THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Report
Office of the General Auditor
September 30, 2013

Internal Audit Report for September 2013

Summary

Three reports were issued during the month:

- **Community Partnering Program and California Friendly-Landscape Program Audit Report**
- **Audit Quality Assurance – Audit Plan Update Report**
- **Cyber Security over Metropolitan Computer Networks**

Discussion Section

This report highlights the significant activities of the Internal Audit Department during September 2013. 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.

Community Partnering Program and California Friendly-Landscape Training Program Audit Report

Background

Metropolitan established the Community Partnering (CP) Program in 1999 to provide funding for sponsorships of water conservation and water-use programs and activities. In addition to sponsoring local events, the CP Program also sponsors organizations at the state and national levels when programs proposed by such organizations meet CP Program goals and objectives. Organizations may request up to $2,000 for educational activities regarding regional water conservation and water-use efficiency issues. Sponsorship funding of $169,451 were made during the period of January 1, 2009 through June 2013 for 185 grant applicants.

The California Friendly-Landscape Training (CFLT) Program was established in 1993 to offer training on water-efficient landscape management practices to residents within Metropolitan's service area. Originally known as the Protector de Agua Program, courses were developed for both residential gardeners and landscape professionals.

In the residential program, customers (residential gardeners) were trained in the basics of irrigation systems, watering and fertilizing, landscape design, and plant identification. Landscape professionals were trained in landscape water management practices such as design, soil preparation, native plant selection, efficient irrigation systems, and water controller technologies. These training programs were initially bound to a classroom format, but were enhanced in 2005 with an on-line training option.

The CFLT Program was initially developed and managed by the Water Resource Management (WRM) Group. At the request of the WRM Group, it was transferred to External Affairs in July 2008 to better align the CFLT Program goals with External Affairs education programs. In December 2010, the CFLT Program was suspended due to budget reductions, although it has been reinstated under the auspices of the WRM Group. The disbursements for the period of January 1, 2009 through December 31, 2010 were $184,987, during which 5,657 individuals attended CFLT Programs.

Opinion
In our opinion, the accounting and administrative procedures over the CP Program and CFLT Program include those practices usually necessary to provide for a satisfactory internal control structure. The degree of compliance with such policies and procedures provided effective control for the period of January 1, 2009 through June 30, 2013.

Comments and Recommendations
There were no material findings to report.

Audit Quality Assurance – Audit Plan Update

Background
In order to ensure that the Audit Department (Department) continues to add value to Metropolitan, we implemented a Quality Assurance and Improvement Program (QA&IP), as set forth by The Institute of Internal Auditors (IIA) in its' International Standards for the Professional Practice of Internal Auditing (*Standards*). Compliance with these *Standards* ensures that the Department provides independent, professional, objective assurance, and consulting services that help improve Metropolitan's operations.

This QA&IP encompasses all types of audit processes. That is, they include internal and external communications, audit planning and field work, staff supervision and development, and preparation and execution of the Annual Audit Plan. The QA&IP requirements are thorough and extensive. There are three components of QA&IP that include conducting training and ongoing quality activities, performing internal quality assessments annually, and obtaining external assessments of audit operations and processes every five years. Towards that end in June 2012, IIA performed an external Quality Assurance Review and judged the Department to be in overall general compliance with the *Standards*, the highest rating possible.

With regard to annual internal quality assessments, we completed the 2012/13 Internal Quality Assessment utilizing the IIA's Quality Assessment guidance and methodology. The principal objectives of this review were to examine our conformity to the *Standards* and department procedures; evaluate our effectiveness in carrying out our mission, as set forth in the Department Charter; and identify opportunities to enhance the Department's value to Metropolitan. We reviewed audit communications with the Board, Audit and Ethics Committee, and management; evaluated risk assessment and audit planning processes; reviewed audit policies and procedures; and analyzed engagement and staff management processes. Additionally, we conducted anonymous surveys of audit clients and audit staff to obtain feedback and identify both strengths and areas for improvement. Central to our assessment was a detailed review of a selection of audit work papers and audit reports, in comparison with the *Standards*.

Conclusions
It is our overall opinion that the Department generally conforms to the *Standards* and Code of Ethics. This rating means the Department has a Charter, policies, and processes that are judged to be in conformance with the *Standards*. However, we noted opportunities for improvement related to the IIA's Practice Advisories or best practices. These observations are related to the Department's compliance with policies and procedures, and methods to enhance the Department's effectiveness.

COMPLIANCE WITH POLICIES AND PROCEDURES

In order to ensure high quality and professional audit work, auditors should conform to established Department policies and procedures. These procedures ensure that resources are properly supervised to achieve objectives, assure quality, and develop staff. Additionally, Department training policies require that auditors obtain minimum Continuing Professional Education (CPE) to ensure that audit skills are developed and industry knowledge remains current.

Our review of a sample of audit work papers indicated that evidence of audit supervision, such as approving audit work papers could be improved. In one instance, an audit report was issued without supervisory sign off of all work papers, as having been reviewed and approved. Additionally, we noted that some auditors did not complete CPE requirements, in accordance with Department procedures.

We have developed steps to strengthen compliance with Department policies and procedures. First, we reminded auditors of existing procedures that require supervisory review and approval of work papers, prior to issuance of audit reports. Next, we reinforced to auditors their responsibility to meet departmental CPE requirements. Finally, we plan to identify potential training courses of greatest benefit to the Department.

ENHANCE DEPARTMENT EFFECTIVENESS

The Department has established internal management, communication, and monitoring processes to ensure that Department staff resources are effectively deployed and communication processes with management are sound. Recently, we introduced Engagement Letters to management to announce the commencement of an audit, identify assigned audit resources, and convey the anticipated timing for the Entrance Conference. Such communication practices are essential to fostering professional working relationships with our audit clients. In addition, we recently introduced internal Planning Conferences to facilitate a robust risk and control assessment discussion in the initial stages of an audit, resulting in more efficient audit work.

As part of our internal quality assessment, we requested anonymous feedback from audit clients concerning the audit process, relationships with staff, and the value added of audits. While the client feedback was largely positive, several clients noted that the duration of audits and adherence to audit scope could be improved. Our analysis of the audit-cycle time from beginning to end for audits completed during FY 2012/13 suggested an opportunity to manage resources more effectively, particularly with respect to audit planning activities. Finally, we identified an opportunity to enhance the quality of the draft audit report preparation and review processes.

We will continue to fine-tune the use of Planning Conferences to help ensure the efficient use of audit resources. Additionally, we plan to identify and implement methods to streamline audit processes and increase auditor productivity. These methods may include identifying enhancements to audit planning, field work and reporting activities through the implementation of checklists, and internal monitoring reports.

Cyber Security Over Metropolitan Computer Networks

Background

Threats to network security have grown and evolved considerably over the past few years. Outside the realm of states and their proxies, corporate spies are using increasingly advanced techniques to steal company secrets or customer data for profit. Moreover, hacktivists with political and antibusiness agendas are also busy. A U.S. Government Accountability Office report published in February 2013 corroborates these trends by noting a 782-percent increase in the number of reported security breaches of federal agencies between 2006 and 2012. The latest attack targets were the U.S. banks, technology companies, media outlets, and public utility agencies. The perpetrators (hackers) have disrupted their targets' online services, defaced their public Web sites, and stolen supposedly protected information including trade secrets, strategic plans, records of transactions, and personal confidential data. Protection against these threats is multifaceted and dynamic; that is, controls should exist at the user, computer, application, server, and network levels. Moreover, constant vigilance is necessary to ensure computer controls remain effective within the evolving cyber environment.

Scope

The objective of this review was limited to an evaluation of the adequacy of security controls over Metropolitan's networks. However, the review differed from traditional network security reviews of password management practices. Our review assessed the vulnerability of our networks against known cyber threats. We utilized a third-party network security tool to simulate a cyber-attack on our networks from the internet, and identify potential security vulnerabilities. We also reviewed network controls that prevent, detect, respond, and recover from cyber threats. We believe that these control components contribute to an Enterprise Grade Network Security Program that serves as a guide in the rapidly evolving cyber security environment.

We would like to thank the staff of the Information Technology Section's Information Security (InfoSec) Unit for providing detailed information regarding Metropolitan's networks, for their assistance in identifying key concerns, and for their aid in discussing the control elements utilized to mitigate these risks.

Our study and evaluation made for the limited purpose described in the preceding paragraphs would not necessarily disclose all material weaknesses in the system. Accordingly, we do not express an opinion on the internal control structure over the use of these technologies.

Comments

Our review revealed that InfoSec has implemented the necessary control components to defend against cyber threats. Our network scans did detect four minor network vulnerabilities. We provided the details of these deficiencies to InfoSec management, who applied technical fixes to resolve the noted weaknesses. Our review also initiated a discussion of the merits of periodic network vulnerability scans. We understand that InfoSec management is considering the efficacy of such tools.

Methodology

We utilized a third party software tool, Nessus® vulnerability and configuration product, to simulate the cyber-attack. Tenable Network Security, Incorporated developed the Nessus product to detect network vulnerabilities, and to perform configuration assessments. Their products and services are in use throughout the U.S. Department of Defense and by many of the Fortune 500 companies.

The Nessus® product features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis. Our tests consisted of scans of the target network systems to identify open communication channels (open ports), and then involved various exploits in search of vulnerabilities. The Nessus® vulnerability scanner utilized various types of attacks that include a continuously undated library of more than 55,000 vulnerability and configuration checks.

We selected two Metropolitan web pages accessible to the public for the review: www.mwdh2o.com and www.bewaterwise.com. Based on the scan results, four minor vulnerabilities were reported by Nessus®. We have confirmed that the impact of identified vulnerabilities were minimal. InfoSec has taken remedy actions to address these issues.

#	Vulnerability	MWD Website	Risk Level
1	ASP.NET DEBUG Method Enabled	bewaterwise.com	Medium
2	Web Server HTTP Header Internal IP Disclosure	bewaterwise.com	Low
3	Web Server HTTP Header Internal IP Disclosure	mwdh2o.com	Low
4	Web Server Uses Plain Text Authentication Forms	mwdh2o.com	Low