



## THE CITY OF SAN DIEGO

DATE: July 14, 2017  
TO: Honorable Members of the Audit Committee  
FROM: Eduardo Luna, City Auditor  
SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan – Fiscal Year 2018**

---

Attached is the IT Risk Assessment and Work Plan proposed by the Office of the City Auditor for Fiscal Year 2018. 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 six 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

OFFICE OF THE CITY AUDITOR  
1010 SECOND AVENUE, SUITE 555, WEST TOWER • SAN DIEGO, CA 92101  
PHONE (619) 533-3165 • FAX (619) 533-3036

*TO REPORT FRAUD, WASTE, OR ABUSE, CALL OUR FRAUD HOTLINE: (866) 809-3500*



### **IT Department Ranking**

- 3) Business Alignment
- 4) Technical Architecture
- 5) Supportability

### **Department Criticality Ranking**

- 6) 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.

### **Carry Over Audits:**

#### **Audits in Report Writing Phase:**

##### *Public Utilities Industrial Control Systems IT Security Audit*

- *Wastewater Industrial Control Systems IT Security Report. Estimated 110 audit hours to complete.*
- *Water Operations Industrial Control Systems IT Security Report. Estimated 130 audit hours to complete.*

#### **Audits Pending System Implementation Completion to Continue:**

##### *Accela Implementation Audit. Estimated 160 audit hours to complete.*

*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.*

#### **Audits Not Started:**

##### *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 900 audit hours.*

**Planned Audits:**


**1) IT Audit of Disaster Recovery Preparedness:**

The tentative objective is to assess the IT Department's Disaster Recovery plan to ensure that it has identified all key applications to be restored in the event of a disaster and has adequate definitions to restore them in a timely manner based on the process risk the application supports. Estimated 1100 audit hours.

**2) Security Audit of Cityhub and Supporting Infrastructure:**

The tentative objective is to determine whether Cityhub data is adequately secured through the application and supporting infrastructure as a data repository for department sensitive information. Estimated 700 audit hours.

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  
Mara Elliott, City Attorney  
Andrea Tevlin, Independent Budget Analyst  
Jonathan Behnke, Chief Information Officer