



## THE CITY OF SAN DIEGO

DATE: January 31, 2017  
TO: Audit Committee Members, Honorable Mayor and Members of the City Council  
FROM: Eduardo Luna, City Auditor  
SUBJECT: IT Audit of the City of San Diego's SAP Privileged User Access Management Process

Transmitted herewith is an audit report on the Department of Information Technology's SAP privileged user access management process. This report was conducted in accordance with the City Auditor's Fiscal Year 2017 Audit Work Plan, and the report is presented in accordance with City Charter Section 39.2. The Audit Results are presented on page 5 of the report. Management provided a response to the confidential report and agreed with all the recommendations.

We would like to thank the Department of Information Technology and Office of the City Comptroller's staff for their assistance and cooperation during this audit. All of their valuable time and efforts spent providing us information are greatly appreciated. The audit staff members responsible for this audit report are Laura Reyes-Cortez, Stephen Gomez, Danielle Knighten, and Kyle Elser.

## Background

### Introduction to Security Audits

In today's interconnected world, information technology provides opportunities to gain incredible efficiencies throughout the business world and our personal life to the extent that millions of people rely on it every day without a second thought. Along with this reliance unfortunately comes the risk that users may steal, corrupt, or damage the systems we rely on to manage our finances, communicate and store personal or sensitive information among countless other uses. As we improve our security, these malicious users find more and more creative ways to gain access to these systems.

Information technology (IT) security audits, as an additional line of defense, independently review IT processes to identify vulnerabilities which hackers or rogue employees may otherwise take advantage. This audit focuses on the City of San Diego's (City) core financial system and the privileged access used to maintain it to ensure the risks that accompany these accounts are appropriately minimized where feasible.

### **Citywide Financial System (SAP)**

The City uses SAP, an Enterprise Resource Planning (ERP) system, to maintain its primary financial, logistical, and personnel records. SAP is used to bring the City's systems and master data together into one, centralized system. The City uses the following seven SAP functional modules to aid in its daily operations: (1) Financials, (2) Logistics, (3) Human Capital Management, (4) Customer Care Solutions, (5) Enterprise Asset Management, (6) Public Budget Formulations, and (7) Business Objects.

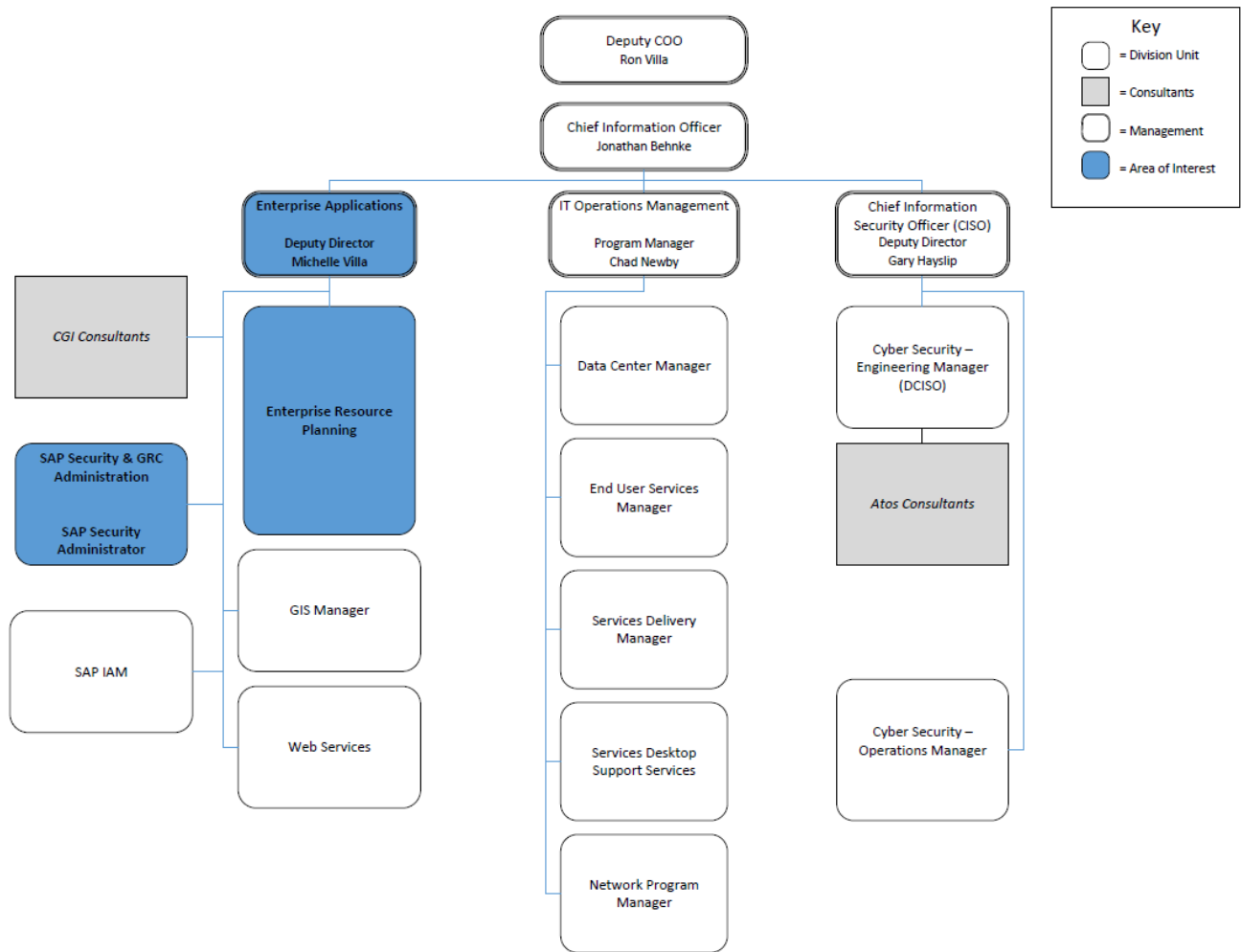
Additionally, the City uses the Governance, Risk, and Compliance (GRC) 10.1 module, for the monitoring and management of system-wide access. Access to and use of SAP is managed by DoIT in conjunction with the departments who own their respective business processes.

### **Department of Information Technology (DoIT)**

DoIT is responsible for providing strategic technology direction; supporting citywide technologies and applications; coordinating citywide infrastructure activities, including IT customer relationship management, IT procurement, and the citywide IT budget; developing and implementing IT operational policies and standards; managing contracts for IT services with various service providers; and managing and implementing IT governance processes.

DoIT consists of seven key areas. [Exhibit 1](#) illustrates the three areas relevant to our audit; however our audit primarily focused on the Enterprise Applications Division.

**Exhibit 1: Department of Information Technology Organization Chart (Abbreviated)**



Source: OCA Generated from Organizational Data

**Enterprise Resource Planning (ERP) Division of the Department of Information Technology (DoIT)**

The Department’s Enterprise Resource Planning (ERP) Division is responsible for providing support for the City’s SAP systems. The ERP Division works with departments throughout the City to help maintain the critical functions that the SAP systems provide for the City. Several groups of users rely on SAP to perform their jobs to varying degrees. The ERP Division’s SAP Security & GRC Administration (SAP Security) Team is responsible for securing access to the SAP system. The SAP Security Team ensures that proper access is granted to end users, including privileged users<sup>1</sup>.

<sup>1</sup> Privileged, or elevated, access relates to a user who, by virtue of function and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users.

## **Inherent Security Risks**

COBIT is an IT enterprise governance framework that is based on more than 40 standards and best practices documents for information technology from standards-setting bodies (public and private) worldwide. COBIT can be used as an authoritative source reference document, providing IT controls criteria for audits.

According to COBIT's Control Practices Guide, potential financial losses and malfunction of business processes can result from inadequate security measures for data and systems, as well as inadequate monitoring and controls. Based on the Control Practices Guide, we identified the following inherent risks related to privileged access to SAP:

- Theft or destruction of sensitive (Personnel Records, SSN, etc.) or financial data (Accounts Payable/Receivable, General Ledger, etc.);
- Modification of sensitive or financial data; and
- Instability of the system that can halt City operations.

Without the appropriate security measures and controls, there is a potential for these risks to occur undetected and uncorrected. The findings outlined in our confidential report identify methods that can be used by rogue internal staff or external hackers if they gain access to a privileged account to realize these risks.

## Audit Results

We identified three audit findings and made five recommendations to address these findings. The Department of Information Technology agreed with the findings and recommendations. Due to IT security related concerns, our findings and recommendations are addressed through a confidential report in accordance with Government Auditing Standards Section 7.41, *Reporting Confidential and Sensitive Information*.

## Objectives, Scope, and Methodology

In accordance with the City Auditor's FY 2017 IT Audit Work Plan, we conducted an IT audit of the City's SAP environment to assess whether privileged user accounts are sufficiently controlled.

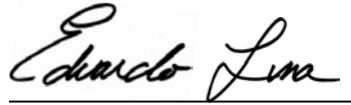
To assess whether privileged user accounts are sufficiently controlled, we reviewed relevant policies and procedures, system logs from May through December 2016, and conducted interviews with staff in the Department of Information Technology and Office of the City Comptroller.

Our testing focused on the control groups below as tailored through our risk and vulnerability assessment:

- Access Controls;
- Monitoring Controls;
- Policy Controls related to Operations and Security; and
- Systems Security Controls.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. COBIT 5 IT Governance framework was also utilized for planning and testing during the audit.

Respectfully submitted,



---

Eduardo Luna  
City Auditor

cc: Scott Chadwick, Chief Operating Officer  
Mary Lewis, Chief Financial Officer  
Stacey LoMedico, Assistant Chief Operating  
Ron Villa, Deputy Chief Operating Officer, Internal Operations  
Rolando Charvel, City Comptroller  
Gary Hayslip, Deputy Director, Chief Information Security Officer, Department of  
Information Technology  
Michelle Villa, Deputy Director, Department of Information Technology  
Ken So, Deputy City Attorney