THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

**Report**
Office of the General Auditor

## Internal Audit Report for November 2015


**Summary**

Four reports were issued during the month:

- **Information Technology Business System Data Backup and Recovery Audit Report and Management Response**
- **Quarterly Board Reports Review**
- **Colorado River Water Users Association Financial Report**
- **Official Statement for the Water Revenue Refunding Bonds, 2015 Authorization, Series A**


**Discussion Section**

This report highlights the significant activities of the Internal Audit Department during November 2015. In addition to presenting background information and the opinions expressed in the audit reports, a discussion of findings noted during the examination is also provided.

## Information Technology Business System Data Backup and Recovery Audit Report and Management Response

**Background**

The Audit Department has completed a review of the Information Technology (IT) controls over the Business System Data Backup and Recovery (Backup and Recovery) processes, as of May 31, 2015, Our review consisted of evaluating the controls over Backup and Recovery practices for computer systems, and data center facilities. We reviewed Backup and Recovery procedures over critical business systems, and tested the Business Technology (BT) Group's ability to recover and restore applications in a timely manner.

In addition, we examined the Water Systems Operations (WSO) Group Disaster and Recovery Plan over the Supervisory Control and Data Acquisition (SCADA) System. SCADA is used for automatic control of water distribution systems, and operates separately from the IT business systems. Finally, we reviewed the Chief Financial Officer (CFO) Business Impact Analysis (BIA) to ensure the data Backup and Recovery Plan was consistent with the IT Disaster Recovery Plan.

The Emergency Management and Business Continuity Operating Policy (A-06) describes how Metropolitan organizes and deploys resources to manage emergencies, and ensures continuity of water system operations and critical business processes. Policy A-06 also provides guidelines for evaluating and responding to emergencies, and explains how the Emergency Response Organization (ERO) Program is activated.

Date of Report: November 30, 2015

The ERO Program is an organizational framework adopted by Metropolitan, based on California's Standardized Emergency Management (SEM) System that provides a structured framework for responding to, and managing emergencies and disasters. Metropolitan's Emergency Management Program consists of three components: Emergency Response Organization, Business Continuity, and IT Disaster Recovery.

1. Emergency Response Organization activities are designed to address the immediate and short-term operational effects of an emergency. The WSO Group Manager is responsible for Emergency Response Organization efforts.

2. Business Continuity consists of strategies needed to reestablish critical business functions, with little or no downtime. The CFO is responsible for these efforts.

3. IT Disaster Recovery defines the processes used to restore the IT infrastructure, critical business systems, and recover user data. The IT Section Manager is responsible for this component.

Crucial to the IT Disaster Recovery Plan is information system Backup and Recovery Policies and Procedures. These activities ensure timely recovery of essential infrastructure, data, and applications to support recovery of critical business functions. The IT Section manages these functions through the combined efforts of two units.

First, the IT Infrastructure Unit controls the Backup and Recovery of day-to-day operations. These efforts involve daily server backups that protect against lost data resulting from corrupted files, the accidental deletion of data, or from a disaster. These processes allow for the recovery of application files to a previous restore point. The IT Infrastructure Unit also administers service contracts for offsite backup tape storage.

Secondly, the Project Planning Unit is responsible for ensuring continuity of the technology infrastructure and systems, by managing the IT Disaster Recovery Plan. The IT Disaster Recovery Plan is designed to ensure timely recovery of critical applications such as Exchange Outlook, Microsoft Office Suite, MyHR, Oracle Financial, Water Information System, Water Quality Labsheet System, and Travel Expense Reporter. Finally, the Project Planning Unit conducts periodic reviews and exercises to validate documented recovery policies, procedures, and assumptions.

**Opinion**

In our opinion, the controls and procedures over IT Backup and Recovery practices provide for a less than satisfactory internal control structure. This opinion is the result of differences between BIA and IT Business System Disaster Recovery Technical Recovery (BSDR) Procedures in identifying critical systems, and defining Recovery Time Objectives (RTOs). It should be noted that management has initiated remedial actions in response to our concerns.

**Comments and Recommendations**

EMERGENCY RESPONSE ORGANIZATION

The Emergency Management Program provides a structured framework for responding to, and managing emergencies and disasters. It consists of three components: Emergency Response, Business Continuity, and IT Disaster Recovery. Emergency Response activities are field-level actions designed to address immediate, and short-term operational effects of an emergency. The Business Continuity Plan consists of strategies needed to reestablish critical business functions, with little or no downtime. Finally, the IT Disaster Recovery Plan component defines the processes used to restore IT infrastructure, critical business systems, and user data.

BUSINESS CONTINUITY PLAN

These efforts consist of policies and procedures that ensure availability of critical business functions through recovery plan development, testing, and training. Central to this process is the preparation of a BIA and risk assessment. The BIA focuses on the consequences of an interruption to critical business functions, and quantifies the financial and nonfinancial impacts associated with a disaster. The objective is to identify mission-essential functions most crucial to ongoing operations. The BIA serves as a starting point for disaster recovery strategies, and identifies RTOs and Recovery Point Objectives (RPOs).

The risk assessment component identifies potential hazards such as an earthquake, fire, supplier failure, utility outage, or cyberattack and evaluates vulnerabilities. Assets at risk include people, property, supply chain, IT, and agency reputation. Points of weakness that make an asset more prone to harm are reviewed, and a mitigation strategy is developed to reduce the probability that an event will have a significant impact.

IT DISASTER RECOVERY PLAN

The IT Disaster Recovery Plan specifies procedures to follow to recover, and protect the IT infrastructure. The IT Section prepares for recovery needs by performing backups of critical applications and data files, to the Disaster Recovery Facility (DRF) located at Lake Mathews. In the event of a disaster, DRF is activated and the Disaster Recovery Plan is used to recover and restore critical IT infrastructure and applications. The IT Disaster Recovery Plan should be reconciled with the BIA report and should be periodically tested, evaluated, and updated. During our review we noted:

1. Reconciliation between BIA and IT BSDR Procedures was not completed. Specifically, we noted the BIA Report dated August 2014, identified 114 applications needed to be recovered in one day or less. However, IT BSDR listed 56 applications for recovery in one day or less.

2. RTOs between BIA and IT BSDR documents were not analogous. RTO is the targeted duration of time and service level within which a business process must be restored after a disaster, to avoid unacceptable consequences associated with a break in business continuity. We noted that BIA prioritized applications by six categories: those to be restored within one day, three days, one week, one month, three months, and those more than three months. The IT BSDR documentation, on the other hand, uses RTO time parameters of immediate, two hours, four hours, eight hours, 12 hours, 24 hours, 48 hours, and one week.

3. RPO analysis documentation could not be located. This analysis, which is essential to BIA, is the age of files that must be recovered from backup storage for normal operations to resume. The RPO is expressed backward in time and can be specified in seconds, minutes, hours, or days. Once the RPO has been defined, it determines the minimum frequency with which system backups must be made.

4. The Business Continuity Plan's alternate site mapping and workspace recovery documentation could not be located. The Business Continuity Plan should identify staff required to recover business processes within given timeframe, after a disruption.

5. Documentation of periodic disaster recovery testing for the interfaces between Microsoft Outlook E-mail and seven Metropolitan applications could not be located. These applications include: Energy Management System, Interim Enhanced Surface Water Treatment Rule, Incident Reporting, MyHR, Oracle Financial, Remedy and Travel Expense Reporter. We understand these applications require an interface with Outlook in order to provide workflow processing such as manager approvals, system alerts, and notification functions.

6. Documentation in support of periodic SCADA Disaster Recovery exercises could not be located. Specifically, we noted that the WSO Group performed a Disaster Recovery exercise for the SCADA system on May 28, 2015. However, documentation review revealed that the previous test was in March 2011.

7. Documentation that SCADA backup tapes were sent monthly to offsite storage could not be located, in accordance with Metropolitan policies. It should be noted that the WSO Group staff have started documenting the pickup and delivery of tape backups to the offsite storage facility.

We recommend the Business Continuity Program Manager and IT Section management reconcile the BIA Application RTO Report to the IT BSDR Technical Recovery Procedures listing. In addition, we recommend RTO and RPO parameters be standardized to ensure consistency, and to normalize risk profiles. We also recommend management develop manual work around recovery procedures, in the event the restoration of IT service is delayed. Lastly, we recommend management establish procedures to ensure recovery exercise documentation is complete, and that posttest reviews are completed.

PHYSICAL SECURITY

Physical security procedures are designed to provide for the safeguarding of facilities, equipment, and resources from accidental destruction, deterioration, or disasters. Security measures include controlled access points, surveillance devices, and may include separating key equipment so a single incident cannot compromise critical assets. Our review of the physical security over SCADA servers revealed two units installed in the same control room. Housing backup servers in the same location increases the risk of damage by a single disaster.

We recommend management physically separate the servers to minimize the risk of damage.

SERVER RECOVERY PROCEDURES

Policies and procedures should be written, reviewed, and updated periodically to reflect changes to organization needs and provide clear guidance to staff. Metropolitan's Operating Policies and Centralized Bare Metal Restore of Windows Clients - Metropolitan Server Administration Guides provide guidance for the rebuild of a Windows Client Server, from a backup. Our review revealed server backup, and restore procedures have not been updated since 2006. We understand recent server upgrades have prompted changes to these procedures.

We recommend IT periodically update the guide.

---

## Quarterly Board Reports Review

We reviewed the Report of Professional Services Agreements (Professional Services Report) and the Report of Contracts for Equipment, Materials, Supplies, and Routine Services of $250,000 or Above (Contracts Report) for the Fourth Quarter of fiscal year 2014/15, published by the Business Technology Group, Administrative Services. The purpose of this review is to gain reasonable assurance that information included in these reports is accurate, complete, timely, and in compliance with the Metropolitan Water District Administrative Code.

PROFESSIONAL SERVICES AGREEMENTS REPORT

**Background**

Administrative Code Section 2720(a)(2) requires that the General Manager report to the Engineering and Operations Committee on the employment of any professional and technical consultant, the extension of any professional and technical consulting agreement, and on the Exercise of Authority under Sections 8121(c) and 8122(h) during the preceding calendar quarter. The Administrative Code also requires the Professional Services Report indicate when a consultant is a former Metropolitan employee.

Administrative Code Sections 2721 - 2723 require the General Counsel, General Auditor and Ethics Officer report quarterly to their respective committee concerning any expert or professional service agreements executed pursuant to their authority under the Administrative Code.

The Professional Services Report is prepared on a quarterly and annual basis to comply with these Administrative Code requirements and identify those contracts administered by the General Manager, General Counsel, General Auditor, and Ethics Officer.

During fiscal year 2014/15, the Professional Services Report disclosed that $182.5 million was paid for consulting and professional services. We compared the amounts expended on professional services during this fiscal year against the prior fiscal year, and noted an increase of $121.8 million. The Electric & Gas Industries Association Agreement 129415, under the Water Resource Management Group for Metropolitan's Regional Conservation Rebate Program, accounted for $113.9 million of the total increase in expenditures amount.

It should be noted that totals reported under the General Counsel's authority exclude payments related to the San Diego County Water Authority litigation, which is accounted for under the Self-Insurance Retention Fund. We also noted that for fiscal year 2014/15, 80 of 493 agreements were sole-source agreements totaling $9,724,445. This is 5.3 percent of total fiscal year-to-date expenditures, compared to 69 of 478 totaling $5,015,824 in fiscal year 2013/14. Fraser Communication Agreement 143867 (Fraser) was $4,748,757 of the total sole-source agreement amount. The Fraser agreement has been audited.

We also noted that 108 of 493 agreements were small purchases of less than $24,999 totaling $488,624 of total fiscal year-to-date expenditures in fiscal year 2014/15. See table below for details.

| FY 2014/15 | General Manager | General Counsel | General Auditor | Ethics Officer |
|---|---|---|---|---|
| Contract Expenditures | $182,176,422 | $1,190,723 | $305,031 | $43,874 |
| Active Agreements | 330 | 37* | 1 | 4 |
| Terminated Agreements | 158 | 3 | 0 | 0 |

*Agreements with transactions during the current fiscal year.

**Testing Procedures Performed**

Our procedures included a cursory review of the reasonableness of the professional service expenditures and analysis of consultants with multiple active agreements, to determine whether an agreement was split into smaller contract amounts to circumvent established approval limits. We also evaluated whether statistics in the Professional Services Report were adequately supported, and assessed the timeliness of board reporting.

**Testing results**
Our review did not reveal any agreements that appeared to be unreasonable, or split to override established approval limits. In addition, our review did not reveal any material differences between reported amounts and supporting documentation. However, we recommend management consider labeling sole-source agreements with a unique identifier for easy reference. Finally, we noted the Professional Services Report was issued to the Board on September 22, 2015.

CONTRACTS FOR EQUIPMENT, MATERIALS, SUPPLIES, AND ROUTINE SERVICES OF $250,000 OR ABOVE REPORT

**Background**
Administrative Code Section 2720(b)(2) requires that the General Manager report to the Finance and Insurance Committee on the execution of any contract authorized under Section 8122(g) – Contracts for Equipment, Materials, Supplies, and Routine Services. This code section states that the General Manager may execute contracts for the purchase of materials, supplies, and other consumable items such as fuels and water treatment chemicals generally identified in the budget regardless of dollar value, provided that sufficient funds are available within the adopted budget for such purchases.

The Contracts Report is prepared on a quarterly basis to report on contracts that comply with these Administrative Code requirements. During the quarter ending June 30, 2015, the Contracts Report disclosed six contracts fitting these criteria. We noted the total maximum amount payable for these contracts was $6.9 million. Two of these contracts were awarded as a result of competitive bidding, and four were sole-source contracts authorized under Administrative Code Section 8140 – Competitive Procurement.

**Testing Procedures Performed**
Our procedures included a cursory review of the reasonableness of expenditures. We also verified that all contracts of $250,000 or more for specified items were included in the Contracts Report, and adequately supported. Finally, we reviewed sole-source agreements for justification and approval, and assessed the timeliness of board reporting.

**Testing results**
Our review did not reveal any discrepancies between contracts and amounts shown in the Contracts Report, and supporting documentation. We also noted that the policies and procedures for competitive bidding, cooperative agreements, and awarding sole-source agreements are in place. Finally, we noted the Contracts Report was issued to the Board on September 22, 2015.

---

## Colorado River Water Users Association Financial Report From April 1, 2014 Through March 31, 2015

We have completed a review of the Colorado River Water Users Association (CRWUA) Financial Report from April 1, 2014 through March 31, 2015. The following summarizes the Scope of Work performed, and results obtained.

Date of Report: November 30, 2015

**Scope and Purpose**
We performed the following procedures to gain reasonable assurance that information included in the CRWUA Financial Report from April 1, 2014 through March 31, 2015 was accurate, and supported by appropriate documentation.

**Background**
CRWUA was founded in 1945, and incorporated in the State of Nevada on December 6, 1968. Its mission is to provide a forum for exchanging ideas and perspectives on Colorado River water use and management with the intent of developing and advocating common objectives, initiatives, and solutions. From April 1, 2014 through March 31, 2015, CRWUA reported total receipts of $386,486, and total disbursements of $439,686. It should be noted there was a net loss of $53,200 during this period due to unanticipated increase in conference costs. As of March 31, 2015, CRWUA total funds available were $605,521.

**Testing Procedures Performed**
1. We agreed with the financial information from the CRWUA Financial Report to source documentation such as bank statements, receipts, and third-party documents.

2. We performed analysis and computations when necessary, and validated 100 percent of information contained in the CRWUA Financial Report to summary documents.

3. We examined monthly bank reconciliations, assessed reasonableness of reconciling items, and accuracy of balances.

Since our examination was limited to the Scope of Work, we do not express an opinion on the internal control structure over the CRWUA Financial Report taken as a whole.

**Testing results**
Our examination did not reveal any material differences between the reported amounts, and supporting documentation.

---

## Official Statement for the Water Revenue Refunding Bonds, 2015 Authorization, Series A

The Audit Department has completed a review of the Official Statement for the Water Revenue Refunding Bonds, 2015 Authorization, Series A. We performed this review to provide the issuer of the Bonds comfort that the Official Statement for the Bonds is complete, consistent with supporting financial records, and accurate in all material respects. We completed our review in accordance with agreed-upon procedures specified by the underwriters. We found such information to be correct in all material respects. We issued letters to the underwriters describing the agreed-upon review procedures performed, and results obtained.

---

Date of Report: November 30, 2015

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

**Date**: November 13, 2015

**To**: Gerald C. Riss, General Auditor

**From**: Thomas Miller, Director of Information Technology
Brent Yamasaki, Section Manager, Water Operations & Planning
Jose Sanchez, Program Manager III, Office of Chief Financial Officer

**Subject**: Response to IT Business System Data Backup and Recovery Audit Report

Thank you for the Audit Department's review of the Information Technology (IT) backup and recovery capabilities. Your findings provided a valuable perspective that will assist staff in continuing to improve upon those capabilities.

Attached is a table outlining management's response to the comments and recommendations contained in your review of controls over IT Business System Data Backup and Recovery processes as of May 31, 2015. You will note that we concur with all of your recommendations and that improvements in many areas identified in the subject Audit had already been in process during the time of your review. Management is committed to completing the efforts outlined in a timely and methodical manner.

As we believe you will find in our responses, management takes seriously their responsibility to help ensure that Metropolitan is able to withstand a significant disruption or disaster while continuing to provide essential services to our service area.

We welcome the opportunity to further discuss any of these issues with you and your staff.

Distribution:
J. Kightlinger
M.L. Scully
D.R. Ghaly
D.C. Man
G.M. Breaux
F.M. Mares
R.K. Patterson
D. Zinke
H.C. Beatty
J.A. Vanderhorst
J.C. Clairday
J.F. Green
G.L. Johnson
D. Pitman
S.H. Sims
D.N. Upadhyay
H. Soper
O.T. Tucker
J.J. Arena
A. Lopez
A. Azmi
G. Wilkins
R. Deaves
M. Van Dyke
R. Robinson
C. Gutierrez
S. Hung

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| Emergency Response Organization Business Continuity & IT Disaster Recovery | 1) Reconciliation between the Business Impact Analysis Report (BIA) and the IT Business System Disaster Recovery Technical Recovery Procedures (IT BSDR) was not completed. Specifically, we noted that the BIA report dated August 2014 identified 114 applications that were critical and needed to be recovered in one day or less. However, the IT BSDR listed 56 applications for recovery in one day or less. | Management has completed some of the tasks identified within BIA and is in the process of completing the remaining tasks. The status of these items is summarized as follows: | | |
| | | **Tasks In Process**<br>a) Confirm Critical Applications. From the original 178 applications identified within the BIA, 106 Mission Essential Applications (MEAs) were presented to Emergency Management Working Group (EMWG) for final approval on Sept 4, 2015. EMWG questioned the need for some MEAs and if the list could be refined and/or manual processes developed that could mitigate for outage of the MEA. | Business Continuity (BC) Program Manager and stakeholders. | January 29, 2016 |
| | | **Tasks Completed**<br>b) Performed a Gap Analysis between IT's BSDR applications and the BIA's applications. | BC Program Manager and IT | Completed July 24, 2014 |
| | | c) Developed an estimated budget and resource required for Disaster Recovery based on the number of applications in the BIA. | IT | Completed July 28, 2015 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| | 2) Recovery Time Objectives (RTO) between the BIA and the IT BSDR documents were not analogous. RTO is the targeted duration of time and service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. We noted that the BIA prioritized applications by six categories; those to be restored within one day, three days, one week, one month, three months, and those more than three months. The IT BSDR documentation, on the other hand, uses RTO time parameters of immediate, two hours, four, eight, twelve, twenty four, forty eight hours, and one week. | Management has completed the task associated with this recommendation. The BC Program and IT agreed to refine the recovery categories / parameters to hours for all Recovery Point Objectives (RPO) and RTOs less than 3 days (i.e., 72 hours and less) and to adopt the BIA durations going out to "more than 3 months". | BC Program Manager | Completed May 26, 2015 |
| | 3) Recovery Point Objective (RPO) analysis documentation could not be located. This analysis, which is essential to the BIA, is the age of files that must be recovered from backup storage for normal operations to resume. The RPO is expressed backward in time and can be specified in seconds, minutes, hours or days. Once the RPO has been defined, it determines the minimum frequency with which system backups must be made. | The BIA recommended that Metropolitan revisit the 15 minute RPO with organizations to ensure that it still meets business needs. That review is dependent on each organization establishing manual procedures to recapture lost data for each of their Mission Essential Functions (MEFs). These procedures are to be developed as part of the upcoming update of BC Plans facilitated by implementation of the BC Program Management System using Fusion Framework, scheduled for launch in January 2016. | BC Program Manager | May 30, 2016 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| | 4) Business continuity alternate site mapping and workspace recovery documentation could not be located. These plans should identify staff required to recover business processes within given timeframe after a disruption. | The BIA recommended that Metropolitan review the data from the BIA against the recovery site capabilities for "workspace recovery" in order to formalize a business recovery site strategy. The BC Program Management System, scheduled for launch in January 2016, has been designed to help identify available workspace for relocation of MEFs disrupted by a disaster. In addition, each organization's BC Plan is to identify the personnel that will be needed to recover each MEF over time. Analysis of this information will permit completion of methods / procedures to match the workspace needs to available workspace as part of the BC Plan. | BC Program Manager | June 30, 2016 |
| | 5) Documentation of periodic disaster recovery testing for the interfaces between Microsoft Outlook email and seven Metropolitan applications could not be located. These applications include: MyHR, Oracle Financial, IESWTR, Energy Management System, Incident Reporting, Travel Expense, and Remedy. We understand that these applications require an interface with Outlook in order to provide workflow processing such as manager approvals, system alerts, and notification functions. | Management concurs with the recommendation in principle. There is a problem running two Microsoft Outlook email systems at Metropolitan that has not been resolved. During the annual Data Center power outage IT runs a DR test with the email system from the DRF facility that integrates with Metropolitan's production applications. In the future IT will be assessing the feasibility of creating a limited test email system to support DR testing without compromising day to day operations and production at risk. | IT | June 30, 2016 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| | 6) Documentation in support of periodic SCADA disaster recovery exercises could not be located. Specifically, we did note that WSO performed a disaster recovery exercise for the SCADA system on May 28, 2015. However, documentation review revealed that the previous test was in March 2011. | Management concurs with the recommendation. SCADA has updated their disaster recovery exercise procedures to ensure that annual SCADA recovery exercises are conducted and documented. Additionally, another disaster recovery exercise was successfully completed in October 2015. | SCADA | Completed October 15, 2015 |
| | 7) Documentation that SCADA backup tapes were sent monthly to offsite storage could not be located in accordance with Metropolitan policies. It should be noted that WSO staff have started documenting the pickup and/or delivery of tape backups to the offsite storage facility. | Management concurs with the recommendation. Offsite storage of SCADA backup tapes was temporarily suspended between January and April 2015 to implement an enhanced system backup application with improved features. During this time staff maintained a master hard drive set to allow recovery of SCADA servers, as a temporary alternate backup method. Offsite storage of SCADA backup tapes has resumed since April 2015. | SCADA | Completed April 30, 2015 |
| | 8) We recommend that the Business Continuity Program Manager and Information Technology Section management reconcile the BIA Application Recovery Time Objectives report to the IT BSDR Technical Recovery Procedures listing. | Management has completed the tasks associated with this recommendation. BC Program Manager adopted IT's RTO categories and the IT DR program adopted the BIA RTO durations. Both will work to prioritize recovery within those timeframes based on the disruption rating of the MEAs supported by the applications. | BC Program Manager and IT | Completed May 26, 2015 and October 30, 2015 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| | 9) In addition, we recommend that the RTO and RPO parameters be standardized to ensure consistency and to normalize risk profiles. | Management concurs with the recommendation. The BC Program and IT agreed to refine the recovery categories / parameters to hours for all RPOs and RTOs less than 3 days (i.e., 72 hours) and to adopt the BIA durations going out to "more than 3 months". These refined recovery timeframes will be used to triage recovery of applications based on the disruption rating of the MEAs supported by the applications. | BC Program Manager | Completed May 26, 2015 |
| | 10) We also recommend management develop manual work around recovery procedures in the event the restoration of IT service is delayed. | Management concurs with the recommendation. The manual procedures for recovering MEFs are to be developed in the upcoming update of BC Plans facilitated by the implementation of the BC Program Management System using Fusion Framework. | BC Program Manager | June 30, 2016 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| | 11) Lastly, we recommend management establish procedures to ensure that recovery exercise documentation is complete and that post-test reviews are completed. | Management concurs with the recommendation. IT's test procedures are outlined within IT Disaster Recovery Program Standard Operations Procedures Manual and test documents are available with post-test reviews since 2005.<br><br>BC Program exercise documentation of Business Recovery Exercise (BRE) procedures and post-exercise follow-up since 2006 are available on the network drive for review.<br><br>SCADA recovery exercise procedures are outlined within the SCADA Disaster Recovery Plan / Exercise Procedures document, which contain post-test exercise results, issues and resolutions. | IT, BC Program Manager, and SCADA | **IT**<br>Completed April 2008<br><br>**BC**<br>Completed May 2007<br><br>**SCADA**<br>Completed April 30, 2015 |

**Response To Internal Audit**
**2015 IT Business System Data Backup and Recovery**

| Review Area | Comments and Recommendations | Management Response | Responsible Area | Target Completion Date |
|---|---|---|---|---|
| Physical Security | 12) Our review of the physical security over SCADA servers revealed two units installed in the same control room. Housing backup servers in the same location increases the risk of damage by a single disaster. We recommend management physically separate the servers to minimize the risk of damage. | Management concurs with the recommendation in principle. A study will be performed to evaluate the feasibility, logistics and cost of ancillary systems (i.e. HVAC, uninterruptible backup power, fire suppression, access security, etc.) to physically house SCADA servers in separate locations within the treatment plants and Desert pumping plants. At the conclusion of the study a capital project will be proposed to separately locate the SCADA servers where physically and economically feasible. | SCADA | June 30, 2016 |
| Server Recovery Procedures | 13) Our review revealed server backup and restore procedures have not been updated since 2006. We understand that recent server upgrades have prompted changes to these procedures.<br>Incomplete and outdated procedures may impact Metropolitan's ability to restore Windows Client Servers in a timely fashion, compromising its ability to meet daily business needs.<br>We recommend that IT periodically update the guide. | Management concurs with the recommendation in principle. It should be noted that the procedures from 2006 were valid until a recent upgrade to the backup and recovery software. During the recent upgrade, staff began working with the vendor to update the procedures. Currently, draft procedures have been developed and staff continues to work with the vendor to finalize the procedures. | IT | January 29, 2016 |