THE CITY OF SAN DIEGO

DATE: October 14, 2015

TO: Honorable Members of the Audit Committee

FROM: Eduardo Luna, City Auditor

SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan – Fiscal Year 2016**

This is the first Annual Citywide IT Risk Assessment and Audit Work Plan proposed by the Office of the City Auditor for Fiscal Year 2016. 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 high 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 Departments recently completed IT 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 significant information systems and corresponding processes. To achieve this, we 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 seven measurable risk factors outlined below:

Auditor Ranking

1) Inherent sensitivity of data
    a. Personal Identifiable Information
    b. Financial Information
    c. Sensitive Information

IT Department Ranking

2) Business Alignment
3) Technical Architecture
4) Application Criticality
5) Security
6) Availability of technical skills to support

Department Criticality Ranking

7) 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 (list of the potential IT audits) 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.

Planned Audits

Planned IT Audits for FY2016

As a result of the IT Risk Assessment, we identified five planned IT audits as described below. They are not all application audits; however they have all been identified as areas of potential IT risk to the City if appropriate processes have not been properly established and maintained.

City Treasurer Application Audits

Due to the inherent risk related to payment remittance, we identified two City Treasurer application audits that will be performed. Specifically, the RTAX online remittance and payment system and BTAX online renewal and payment system. Estimated 450 audits hours for each application.

SAP User Access/ Provisioning Audit

This audit will focus on the access granted in SAP focusing on privileged user accounts, segregation of duty conflicts, their mitigating controls and a review of the access provisioning process. Estimated 450 audit hours.

Data Center Security Audit

Further, as identified during the Risk assessment background research, our office will perform an audit of the IT Contract management; specifically the Security Management and Integration of the Atos Datacenter Contract.

This audit will review the Contractual Management of Security on the part of Atos, the methodology used by our Security Department to hold Atos accountable according to these requirements, and the integration of the Atos datacenter into the overall City Security Plan. Estimated 450 audit hours.

Accela System Implementation Audit

Finally, our office plans to perform a cursory audit of the Accela software implementation taking place this Fiscal Year. 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. Estimated 200 audit hours during FY2016. This audit will not be completed until the system is implemented in the following fiscal year.

Resources & Available Audit Hours:

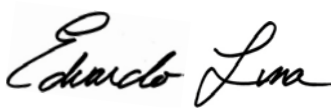
We estimate 2,000 audit hours will be available for our two IT Auditors to work on these planned IT audits for the remainder of the Fiscal Year 2016.

Future Annual Risk Assessment Methodology Adjustments

Our office utilizes the COBIT framework and ISACA guidance for performing the IT Audits we have conducted in the past. For a Risk Assessment, COBIT 5 breaks down IT Audits through its framework based on IT Domains, Processes and Activities. Unfortunately, we did not have enough information to rank the IT department's processes and corresponding City IT processes by these categories in a comprehensive manner. As a result we manually ranked the processes and utilized the application portfolio to create the FY2016 Risk Assessment.

However, during our FY2016 audits of the City's information systems, our intent is to rank the City's IT Domains, Processes and Activities to facilitate the use of the COBIT 5 framework in the FY2017 IT Risk Assessment.

Respectfully submitted,



Eduardo Luna
City Auditor

cc: Honorable Mayor Kevin Faulconer
Honorable City Councilmembers
Scott Chadwick, Chief Operating Officer
Stacey LoMedico, Assistant Chief Operating Officer
Mary Lewis, Chief Financial Officer
Jonathan Behnke, Chief Information Officer
Brian Pepin, Director of Council Affairs
Jan Goldsmith, City Attorney
Andrea Tevlin, Independent Budget Analyst
Gail Granewich, City Treasurer
Robert Vacchi, Director, Development Services
Gary R. Hayslip, Deputy Director, Chief Information Security Officer