UTA

Internal Audit

2016 Business Continuity / Disaster Recovery Internal Audit Report

Approved: Isaac S. Clarke

Isaac S. Clarke

May 13, 2016
Report Reference: R-16-2

Executive Summary

Background and Procedures Performed

Disaster recovery and business continuity planning are integral parts of the overall risk management for an organization. While unable to eliminate all risks, the Utah Transit Authority (UTA) should have disaster recovery and business continuity plans to prepare for potential disruptive events and disasters impacting UTA. Business continuity planning should not only addresses how to respond to smaller disruptions or isolated incidents, but also to wide-spread natural or man-caused disasters that limit or completely shut-down UTA. Business continuity planning also includes disaster recovery planning that provides a road map to restore operations while minimizing the long-term negative impact to UTA.

An internal audit of the design and operational effectiveness of UTA's controls that address the continuity of operations and the recovery from large scale disasters was performed. The period of the audit was from January 1, 2015, to March 7, 2016. The primary areas of focus include:

- Business Continuity Governance
- Risk Assessment and Impact Analysis
- Risk Based Plan Design
- Plan Implementation and Integration
- Training and Communication
- Compliance Monitoring
- Information Technology
- Periodic Plan Testing and Maintenance

Procedures performed on each process in this review included inquiries of functional management and personnel to understand the business processes and control framework, review of process and procedural documentation, and inspection of management documentation to determine whether the identified controls have been implemented and are functioning as intended.

Key Management Issues

UTA lacks a business continuity plan that is based on a comprehensive risk assessment and integrates related activities across the organization. Additionally, ownership for business continuity planning rests upon the Emergency Management Program Manager rather than with operations leadership. It is recommended that a periodic risk assessment be performed to assess the threats to operations and that the UTA Continuity of Operations Plan (COOP) be prepared based on the identified risks. While the Emergency Management Program facilitator should continue to help facilitate planning and training activities, it is recommended that the COOP and related documentation specific to a site or function (Plan documentation) should be owned by the respective operational leadership. Plan documentation should align with UTA's Emergency Preparedness, Emergency Operations and Transit Agency Safety Plans and should integrate the emergency, continuity and disaster recovery activities performed across UTA. Once completed, Plan documentation should be communicated and accessible to employees and regular training should be provided. Plan documentation should also be reviewed annually to ensure its accuracy, completeness and alignment with current risks facing organization.

Overall Process Conclusion

While UTA has effective processes to respond to isolated incidents that more commonly disrupt service, controls are not designed and operating effectively to address the continuity of operations and recovery from large scale disasters.

Intentionally Left Blank

Table of Contents of Protected Information

Findings and Recommendations

1. *Leadership over sites and functions within UTA should own the Plan documentation specific to the areas of their responsibility.* Inappropriate delegation of planning activities and the lack of senior-level management involvement during the plan's development, implementation, and maintenance phases is a key factor leading to poor business continuity planning and execution[1]. Each document related to business continuity, disaster recovery and emergency management should note a specific individual (with oversight for the pertinent organization) who owns the document and is accountable for policies and procedures therein. Document owners may delegate the duties of documenting or updating to others within their organization, but they are ultimately responsible for reviewing and approving the initial documents and any subsequent changes.

   Failure to appropriately assign ownership within the organization for policies and procedures may result in lower levels of acceptance, out-of-date or inaccurate documentation, and inconsistent interpretation or execution of the Continuity of Operations Plan (COOP) during a disaster. The inconsistent or incorrect interpretation and execution of the COOP or related plans during a disaster may result in additional harm to customers and employees, loss of assets and reputational damage to UTA.

   Audit procedures found that an excessive amount of reliance is placed upon the Emergency Management Program Manager (EMPM) by operations leadership. While not explicitly stated, the EMPM owns the business continuity planning process, the COOP and is considered the expert (although not the owner) regarding much of the related documentation specific to sites or functions. Internal Audit also noted that certain key documents did not have a specified owner and/or the owner was not recorded in the Plan documentation (e.g., COOP, Bus Bridge Manual, FrontRunner Emergency Preparedness Plan, and Safety Committee Tracking Matrix).

   Recommendation R-16-2.1: *The Interim President / Chief Executive Officer should transfer ownership of the continuity of operations from the Emergency Management Program Manager to the Acting Vice President of Operations.*

   Recommendation R-16-2.2: *The Acting Vice President of Operations should work with the Emergency Management Program Manager to oversee the completion of the Continuity of Operations Plan and ensure that it aligns with the Emergency Preparedness Plan and integrates the business unit activities across UTA.*

   Recommendation R-16-2.3: *The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that ownership of site or mode specific documentation is properly assigned to those with oversight for the site, organization, and/or mode, and that the owner is noted within each plan document.*

[1] (2005 Business Continuity Survey conducted by the CPM Group and Deloitte and Touche LLP)

2. *UTA, business unit and mode leadership should have formal plans to address the continuity or winding down of operations due to a disaster and the restoration of services following a complete shutdown.* UTA has prepared a Transit Agency Safety Plan (TASP) and Emergency Preparedness Plan to comply with Part 659 of Title 49 (transportation) of the Code of Federal Regulations. Best practices suggest that UTA should also design and implement a COOP to ensure that the organization is able to perform its critical functions during and/or resume operations after a wide range of disasters caused by outside sources such as nature, utility or technology failures, accidents or other man-made emergencies.

   Failure to have a COOP may result in unnecessarily putting UTA's customers, employees, assets and reputation at risk during a disaster or during a restoration of services afterward.

   Audit procedures found that UTA Emergency Management has been working on a COOP in 2015—in response to the 2015 Three-year Safety and Security Review by the State Safety Oversight Agency in behalf of the Federal Transit Administration (FTA). Evidence of progress made toward its completion includes a partially drafted COOP, the completion of the Emergency Operations and Family Assistance Plans, and the formation of the Emergency Operations Center group. However, while progress has been made, the following are opportunities for improvement noted during the audit:

   - The draft COOP lacked input from the business units and departments.
   - The draft COOP and related documentation specific to a site or function did not address disaster recovery.
   - The Bus and Light Rail modes had standard operating procedures to manage emergencies, but did not have a governing document in place to tie together the procedures relevant to business continuity and emergency management.

   Recommendation R-16-2.4: *The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that the Continuity of Operations Plan integrates business continuity activities from across UTA and addresses the winding down of operations due to a disaster and the restoration of services following a complete shutdown.*

   Recommendation R-16-2.5: *The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that all service modes have a governing document for the continuity of operations that, at the very least, provides direction as to which standard operating procedures are applicable to foreseeable emergencies and disasters.*

3. *Formal risk assessments must be performed periodically to identify new risks to UTA as a whole and to the individual business units and to determine whether plans adequately address to the identified risks.* Performing a risk assessment in conjunction with a business impact analysis enables an organization to clearly identify key risks to its most critical activities and resources. The information resulting from the assessment allows UTA to identify where risks exceed its risk appetite, and is the foundation for developing business continuity strategies and the COOP to reduce the likelihood of a disruption, shorten the period of the disruption, and limit the impact to the delivery of its key services. Periodic follow-up assessments will help identify changes within the organization and its environment that may require changes to the COOP.

   Failure to accurately understand the key risks and their impact to the activities and resources critical for delivering services limits the effectiveness and completeness of the Authority's plans for maintaining continuity of operations, safely executing a controlled shutdown or recovering from a disaster.

   While UTA Emergency Management had completed a HAZUS Assessment from the Federal Emergency Management Agency (FEMA) to evaluate hazards related to earthquakes and flooding, UTA Security had accessed certain security threats, and UTA employees actively report incidents or potential workplace hazards; audit procedures identified the following exceptions:

   - No formal risk assessment had been performed recently to identify business or operational risks (beyond damage to facilities and security risks) to the business units or different transportation modes.
   - Plan documentation did not prioritize critical business processes and resources based on potential risk to the various organizations.

   Recommendation R-16-2.6: *The Emergency Management Program Manager should ensure that a formal risk assessment is performed to identify risks to UTA as a whole and/or to the individual business units and to determine whether Plan documentation adequately addresses the risks.*

4. *Plan documentation at the business unit or mode level should be reviewed for accuracy and completeness each year and approved by the executive owner.* Reviewing documentation regularly helps ensure that the personnel, contact information, policies and procedures found therein are accurate, complete and applicable to the current environment. The review process also raises leadership and staff awareness of the plan.

   Failure to regularly review and approve Plan documentation may result in outdated, inaccurate and incomplete plans. Incorrect Plan documentation may result in incorrect or ineffective actions being taken by personnel in response to an emergency or disaster causing additional harm to customers and employees, loss of assets and reputational damage to UTA.

   Audit procedures found over 20 different cases where Plan documentation was incomplete or inaccurate, or the hard-copy on-hand was not the most current version of the document.

   Recommendation R-16-2.7: *The Emergency Management Program Manager should ensure that owners of Plan documentation are reviewing their respective documents annually to ensure that the content is accurate and complete.*

5. *Plans should be communicated and made accessible to personnel and current hard copies should be maintained at primary and backup locations.* Employees need to have a general awareness and familiarity with Plan documentation if they are expected to perform the related procedures in the case of a disaster. Communicating plans and maintaining current copies of Plan documentation in locations that are accessible by employees provides them an opportunity to read and familiarize themselves with the plan. Hard copies of Plan documentation should be readily available to personnel in the event of a power outage or the inability to access to on-line copies.

   Failure to communicate business continuity or disaster recovery plans to personnel may result in additional harm to customers and employees, loss of assets and reputational damage to UTA due to employees' lack of familiarity with the plan.

   Audit procedures revealed that Plan documentation was not retained and communicated consistently across the organization. Additionally, there is no standard requiring how this information was to be communicated or how and what documents are to be distributed.

   Recommendation R-16-2.8: *The Emergency Management Program Manager should develop a policy for communicating Plan documentation. The policy should specify:*

   - *What documents need to be communicated to employees*
   - *The form and frequency for communicating Plan documentation*
   - *The requirements for storing hard copies*
   - *That the document has been reviewed with the General Counsel's office to ensure sensitive information is properly restricted*

6. *Plan documentation and activities at the business unit and department level should be integrated with one another and with the corporate level plans.* Business units and departments are interdependent for certain support services in the event of an emergency or disaster. Plan documentation specific to each organization should identify those dependencies and ensure that planned activities are aligned to facilitate the appropriate level of communication and coordination in responding to an emergency or disaster.

   Failure to integrate business unit and department documentation and activities with each other and with the corporate level plans may result in additional harm to customers and employees, loss of assets and reputational damage to UTA.

   Audit procedures identified a lack of integration of Plan documentation between the business units and departments—particularly between the business units and IT. It was also noted that essential third party providers were not consistently captured in Plan documentation.

   Recommendation R-16-2.4 (repeated): *The Acting Vice President of Operations should ensure that the Continuity of Operations Plan integrates business continuity activities from across UTA and addresses the winding down of operations due to a disaster and the restoration of services following a complete shutdown.*

7. *Employees should be trained and tested on the performance of emergency management, business continuity and disaster recovery operations.* UTA Emergency Management oversees monthly Emergency Operations Center (EOC) trainings, exercises, semi-annual emergency simulations and semi-annual site drills at each UTA facility. Training sessions and simulated practices help familiarize personnel with their roles and responsibilities in the event of a disaster as well as the policies and procedures related to the Emergency Operations Plan (EOP) and COOP.

   Failure to adequately train personnel regarding their emergency management, business continuity and disaster recovery responsibilities may result in their inability to perform in the event of an actual disaster.

   The audit procedures performed found that participation in EOC trainings and simulations is not consistently recorded.

   Recommendation R-16-2.9: *The Emergency Management Program Manager should record attendance at EOC trainings, exercises and simulations. The Emergency Management Program Manager should also report individuals or organizations who consistently fail to participate in training to the Chief Safety and Security Officer for escalation to Corporate Staff.*

8. *The Emergency Operations Center sites should be set-up and stocked with the necessary equipment to execute the Emergency Operations Plan.* The EOC is a critical part of the EOP and COOP. The primary and secondary EOC sites should be fully equipped with the necessary equipment for the EOC to perform its responsibilities during a disaster.

   Failure of the EOC operating as planned due to it being inadequately equipped may result in the inability to execute the COOP or other emergency plans.

   Audit procedures found that UTA possesses much of the necessary EOC equipment. However, UTA is in the process of relocating the primary and secondary sites and neither site has been set-up and stocked with all of the necessary equipment.

   Recommendation R-16-2.10: *The Chief Safety and Security Officer should ensure that plans to set-up and equip the primary and secondary EOC sites are completed.*

Management Action Plans

The following are the planned actions that UTA Management has drafted in response to the findings and recommendations proposed by Internal Audit in the preceding section.

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.1	Yes	Interim President / Chief Executive Officer	August 1, 2016
Recommendation:	*The Interim President / Chief Executive Officer should transfer ownership of the continuity of operations from the Emergency Management Program Manager to the Acting Vice President of Operations.*		
Action Plan:	The Interim President / Chief Executive Officer will transfer ownership of the continuity of operations from the Emergency Management Program Manager to the Acting Vice President of Operations.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.2	Yes	Acting Vice President of Operations	December 31, 2016
Recommendation:	*The Acting Vice President of Operations should work with the Emergency Management Program Manager to oversee the completion of a Continuity of Operations Plan and ensure that it aligns with the Emergency Preparedness Plan and integrates the business unit activities across UTA.*		
Action Plan:	The Acting Vice President of Operations will work with the Regional General Managers, the Emergency Management Program Manager and support service providers to complete the UTA Continuity of Operations Plan that integrates the business unit activities across UTA and aligns with the Emergency Preparedness Plan.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.3	Yes	Acting Vice President of Operations	December 31, 2016
Recommendation:	*The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that ownership of site or mode specific documentation is properly assigned to those with oversight for the site, organization and/or mode, and that the owner is noted within each plan documented.*		
Action Plan:	The Acting Vice President of Operations will work with the Regional General Managers, the Emergency Management Program Manager and support service providers to ensure that ownership for site or mode specific documentation related to the UTA Continuity of Operations Plan is properly assigned and noted within each document.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.4	Yes	Acting Vice President of Operations	December 31, 2016
Recommendation:	*The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that the Continuity of Operations Plan integrates business continuity activities from across UTA and addresses the winding down of operations due to a disaster and the restoration of services following a complete shutdown.*		
Action Plan:	The Acting Vice President of Operations will work with the Regional General Managers, the Emergency Management Program Manager and support service providers to ensure that the Continuity of Operations Plan integrates business continuity activities from across UTA and addresses the winding down of operations due to a disaster and the restoration of services following a complete shutdown.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.5	Yes	Acting Vice President of Operations	December 31, 2016
Recommendation:	*The Acting Vice President of Operations should work with the Emergency Management Program Manager to ensure that all service modes have a governing document for the continuity of operations that, at the very least, provides direction as to which standard operating procedures are applicable to foreseeable emergencies and disasters.*		
Action Plan:	The Acting Vice President of Operations will work with the Regional General Managers, the Emergency Management Program Manager and support service providers to prepare regional continuity of operations plans that integrate with the UTA Continuity of Operations Plan and provide clear directions as to procedures to be performed in the event of foreseen emergencies and disasters.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.6	Yes	Emergency Management Program Manager	October 31, 2016
Recommendation:	*The Emergency Management Program Manager should ensure that a formal risk assessment is performed to identify risks to UTA as a whole and/or to the individual business units and to determine whether Plan documentation adequately addresses the risks.*		
Action Plan:	The Emergency Management Program Manager will facilitate the performance of a comprehensive risk assessment to identify risks to UTA to ensure that the Plan adequately addresses critical risks to the continuity of operations or to the restorations of services following a large scale emergency or disaster.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.7	Yes	Emergency Management Program Manager	August 19, 2016
Recommendation:	*The Emergency Management Program Manager should ensure that owners of Plan documentation are reviewing their respective documents annually to ensure that the content is accurate and complete.*		
Action Plan:	The Emergency Management Program Manager will develop and implement a standard operating procedure for document owners to follow in order to perform and document their reviews of Plan documentation to ensure that the content is accurate and complete.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.8	Yes	Emergency Management Program Manager	June 15, 2016
Recommendation:	*The Emergency Management Program Manager should develop a policy for communicating Plan documentation. The policy should specify:* • *What documents need to be communicated to employees* • *The form and frequency for communicating Plan documentation* • *The requirements for storing hard copies* • *That the document has been reviewed with the General Counsel's office to ensure sensitive information is properly restricted*		
Action Plan:	The Emergency Management Program Manager will document within each plan the requirement for storing hard copies, a sign off sheet that the plan has been reviewed by general counsel, and will update the plans tracking matrix to include how the plan is communicated and to whom. Note: As these changes are administrative in nature, the updated documents will be held as drafts for the upcoming as this year's plan documents have already been signed.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.9	Yes	Emergency Management Program Manager	April 27, 2016
Recommendation:	*The Emergency Management Program Manager should record attendance at EOC trainings, exercises and simulations. The Emergency Management Program Manager should also report individuals or organizations who consistently fail to participate in training to the Chief Safety and Security Officer for escalation to Corporate Staff.*		
Action Plan:	The Emergency Management Program Manager has implemented a new protocol to record participant attendance at EOC trainings, exercises and simulations. The Emergency Management Program Manager will report individuals or organizations who consistently fail to participate in training to the Chief Safety and Security Officer for escalation to Corporate Staff.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-2.10	Yes	Chief Safety and Security Officer	December 31, 2016
Recommendation:	*The Chief Safety and Security Officer should ensure that plans to set-up and equip the primary and secondary EOC sites are completed.*		
Action Plan:	The Chief Safety and Security Officer will oversee the completion of the primary and secondary EOC sites to ensure that they meet the planned specifications and are adequately equipped for the EOC to perform its duties during or after an emergency.		

Report Distribution

This report is to be distributed directly to the following individuals.

- Interim General Manager/President/CEO
- Chief of Staff and Chief Safety and Security Officer
- Acting Vice President of Operations
- Emergency Management Program Manager

Appreciation is expressed to the Emergency Management Program Manager, the Regional General Managers and to the many Emergency/Safety personnel for their cooperation in supporting this review.

Audit Team Members

Auditors assigned to this project were Riana De Villiers and Brian Ledbetter.