CITY OF PALO ALTO OFFICE OF THE CITY AUDITOR

August 20, 2018

The Honorable City Council
Palo Alto, California

Policy and Services Recommendation to Accept the ERP Planning: Information Technology and Data Governance Audit

The Office of the City Auditor recommends acceptance of the ERP Planning: Information Technology and Data Governance Audit. At its meeting on June 21, 2018, the Policy and Services Committee approved and unanimously recommended that the City Council accept the report. The City Auditor's report to the Policy and Services Committee and the transcript minutes are available on the City's Policy and Services Committee website.

Respectfully submitted,

Harriet Richardson

Harriet Richardson
City Auditor

ATTACHMENTS:

- Attachment A: Information Technology and Data Governance Audit (PDF)

Department Head: Harriet Richardson, City Auditor

Attachment A

CITY OF
PALO
ALTO

ERP Planning: Information Technology and Data Governance

June 13, 2018

Office of the City Auditor

Harriet Richardson, City Auditor
Steve Hendrickson, Management Specialist
Houman Boussina, Senior Performance Auditor

Page intentionally left blank for double-sided printing

CITY OF PALO ALTO

OFFICE OF THE CITY AUDITOR

EXECUTIVE SUMMARY

ERP Planning: Information Technology and Data Governance

June 13, 2018

PURPOSE OF THE AUDIT

The purpose of this audit was to determine if the City has:

- Information technology (IT) governance policies and procedures to align City IT systems with City goals and objectives.
- Data governance policies and procedures to maintain confidentiality, integrity, availability, and usefulness of the City's data.

The audit also assessed whether IT or data governance changes need to be made to prepare for future IT systems.

CONCLUSION

The City does not have a sufficient IT or data governance structure, including policies and procedures that clearly define roles and responsibilities. It is essential for the City to develop IT and data governance processes prior to implementing a new ERP system to ensure that implementation and ongoing operation of the system are successful, in alignment with City goals and objectives, and that existing data are accurate, consistent, and complete before being migrated into the new system.

REPORT HIGHLIGHTS

Finding 1: **(Page 6)**	The City does not have a mature information technology (IT) governance structure to ensure that the City's IT systems, including the new ERP system, fully align with departments' operational goals and objectives, prevent project cost overruns, and protect unauthorized access to confidential information.
Finding 2: **(Page 14)**	The City has important data that are not sufficiently accurate, consistent, and complete, which creates a risk of operational failures, financial losses, and legal claims. This can cause decision makers and the public to draw inaccurate conclusions from the data and will present challenges in the City's migration to the future ERP system.
Key Recommendations:	• Assign roles and responsibilities for IT and data governance to ensure that governance covers all key aspects of the City's information systems and data management. • Adopt industry standard frameworks, such as COBIT for IT governance overall and the Data Management Association's Data Management Body of Knowledge, for data governance.

Page intentionally left blank for double-sided printing

TABLE OF CONTENTS

ABBREVIATIONS	
ASD	Administrative Services Department
DAMA	Data Management Association
DMBOK	Data Management Body of Knowledge
GTAG	Global Technology Audit Guide
ISO	International Organization for Standardization
IIA	Institute of Internal Auditors
IEC	International Electrotechnical Commission
IT	Information Technology
NIST	National Institute of Standards and Technology
SOD	Segregation of Duties

Page intentionally left blank for double-sided printing

INTRODUCTION

Objective

The purpose of this audit was to determine if the City has a citywide:

- Information technology (IT) governance structure, including policies and procedures to align City IT systems with City goals and objectives.
- Data governance structure, including policies and procedures to maintain confidentiality, integrity, availability, and usefulness of the City's data.

The audit also assessed whether IT or data governance changes need to be made to prepare for future IT systems, including the new City's new ERP system.

Background

Information Technology Governance Defined

IT governance is the leadership, organizational structures, policies, and processes to ensure that IT supports the organization's strategies and objectives within budgetary and staffing constraints. Data governance is a subset of IT governance. It focuses on data management overall by providing the guidance necessary to manage data as an asset, including its availability, usability, integrity, and security. Governance activities are broad and set the stage for more specific management and operational activities. For example, project governance is another subset of IT governance that establishes governance structures and management responsibilities for individual projects, such as projects for acquiring and implementing new IT systems. Finding 1 discusses selected governance activities recommended by The Institute of Internal Auditors (The IIA) and by ISACA, an international body that publishes IT best practices and sets standards for information technology.[1]

Data governance and security

Data is the representation of text, numbers, graphics, images, sound, or video. It is the foundation of information and informed decisions and actions. Data quality is synonymous with information quality, since poor data quality results in inaccurate information and poor business performance. Data governance requires authority and oversight of data management. Effective data security policies and procedures ensure that the right people can

[1] ISACA previously stood for Information Systems Audit and Control Association, but the organization now calls itself ISACA.

use and update data in the right way, and that all inappropriate access and change is restricted.[2]

Master data provides information and context about key business elements such as employees and vendors (e.g., connected electronic records in the ERP system that uniquely identify an employee and provide identifying, payroll, and benefits information that does not change often). Business transactions, such as vendor and employee payments, require accurate, consistent, and complete master data.

Roles and responsibilities

The Palo Alto Municipal Code requires the IT Department to provide leadership to the City Council and management on alignment of technology with City initiatives, policies, and strategic objectives and to direct and manage interdepartmental technology governance. The IT Department has established a goal to maintain and mature an IT governance process to ensure alignment between technology priorities, project risks, City goals, and available funds.

ERP Planning and Risks

In 2014, the City hired Plante Moran, a consulting firm, to evaluate the City's current Enterprise Resource Planning (ERP) environment and provide an updated vision of the City's ERP needs. The ERP is business management software and technology that integrates key business activities of the City, such as purchasing, inventory, utilities, accounting, payroll, and information technology. In its report, Plante Moran recommended that the City replace the existing ERP system (SAP) that has been in place since 2003. As part of this effort, the IT Department gathered business requirements from each City department and issued a Request for Proposal (RFP), with a goal of selecting a new ERP system for the City by April 2018. The IT Department has planned a phased process to migrate the City's business data and processes into a new ERP system. The migration process is expected to be completed by June 2022.

ERP risks may prevent the City from realizing the anticipated benefits of an ERP system once it is implemented. Risk areas include:

[2] Data Management Association, *The Data Management Body of Knowledge*, Technics Publications, LLC, New Jersey, 2010, *available for purchase at* https://dama.org/content/body-knowledge

- Insufficient project management and program governance
- Poor data quality
- Inefficient or ineffective interfaces with other systems
- Incompatibility with business processes
- Underused software functionality
- Ineffective access controls/security
- Insufficient technical infrastructure

The risks involved with acquiring and implementing a new ERP system were the impetus for us to initiate this IT governance audit.

Scope

While we assessed the City's information technology and data governance activities and controls that apply to current IT systems, including the current SAP system and other applications that may be migrated or interfaced with the new ERP system, we considered IT governance as it relates to the City as a whole. We focused on Citywide IT and data governance rather than more specific project governance and management activities.

Methodology

To accomplish our objective, we:

- Identified and reviewed applicable standards for IT and data governance (see Appendix 1) including:
  - Global Technology Audit Guide (GTAG) 17: Auditing IT Governance, a publication from The Institute of Internal Auditors that covers the IT governance needed to support organizational strategies and objectives.[3]
  - COBIT 5, an ISACA online publication that provides a comprehensive IT governance and management framework. It provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.[4]
  - Data Management Body of Knowledge (DMBOK), a Data Management Association (DAMA) publication that provides a data governance and management framework to ensure

[3] The Institute of Internal Auditors (IIA), *Global Technology Audit Guide (GTAG) 17: Auditing IT Governance, 2018,* available for purchase at https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG17.aspx.

[4] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,* available for purchase at http://www.isaca.org/cobit/pages/default.aspx.

high-quality data, which is the foundation for information and informed decisions and actions.[5]

- Conducted a risk assessment to identify and prioritize risks associated with IT and data governance.
- Created and administered to all City departments a questionnaire to understand the City's data governance activities. We separately administered an IT governance survey to the IT Department and a modified data governance survey to reflect the department's responsibilities and expertise in these areas. To assess the overall sufficiency of the City's IT and data governance processes, we converted the responses to a numeric rating based on a simplified application of the COBIT Self-assessment Guide, which provides a framework to rate the maturity of business processes.[6] Exhibit 1 provides an overview of the COBIT process capability levels, which show the evolution of a business process, from incomplete to optimized. Exhibit 2 shows the nine process attributes used to determine process capability levels.

EXHIBIT 1
Process Capability Levels

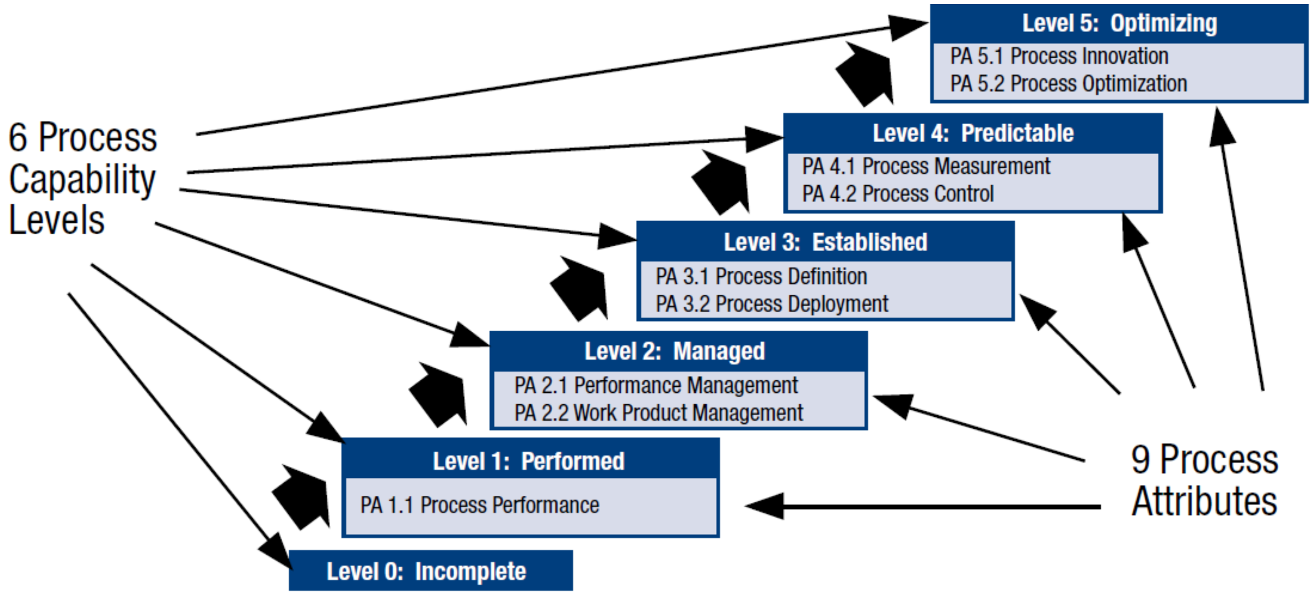
0 = Incomplete	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
1 = Performed	The implemented process achieves its process purpose.
2 = Managed	The performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3 = Established	The managed process is now implemented using a defined process that is capable of achieving its process outcomes.
4 = Predictable	The established process now operates within defined limits to achieve its process outcomes.
5 = Optimizing	The predictable process is continuously improved to meet relevant current and projected business goals.

SOURCE: ISACA, Self-assessment Guide: Using COBIT® 5, 2013

[5] Data Management Association (DAMA), *Data Management Body of Knowledge (DMBOK),* available for purchase at https://dama.org/content/body-knowledge.

[6] ISACA, *COBIT 5 Self-assessment Guide: Using COBIT 5,* available for purchase at http://www.isaca.org/cobit/pages/default.aspx

EXHIBIT 2
Process Attributes


6 Process Capability Levels
Level 5: Optimizing
PA 5.1 Process Innovation
PA 5.2 Process Optimization
Level 4: Predictable
PA 4.1 Process Measurement
PA 4.2 Process Control
Level 3: Established
PA 3.1 Process Definition
PA 3.2 Process Deployment
Level 2: Managed
PA 2.1 Performance Management
PA 2.2 Work Product Management
Level 1: Performed
PA 1.1 Process Performance
Level 0: Incomplete
9 Process Attributes

SOURCE: ISACA, Self-assessment Guide: Using COBIT® 5, 2013

Compliance with government auditing standards

We conducted this performance audit of information technology and data governance in accordance with our FY 2017 Annual Audit Work Plan and generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We would like to thank City management and staff for their time, cooperation, and assistance during the audit process.

Finding 1

Better information technology governance can help ensure that IT systems, including the new ERP system, support City goals and objectives

Summary

The City does not have a mature information technology (IT) governance structure, including policies and procedures to ensure that its IT systems, including the new ERP system, will align with departments' operational goals and objectives; prevent unexpected and excessive project costs associated with poor ERP planning, budgeting, and execution; and protect unauthorized access to confidential information. It is essential for the City to develop IT governance processes prior to implementing a new ERP system to ensure that roles and responsibilities are understood and to achieve success in the implementation and ongoing operation of the new system.

Existing information technology governance processes not mature or complete

The Palo Alto Municipal Code requires the IT Department to direct and manage interdepartmental technology governance. While the IT Department has implemented some governance processes, their focus is on project governance, or ensuring that individual IT Department projects meet their intended goals. The processes are not sufficient to ensure that the overall portfolio of IT Department projects and activities support all departments' business goals and objectives. We compared the IT Department's responses to our questionnaire to the COBIT 5 process capability model, and developed maturity ratings for the IT Department's governance processes. The results show that IT does not have sufficient policies and procedures or clearly assigned and defined roles and responsibilities for the following governance components on a citywide basis. There is not clear:

- Assignment of governance roles and responsibilities
- Alignment of IT with City departments' priorities
- Definition of IT staffing and funding
- Identification and mitigation of IT risks
- Measurement and monitoring of outcomes

The sections below discuss gaps between the City's existing IT governance and COBIT standards (see Appendix 2). IT governance can help ensure that the City selects and implements its new ERP to better align with departments' operational goals and objectives and prevent unexpected and excessive project costs associated with poor ERP planning, budgeting, and execution.

The City has not adopted an information technology governance framework

Although the IT Department is responsible for information technology governance, IT governance is managed within the IT Department instead of on a citywide level. The processes the IT Department has are not sufficient or complete, based on our comparison with the COBIT IT governance and management framework.

The City has not adopted an industry-recognized framework, such as COBIT, or rated its information technology governance processes using such standards to identify gaps and risks in its governance practices. The IT Department has a goal in the City's operating budget book to maintain and mature an IT governance model but does not include any performance metrics to show progress or whether a model has been developed and implemented. The IT Department has not created IT governance policies and procedures to ensure governance activities consistently address all departments' IT needs on an ongoing basis. COBIT sets forth standards to ensure that IT activities align with entitywide business unit goals and objectives and support development of IT policies and procedures, assignment of roles and responsibilities, and the adoption of performance metrics to measure success.

Governance roles and responsibilities not clearly or sufficiently assigned

COBIT standards call for allocating governance responsibility, authority, and accountability. Applying the standards can help ensure that communication and reporting mechanisms provide the appropriate information for oversight and decision making. The IT Department has defined IT roles and responsibilities for its staff, created workplans to manage its projects, and currently leads various committees to manage the City's systems and security. However, the City does not have sufficiently defined and clearly assigned governance roles citywide, nor specific policies and procedures, to ensure ongoing alignment of IT services and systems with departments' goals and objectives. For example, in our 2017 audit of Continuous Monitoring: Overtime, we found that the City's public safety departments could not connect their stand-alone scheduling systems to SAP. This required staff to enter their time in two different systems and manually reconcile the entries to identify inconsistences between the systems.

Governance should ensure information technology supports all departments' goals and objectives

In 2012, the IT Department created a dedicated IT governance and planning manager position who reported to the IT Department director and an IT Governance Review Board (board). The board included staff from various City departments. The IT Department took these steps to ensure proper planning and prioritization of IT activities, create partnerships between departments and IT for inclusive decision making, and increase project visibility to better prepare for project impacts. However, the City no longer staffs the IT governance and planning manager position, and there is no process to comprehensively manage all of the City's information systems to align specifically with departments' goals and objectives. The board meetings now only include IT management staff, and governance responsibilities are assigned to a senior technologist who reports to the manager of the IT Project Services Division. The senior technologist meets with selected department contacts to discuss their needs, and the manager meets with staff in the Administrative Services, Utilities, and Public Works Departments to identify operational concerns in SAP and to manage SAP projects on an ongoing basis.

The City also has an SAP steering committee and project management office with representatives from some City departments who meet to provide oversight of projects and issues specific to SAP. Although the IT Department currently includes staff from all departments in the limited process to select and implement the City's new ERP system, the specific and limited nature of this inclusiveness does not represent an ongoing governance process. Governance should be embedded in the enterprise and continually identify and engage with the enterprise's stakeholders to clearly understand, document, and address their business requirements.

Governance must be properly staffed and funded

The IT Department follows the City's standard budget processes to staff and fund its operations and systems. It also has internal staff development plans to provide and track training to develop staff and support the City's IT systems. Governance standards call for the availability of adequate and sufficient IT-related capabilities, including funding, staffing, process, and technology, to support enterprise objectives and ensure optimal use of the IT systems' capabilities. For example, having sufficient and well-trained staff to support City staff in how to use the new ERP system, remain current on existing and future system capabilities, and improve business processes based on system features and capabilities would ensure a long-term and successful implementation of the new ERP system. Past City Auditor's Office audits identified numerous examples of implemented information systems that had not been leveraged. For example, the 2014 Inventory Management Audit identified that although the City had implemented the SAP inventory system, ASD staff were not aware of important, out-of-the-box functions such as reports on dead stock and inventory turnover. Staff in City departments did not have an understanding of the system configuration or access to staff with technical expertise and time to optimize the system to better align with its business needs.

Increased City department involvement needed to address information security risks

The IT Department has completed several internal and external information security risk assessments and has adopted security policies and procedures. In 2015, Coalfire Systems, Inc. (Coalfire), a consultant, issued an information security risk assessment report that identified 232 risks covering 15 operational areas (e.g., IT policies, data privacy) in the City. The IT Department has identified and tracked the status of the risks over time, including priority, actions, and decisions to accept risks. However, the IT Department has emphasized the confidentiality of the Coalfire report and has not shared details or sufficiently explained these risks to City departments and stakeholders who should have been included in the decision making process to address the risks. The IT Department's chief information security officer organizes and leads an Information Security Steering Committee (committee) to inform departments about security matters and initiatives.[7] The committee met in June 2015 to discuss Coalfire's findings, but the IT Department did not provide the report or documentation of its risk management decisions or recommendations to the committee and did not include committee members in a meaningful, informed decision making process to address the security risks. Governance standards call for an understanding of the enterprise's tolerance for risk and say that this should be properly communicated citywide, but this has not been done. As of March 2018, the IT Department had decided to accept 115 (44 percent) of the 263 risks identified in the Coalfire report.

[7] The ISSC generally meets quarterly at City Hall and includes representatives from each City department.

IT Department risk management document contains errors and may be misleading

In response to our concerns about broader information security governance activities, the IT Department provided documentation of its decisions and actions to address the Coalfire report findings. Although specific risk management actions are beyond the scope of this governance audit, we noted items in the document that raise concerns about its validity and usefulness in addressing the large number of security risks in the Coalfire report, including information and physical security risks in the City. For example, in response to Coalfire's observation that a segregation of duties (SOD) analysis is not formally performed on a periodic basis, the response shows the City's disposition as: "Per SOD Policy this is completed." The same SOD policy is referenced as the remedy for an observation that only one individual understands how to maintain and manage the City's Geographic Information System. The City's only formal SOD policy addresses the IT Department's own system administrator responsibilities and not segregation of duties among the various City business process, which was the context of the Coalfire report finding.

Better governance needed to address unresolved security vulnerabilities

The City's IT Department has prioritized security, but there are unresolved, long-standing security vulnerabilities that will require a citywide effort to address. For example, our office has informed the IT department and senior management of ongoing concerns about unsecured, personally identifiable information in the City's shared-access network drives. These drives are unorganized and contain thousands of folders and files that are not governed by any policies or procedures. This report omits further details pertaining to the security vulnerabilities to avoid inappropriate access and dissemination of sensitive or confidential information. We have provided City management a separate, confidential report with details and recommendations to address the security vulnerabilities.

Knowledge of City's data is a prerequisite to effective security

A recent ISACA announcement states that before you can secure your data, you have to know your data, including what data you have, where you have it, why you have it, and how you are using it. A good governance framework not only covers data visibility, intelligence and insight, but also provides strategic direction for security activities to ensure that cybersecurity objectives, such as effective risk and resource management, are achieved. Finding 2 discusses the need for better citywide data governance.

No metrics to show whether information systems meet citywide business goals and objectives

The IT Department has developed key performance indicators, such as service work order counts and response times, costs by City department, computer counts, and user login counts. It also participates in the City's budgeting and performance reporting processes that show overall user satisfaction, service desk requests resolved, and workload metrics. However, IT has not established metrics that provide information regarding whether information systems meet departments' business goals and objectives. Governance standards include sample metrics such as:

- Percent of management roles with clearly defined accountabilities for IT decisions
- Percent of IT services where expected benefits are realized
- Percent of enterprise goals and requirements supported by IT strategic goals
- Level of business executive awareness
- Understanding of IT innovation possibilities

Plante Moran identified governance concerns

Plante Moran reported challenges that can be addressed through implementing COBIT or other industry-recognized governance standards. Plante Moran's survey of City staff identified:

- Inefficiencies due to redundant data entry, manual processes and unused system functionality
- Unrealized benefits from current City SAP investments
- Heavy reliance on IT and outside consultants for SAP enhancement requests
- Limited reporting capabilities
- Lack of an intuitive user interface
- Limited ongoing training available
- SAP complexities frustrate users and discourage use of current systems to satisfy business needs
- Loss of SAP institutional knowledge due to staff attrition

Models of information technology governance policies and procedures are available from other jurisdictions

Other cities and public sector agencies have implemented IT governance policies and procedures. For example, Portland, OR, has a Technology Project Intake policy that requires maintaining a citywide enterprise IT perspective, in which the Technology Oversight Committee places importance on understanding customer business needs as they relate to technology and providing IT management with greater visibility of its customers plans and priorities; and Modesto, CA, has an IT Steering Committee Charter that requires the committee to oversee IT strategic alignment and investment priorities. We also identified several universities that have IT governance policies and procedures.

Recommendations

To ensure the successful implementation of the new ERP system, we recommend that the City Manager place emphasis on developing and implementing a strong, citywide IT governance structure prior to implementing a new ERP system by implementing the following recommendations:

1.1. Assign roles and responsibilities for IT governance (e.g., "chief governance officer") to an existing City position that reports or could potentially report directly to the City Manager or the Chief Information Officer. The roles and responsibilities should include:

- Ensuring that City departments and stakeholders who are the users of the City's information systems are included in governance processes and decision making, including decisions to address security risks.
- Ensuring that there is a process to validate the accuracy and completeness of key IT reports that are used in decision making or reporting (e.g., the City's document that shows decisions on addressing risks identified in the Coalfire report; decisions regarding departmental roles and responsibilities for the new ERP system).
- Ensuring that governance covers all key aspects of the City's information systems (e.g., ensuring that the IT Department has policies and procedures to address the use, organization, security, and access rights for the City's network drive).

1.2. Adopt an industry standard IT Governance framework, such as COBIT, and a process assessment and rating or maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., "established") or higher for:

- IT staffing and funding
- IT governance roles and responsibilities
- Aligning IT with departments' priorities

- Measuring and monitoring IT governance outcomes
- Identifying and mitigating IT risks

Finding 2

Better citywide data governance will lead to better data in the new ERP system

Summary

The City has not assigned data governance roles and responsibilities to ensure that its data is available, usable, accurate, and consistent. Most City departments do not have sufficient governance processes to ensure that their data is reliable, secure, and useful. The City has important data that is not sufficiently accurate, consistent, and complete, which creates a risk of operational failures, financial losses, and legal claims. This can cause decision makers and the public to draw inaccurate conclusions from the data and will present challenges in the City's migration to the future ERP system. It is essential for the City to develop data governance processes prior to implementing a new ERP system to ensure that data is accurate, consistent, and complete before being migrated into the new system.

Limited and poor quality data has adversely impacted the City

Data and the information created from data are widely recognized as organizational assets that need the partnership of business leadership and technical expertise to effectively manage. Accurate data and information are needed for decision making, operations, and public transparency. Although City departments, rather than the IT Department, are considered the data owners, departments generally do not have sufficient data governance processes to provide reliable, secure, and useful information. Past City Auditor’s Office reports provide a broad, yet consistent perspective of ongoing, negative outcomes associated with insufficient data governance roles, responsibilities, and processes for the following areas (see Appendix 3):

- **Data Integrity** refers to the accuracy, consistency and completeness of city data. Our 2017 Continuous Monitoring Audit: Payments identified that almost 41,000 (94 percent) of the City’s 43,642 active vendor records in SAP are unused, duplicates, inconsistent, and/or incomplete, which increased the risk of duplicate, erroneous, and fraudulent payments, as well as incorrectly reported tax information.
- **Data Inventory** is a comprehensive list of system data, including descriptions and interrelationships of data items that underlie a particular business process. Our 2015 Utility Meter Audit: Procurement, Inventory, and Retirement identified incomplete, inaccurate, inconsistent, and irreconcilable

information in the City's data inventory of utility meters. SAP's capabilities were not fully used to support and coordinate the meter workflow process and its data, which resulted in customer billing errors. The Utilities Department subsequently identified some of these errors, and we identified others and cited them in our audit, Accuracy of Water Meter Billing.

- **Data Migration** is the transfer of data between systems. Our 2013 Employee Health Benefits Administration Audit identified incomplete City retiree data in SAP because it had not been migrated from the City's legacy Lawson system. This resulted in using time consuming manual processes and Excel spreadsheets to track retiree health benefits and the City's payment obligations.
- **Data Security and Access** exists to prevent unauthorized access, use, and change of city data. Our 2011 SAP Security Audit identified improperly secured super user accounts that allowed unrestricted access to the City's data. SAP logs lacked sufficient information to effectively assess the vulnerabilities.
- **Legal Compliance** is the aspect of data governance that ensures that managing and disclosing city data complies with data security and access laws. Our 2012 Special Advisory Memorandum identified a significant SAP security vulnerability that allowed certain individuals with SAP access to view employee personal information that they did not have a business need to know. Under state law, the combination of name and social security number is "personal information." Agencies must notify individuals if their personal information is acquired by an unauthorized person in a way that amounts to a security breach under the law.[8]
- **Availability** means the city's data is easily available for its intended purpose. In our 2016 Disability Rates and Workers' Compensation Audit, we found that the data necessary for disability leave management had not been captured through SAP time reporting. We also found that Human Resources Department staff did not have online access to workers' compensation claims data maintained by a third-party provider.

[8] See citation in California Civil Code, available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29.

- **Usability** is the aspect of data governance that ensures the data readily meets users' requirements. Our 2011 SAP Security Audit discussed limitations on our SAP access and that an important, free auditing tool in SAP had not been configured, tested, or provided to us. The audit explained that ASD, at the time responsible for the IT function, did not view the Auditor's Office access as high priority. The Palo Alto Municipal Code provides that the Office of the City Auditor will have unrestricted access to obtain sufficient and appropriate evidence to conduct audits.

Most City departments do not have data policies and procedures

Most City departments do not have sufficient data governance processes to provide reliable, secure, and useful information. We compared the departments' responses to our questionnaire to the criteria in the COBIT 5 process capability model and developed maturity ratings for citywide governance processes. The results show that the City does not have sufficient data governance policies and procedures or clearly assigned and defined roles and responsibilities for data inventory, integrity, migration, security & access, legal compliance, availability, and usability.

The City has not adopted a data governance framework

The City has not assigned data governance roles and responsibilities to ensure that its data is available, usable, accurate, and consistent. Achieving long-term data quality is more feasible when people throughout the organization understand the value of high-quality data and the negative impact of poor-quality data. Establishing clear roles and responsibilities for ensuring high quality data is essential to achieve this. The IT Department has adopted an information security framework, assigned security roles and responsibilities, and created security policies and procedures. However, these do not address Citywide data governance, which should include a citywide approach to data and information that has been adopted as a set of policies and procedures that encompass the full lifecycle of data, from planning to creating/acquiring through use and disposal. This includes establishing decision-making authority and standards regarding data security, data inventories, content and records management, data quality control, data access, and data sharing, as well as ongoing compliance monitoring of all of the above. Regular monitoring of data quality helps to catch and fix issues before they cause major problems.

Using the DAMA-DMBOK or a similar framework can help ensure that the City makes informed data governance decisions and implements relevant and useful data management processes. A process maturity framework such as the COBIT Self-assessment Guide can help the City rate and monitor its data governance processes in conjunction with the use of DAMA-DMBOK or a similar framework.

Plante Moran identified data concerns

Plante Moran, the City's consultant for the new ERP and Utility Billing Planning systems, stated in its November 2014 Enterprise Resource Planning System Evaluation report that the City's installation of its current SAP system uses a process that perpetuates data errors in the system and continues to cause data integrity issues. [9] Plante Moran identified examples of data reliability, access, reporting, and usability limitations in the current SAP system and recommended that the City establish a governance structure to successfully select, implement, and maintain the new ERP system. The City has implemented a project governance structure to select and implement the new ERP system but not a broad IT or data governance framework (see Finding 2) to address the City's data integrity challenges that could carry over into the new ERP system.

Security policies and procedures not available to staff

The IT Department has adopted data security standards and internal security policies and procedures for the City that are published by the International Organization of Standardization (ISO) and International Electrotechnical Commission (IEC). It also engaged private-sector security experts to assess security vulnerabilities. In response to our concerns about the lack of access to and visibility of these City's security policies and procedures, the IT Department published them on the City's intranet in December 2017 to inform all City staff of the adopted standards and acceptable secure practices. In addition, the City has adopted the proprietary ISO/IEC 27000 security standard. However, this standard cannot be openly distributed, shared, or incorporated into the City's policies and procedures without specific permission and licensing.[10]-The IT Department purchases

[9] Plante Moran's report is available at http://www.cityofpaloalto.org/civicax/filebank/documents/51141

[10] ISO/IEC 2700 is described at https://www.iso.org/isoiec-27001-information-security.html

additional copies of the ISO/IEC 27000 standard as needed and prepares work products, such as presentations, that are based on the standard. The IT Department has not assessed whether the City's security policies and procedures meet the ISO/IEC 27000 standard (i.e., to identify any gaps between the City's policies and procedures and relevant controls in ISO/IEC 27000).

National Institute of Standards and Technology (NIST) security standards are comprehensive and appropriate for the City

A more appropriate standard for citywide adoption would be the National Institute of Standards and Technology (NIST) security standards because they are designed for the government sector, are not copyrighted, and are readily accessible, without charge, on the internet.[11] NIST SP 800-53 is a comprehensive control framework that provides 276 controls; ISO/IEC 27000 addresses only 196 of those controls. For example, NIST control "AC-22" requires specific steps to ensure that publicly accessible information is appropriate (e.g., does not include information protected under the Privacy Act), but ISO/IEC 27000 does not address this issue. Although there is no specific requirement for local governments to use NIST standards, a May 2017 presidential executive order requires federal executive departments and agencies to use the more comprehensive NIST cybersecurity framework to manage cybersecurity risks. A previous external financial audit firm recommended that the City adopt and implement the NIST SP 800-53 control framework, which NIST designed for the federal government but also recommended to state, local, and tribal governments, as well as private sector organizations.

Data governance policies and procedures from other jurisdictions

Other cities and public sector agencies, such as the cities of Portland and Modesto, have implemented citywide data governance policies and procedures. For example, Modesto has a data governance charter, a data governance board that oversees the charter, and data governance committees to address citywide, initiative-specific data issues and requirements. Modesto's procedures include a data checklist to help verify data quality, usability, and security. At the federal level, the Office of Management and Budget has formally chartered the Data Standards Committee as an advisory body to focus on clarifying

[11] The NIST security standards are available at https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

existing data element definitions and identifying needs for new standards.

Recommendations

To ensure the successful implementation of the new ERP system, we recommend that the City Manager place emphasis on developing and implementing a strong citywide data governance structure prior to implementing a new ERP system by implementing the following recommendations:

2.1. Assign roles and responsibilities for data governance (e.g., a "chief data governance officer") to an existing position that reports or could potentially report directly to the City Manager or the Chief Information Officer.

2.2. Adopt an industry standard data governance framework, such as the DAMA-DMBOK, and a process maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., "established") or higher for:

- Inventory
- Integrity
- Migration
- Security & Access
- Legal Compliance
- Availability
- Usability

APPENDIX 1 – Industry Standard IT and Data Governance Frameworks

Framework	**Description and Reference**
Global Technology Audit Guide (GTAG) 17: Auditing IT Governance	An Institute of Internal Auditors (IIA) online publication that covers the IT governance needed to support organizational strategies and objectives. Available for purchase at: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG17.aspx
COBIT 5: A Business Framework for the Governance and Management of Enterprise IT	An ISACA online publication that provides a comprehensive IT governance and management framework to create optimal value from IT. Available for purchase at: http://www.isaca.org/cobit/pages/default.aspx
Data Management Association, The Data Management Body of Knowledge	Data Management Body of Knowledge, a Data Management Association publication that provides a data management framework. Available for purchase at: https://dama.org/content/body-knowledge
National Institute of Standards and Technology (NIST) Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations	U.S. Federal Government publication containing a comprehensive catalog of technical and nontechnical security and privacy controls designed for the government sector. Available at: https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

APPENDIX 2 - Summary of Information Technology Governance Components and City Status

Component of IT Governance	**Status**
Assign IT Governance Roles & Responsibilities	IT governance and planning position no longer staffed and IT Governance Review Board no longer includes departments. No citywide IT governance policies and procedures or roles and responsibilities.
Align IT with Departments' Priorities	Senior technologist informally meets with departments. Various project management committees. No citywide IT alignment policies and procedures or roles and responsibilities.
Establish IT Staffing & Funding	IT Department follows City's budget and staffing processes. No citywide IT system-specific staffing policies and procedures or roles and responsibilities.
Identify and Mitigate IT Risks	IT Department has completed internal and external information security assessments and adopted security policies and procedures. No citywide information system risk assessments to more broadly identify information system security, operational, financial, health and safety, and reputational risks.
Measure & Monitor IT Governance Outcomes	The IT Department has developed Key Performance Indicators such as service work order counts, costs by City department, computer counts, and user login counts. No IT metrics that provide information regarding whether information systems meet departments' business goals and objectives.

APPENDIX 3 – Summary of Data Governance Components and City Status

Key Components of Data Governance	**Status of City Practices**
Inventory: The City should have created a comprehensive list of system data which includes descriptions and interrelationships of data items.	Some departments have limited data inventories. No citywide policies and procedures, standards, or roles and responsibilities exist outlining the City's policies on creating data inventories.
Integrity: Calls for the City to maintain accurate and complete city data	Some systems have limited preventive measures to ensure integrity. Some departments periodically review selected data to ensure it continues to be accurate and complete. No citywide policies and procedures, standards, or roles and responsibilities define the City's measures to maintain the integrity of its data.
Migration: That aspect of data governance in which city departments properly plan for the transfer of data between systems.	Some departments have planned data migration for selected projects. No citywide policies and procedures, standards, or roles and responsibilities describing to City departments' best practices for migrating data between systems.
Security & Access: Refers to steps the City should take to prevent the unauthorized access, use and change of city data.	IT Department has information security roles and responsibilities and policies and procedures. City uses a basic access control process for SAP. However, security policies and procedures are not available citywide and no citywide standard for access controls for departments' information systems.
Legal Compliance: Ensures that the handling and disclosure of city data follow state and federal laws.	IT Department and Utilities Department have legal compliance policies and procedures. No citywide legal compliance policies and procedures, standards, or roles

	and responsibilities.
Availability: Means that city data is readily available.	No citywide data availability policies and procedures or roles and responsibilities have been established.
Usability: Ensures that the data meets the users' requirements.	No citywide data usability policies and procedures or roles and responsibilities have been established.

APPENDIX 4 – City Manager's Response

The City Manager has agreed to take the following actions in response to the audit recommendations in this report. The City Manager will report progress on implementation six months after the Council accepts the audit report, and every six months thereafter until all recommendations have been implemented.

			To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
Recommendation	**Responsible Department(s)**	**Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan**	**Current Status**	**Implementation Update and Expected Completion Date**
Finding 1: Better information technology governance can help ensure that IT systems, including the new ERP system, support City goals, and objectives				
To ensure the successful implementation of the new ERP system, we recommend that the City Manager place emphasis on developing and implementing a strong, citywide IT governance structure prior to implementing a new ERP system by implementing the following recommendations:				
1.1. Assign roles and responsibilities for IT governance (e.g., "chief governance officer") to an existing City position that reports or could potentially report directly to the City Manager or the Chief Information Officer. The roles and responsibilities should include:	Information Technology	Agree. Target Date: December 31, 2019 Corrective Action Plan: The IT Department implemented IT Governance citywide in 2012 and since then it has been rightsized to reflect		

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
• Ensuring that City departments and stakeholders who are the users of the City's information systems are included in governance processes and decision making, including decisions to address security risks. • Ensuring that there is a process to validate the accuracy and completeness of key IT reports that are used in decision making or reporting (e.g., the City's document that shows decisions on addressing risks identified in the Coalfire report; decisions regarding departmental roles and responsibilities for the new ERP system). • Ensuring that governance covers all key aspects of the City's information systems (e.g., ensuring that the IT Department has policies and procedures to address the		the evolving needs of the City. The roles and responsibilities for a leader in IT governance have already been assigned to an individual who reports to the Chief Information Officer (CIO). The IT Department agrees that work is required to address gaps in our city IT governance processes today including leadership roles, communications, reporting, and decision-making.		

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
use, organization, security, and access rights for the City's network drive).				
1.2. Adopt an industry standard IT Governance frameworks, such as COBIT, and a process assessment and rating or maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., "established") or higher for: • IT staffing and funding • IT governance roles and responsibilities • Aligning IT with departments' priorities • Measuring and monitoring IT governance outcomes • Identifying and mitigating IT risks	Information Technology	Agree. Target Date: December 31, 2019 Corrective Action Plan: IT Department agrees to identify and adopt an appropriate, rightsized, industry-recognized, IT governance framework. The IT Department working with the City Manager's Office will determine the appropriate level of IT Governance maturity required for enabling organizational success.		
Finding 2: Better citywide data governance will lead to better data in the new ERP system				
To ensure the successful implementation of the new ERP system, we recommend that the City Manager place emphasis on developing and implementing a strong citywide data governance structure prior to implementing a new ERP system by implementing the following recommendations:				
2.1. Assign roles and responsibilities for data governance (e.g., a "chief data governance officer") to an	Information Technology	Agree. Target date: July 1, 2019		

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
existing position that reports or could potentially report directly to the City Manager or the Chief Information Officer.		Corrective Action Plan. In January 2017, the IT Department hired a qualified data analyst with responsibility for citywide data governance. The role currently reports up through the Chief Information Officer (CIO). The IT Department agrees to request elevation of this role from City Council to a more senior classification to reflect the increased responsibilities expected as a result of implementing an industry-standard data governance framework.		
2.2. Adopt an industry standard data governance framework, such as the DAMA-DMBOK, and a process maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., “established”) or higher for: • Inventory • Integrity • Migration	Information Technology	Agree Target date: December 31, 2019 Corrective Action The IT data lead will work to implement the citywide data strategy that is currently being developed and is part of the FY19-21 IT strategy. Adoption of a standard data governance		

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
- Security & Access - Legal Compliance - Availability - Usability		framework was already identified as a goal in this plan. IT Department agrees to identify and adopt an appropriate, rightsized, industry-recognized, data governance framework. The IT Department working with the City Manager's Office will determine the appropriate level of data governance maturity required for enabling organizational success.		