed in 2018, there were varying levels of involvement and review by division/office management, and prior to that the last formal review was done in 2013. We also found there is no secondary review of new and revised Plan content.<br>Although ETF performs annual testing exercises, we found there has been no systematic testing that provides sufficient coverage for the essential business services. Recovery Team Members indicated a testing exercise would help them build confidence with their recovery plan efforts. We are aware that COOP Implementation Team Directors have developed a risk-based testing tool that will be utilized beginning in 2019. | Without adequate review of essential business services by division/office management, there could be essential services that are not properly identified in the Plan and, therefore, would not be included during Plan activation. Also, non-essential services may be identified as essential, resulting in the use of valuable resources during Plan activation.<br>Without adequate testing that includes a broad range of COOP Implementation Team and Recovery Team Staff, there could be essential services that cannot be performed, and |

| | |
|---|---|
| | COOP Implementation Team and Recovery Team Members may lack confidence in their ability to fully resume operations. |

**Recommendation**

To ensure the accuracy and completeness of COOP Plan content, the COOP Implementation Team Directors should develop a process that requires division/office management to conduct a secondary review of the Plan content and implement a consistent annual review of all existing and updated content maintained in Sustainable Planner. The annual review should include a reassessment of all essential and non-essential services to identify any needed Plan changes.

Continue efforts to develop a systematic way to identify a risk-based, multi-year testing strategy to ensure appropriate coverage of the essential business services so that all COOP Implementation Team and Recovery Team Members are adequately prepared and trained.

**Management Response**

Management agrees. The Sustainable Planner application only shows completion status of component surveys and lacks a reporting query for review status. A process improvement will be made by the Deputy Agency Continuity Manager to ensure validation by all COOP management (including all Call Tree Leads/Back-ups, Business Service Plan Owners and division management) is documented in our COOP records.

**Responsible Staff:** Deputy Agency Continuity Manager

**Completion Date:** December 31, 2019

| **Finding** | **Risk/Effect** |
|---|---|
| ***3. COOP Plan Documentation***<br>We found several COOP Plan documents were outdated and incomplete. For example, the Facility Manager Checklist, Power Outage Protocols, and Call Center Outage Contingency Plan documents all need updating. A Delegations of Authority Plan needs to be developed.<br>Plan documentation is currently housed in three areas—Sustainable Planner, COOP SharePoint site, and/or a restricted | Without complete, current and accessible Plan documentation, COOP Assigned Staff may not have the information and resources needed to efficiently implement |

| | |
|---|---|
| folder on the shared drive. We found there is no strategy on where specific Plan documents will be saved. This can result in confusion for COOP Assigned Staff needing to access relevant information, and potential duplication of effort. For example, the same Call Tree documentation is currently maintained in all three of these locations, resulting in duplication of effort to maintain.<br>While some COOP documents need revising, several key documents, such as the Call Trees, have been kept current. Also, we are aware that the Deputy Agency Continuity Director has developed a strategy to update the Plan and has identified tools that could assist in the maintenance of the Plan. | the Plan and resume essential business services. Outdated resources could be used, resulting in confusion and incomplete execution of the Plan. |
| **Recommendation**<br>The COOP Implementation Team Directors continue efforts to bring the Plan up to date and develop a long-term strategy to ensure:<br>• The Plan is complete and stays current;<br>• Only the authoritative copy is maintained; and<br>• The Plan is strategically organized for easy access and maintenance. | |
| **Management Response**<br>Management agrees. Content reorganization in the shared drive was completed. The COOP Team is in the process of determining the appropriate locations for housing all official COOP Plan content to ensure a systematic approach to content management including documentation of the frequency and validation of content updating. Content management will also include dedicated work sessions to complete the development of the ETF Connect COOP site on the Share Point platform. The revised Facilities Checklist has been drafted and re-scoped so that two separate Advance Teams – one facilities- and safety-specific, the other IT-specific - now assume responsibility for advance alternate site preparations in the event DOA COOP/COG assigns one to ETF.<br>**Responsible Staff:** Deputy Agency Continuity Manager, COOP Implementation Team<br>**Completion Date:** December 31, 2019 | |

### *Process Improvement Observations*

Minor potential process improvements were communicated to the COOP Implementation Team Directors for consideration, including the development of a mitigation strategy to digitize all batch print jobs needed to complete manual final calculations of retirement annuities.

.

## Audit Methodology

The OIA conducted this audit by:

- obtaining an understanding of the DOA guidelines and FEMA best practices for state agency COOP Plans;
- obtaining an understanding of ETF's process for conducting a business impact analysis to identify essential business services, and for maintaining and testing the Plan;
- reviewing ETF's readiness and compliance with DOA guidelines and FEMA best practices, by interviewing key staff and reviewing Plan documentation;
- reviewing ETF's essential business services documented in Sustainable Planner and ETF's SharePoint site for reasonableness and completeness; and
- reviewing ETF's WFH Plan.