CONTINUITY OF OPERATIONS AUDIT

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

April 16, 2014

INTRODUCTION

Purpose

The purpose of the audit is to give assurance that the development of the Metropolitan Council's Continuity of Operations (COOP) program follows established practices and is adequate to address continuity risks. This audit does not give assurance on the adequacy of specific COOP plans, as this can only be accomplished through formal testing exercises.

Scope

The scope of the audit covered the following:

- Governance and executive support
- Program implementation
- Risk assessment, business impact analysis and recovery strategy development
- COOP plan development, maintenance and testing

Methodology

- Research State of Minnesota requirements for continuity of operations planning and other "best-practice" information
- Review implementation plan, existing COOP plans and business impact analysis
- Interviews with key staff responsible for COOP program development and governance

Assurances

This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the U. S. Government Accountability Office's *Government Auditing Standards*.

Background

Continuity of operations (COOP) planning is “the process by which an organization prepares for future incidents that could jeopardize the organization’s core mission and its long-term viability.” COOP planning is an established discipline that occurs in several defined stages, summarized in Appendix 1 below from the State of MN Enterprise Continuity of Operations Standard. The COOP planning process is not linear—an organization does not move from one stage to the next until everything is complete. Rather, the process is cyclical. The program is established and must be continually maintained to mitigate the risks of service interruption.

COOP planning is required of State agencies based on Executive Order 13-13, which states that the Met Council/Metro Transit shall carry out the general emergency preparedness, planning, response, recovery, hazard mitigation continuity of operations and service continuation described within the executive order. The MN.IT Services Office has established continuity of operations policies and standards based in part on this executive order.

An initial business impact analysis was completed June of 2009. A project manager was hired in July of 2010 to develop and manage the COOP program at which time a second business impact analysis was performed. A project management consultant was brought on to help develop a project implementation plan November of 2012. The consultant’s role was eventually transferred into a project manager based in the IS Project Management Office. An additional staff member was hired to support continuity of operations in March, 2014.

There have been several audit findings related to continuity of operations and disaster response. An internal audit report from 2005 recommended a comprehensive disaster recovery/business continuity plan be developed. The Federal Transit Administration’s Financial Management Oversight (FMO) review from January 2011recommended a comprehensive disaster recovery plan be developed in conjunction with the Pandemic Flu plan. Management responses are still under review by the FTA. The Triennial Review from September 2012 reiterated the FMO findings review from the previous year.

OBSERVATIONS

Program Governance and Executive Support

Policies and standards have not been formally adopted.

Objectives of the COOP program have been developed and are included in COOP plans, but these have not been formally adopted as program standards. A program as large and complex as COOP, and requiring the continued participation of every business unit at the agency will benefit from establishing organizational policies and standards. Policies establish the program as a priority for the organization and require the cooperation of all business units. Standards establish the minimum requirements for each program area, and thus help guide implementation, judge program quality, communicate about the program and make the program auditable to internal standards.

Formal policies and standards also help mitigate a single-point of failure with the COOP project manager, meaning if something were to happen to them the program would already be defined and not need to be recreated. The State of Minnesota has created general policies and standards for the implementation of their COOP program which could also be adapted for agency use.

A COOP steering committee has been established, but its overall role in program governance can be improved.

A steering committee has been formally established and has adequate representation from across the agency, but lacks a clear role in program governance. The steering committee was established approximately 2.5 years from the time the program began. It has met four times at the time of the audit.

The steering committee is an integral part of program governance during the early stages of program development, but also as the program matures and must be continually maintained in the organization. Establishing a clear role for the committee will help mitigate a single-point of failure with the program manager to deliver and maintain the program, address obstacles which may be encountered during implementation and keep the program accountable to approved strategies and deadlines.

A strategic plan for the COOP program has been established, but an implementation plan with timelines for completion would help address program development risk.

Program development timelines have focused on one program area at a time, such as the development of COOP plans. A strategic plan with program growth and maturity milestones for different program areas has been created and circulated, but timelines and plans for reaching these milestones are not present. As a result, the program risks being understood one stage at a time instead of seeing what is required to implement a complete program. Program risks are also present without timelines for completion.

A consultant was brought on to help develop a program implementation plan. Several other documents were either created or modified from existing program documents to create a “COOP Program Management Plan.” The Program Management Plan included several parts, such as a business engagement model, communications plan, risk management plan and resource management plan. Several of these components, such as the communications plan, may be helpful for the program to formally adopt into their process.

With current resources and implementation strategies, COOP plan development for priority 1 and 2 services will be complete by 2017 (though at the time of the audit additional resources were being brought on which will likely speed the pace of implementation.) According to the State of Minnesota COOP standards, a business impact analysis must be completed “after every major change to the entity or at least every four years.” BIA data is confirmed during the plan development process, but there is risk the program will not meet this recommended frequency given the current pace of implementation.

Other important program areas, such as maintenance of plans, testing, a formal employee awareness program and creating plans for priority 3 and 4 services are not formally part of the implementation timeline. Given the dynamic nature of the organization, a plan for addressing changes in the organization should also be considered.

COOP activities are not present in annual work plans or performance evaluations for all business units.

The COOP program depends on the continuing participation of personnel in each business unit of the agency. Lacking adequate resources and prioritization at the business unit level increases the risk that the overall level of preparedness will not be sufficient during a disaster. Coordination of COOP activities and business unit work plans, and including COOP participation in annual performance evaluations will help mitigate this risk.

The relationship between COOP and other emergency response programs is not clearly defined.

Continuity of operations (COOP) planning is closely related to other emergency management programs that have taken place at the Council, such as the creation of emergency response and disaster recovery plans. The similarity of these programs has lead to confusion among some stakeholders about the scope and responsibilities for each program. This could lead stakeholders to misunderstand the level of overall preparedness and coordination of response, as well as affect stakeholder buy-in for the COOP initiative. As a result, clarification of the COOP program and its relationship to these past efforts are important to communicate as the program matures.

Risk Assessment

A risk assessment identifying specific threats to the organization was not performed, but an “all-hazards” approach is adequate with management approval.

An “all-hazards” approach to COOP planning was performed, which eliminates the need for a formal risk assessment. A risk assessment identifies the likelihood and impact of individual threats to the organization. It offers a formal mechanism to consider ways to mitigate risks from credible events and can help scope the overall COOP process. The downside of this approach is the difficulty of accurately assessing the credibility of events. On the other hand, an all-hazards approach plans for the “worst-case scenario,” or total loss of a building, instead of assessing the likelihood of individual threats. This approach has merits. Since service disruptions have the same effect no matter how they occur, it can save time by considering the worst-case scenario as a base assumption. All-hazard plans are flexible enough to be used during lesser disasters.

A formal risk assessment is part of the State Continuity of Operations Standards. If these standards are adopted a risk assessment should be performed. However, an all-hazards approach is adequate to address continuity risk provided it meets the risk tolerance set by management. It is recommended that an all-hazards approach is detailed in approved program standards to document the rationale of the approach and consider a formal mechanism to document and follow-up on risk mitigation strategies should risks be identified.

Business Impact Analysis (BIA)

Recovery point objectives for technology were not identified during the BIA.

The recovery point objective (RPO) refers to the amount of data that can be lost and recreated manually should a disaster affect technology systems. RPO identification helps determine the necessary backup required for technology. Identification of RPO is a State of Minnesota Standard for COOP.

As the COOP program operates from the IS department, there is awareness of current backup strategies for technology. However, the systematic identification of RPO helps assure management and process owners that technology dependencies are adequately addressed by the COOP program and IS department. RPO should be identified, approved by management and process owners, and technology recovery strategies developed as necessary.

External dependencies for services and technology were not identified during the BIA.

External service and technology dependencies are each identified during the plan development process. The suggested practice is to identify external dependencies earlier during the BIA, as indicated by the State standards. This allows the impact of service interruption to be assessed if a disaster only affects an external source. The risk of identifying external dependencies later in the COOP process is that management won't have information necessary to understand and prioritize the impact of service disruptions if external dependencies are not considered. Prioritization based on external vendor dependencies can increase the scope of work. What is essential is that external dependencies are identified, management is made aware of them, and there is plan to address continuity risks from external vendors as needed.

A process has been created for including COOP considerations in the selection of technology vendors. A similar process should be considered for selecting external service providers and reflected in program maturity goals.

COOP Plans

A strategy for storage, accessibility and annual maintenance of COOP plans is not defined.

Currently there isn't a documented strategy for storage of completed COOP plans and how they will be made accessible to recovery personnel in case of an emergency. Annual maintenance is also required to address risks that come with out-of-date plans. Plan creation is still at an early stage, but these requirements are essential to the usefulness of plans during a disaster.

Strategies for transitioning back to normal are not present in COOP plans.

At the time of the audit only a small number of service recovery COOP plans were available for review. These plans did not include strategies for transitioning back to normal operations from a recovery state. Not having plans in place increase the risk of having issues during transition. For example, data may need to be entered manually into systems when they are restored and regulatory expectations may need to be resolved. Planning for a return to normal service will be an important consideration as the program reaches maturity milestones.

CONCLUSION

Overall, the COOP program has followed established continuity of operations planning practices. Governance emerged as a key area for improvement of the COOP program with specific recommendations for the risk assessment, business impact analysis and COOP plans.

The greatest challenge has been transitioning from plan development to a sustained, cyclical program within the organization in a timely manner. This is in part due to the size and complexity of the agency and the resources available to the program, though additional resources were allocated during the audit. Improved program governance can address these challenges in several ways:

- Polices and standards will help define the overall program and help stakeholders judge the quality of implementation.
- Defining the role of the steering committee will develop a cross-departmental body responsible for addressing implementation challenges, keeping program development on schedule and scrutinizing program development strategies.
- An implementation plan defining timelines, agreed upon program maturity milestones and strategies for development can make the project more manageable and accountable

RECOMMENDATIONS

Program Evaluation and Audit recommendations are categorized according to the level of risk they pose for the Council. The categories are:

- **Essential** – Steps must be taken to avoid the emergence of critical risks to the Council or to add great value to the Council and its programs. Essential recommendations are tracked through the Audit Database and status is reported twice annually to the Council's Audit Committee.
- **Significant** – Adds value to programs or initiatives of the Council, but is not necessary to avoid major control risks or other critical risk exposures. Significant recommendations are also tracked with status reports to the Council's Audit Committee.
- **Considerations** – Recommendation would be beneficial, but may be subject to being set aside in favor of higher priority activities for the Council, or may require collaboration with another program area or division. Considerations are not tracked or reported. Their implementation is solely at the hands of management.
- **Verbal Recommendation** – An issue was found that bears mentioning, but is not sufficient to constitute a control risk or other repercussions to warrant inclusion in the written report. Verbal recommendations are documented in the file, but are not tracked or reported regularly.

1. (Essential) Develop or adopt policies and standards for the COOP program. Consider adopting standards created by the State or those found in existing program documents for the following key program areas:
    - risk assessment/all-hazards approach
    - business impact analysis, including recovery time objective, external dependencies and frequency
    - recovery strategies, including transition back to normal operations
    - COOP plan documentation, including storage and accessibility
    - COOP plan maintenance, including a formal schedule for maintenance
    - COOP plan testing, including a formal schedule for testing
    - employee awareness

Management Response: *We agree that development of a business continuity policy and procedures (standards) will mitigate organizational risk by the formal definition and approval of business continuity best practices, rules, principles and guidelines for the Met Council. A policy will facilitate accomplishment of long-term business continuity goals by shaping important decisions and activities. Development of supporting procedures (standards) will provide additional structure for the organization to follow in key program areas. We will develop a policy and supporting processes for consideration and approval by executive management.*

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *September 2014 – approved policy is adopted.*

2. (Essential) Develop an implementation plan based on existing growth and maturity milestones for all program areas with timelines for completion. Metrics to inform stakeholders of program implementation status, maturity goals and quality should be considered for reporting.

Management Response: *We agree that development of an implementation plan and timeline, which incorporates all business continuity program areas, will better allow stakeholders to fully understand the enterprise program progress, maturity, and outstanding risk areas.*

Staff has developed a "baseline" implementation plan for mission-essential services. Baseline plans identify recovery strategies and continuity plans for mission-essential services with recovery time objectives of 1 week or less. For divisions/departments that do not have mission-essential services, a baseline COOP will address the NIMS reporting structure, essential communications structures (employees, vendors, customers, stakeholders) and call trees, and high-level recovery strategies. Development of metrics to keep stakeholders informed is within the scope of the implementation plan.

We will work to develop a complete business continuity implementation plan which addresses and incorporates all program areas, provides estimated timelines for completion, and allows for tracking and reporting of relevant metrics for Met Council stakeholders.

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *July 2014*

3. (Essential) Clarify the role of the steering committee to support COOP program development and continued maintenance in the organization. Potential roles for the steering committee include:
   - Monitoring the progress of the program against its goals and keeping program goals under review
   - Encourage and strengthen links between the program and other parts of the agency
   - Review and approve program implementation strategies to meet program goals
   - Review and approve recovery strategies for services and technology

Management Response: *We agree that strong leadership support is an essential component of business continuity program success in the organization, and that the topics / issues identified above should each be addressed. The appropriate management structure for reporting and ownership will be identified and the role and functions of the COOP Steering Committee will be clarified.*

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *June 2014*

4. (Significant) Develop or implement a communications plan to inform stakeholders of the program and its maturity in the organization.

Management Response: *We agree with this recommendation and will begin development of a multi-faceted Business Continuity Program communications plan that provides relevant information to various stakeholders.*

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *September 2014*

5. (Significant) Clarify the relationship between COOP and other emergency management response programs. Clarifying the differences in scope and responsibilities will help mitigate the risk that stakeholders misunderstand the level of overall emergency preparedness

Management Response: *We agree with this recommendation and will address and clarify this issue within the Business Continuity policy.*

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *September 2014*

6. (Consideration) Include COOP participation in yearly performance evaluations for key personnel and the coordination of COOP activities and annual work plans and in program policies, standards or maturity milestones. The success of COOP depends on the continued participation of all business units. Following the above steps will help mitigate the risk that some business units will not prioritize or resource COOP planning, negatively affecting overall emergency preparedness.

Management Response: *We agree with this recommendation and will identify and explore options with the COOP Steering Committee, with final decisions / outcomes possibly being incorporated within the Business Continuity policy.*

Staff Responsible: *Kathy Matter, Dave Hinrichs*

Timetable: *November 2014*

APPENDIX

Appendix 1: COOP Program Stages

Program Stage	Description
Management Commitment and Support[1]	- Establish steering committee and hire program manager - Develop policies and standards - Adequately resource program
Risk Assessment and Mitigation	- Identify credible events that could interrupt services - Develop mitigation strategies for credible events
Business Impact Analysis	- Identify and prioritize critical business processes - Identify impact should a service be disrupted - Identify internal and external service dependencies - Define recovery time objective (RTO) for how soon service needs to be recovered to avoided unacceptable consequences - Define recovery point objective (RPO) for how much data can be lost and recreated manually for technology systems
Service and Technology Recovery Strategies	- Develop testable recovery strategies for each critical service and technology - Strategies developed according to RTO and RPO
COOP Plans	- Plans are documented, include planning assumptions and necessary detail for recovery of services and technology - Team structure according to National Incident Management System (NIMS)
Maintenance and Testing	- Establish a formal program to maintain COOP readiness - Establish a formal program of testing and follow-up to verify recovery strategy effectiveness
Employee Awareness and Training	- Establish a formal employee training and awareness program for COOP

[1] This stage was taken from the Global Technology Audit Guide, Chapter 10. All remaining stages were taken from Minnesota State Standards.

METROPOLITAN
COUNCIL

390 Robert Street North
St Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org