THE CITY OF SAN DIEGO

DATE: July 20, 2016

TO: Honorable Members of the Audit Committee

FROM: Eduardo Luna, City Auditor

SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan – Fiscal Year 2017**

Attached is the IT Risk Assessment and Work Plan proposed by the Office of the City Auditor for Fiscal Year 2017. The IT Audit Work Plan was developed by identifying and ranking the major risks associated with the City's significant information systems and corresponding processes. We designed our IT Audit work plan to address what we considered to be risk areas, while limiting the scope of work to what we can realistically accomplish with the IT staff resources available. For security reasons, the detailed risk scoring for each application was not included in this report.

Risk assessment is a process of systematically scoring (or rating) the relative impact of a variety of "risk factors." A risk factor is an observable or measurable indicator of conditions or events that could adversely affect the organization. Risk factors can measure inherent risks or organizational vulnerability.

Creating the IT Risk Assessment

The first step in creating the City's IT Risk Assessment model was to define the IT audit universe. The IT audit universe is a listing of all of the City's information systems and corresponding processes. We utilized the IT Department's application portfolio and accompanying information to identify the known active information systems in the City's network.

The next step in creating the risk assessment model was to identify and rank the major risks associated with each of the City's information systems and corresponding processes. To achieve this, the Auditors leveraged the information that the IT Department had collected on the information systems portfolio regarding department, application, process and various risk information to perform a risk assessment. The assessment utilized the eight measurable risk factors outlined below:

Auditor Ranking

1) Inherent Sensitivity of Data
    a. Personal Identifiable Information
    b. Financial Information
    c. Sensitive Information
2) IT Process Audit Risk Scores

IT Department Ranking

3) Business Alignment
4) Technical Architecture
5) Application Criticality
6) Security
7) Availability of Technical Skills to Support

Department Criticality Ranking

8) Mission Criticality of Applications
    a. Mission Critical
    b. Business Critical
    c. Standard Business Operational

Scoring the IT Universe

The score assignment relates to the impact to the City if an application were compromised or hacked and the corresponding processes they supported were compromised as a result. For example, the City Library rated their catalogue system as mission critical to their operations; however, the City would not experience significant risk if this system were hacked based on the data contained in the system. Conversely, the impact of the data theft could be incredibly damaging and open the City to costly litigation if it contained personal information such as social security numbers, while the business criticality may be very low.

The final step in completing the Citywide IT Risk Assessment was to calculate the total risk score for each application in order of highest risk score to the lowest by combining the risks scores from the three identified categories to identify the highest risk systems for our review. The list of potential IT audits and rankings were not included in this report for security reasons. Additionally, the data center contract security requirements review was removed from the previous year's audit work plan based on actions that the IT department is already taking in that area to address the identified risks.

Planned Audits:

1) Security Audit of Public Utilities PCS and SCADA systems:

The tentative objective is to assess the IT control environments of the Plant Control System (PCS) and the Supervisory Control and Data Acquisition (SCADA) system for remote monitoring and control of remote utility equipment. Estimated 600 audit hours.

2) Citywide Privileged User Management:

The tentative objective is to determine if the City appropriately manages privileged accounts on non-outsourced servers, desktop computers, and standard images. Estimated 300 audit hours.

3) Data Security Controls Audit of Sensitive Police Department Data:

The tentative objective is to determine if the Police Department utilizes sufficient IT controls over their sensitive data to prevent loss or theft. Estimated 800 audit hours.

Planned On-Going Audit:

Accela Implementation:

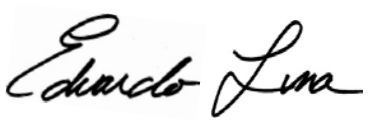
We are entering the second phase of our Accela software implementation audit. The scope of this audit is to ensure Accela is configured to mitigate the risks we have identified and to make sure proper system implementation procedures are followed. The Development Services Department anticipates going live with Accela in May 2017. Estimated 350 audit hours for fiscal year 2017.

Carry Over Audits:

SAP User Provisioning Audit *(In Progress):*

This audit focuses on the access granted in SAP, specifically privileged user accounts, segregation of duty conflicts, their mitigating controls, and a review of the access provisioning process. Estimated 330 audit hours remaining.

Respectfully submitted,



Eduardo Luna
City Auditor

cc: Honorable Mayor Kevin Faulconer
Honorable Members of the City Council
Scott Chadwick, Chief Operating Officer
Stacey LoMedico, Assistant Chief Operating Officer
Marshall Anderson, Director of Council Affairs
Jan Goldsmith, City Attorney
Andrea Tevlin, Independent Budget Analyst