City of Palo Alto
Office of the City Auditor

Policy & Services Committee
October 12, 2021

bakertilly
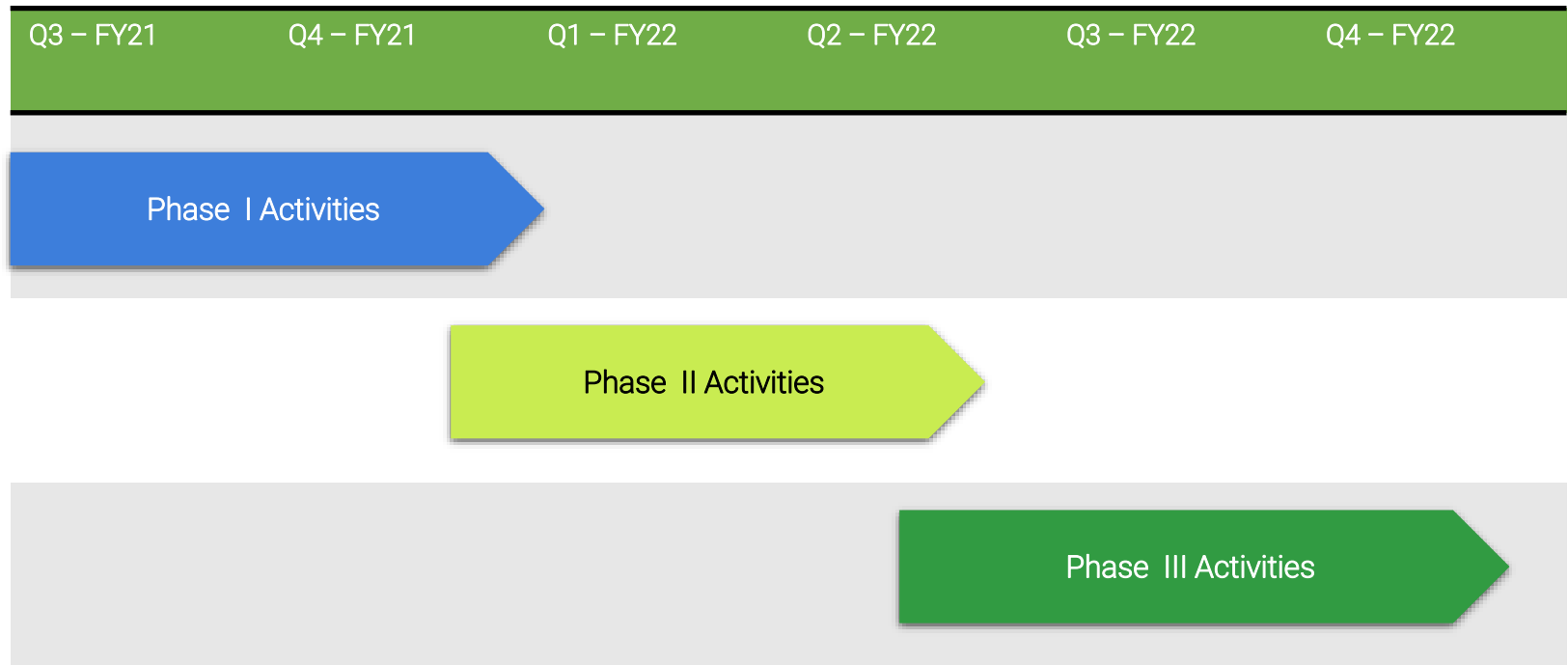now, for tomorrow.

CITY OF
PALO ALTO

Agenda

- Review the Utility Work Order & Accounting Task Order

- Present the IT Risk Management Assessment Report

- Review the OCA Annual Report

- Questions & Discussion

Task Order Approval

Utility Work Order &
Accounting Review

Audit plan – overview of phases

Q3 – FY21	Q4 – FY21	Q1 – FY22	Q2 – FY22	Q3 – FY22	Q4 – FY22

Phase I Activities

Phase II Activities

Phase III Activities

Audit Activities – Phase III

	Project Title	Audit Objectives
X	Utility Work Order & Accounting Review	• Perform an initial assessment to identify high risk subprocesses in the work order process (e.g., labor, materials, specific utility). • Document and evaluate the processes and controls in place to ensure proper recording of costs. • Perform tests to determine the accuracy of attributed costs for a sample of completed work orders.

Policy & Services Committee Action

The City Auditor recommends that the Policy & Services Committee take the following action:

- Forward the Utility Work Order & Accounting Review Task Order City Council for Consent

IT Risk Management Assessment

IT Risk Management Assessment

- IT risk management overview

- Project background

- Audit review/approval

- Questions & discussion

The CAO thanks the IT Services Department of their work on this audit activity – **THANK YOU!**

Important Considerations

- Risk ratings in Appendix A **are not necessarily intended to** indicate an internal control weakness or indicate the operating effectiveness of the City's information technology internal control environment

- The OCA is planning to recommend additional IT audit / cybersecurity audit work

- Redacted information

- Approval by Council indicates approval of the corresponding Action Plans highlighted in Appendix D

What is IT Risk Management?

The policies, procedures and technologies used to mitigate threats by malicious actors and maintain data confidentiality integrity and availability.

Plans and framework that protect the value for the City across all functional areas and mitigates potential risks.

Covers key risk areas of cyber security, database/data management, disaster preparedness and recovery, and vendor management.

Advances the IT Department's mission "to provide innovative technology solutions that support City departments in delivering quality services to the community".

IT Risk Framework
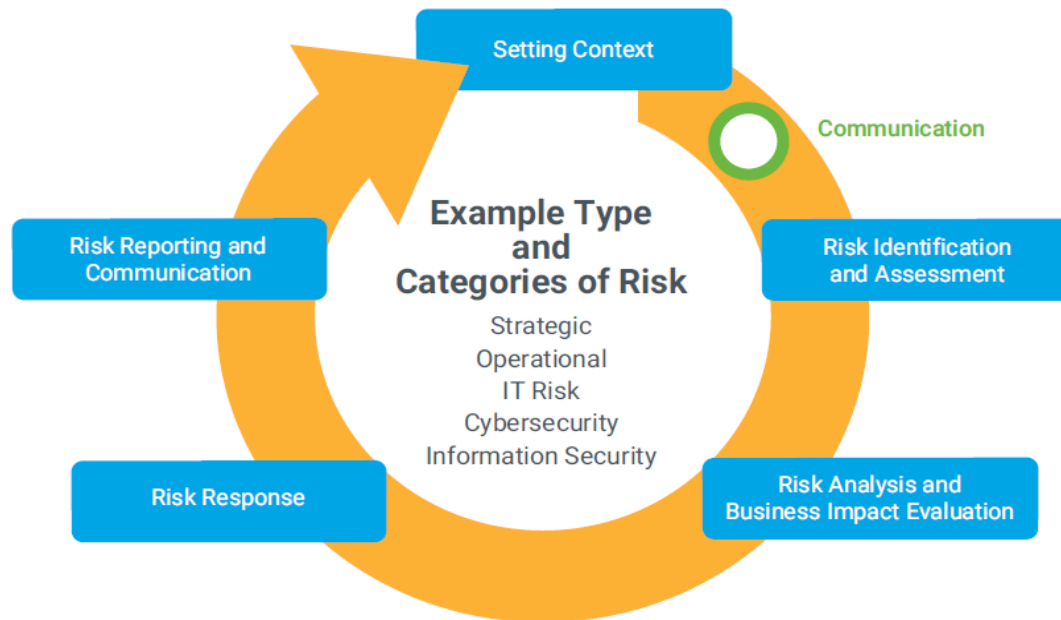
Source: Adapted from ISACA, *Getting Started With Risk Management*, USA, 2018, fig. 2, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgsr*

Project background

Objectives for the audit activity include:

- Understand the key risk areas within IT governance strategy and risk management environment
- Evaluate the adequacy of the IT risk management framework and key internal controls
- Offer recommendations for improvement to the City's IT risk mitigation and management strategy

Identified Frameworks

The OCA evaluated a variety of frameworks to evaluate the current sate of risk management, and selected COBIT 5 as the risk management program framework for future implementation.

Information Gathering

The OCA reviewed background information and interviewed key personnel to understand the City's IT risk management strategy, risk assessment process and any security or baseline frameworks. .

Analysis and Testing

The OCA reviewed the IT risk management framework and internal controls to determine if design mitigates key risks.

Recommendations

Finally, the OCA identified opportunities for improvement and prepared a report.

Findings & Recommendations

Step	Observation	Recommendation
1	Responsibilities and action plans for critical assets have not been identified, a risk appetite has not been established and KPI and metrics to evaluate the achievement of strategic objectives and outcomes of IT Strategy FY19-FY21 were not developed.	**Setting Context:** We recommend The City establish its risk appetite and tolerance when developing strategy. Implementing a proactive IT risk management process is critical because the IT Departments provides numerous technology needs Citywide for Palo Alto.
2	The City does not have an overall formal risk identification process, risk register or risk assessment process.	**Risk Identification and Assessment:** Develop a risk register and risk assessment process.
3	Rating and ranking risks or conducting a business impact evaluation has not been undertaken. A Citywide criteria has not been established and important events and near misses around IT affecting the City are not identified, analyzed and risk-rated.	**Risk Analysis and Business Impact Evaluation:** Use standard criteria to measure the likelihood, impact, frequency and magnitude of the risk scenarios from a top-down or bottom-up approach.

Findings & Recommendations

Step	Observation	Recommendation
4	Overarching IT risk management response procedures have not been implemented and risk action plans are not developed.	**Risk Response:** Based on the analysis and the organization risk appetite, plan and implement a mitigation approach to avoid, share, transfer or accept the risks identified.
5	There is no formal process for IT Management and City Council's regular and routine consideration, monitoring and review of IT risk management	**Risk Reporting and Communication:** Monitor risks and report timely and accurate risk information to decision makers and stakeholders (including City Council).

Policy & Services Committee Action

The City Auditor recommends that the Policy & Services Committee take the following action:

- Forward the IT Risk Assessment Review report to City Council for consent

Annual/Quarterly Status Report

Scope of work overview

Task 1: Citywide risk assessment

Task 2: Preparation of the annual audit plan

Task 3: Financial audit tasks

Task 4: Execute the annual plan

Task 5: Preparation of quarterly reports and annual status report

Task 6: Evaluation and benchmarking

FY21 Updates

Task	Key activities
1. Citywide risk assessment	• Approved by City Council – March 1, 2021 • Current FY Risk Assessment Process is pending kick-off
2. Annual audit plan	• Approved by City Council – March 1, 2021 • Current FY Risk Assessment Process is pending kick-off
3. Financial audit	• The final FY20 audit reports were approved • One-year contract extension approved by City Council due to extraordinary circumstances; FY21 audit is underway • Request for Proposals (RFP) has been developed and responses will be evaluated in Oct/Nov

Progress to date

Task	Key activities

4. Execute audit plan	• Ten (10) total task orders are approved
	• Nine (9) audit activities are currently in progress
	   • 2 approved by P&S (including IT Risk if approved)
	   • 3 reports drafted and are routed for final review
	   • 4 projects are in fieldwork
	• **Reviewing one (1) task order today**
	• **Reviewing one (1) report today**

5. Periodic reporting, hotline monitoring, admin tasks	• Reviewed and Fraud/Waste/Abuse Hotline reports • Delivered quarterly reports • **Reviewing the Annual Report today** • Attended meetings: City Council, ELT, Agenda Planning
6. City Auditor evaluation	• Preliminary planning for initial peer review

Reports issued – FY21

Reports Issued	Audit Activities in Progress
2	7

The City Auditor has delivered two (2) reports to Council, including the Risk Assessment Report and Annual Audit Plan, as well as two (2) reports to P&S. Seven (7) projects are currently in progress, three of which reports are routed for final approval prior to P&S. If the task orders on today's agenda are approved, a total of one (1) additional project will be pending kick-off.

Audit activities
(bold in progress)

- Task 4.1 – Construction Project Controls
- Task 4.2 – Asset Capitalization
- Task 4.3 – Assessment of SAP Functions & Internal Controls
- Task 4.4 – IT Risk Management
- Task 4.5 – Investment Management (potentially to be deferred / re-prioritized)
- Task 4.6 – Power Purchase Agreement Review
- Task 4.7 – Economic Recovery Advisory
- Task 4.8 – Public Safety Building
- Task 4.9 – Building Permit Process
- Task 4.10 – Non-Profit Agreement Risk Management
- Task 4.11 – Utility Work Order & Accounting Process Review (pending review today)

Fraud, waste & abuse

Hotline Reports & Updates		
Quarter	Received	Closed
Prior Period(s)	1	1
January – March 2021	1	1
April – June 2021	0	0
July – September 2021	0	0

The City Auditor, in conjunction with the City Manager and City Attorney, reviewed and closed two (2) Hotline reports filed in the prior year.

Open Audit Findings

Open Findings 2018 - Present	Closed Findings
37	24

The City Auditor has reviewed audit activities for the years 2018-present. There are a total of 37 open findings during that period, of which 24 are closed, representing 65% of items.

Audit Activities Considered in FY22 Plan

The OCA will evaluate audit priorities in the FY22 risk assessment and audit planning process and will consider whether the following will continue to be priorities:

- Investment Management
- Application Lifecycle Management
- SAP Functionality and Internal Controls (Phase 2)
- Wastewater Treatment Plant Agreement

Continuous Improvement

The OCA is and will continue to seek opportunities for continuous improvement. In FY22, this will include:

- Frequency of Council member discussions

- OCA team member involvement in periodic discussions

- Report review process enhancements, including improved coordination between OCA, CMO, and the Office of the City Attorney

- Council agenda planning

Policy & Services Committee Action

The City Auditor recommends that the Policy & Services Committee take the following action:

- Forward the Office of the City Auditor's Annual Report to City Council for Consent

Questions & discussion

Thank you!

Kyle O'Rourke, City Auditor
city.auditor@cityofpaloalto.org

(650) 329-2667