



Internal Audit Report for April 2019

Summary

Two reports were issued during the month:

- 1. Privileged Account Management Audit Report**
- 2. Quarterly Consulting and Services Contracts Review Report for Period Ending December 31, 2018**

Discussion Section

This report highlights the significant activities of the Internal Audit Department during April 2019. In addition to presenting background information and the opinion expressed in the audit report, a discussion of findings noted during the examination is also provided.

Privileged Account Management Audit Report

The Audit Department has completed a review of cybersecurity controls over Privileged Account Management as of October 31, 2018.

Scope

Our review consisted of evaluating the management of privileged accounts by the Cybersecurity Unit (Cybersecurity) of the Information Technology Group (ITG). Specifically, we reviewed privileged account user assignments, access control and activity tracking. The platforms we reviewed included network routers, firewalls, Windows domains, HP-UX UNIX operating systems, Oracle database management system (DBMS), and SQL database servers.

Background

The Information Technology Group delivers information technology services and solutions for Metropolitan business applications, control systems, mobile/wireless computing, telecommunications, network services, and cybersecurity. The Cybersecurity Unit is responsible for monitoring daily security operations, implementing security controls, and establishing policies and standards over the Metropolitan's network routers, firewalls, operating systems, database management systems, and business applications. The Cybersecurity Unit reports to ITG and consists of eight staff members with a combined operational budget and capital improvement funding of \$6.4 million for fiscal year 2018/19.

Opinion

In our opinion, the cybersecurity controls over Privileged Account Management include those practices usually necessary to provide for a generally satisfactory internal control structure. The degree of compliance with such policies and procedures provided effective control for the period ending October 31, 2018. Although this opinion is an acceptable rating, we do express concern over exposures related to the sharing of privileged accounts. During our review, ITG began implementing revised policies, procedures and account management tools which will address these concerns. We understand that they plan to complete these initiatives by September 1, 2019. We encourage ITG to complete these actions.

Comments and Recommendations**PRIVILEGED ACCOUNT ACCESS MANAGEMENT**

Access to Metropolitan's systems and platforms is restricted through user accounts and passwords. For day-to-day business operations, employees are assigned a user account access profile that is commensurate with their operating responsibilities. These profiles limit permanent access privileges to those systems, roles and functions related to the employee's regular duties.

Privileged accounts, on the other hand, grant permanent Domain account credentials to users such that they have the ability to change system configurations, install software, change user account profiles or access secure data. Consequently, malicious parties may seek to hijack privileged accounts in order to exploit the Domain Admins account credentials with anonymity that compromises detection. Accordingly, ITG restricts the use of privilege accounts in all but essential circumstances.

During our review we noted that policies and procedures do not address the specific circumstances for privileged accounts. Additionally, we noted that privileged accounts are shared and passwords are not set to change every 60 days on the following platforms:

Platform	Server	Audit observation on the noted Privileged/Service/Shared Accounts
Windows Domains		301 service accounts
Windows Server	usmwd275	1 administrator account and 2 service accounts
Windows Server	usmwd298	1 administrator account and 3 service accounts
Windows Server	usmet33	1 administrator, 1 group shared account, and 1 service account
Windows Server	lmex10csht01	1 administrator and 6 service accounts
Windows Server	lmex10mbs01	1 administrator and 6 service accounts
HP-UX UNIX	itsrv31c	30 service accounts and 3 group shared accounts

Palo Alto Firewalls		2 shared accounts with super user privileges.
Oracle Database Management System Servers		158 privileged/service accounts are shared accounts.
Microsoft SQL Servers		11 administrator and 275 power user accounts

Lack of compliance to sound policies and procedures may result in unauthorized system access and undetected intrusions.

We recommend that ITG establish privileged account policies and procedures including:

- Maintaining a complete inventory of privileged accounts
- Minimizing the number of privileged accounts
- Minimizing usage of default administrator, root and similar accounts
- Mandatory password expiration
- Prohibition against sharing privileged accounts
- Logging and monitoring of privileged account activity
- Assigning privileged accounts in accordance with the principal of least privilege

Quarterly Consulting and Services Contracts Review Report for Period Ending December 31, 2018

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 (Contracts Report) for the Second Quarter of fiscal year 2018/19, issued by the Chief Administrative Office. 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

Scope

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.

Background

Administrative Code Section 2720(e)(2) requires that the General Manager report to the Organization, Personnel and Technology 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 to indicate when a consultant is a former Metropolitan employee. Administrative Code Sections 2721-2723 require the General Counsel, General Auditor and Ethics Officer to 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 the quarter ending December 2018, the Professional Services Report disclosed that \$32.48 million was paid for consulting and professional services. 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.

For the quarter ending December 2018, 53 of 387 agreements were sole-source agreements totaling \$2.9 million. This represents 9% of total fiscal year-to-date expenditures for fiscal year 2018/19. We also noted that 85 of 387 agreements were small purchases of less than \$24,999, totaling \$387,604. See tables below for detail:

Fiscal 2018/19 Year-to-Date Q2	General Manager	General Counsel	General Auditor	Ethics Officer
Contract Expenditures	\$32,088,799	\$242,094*	\$154,300	\$14,507
Active Agreements	361	110	1	2
Agreements Terminated	23	3	-	-

* For agreements with transactions during the current fiscal year.

Govt. Agencies	RFP	RFQ	Small Purchases	Sole Source	Total**
\$536,711	\$17,264,821	\$11,394,870	\$387,604	\$2,893,048	\$32,477,053
12	43	194	85	53	387
2%	53%	35%	1%	9%	100%

**Total does not include General Counsel’s Expenditures

Opinion

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 the reported amounts and supporting documentation. Finally, we noted the Professional Services Reports for the quarter ending was issued to the Board on April 9, 2019.

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

Scope

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 assessed the timeliness of board reporting.

Background

Administrative Code Section 2720(e)(2) requires that the General Manager report to the Organization, Personnel and Technology 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 December 31, 2018, the Contracts Report disclosed ten contracts that fit these criteria. We noted the total maximum amount payable for these contracts was \$10.9 million. Seven of these ten contracts were awarded as a result of competitive bidding, whereas the remaining three were sole sourced.

Opinion

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 and sole source agreements are in place. Finally, we noted for quarter ending December 31, 2018 Contracts Report was issued to the Board on April 9, 2019.