Item #1 – Study Session:

Review of Citywide Risk Assessment and Internal Audit Work Plan

October 22, 2024

1

Background

City of
Santa Clara
The Center of What's Possible

- The formal role of the City Auditor's Office was established by the Council approved Internal Audit Charter in July 2019.
- The Charter formalizes the internal audit activities, purpose, authority, and responsibility.
- Accountable to the City Council through the Audit Committee
- The Auditor's Office activity will remain free from interference by any element in the organization, including matters of audit selection, scope, procedures, frequency, timing, or report content to maintain it's status as a wholly independent office.
- Maintain strict accountability for confidentiality and safeguarding records and information.
- The office is authorized to have full, free, and unrestricted access to all functions, systems, records, physical properties, and personnel information pertinent to carrying out the projects in the Audit Work Plan. All employees are requested to assist the City Auditor's Office activity in fulfilling its roles and responsibilities.

2

2

Background

City of
Santa Clara
The Center of What's Possible

- The City Auditor's Office conducts its work under the auditing standards prescribed by the Institute of Internal Auditors (IIA) which requires the City Auditor's Office to "establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals" and consider the input from senior management and a governing board.
- The Auditor's Office was established under a "co-source" model to perform its duties.
- Accordingly, in 2022, the City Auditor's Office engaged Baker Tilly US, LLP (Baker Tilly) to conduct a citywide risk assessment and prepare an annual audit work plan for the next five years.
- In attendance from Baker Tilly to assist in the presentation of the report is Chiemi Perry, Manager, Risk Advisory.

3

3

Risk Assessment

7.Assessment
Assess the progress against the audit plan

1.Risk Assessment
Identify, measure, and prioritize risk

6.Monitoring
Monitor emerging risks and changes in organization and environment

2.Risk-based Audit Plan
Allocate internal audit resources

Internal Auditing Annual Cycle

5.Follow-Up
Follow up on management's corrective actions

3.Engagement
Plan and execute approved audits

4.Reporting
Communicate audit results

Risk – The possibility of an event or condition occurring that will have an impact on the ability of an organization to achieve its objectives*

Purpose – To develop an audit plan that assigns internal audit resources to the activities that add the most value to an organization

Process - Identifying and measuring risks associated with the audit universe

4

4

Risk Assessment Methodology

Phase I	Phase II	Phase III	Phase IV
Planning	Information gathering	Analysis	Reporting

Ongoing project management and collaboration

5

Risk Assessment Methodology

Risk Assessment Phases	
Planning	– Prepared risk assessment survey questions and the online survey tool. – Scheduled interviews with council members and Senior Leadership Team members.
Information Gathering	– Reviewed key documents such as Council Priority Matrix, the biennial budget documents, the annual comprehensive financial report, departmental strategic plans, the information on the City's website, and other relevant documents. – Sent a link to the online survey to the selected 56 City's employees including SLT members who were not scheduled to be interviewed. The survey responses were downloaded in Excel spreadsheet. – Updated the risks in the existing risk matrix based on interviews with City Council members and SLT members, survey responses, and review of key documents.
Analysis	– Analyzed the survey responses. – Scored the auditable units (Appendix A) in the risk matrix based on the likelihood and the impact of potential adverse events for various risk factors (Appendix B). – Identified potential internal audit activities with high risk scores.
Reporting	– Summarized the approach and results of the risk assessment.

6

Risk Assessment Methodology

Example of Audit Universe:

City Clerk's Office
- Assistant City Clerk - Council/Administration Support
- Assistant City Clerk - Public Information/Legislation Records Management
- Assistant City Clerk - Political Reform Act
- Elected City Clerk - Election

City Manager's Office
- City Council Support - Policy Support for Decision Making
- City Council Support - Intergovernmental Relations & Advocacy
- Leadership and Management Services - Day to Day Operations
- Leadership and Management Services - Strategic Planning
- Leadership and Management Services - Community Outreach & Engagement
- Citywide Programs
- Stadium Operations
- Citywide Strategic Programs & Initiative
- Convention Center

City of Santa Clara — The Center of What's Possible

7

7

Risk Factor Impact/Definition:

City of Santa Clara — The Center of What's Possible

Factor	Definition	Weight
Impact Factors (the effect on the organization)		
Magnitude	A measure of materiality based on pervasiveness or volume of dollars or transactions; Scores based on the budgeted expenditure amount Extreme - 5: $50M or more Material - 4: $10M or more; Less than $50M Significant - 3: $3M or more; Less than $10M Moderate - 2: $1M or more; Less than 3M Inconsequential - 1: Less than $1M Added 1 to the magnitude of the Information Technology Department due to the pervasive nature of its work	30%
Customer / Resident Experience	Negative experience by customers and residents, such as perceived or actual safety concerns and unsatisfactory services, impacts negatively on the reputation / credibility of the organization Extreme - 5: Direct impact on health and safety Material - 4: Direct impact on transparency Significant - 3: Direct impact on customer satisfaction/City's reputation Moderate - 2: Indirect impact on customer satisfaction/City's reputation Inconsequential - 1: Immaterial impact on reputation / credibility	35%
Achievement of Organizational Goals	The greater the effect that a department or process has on the organization meeting strategic objectives and goals, the greater the related risks Extreme - 5: Directly relates to the City Council Priorities Material - 4: Supports the function/process directly related to the City Council Priorities Significant - 3: Has performance/workload measures related to Strategic Pillars Moderate - 2: Somewhat relates to the organizational goals Inconsequential - 1: Does not relate to City's priorities and goals	35%
	HIGHEST TOTAL SCORE FOR IMPACT: 5	100%

8

8

4

Risk Factor - Likelihood:

Likelihood Factors (the probability of the risk occurring)		
Complexity	A measure of the difficulty in performing a process or function. As a process or function becomes more complex, the greater the opportunity for errors 5 - Very high complexity 4 - High complexity 3 - Medium complexity 2 - Low complexity 1 - Very low complexity	25%
Policies and Procedures	Policies and Procedures are a complete set of written instructions that guide personnel in the successful execution of their duties and the duties of the office for which they work. If the policies and procedures are adequate and up-to-date, a risk is lower 5 - No or little written P&P 4 - Some written P&P 3 - Basic P&P requiring improvements 2 - Adequate but outdated P&P 1 - Adequate and up-to-date P&P or Not Applicable	10%
Regulatory Compliance	Measures the existence of and potential noncompliance with, government regulations and other applicable laws, standards, and policies/procedures 5 - Requirements to meet more than a few laws/regulations and professional standards specific to the division's responsibilities 3 - Requirements to meet one or two laws/regulations and professional standards specific to he division's responsibilities 1 - No requirement to meet any laws/regulations or professional standards specific to he division's responsibilities	25%

9

9

Risk Factor – Likelihood (cont.):

Monitoring	Consider the existence of monitoring activities, including the results of last audits by Internal Auditor, External Auditor, Regulators, etc. and other known deficiencies 5 - Overall, there is no mechanism to monitor the status of performance goals/compliance requirements 4 - For only some significant performance goals/compliance requirements, there is an annual or semi-annual reporting, management review process and/or audits by an external party to identify the status of performance goals/compliance requirements 3 -For all significant performance goals/compliance requirements, there is an annual or semi-annual reporting, management review process and/or audits by an external party to identify the status of performance goals/compliance requirements 2 - For only some of significant performance goals/compliance requirements, there is a periodic (weekly/monthly/quarterly) reporting process to ensure performance goals/compliance requirements are met 1 - For all significant performance goals/compliance requirements, there is a periodic (weekly/monthly/quarterly) reporting process to ensure performance goals/compliance requirements are met	10%
Specific Risks	Consider the existence of specific risk events/conditions and their significance 5 - Identified risk event(s)/condition(s) seem to significantly affect the likihood 3 - Identified risk event(s)/condition(s) seem to have some impact on the likihood 1 - No or very minor risk event(s)/condition(s) have been identified	30%
	HIGHEST TOTAL SCORE FOR LIKELIHOOD: 5	100%

10

10

Slide 11

City of Santa Clara
The Center of What's Possible

Risk Factor – Other:

Other Risk Factor		
Fraud Schemes	Consider the susceptibility to fraud, which is the opportunity for employees/vendors/customers/fraudsters to misappropriate resources or defraud the organization* 5 - High Risk 3 - Moderate Risk 1 - Low Risk	100%

HIGHEST TOTAL SCORE FOR OTHER: 5   100%

HIGHEST TOTAL SCORE 30

* Considered fraud schemes listed in the Fraud Tree provided in the "Occupational Fraud 2022: A report to the Nations" by Association of Certified Fraud Examiners. Also considered are cyber fraud schemes.

11

11

Slide 12

City of Santa Clara
The Center of What's Possible

Excerpt of Risk Assessment Matrix:

The 127 auditable units (Appendix A) are scored using the Risk Factors (Appendix B)

12

Top Risk Areas:

City of
Santa Clara
The Center of What's Possible

Department	Function	Risk Area	Total Risk Score
Electric Utility	Utility Operations - Substation Maintenance	Cybersecurity / Work order and asset management / Construction project controls / Safety program	23.2
Electric Utility	Utility Operations - Transmission & Distribution	Cybersecurity / Work order and asset management / Construction project controls / Safety program	23.2
Electric Utility	Utility Operations - Generation	Cybersecurity / Work order and asset management / Construction project controls / Safety program	23.0
Police	Field Operations - General Patrol	Overtime / Body-worn camera management / Use of force policies	22.7
Electric Utility	Utility Operations - Power System Controls	Cybersecurity / Work order and asset management	22.0
Electric Utility	Utility Operations - SVP Systems Support	Cybersecurity	21.8
Fire	Field Operations	Overtime	20.1
Police	Administrative Services - Departmental Support	Evidence processing and storage	19.8
Public Works	Streets	Maintenance service requests / Grant management	19.7
Police	Investigations - Records	Case management	19.3
City Manager's Office	Convention Center	Convention center operation	19.2
Community Development	Building - Field Inspection	Building Inspection process	19.1
Community Development	Building - Permit Services	Building permitting process	18.7
Parks & Recreation	Parks	Park operations (infrastructure and revenue)	18.4
Finance	General Accounting	Payroll (including timesheet processing) / Vendor master file	18.1
City Manager's Office	Stadium Operations	Stadium operation	17.7
Public Works	Engineering - Traffic	Grant management / Administration of the Shared Mobility Permit Program	17.5
Electric Utility	Resource Planning & Engagement - Resource Management	Power Purchase Agreements / Energy wholesale trading risk management	17.3
Police	Administrative Services - Administration	Record management	17.3
Human Resources	Employee Benefits and Records - Workers' Compensation & Safety	Safety program	17.2
Information Technology	Contract Services	Cybersecurity / Managed Service Provider (MSP) contract management	17.2
Community Development	Building - Plan Review	Building permitting process	17.1

13

13

Top Risk Areas:

City of
Santa Clara
The Center of What's Possible

Department	Function	Risk Area	Total Risk Score
Police	Administrative Services - 911 Dispatch/Communications	911 Dispatch operations	16.6
Police	Field Operations - Traffic	Traffic enforcement	16.5
Electric Utility	Utility Operations - Electric Compliance	Compliance program	16.7
Human Resources	Recruitment, Classification and Staff Development - Selection & Classification	Citywide succession planning and staff development/ Employee records management	16.6
Library	Administration	Memorandum of Understanding (MOU) with the Santa Clara Library Foundation & Friends	16.3
Water and Sewer Utilities	Water Construction,Maintenance,Operations - Water Construction	Construction project controls	16.3
Water and Sewer Utilities	Water Construction,Maintenance,Operations - Water System Operations	Rate setting practices	16.2
Information Technology	Enterprise Services - Application Services	Application portfolio management / Data classification / Payment Card Industry Data Security Standard (PCI DSS) compliance	15.8
Police	Administrative Services - Professional Standards	Training	15.8
City Manager's Office	Citywide Strategic Programs & Initiative	Property management / Santa Clara Tourism Improvement District (SCTID)	15.7
City Manager's Office	Leadership and Management Services - Day to Day Operations	Business Continuity / Enterprise Risk Management	15.6
Finance	Purchasing	Procurement process (including procurement card administration)	15.5
Public Works	Engineering - Field Services	Construction project control / ADA Compliance	15.4
Water and Sewer Utilities	Water Engineering - Water Resources	Water conservation and sustainability programs	15.2
Community Development	Building - Code Enforcement	Code enforcement	15.1
Water and Sewer Utilities	Sewer - System Maintenance	Work order process and asset management	15.0
City Clerk's Office	Assistant City Clerk - Public Information/Legislation Records Management	Public Records Act process efficiency and effectiveness / Record management and retention program	14.8
Electric Utility	Resource Planning & Engagement - Greenhouse Gas Program	Renewable energy program	14.7
Police	Investigations - General Investigation	Case management	14.6
Finance	Municipal Services - Utility Billing Services	Utility billing and collection process	14.6

For Total Risk Score: low risk (Green) < 9; 9 ≤ moderate risk (Yellow) < 16; 16 ≤ high risk (Red)

14

Proposed Audit Workplan:
Audit Project Update for 2024-2025

City of Santa Clara
The Center of What's Possible

- Update of the 2023-2024 audit plan based on factors such as:
  - Risk rating
  - Pervasiveness of the process or control
  - Audit coverage
  - Timing of projects
  - Value-added activities that help the City enhance the ability to manage risks, strengthen accountability, and improve efficiency and effectiveness

- A variety of projects for a 24-month period
  - Flexibility to adjust the timing of audits
  - Amendments during a year in response to changes in the City's environment such as organizational structure, operations, risks, systems, and controls

15

15

Proposed Audit Workplan:
Proposed 2024-2025 Plan

City of Santa Clara
The Center of What's Possible

Department	Project Title	Preliminary Audit Objectives	Estimated Hours
Human Resources / Citywide	Citywide succession planning and staff development	- Determine whether adequate policies and procedures are in place for developing and maintaining a citywide succession plan to ensure continuity in key positions for all departments. - Determine whether the City provides adequate personal professional development training to staff to ensure that qualified staff are prepared to assume increased responsibilities when necessary	300
Finance Department	Purchasing	- Determine whether adequate controls are in place and working effectively to ensure that the appropriate vendors are selected in a timely manner and monitored properly to achieve desired objectives. - Determine whether procurement cards are administered to ensure that only the authorized users can make purchases in accordance with the requirements and guidelines. - Determine whether internal controls over procurement card transactions are in place and working effectively to prevent and detect errors and irregularities, including duplicate, unauthorized, or improper transactions.	450
Police Department Fire Department	Public safety personnel overtime	- Determine whether adequate policies and procedures are in place to ensure the appropriate usage of overtime for the public safety personnel. - Determine whether the overtime practices, including recording and reporting, comply with the City's policies and procedures	360
Electric Utility Department	Safety program	- Determine whether the Electric Utility Department has adequate mechanisms in place to identify and mitigate the safety hazards at workplace. - Determine whether the Electric Utility Department's internal controls are working effectively to ensure a safe workplace.	400
Parks & Recreation Department	Park operation	- Determine whether the internal controls over the maintenance of parks are working effectively to ensure safety. - Determine whether the internal controls over fee collection are working effectively	360
Department of Public Works	Construction project control assessment	Determine whether internal controls over construction projects are adequate and working effectively	360
Community Development Department	Code Enforcement	Assess the efficiency and effectiveness of the code enforcement process	350
Electric Utility Department	Compliance program	- Determine whether the Electric Utility Department had adequate mechanisms in place to keep track of all federal, state, and other compliance requirements. - Determine whether the Electric Utility Department assess risks associated with each compliance requirement and monitor the compliance status to ensure that the requirements are met.	300
Library Department	Memorandum of Understanding (MOU) with the Santa Clara Library Foundation & Friends	Determine whether the internal controls to monitor the compliance with the MOU requirements are in place and working effectively	240
Water and Sewer Utilities Department	Work order process and asset management	Determine whether the internal controls over the work order process are adequate and working effectively	420
City Clerk's Office	Record management and retention program	- Determine whether citywide record management and retention policies and procedures are properly established in accordance with laws and regulations. - Determine whether internal controls are working effectively to ensure compliance with the record management and retention policies and procedures	300
Community Development Department Electric Utility Department	Follow-up on corrective actions	Follow up on previous audit reports to ensure corrective actions included in management responses in each completed audit report	80

16

16

8

Questions?

17