



## THE CITY OF SAN DIEGO

DATE: July 15, 2020  
TO: Honorable Members of the Audit Committee  
FROM: Kyle Elser, Interim City Auditor  
SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan – Fiscal Year 2021**

---

Attached is the IT Risk Assessment and Work Plan proposed by the Office of the City Auditor for Fiscal Year 2021. 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 and IT process 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 is to define the IT audit universe. The IT audit universe is a listing of all City information systems and corresponding processes both automated by those systems and supporting those systems. 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 requested information from the IT Department on the information system and network portfolios regarding department, application, process and various risk information to perform a risk assessment. The assessment utilized the eight measurable risk factors outlined below:

OFFICE OF THE CITY AUDITOR  
600 B Street, SUITE 1350, 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



### **Auditor Ranking**

- 1) Inherent Sensitivity of IT Process
- 2) IT Process Audit Risk Scores Compiled from Previous IT Audits
- 3) Significance of Major Modifications to the IT Landscape
- 4) Core IT Service Providers Independent Auditor Attestation Assessment

### **IT Department Ranking**

- 5) Business Alignment
- 6) Technical Architecture
- 7) Supportability

### **Department Criticality Ranking**

- 8) Mission Criticality of Applications and Supported Business Processes

### **Scoring the IT Universe**

The score assignment relates to the impact to the City if an application or network service 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 from a financial or human capital supporting system 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 and IT process 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.

Based on the results of our Citywide IT Risk Assessment, we have prepared the following IT Audit Work Plan for Fiscal Year 2021. Our estimated audit hours for each IT audit project are based on our knowledge of the complexity of the activity selected for audit. The actual hours may vary based on the extent and complexity of findings revealed during audit testing.

## **IT Audit Work Plan for Fiscal Year 2021**

### **Carry Over Audits:**

*The IT Audit of Legacy Applications is currently wrapping up fieldwork and requires 150 audit hours in FY2021 for completion.*

*The Audit of IT Service Delivery Effectiveness is in the planning stage and requires 570 hours in FY2021 for completion.*

### **Planned Audits:**

#### **1) Audit of the IT Procurement and Vendor Management Process:**

The tentative objective of this IT Audit is to assess the effectiveness of the controls over the IT procurement and vendor management process. Estimated 1,000 audit hours.

#### **2) IT Application Audit of the Fire Department's Emergency Response Management System:**

This audit will focus on testing the IT general controls and IT security controls of the Fire Department's Emergency Response Management System. Estimated 600 audit hours.

**IT Audit Reports Issued in Fiscal Year 2020:**

- 1) CONFIDENTIAL – Performance Audit of IT Network Perimeter Security
- 2) IT Performance Audit of Citywide Data Classification and Sensitive Data Encryption
- 3) CONFIDENTIAL - IT Performance Audit of Citywide Data Classification and Sensitive Data Encryption

Respectfully submitted,



---

Kyle Elser  
Interim City Auditor

cc: Honorable Mayor Kevin Faulconer  
Honorable Members of the City Council  
Honorable City Attorney Mara Elliott  
Kris Michell, Chief Operating Officer  
Jeff Sturak, Assistant Chief Operating Officer  
Matthew Helm, Chief Compliance Officer  
Jonathan Behnke, Chief Information Officer  
Jessica Lawrence, Director of Council Affairs  
Andrea Tevlin, Independent Budget Analyst