September 14, 2023

Honorable Mayor, City Council, and Audit Committee Members
City of San Diego, California

Citywide Information Technology (IT) Risk Assessment and Work Plan – Fiscal Year 2024

This memorandum outlines the IT Risk Assessment and Work Plan proposed by the Office of the City Auditor (OCA) for Fiscal Year 2024. 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 this IT Audit Work Plan to address what we considered to be the highest 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 City of San Diego and its residents. Risk factors can measure inherent risks—including the security, availability, and confidentiality of data—or organizational vulnerability—such as the potential effect of a breach of security, loss of availability, or breach of confidentiality of the data has on the City's ability to provide services to its residents.

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 known City information systems and corresponding processes both automated by those systems and supporting those systems. We utilized the Department of Information Technology's (DoIT) 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, OCA requested information from DoIT on the information system and network portfolios regarding department, application, process, and various risk

600 B Street, Suite 1350, Mail Station 605B
San Diego, CA 92101
cityauditor@sandiego.gov

T (619) 533-3165
To report fraud, waste, or abuse, call our fraud hotline: (866) 809-3500
sandiego.gov/auditor

information to perform a risk assessment. During these first two steps, we identified some potential gaps in our knowledge of City systems and processes, as well as our information about the importance of those systems and processes to critical City services. As such, we are recommending a risk assessment improvement project in this year's work plan.

Scoring the IT Universe

The systems and processes were ranked by the type of City services the owning department provides—including systems and processes supporting public health and safety (such as public safety dispatch or water treatment and infrastructure), running the City (such as financial or internal services), or providing quality of life benefits to City residents (such as parks or library services). Then, the systems and processes were ranked according to their criticality to providing those services. Specifically, we focused on:

- Mission critical systems and processes that can directly impact the City of San Diego's ability to provide public services—with a direct impact to public health and safety—and require continuous availability;
- Business critical systems and processes that require continuous availability, but these systems could be temporarily interrupted without a catastrophic impact; and
- Standard business operations systems and processes that contribute to efficient business operation but do not directly impact public health and safety or business critical services.

For applications, departments provided their rankings of criticality to DoIT.[1] For processes, OCA ranked the risks.

The rankings were then combined to create a score for both applications and processes. The score assignment relates to the impact to the City if an application or IT process were compromised or hacked and the corresponding City processes they supported were compromised as a result. We also solicited input from the Audit Committee and City Council, DoIT, operational departments, OCA staff based on past audit work and research, and the public.

The final step in completing the Citywide IT Risk Assessment was to evaluate the results of the risk scoring, consider suggested audit topics, and determine which audits would be

[1] We reviewed department rankings and applied auditor judgment to raise or lower systems that we knew to be directly related to achieving the highest ranked City services. For example, although PUD has some services that may affect life and safety—such as water treatment and infrastructure, we determined that PUD's billing system was a business critical rather than a mission critical system, because its compromise would not result in loss of life.

most beneficial to the City and achievable with our IT audit resources. As a result, we are proposing the following audits and a risk assessment improvement project for Fiscal Year 2024:

Carry Over Audits:

IT Audit of Body Worn Cameras – Budgeted separately in Fiscal Year 2024 Citywide Risk Assessment and Work Plan, which was approved by the Audit Committee at the July 26, 2023 meeting.

Planned Audits:

1) **IT Performance Audit of Citywide Cybersecurity Defenses**

   The primary goal of this audit is to evaluate the effectiveness of Citywide cyber defenses against both internal and external cyber threats, including cyberattacks. The audit may include a contract for specialized cybersecurity skills, which OCA anticipates could be funded through its current budget allocation. Estimated 1,000 hours.

2) **IT Performance Audit of Accela Availability and Integration**

   The tentative objective of this audit is to assess if Accela is sufficiently available and integrated with other critical City systems to operate and enable DSD staff to issue permits in a timely manner. Estimated 800 hours.

Planned IT Audit Improvement Project:

1) **Risk Assessment Improvement Project**
   This project aims to enhance the IT risk assessment process by achieving a comprehensive application portfolio. The project may include, but not be limited to, surveying departments, users, and providers to ensure a thorough assessment. This initiative encompasses all IT systems and applications, regardless of their management by DoIT. The refined application portfolio will serve as the foundation for the FY2025 IT Risk Assessment. Estimated 200 hours.

Previously Approved Audit:

Originally approved in the FY2022 IT Risk Assessment and Audit Work Plan, the IT Performance Audit for the Fire-Rescue Department's Network Security was carried over to the FY2023 Citywide Risk Assessment and Audit Work Plan. In the FY2024 plan, it was determined that the proposed IT Performance Audit of Citywide Cybersecurity Defenses

would include the Fire-Rescue Department's network. Therefore, the new proposed audit will address the previously approved audit's risks.

Respectfully submitted,

Andy Hanau
City Auditor

cc: Honorable Mayor Todd Gloria
Honorable Members of the City Council
Honorable City Attorney, Mara Elliott
Charles Modica, Independent Budget Analyst
Eric Dargan, Chief Operating Officer
Matt Vespi, Chief Financial Officer
Christiana Gauger, Chief Compliance Officer
Jonathan Behnke, Chief Information Officer