Business Continuity Audit Report
22-06

Internal Audit Division
November 2022

Texas Department of Motor Vehicles

Business Continuity Audit Report, 22-06

Executive Summary

Continuity planning allows an organization to maintain operations during and after a disruptive event such as a natural disaster, pandemic, or terrorist attack. A Continuity of Operations Plan (Plan) is the roadmap that documents how an organization will perform operations during the disruption period. At the Texas Department of Motor Vehicles (TxDMV), this Plan is the responsibility of the Business Continuity Coordinator, who reports to the Chief Information Security Officer in the Information Technology Services Division.

The objective of the audit was to determine whether TxDMV has designed and implemented controls to ensure operational resilience in accordance with state requirements and best practices. The audit scope was March 2021 to August 2022.

WHAT WE FOUND

The audit found that business continuity planning processes are at a <u>Level 2 – Informal and Reactive</u>: The function achieves its purpose with basic processes and activities that are not very organized or followed. The Internal Audit Division (IAD) issued two results:

- **Result #1**: The Department performs a comprehensive risk assessment but should standardize Business Process and Business Impact Analysis as part of the Continuity of Operations planning process

- **Result #2**: The Department should ensure that the Continuity of Operations Plan includes all required elements and establish a schedule for testing and maintenance tasks

WHAT WE RECOMMEND

IAD made two **HIGH** priority recommendations to strengthen continuity planning processes:

Facilitate business process analysis in a systematic manner for all Department divisions.

Update the continuity multi-year strategic plan to ensure it addresses all elements and implement training so employees are aware of their roles.

Table of Contents

Background

Continuity planning allows an organization to maintain operations during and after a disruptive event such as a natural disaster, pandemic, or terrorist attack. Multiple plans and documents contribute to preparing for organizational resilience. These can include:

- Continuity of Operations Plan: a roadmap that documents how an organization will perform essential functions during a disruption to maintain operations;

- Occupant Emergency Plan/Facility Emergency Plan: procedures to safeguard life and property in and around a facility during emergencies (for example, evacuation protocols);

- Pandemic Plan: a strategy to mitigate illness and impact on staff while maintaining essential functions in a period of significant absenteeism; and

- Disaster Recovery Plan: steps to restore information systems following major disruptions that prevent access to primary facility infrastructure.

The Continuity of Operations Plan and the Disaster Recovery Plan (DRP) are related but not interchangeable. The Continuity of Operations Plan addresses business processes and operations. The DRP is specific to information systems (servers, applications, etc.) The systems covered by the DRP might be required for the operation of essential functions, making the DRP a component of the Continuity of Operations Plan.

Within the Texas Department of Motor Vehicles (TxDMV or Department), the Continuity of Operations Plan and the Disaster Recovery Plan are the responsibility of the Business Continuity Coordinator, who reports to the Chief Information Security Officer in the Information Technology Services Division. The Continuity of Operations Plan also includes a pandemic plan. Procedures related to on-site safety during an emergency are included in the Safety Manual, which is overseen by the Safety Officer within the Finance and Administrative Services Division.

The Department contracts with an outside vendor to oversee and administer the disaster recovery program. The contract is managed by the Department of Information Resources. Because these tasks are conducted outside TxDMV, this audit focuses on the Continuity of Operations Plan.

Audit Engagement Team

The audit was performed by Naomi Marmell (Internal Audit Contractor), and Salem Chuah (Internal Audit Director).

Audit Results

Audit Result #1: The Department performs a comprehensive risk assessment but should standardize Business Process and Business Impact Analysis as part of the Continuity of Operations planning process
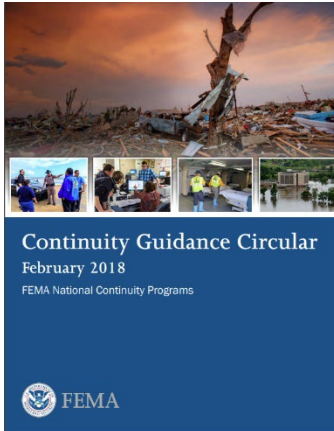
The State Office of Risk Management requires state agencies to adhere to the continuity of operations standards set by the Federal Emergency Management Agency (FEMA) Continuity Guidance Circular (Circular). According to the Circular, organizations should conduct a risk assessment, a business process analysis, and a business impact analysis, with the end goal of identifying essential functions. This is a requirement prior to drafting a Continuity of Operations Plan (Plan), which ensures that processes are in place to prevent risks from disrupting the essential functions. While the Circular does not specify how each step should be completed, it includes a list of questions that each step should answer.

The Department completed a comprehensive risk assessment; however, the Business Process Analysis and Business Impact Analysis should be completed in a systematic manner.
The Plan includes a risk assessment, Business Process Analysis (BPA), and a Business Impact Analysis (BIA) as required. The risk assessment addressed all four questions included in the FEMA Circular: it identifies threats and hazards, describes the effect to the Department, estimates likelihood, and calculates overall risk.

However, the BPAs were inconsistent and incomplete, because divisions provided different information and did not answer all FEMA Circular questions. One division provided step-by-step instructions for multiple processes but did not identify inputs and outputs or necessary resources. Some divisions provided their own continuity plans rather than an assessment of their processes. Other divisions included inputs, outputs and necessary resources but did not provide information on their processes and had no documents less than five years old.

The Circular states that performing a BPA should be approached systematically and with a focus on clearly describing the details regarding how each task and activity is performed. The Plan itself states that Business Process Analysis provide procedures detailed enough to enable another similarly trained individual, other than the person primarily responsible for the work, to follow them.

Also, the Business Impact Analysis groups functions together so that specific functions and processes are indistinguishable. The Plan lists specific essential functions, but there is no documentation of how these functions were identified and prioritized. For example, the BIA groups divisions such as Enforcement, Hearings, and Internal Audit together and treats these

divisions all as equally essential, while the Plan only includes Enforcement and Hearings. Additionally, the BIA did not assess risk vulnerabilities at the function or process level, as required by the Circular.

The Business Continuity Coordinator (BCC) noted that there are no documented procedures for the review and maintenance of the Plan, including planning activities such as the BPAs and BIAs. There has been turnover in the BCC position, with the prior BCC serving from April 2021 through September 2022, as well as turnover in the Chief Information Security Officer during this time.

As a result, the priorities in the Plan do not reflect the documentation contained within the BIA and auditors cannot provide assurance that the mitigation plans directly address the risks specific to essential functions. Also, the BPA is intended to provide guidance in carrying out essential functions if usual personnel are not available. Without this guidance, these functions could be interrupted during a disaster.

Recommendation
1.   Establish and document procedures for the continuity planning process, including the use of Business Process Analysis templates for all Department divisions and incorporation into the Continuity of Operations Plan **(HIGH)**.

Audit Result #2: The Department should ensure that the Continuity of Operations Plan includes all required elements and establish a schedule for testing and maintenance tasks

In addition to the FEMA Circular, FEMA also publishes a Continuity Assessment Tool. This tool distills the requirements in the Circular into a set of elements that can be tested and evaluated. Each element is rated on a ten-point scale divided into three categories: red (zero to three points), yellow (four to seven points), and green (eight to ten points). The points reflect how fully an organization has achieved the element's objective. The Assessment Tool comprises of 66 elements, divided into three stages to match the organization of the Circular: Initiating, Building, and Maintaining. To avoid redundancy and facilitate communication of results, auditors narrowed the scope of testing to 36 elements and categorized them as:

- General content;

- Testing, training, and exercises; and

- Maintenance.

Auditors assigned each element a color value using the criteria in the Assessment Tool. Figure 1 below shows the number and rating of elements in each category. Appendix 3 outlines the elements that were tested.

Figure 1: Elements in Compliance with FEMA Circular

Category	Fully Compliant (Green; 8 to 10 points)	Partially Compliant (Yellow; 4 to 7 points)	Not Compliant (Red; 0 to 3 points)
General (14 elements tested)	9	3	2
Training and Testing (11 elements tested)	0	2	9
Maintenance (11 elements tested)	3	6	2

The Continuity of Operations Plan includes most of the required elements.
The Plan fully or partially incorporates 12 (86 percent) of the 14 general elements selected for testing from the FEMA Circular, such as procedures for activating the plan and resuming normal activities, an inventory of essential records, and orders of succession. The Plan does not discuss integrating critical external partners into the continuity planning process or the needs of staff with disabilities who might require accommodation if the plan were activated. Both of these elements could reduce the effectiveness of Plan activation: without input from external partners, the Department might not use mitigation strategies that meet stakeholder needs, and without an opportunity to request accommodations, some staff might not be able to assist in carrying out essential functions.

Due to the turnover and incomplete procedures mentioned previously, the Plan has not been reviewed and updated on schedule (see section below for more detail) and has not been checked against FEMA standards to ensure that all elements are addressed.
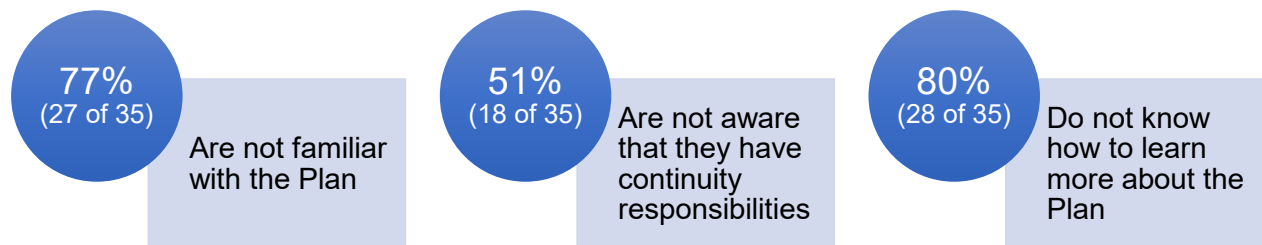
The Department should conduct regular testing, training, and exercises.
The Department has not been conducting testing, training, and exercises. System testing is not addressed in the Plan and has not been performed. This leaves the department open to the risk that critical systems might fail when activated.

While the Plan addresses training and exercises, these activities have not been conducted in the past few years. The State Office of Risk Management issued a letter in April 2022 clarifying that responding to an actual incident – such as the COVID-19 pandemic – could serve as a substitute for conducting preparedness exercises. However, state agencies resumed normal operations in June 2021, and exercises did not resume.

The Department does not include continuity awareness training in New Employee Orientation or as part of ongoing training requirements. As a result, staff are unaware of their roles and responsibilities regarding continuity of operations. Auditors surveyed a sample of Department staff and found that the majority of staff are not familiar with the Plan, are not aware that they have responsibilities under the Plan, and do not know how to learn more (see Figure 2 below).

Figure 2:

77% (27 of 35) Are not familiar with the Plan	51% (18 of 35) Are not aware that they have continuity responsibilities	80% (28 of 35) Do not know how to learn more about the Plan

Some Department staff have specific continuity roles, as division points of contact (POC) and/or members of the Emergency Response Group (ERG). The ERG is responsible for setting up essential functions in a secondary location if an event occurs that renders the Camp Hubbard campus unusable. In a survey of all POC and ERG staff (based on the rosters in the current draft of the Plan), many reported receiving no training or briefings in the past year and said that they were not confident they would know how to respond if the Plan was activated. Moreover, respondents who were assigned to the ERG were unaware of this assignment (see Figure 3 below). While many staff can telecommute, some work is still required on site at Camp Hubbard that would need to be relocated in an emergency. If staff are unaware of their ERG responsibilities, this could delay the resumption of essential functions.

Figure 3:

62% (13 of 21)	52% (11 of 21)	73% (8 of 11)
•Reported receiving no training or briefings in the past year	•Were not confident they would know how to respond if the Plan was activated	•Were unaware of their assignment to the ERG
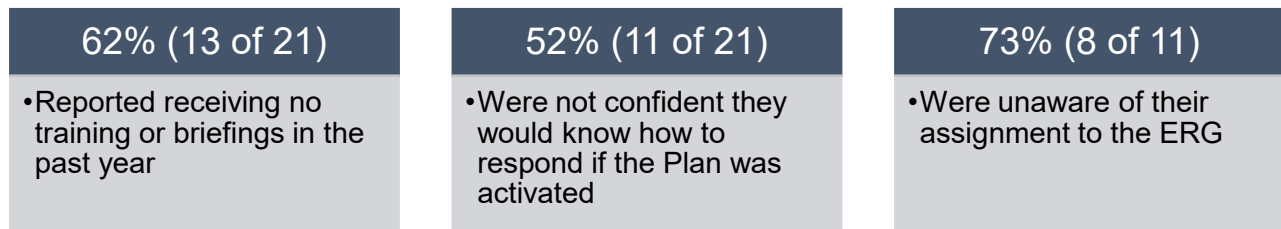
FEMA requires regular testing of alert and notification systems, activation procedures, communications, and systems and equipment. FEMA standards also require that all staff receive basic continuity awareness training, and that training is provided for staff with specific continuity roles.

In addition to the turnover previously discussed, the Department has not kept up with these requirements because there is not an overarching strategic approach. The FEMA Circular requires a multi-year strategic plan for continuity planning, as well as performance metrics and continuous improvement activities (such as Corrective Action Programs or After-Action Reports following an exercise or incident). While the current draft of the Plan contains a multi-year strategic plan, it has not been kept up to date. It was not adjusted to reflect changes due to the pandemic and it has no entries beyond 2022.

The Department should ensure that the Plan and all its supporting information is regularly reviewed and updated.
The most recent finalized update to the Plan was August 2020. An updated draft was prepared in 2022 but has not yet been approved. Some of the information contained in the Appendices is out of date. For example, the Business Process Analysis and the delegation of authority both refer to the Enterprise Project Management Office, which was integrated into the Information Technology Services Division in 2019. Contact lists and role assignments included staff no longer with the Department, and a few staff responding to the continuity roles survey reported that their roles had changed but had not been updated in the Plan.

The FEMA Circular sets requirements for review frequency:

Plan Area	Monthly	Annually	Biennially
Role Assignments	X		
Orders of Succession / Delegation of Authority		X	
Review of Plan		X	
Planning documents (e.g., BPA)			X

The Plan with its appendices is intended to be a comprehensive guide for maintaining essential services during an incident. If information is out of date or does not reflect current operations,

essential functions might be disrupted. The multi-year strategic plan includes a review and update schedule, but as previously discussed the strategic plan is itself not up to date.

Recommendation

2. Update the continuity multi-year strategic plan that provides for the maintenance and review of continuity plans **(HIGH)**. This should include:

   a. Establishing a regular schedule for updating the Continuity of Operations Plan to ensure it addresses all required elements and is reflective of the Department's current environment; and

   b. Conducting general training for Department employees and more specific training for those who are part of the Emergency Response Group.

Appendix 1: Objective, Scope, Methodology, and Rating Information

Objective

To determine whether TxDMV has designed and implemented controls to ensure operational resilience in accordance with state requirements and best practices.

Scope and Methodology

The scope of the audit included the second quarter of Fiscal Year 2021 through the end of Fiscal Year 2022. Information and documents reviewed in the audit included the following:

- Interviewed Business Continuity Coordinator

- Selected a random sample of ten percent of TxDMV staff (excluding upper management and staff with assigned continuity roles)

- Surveyed sample of 66 TxDMV employees

- Surveyed 32 employees assigned as divisional points of contact and/or members of the Emergency Response Group

- Reviewed information technology vendor contracts

- Reviewed Texas Labor Code 412.054

- Reviewed Federal Emergency Management Agency Continuity Guidance Circular and Assessment Tool

- Reviewed Department's Continuity of Operations Plan and Appendices and evaluated using the Circular and the Assessment Tool

- Reviewed National Institute of Standards and Technology Special Publication 800-34: Contingency Planning Guide for Federal Information Systems

The audit scope initially included both the Continuity of Operations Plan and the Disaster Recovery Plan. Auditors excluded the Disaster Recovery Plan after reviewing the responsibilities of the vendor selected to provide disaster recovery services for key Department information systems.

This audit was included in the FY2022 Second Six Month Internal Audit Plan. IAD conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the Internal Standards for the Professional Practice of Internal Auditing. Those standards require that IAD plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on our audit objectives. IAD believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives

Report Distribution

In accordance with the Texas Internal Auditing Act, this report is distributed to the Board of the Texas Department of Motor Vehicles, Governor's Office of Budget, Planning, and Policy, Legislative Budget Board, and the State Auditor's Office.

Ratings Information

Maturity Assessment Rating Definition

IAD derived the maturity assessment ratings and definitions from the Control Objectives of Information and Related Technologies (COBIT) 5 IT Governance Framework and Maturity Model, the Enterprise Risk Management (ERM) Maturity Model, and the ISACA Maturity Model. The model was adapted for the TxDMV assurance audit purposes and does not provide a guarantee against reporting misstatement and reliability, non-compliance, or operational impacts. The ratings and definitions are provided in Table 1.

Table 1. Maturity Assessment/Process Capability Rating Definitions

Rating	Name	Definition
1	Minimal	The function may have policies and procedures established for some activities but relies on intuition and handles issues on an ad-hoc basis.
2	Informal and Reactive	The function achieves its purpose with basic processes and activities that are not very organized or followed.
3	Established	The function achieves its purpose in an organized way, following established processes, but those processes may not be consistently followed or well communicated.
4	Predictable	The function fully achieves its purpose, is well-defined, and its performance is quantitatively measured. The function is fully integrated within the Department, the function has full resources to achieve business objectives, and policies and procedures are regularly improved.
5	Optimized	The function fully achieves its purpose, is well-defined, and its performance is quantitatively measured. There is continuous improvement that is pursued, and technology is heavily leveraged to automate workflow and improve quality and effectiveness of processes.

Recommendation Rating Criteria

The IAD rates audit recommendation's priority (i.e., HIGH or LOW) to help the TxDMV Board and executive management identify the importance of the recommendation. The criteria for Low and High Priority are documented in Table 3.

Table 3. Recommendation Priority Criteria

Priority	Criteria
Low	• Requires only a written policy or procedure update • Is within an acceptable range of risk tolerance for the Department • A non-reoccurring or regulatory external audit issue
High	• Executive Management or Board Request • Not within an acceptable range of the risk tolerance of the division • New process had to be developed to address recommendations • Regulatory impact or reoccurring issue

Appendix 2: Survey Results

General Staff Survey

35 responses were received for all questions.

Question 1: Which of the following most closely matches your understanding of what "continuity of operations" means?	Total	Percent
"Continuity of operations" is the system that ensures an organization can provide its essential services even after a major disruptive event like a natural disaster	21	60%
"Continuity of operations" is like succession planning, making sure that potential leaders are identified and trained so there's continuity of leadership when executives or other key staff leave the agency.	1	3%
"Continuity of operations" means having robust policies and procedures in place so that an organization can continue to operate effectively after a change in leadership.	10	29%
None of these is the definition of "continuity of operations"	0	0%
I don't know	3	9%

Question 2: I have received training about continuity of operations	Total	Percent
TRUE	4	11%
FALSE	12	34%
I don't know/I don't remember	19	54%

Question 3: My job has no role in continuity of operations.	Total	Percent
TRUE	5	14%
FALSE	17	49%
I don't know/I'm not sure	13	37%

Question 4: I am familiar with the Continuity of Operations Plan (COOP).	Total	Percent
TRUE	8	23%
FALSE	13	37%
I don't know/I'm not sure	14	40%

Question 5: I know how to find information about continuity of operations and the COOP.	Total	Percent
TRUE	7	20%
FALSE	13	37%
I don't know/I'm not sure	15	43%

Question 6: In your own words, please describe what continuity of operations means to you and what effect it has on your job at TxDMV.	Total	Percent
Correctly described continuity of operations and articulated the effect on their job	5	14%
Correctly described continuity of operations but did not describe an effect	12	34%
Incorrect understanding of continuity of operations	8	23%
I don't know/I'm not sure	7	20%
Blank/no answer	3	9%

Assigned Roles Survey

21 responses were received for all questions.

Question 1: I am a:	Total	Percent
Continuity of operations Point of Contact for my division	10	48%
Member of the Emergency Response Group	1	5%
Both	4	19%
Neither	6	29%

Question 2: I have been in that role for:	Total	Percent
Less than six months	2	10%
Six months to two years	3	14%
Two to five years	3	14%
More than five years	9	43%
Not applicable because I am not in the Emergency Response Group nor am I a point of contact for my division	4	19%

Question 3: I have been informed of what my role is regarding continuity of operations	Total	Percent
TRUE	14	67%
FALSE	2	10%
I don't know/I'm not sure	5	24%

Question 4: I have, at any time, received training or briefings on my continuity of operations role (if any)	Total	Percent
TRUE	11	52%
FALSE	4	19%
I don't know/I don't remember/not applicable	6	29%

Question 5: I have received training or briefings on my continuity of operations role (if any) within the past year	Total	Percent
TRUE	8	38%
FALSE	10	48%
I don't know/I don't remember/not applicable	3	14%

Question 6: The Continuity of Operations Plan accurately identifies essential functions and personnel.	Total	Percent
TRUE	12	57%
FALSE	2	10%
I don't know/I'm not sure	7	33%

Question 7: The Continuity of Operations Plan is comprehensive and doesn't leave out anything we'd need to know in an emergency.	Total	Percent
TRUE	10	48%
FALSE	2	10%
I don't know/I'm not sure	9	43%

Question 8: I feel confident that I would know what to do if the Continuity of Operations Plan were activated	Total	Percent
TRUE	10	48%
FALSE	4	19%
I don't know/I'm not sure	7	33%

Question 9: In your own words, please give a general description of what your roles and responsibilities are regarding continuity of operations and the Continuity of Operations Plan	Total	Percent
Assist with operations	3	14%
Provide information	6	29%
Backup/not actively involved	3	14%
I don't know/I'm not sure	4	19%
Blank/no answer*	5	24%

*"no answer" also includes responses that provided other information but did not directly answer the question

Appendix 3: Continuity Assessment Tool

	Assessment Element	Rating
General	Has the organization integrated critical external partners into the continuity planning process?	**Red**
	Has the organization coordinated the continuity planning effort with other incident management, risk management, and preparedness planning efforts, such as the Occupant Emergency Plan, Emergency Operations Plan, Information Technology/Disaster Recovery, and pandemic plan?	**Green**
	Has the organization developed a comprehensive continuity plan?	**Green**
	Has the organization identified and planned for mitigation options to support the continuance of essential functions, such as identifying alternate sites, teleworking, developing devolution plans, or entering into mutual aid agreements?	**Green**
	Has the organization established and documented orders of succession to ensure an orderly and predefined transition of leadership?	**Green**
	Has the organization established and documented delegations of authority to make key decisions, conduct essential functions, and direct the organization?	**Yellow**
	Has the organization clearly explained the expectations, roles, and responsibilities for all personnel during a continuity plan activation?	**Green**
	Has the organization implemented a strategy to communicate the organization's operating status to all staff and with external stakeholders?	**Green**
	Has the organization implemented a process to account for all staff, including contractors, in the event of an emergency?	**Yellow**
	Has the organization ensured the needs of personnel with disabilities are considered during the continuity planning process?	**Red**

	Has the organization provided guidance to employees on individual and community preparedness actions to ensure readiness during a continuity activation?	**Yellow**
	Has the organization identified and inventoried essential records, including emergency operating records and legal and financial rights records?	**Green**
	Has the organization developed a plan or procedures to activate your continuity plan?	**Green**
	Has the organization developed a plan or procedures to recover from the effects of an emergency and transitioning back to normal operations after a continuity activation?	**Green**
Training Testing & Exercises	Has the organization conducted testing of alert and notification procedures?	**Red**
	Has the organization conducted testing of activation procedures?	**Red**
	Has the organization conducted testing of accountability procedures?	**Red**
	Has the organization conducted testing of the interoperable and available communications capabilities that support identified essential functions?	**Red**
	Has the organization conducted testing of critical systems and equipment and strategies to meet associated recovery time objectives?	**Red**
	Have all staff members completed continuity awareness training?	**Red**
	Has the organization trained continuity personnel on continuity plans and strategies?	**Yellow**
	Has continuity personnel participated in regular continuity training activities with other continuity programs (both internally and externally)?	**Red**
	Has the organization regularly conducted organization-wide continuity exercises that include exercising of mitigation options that support the continuance of essential functions?	**Yellow**

	Has the organization conducted exercises of the reconstitution plan or procedures to exercise recovery from the effects of an emergency and transitioning back to normal operations after a continuity activation?	Red
	Has the organization exercised with internal and external partners to coordinate continuity plans and programs?	Red
Maintenance	Has the organization developed a multi-year strategic plan to provide for the development, maintenance, and review of the continuity plan and program?	Green
	Has the organization developed metrics or success criteria in order to evaluate the continuity plan and program on a regular basis?	Red
	Has the organization established a working group that reviews and revises the continuity plan acccording to a regular, formal schedule?	Yellow
	Has the organization reviewed and updated, as needed, its Business Process Analysis (BPA)?	Yellow
	Has the organization reviewed and updated, as needed, its risk assessments?	Green
	Has the organization reviewed and updated, as needed, its BIA?	Green
	Has the organization reviewed and updated, as needed, its orders of succession and delegations of authority?	Yellow
	Has the organization reviewed and updated essential records and the essential records inventory, including emergency operating records and legal and financial rights records?	Yellow
	Has the organization's continuity program established a Corrective Action Program (CAP) to track and implement areas for improvement from tests, training, and exercise events and real-world activities?	Red
	Has the continuity planning team met on a regular basis?	Yellow
	Has the organization regularly updated appropriate point-of-contact rosters of continuity personnel?	Yellow

Appendix 4: Management Response and Action Plan

The Information and Technology Services Division provided the following response:

> *Management agrees with the recommendations and will establish and document procedures to include the use of Business Process Analysis templates for all Department divisions in the continuity planning process and will update the continuity multi-year strategic plan to ensure the Continuity of Operations Plan includes all required elements and is tested accordingly. ITSD is in the process of hiring a new Business Continuity/Disaster Recovery Coordinator and the completion of these tasks will depend on when the new person is onboarded and has had a reasonable amount of time to gather information and ensure processes are developed in coordination with all key stakeholders.*

Recommendation	Responsible Department and Section/Unit	Department Response	Completion Date
1. Establish and document procedures for the continuity planning process, including the use of Business Process Analysis templates for all Department divisions and incorporation into the Continuity of Operations Plan **(HIGH)**.	Information Technology Services Division, Business Continuity/Disaster Recovery Coordinator	Will establish and document procedures for the continuity planning process, including the use of Business Process Analysis templates for all Department divisions and incorporation into the Continuity of Operations Plan. ITSD is in the process of hiring a new Business Continuity/Disaster Recovery Coordinator and the completion of this task will depend on when the new person is onboarded and has had time to gather information and assess the gaps to ensure the process is developed in coordination with all key stakeholders.	January 31, 2024]
2. Update the continuity multi-year strategic plan that provides for the maintenance and review of continuity plans **(HIGH)**. This should include: c. Establishing a regular schedule for updating the Continuity of Operations Plan to ensure it addresses all required elements and is reflective of the Department's current environment; and d. Conducting general training for Department employees and more specific training for those who are part of the	Information Technology Services Division, Business Continuity/Disaster Recovery Coordinator	Will update the continuity multi-year strategic plan. ITSD is in the process of hiring a new Business Continuity/Disaster Recovery Coordinator and the completion of this task will depend on when the new person is onboarded and has had time to gather information and establish timelines for Continuity of Operations Plan updates and to develop and implement employee training as required.	January 31, 2024

Recommendation	Responsible Department and Section/Unit	Department Response	Completion Date
Emergency Response Group.			