IT PERFORMANCE AUDIT OF CITYWIDE DATA CLASSIFICATION AND SENSITIVE DATA ENCRYPTION

The City must further formalize its data management program to enable comprehensive data management, including the classification and security of its data.

Office of the City Auditor

City of San Diego

OCA

Independent • Objective • Accurate

May 2020

This Page Intentionally Left Blank

THE CITY OF SAN DIEGO

May 29, 2020

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

Transmitted herewith is an IT performance audit report on the City's Data Classification and Sensitive Data Encryption Program. This report was conducted in accordance with the City Auditor's Fiscal Year 2020 Audit Work Plan, and the report is presented in accordance with City Charter Section 39.2. The Results in Brief are presented on page 1. Audit Objectives, Scope, and Methodology are presented in Appendix B. Management's responses to our audit recommendations are presented after page 50 of this report. We also issued a confidential report addressing IT related concerns in accordance with Government Auditing Standards Section 7.61, Reporting Confidential and Sensitive Information.

We would like to thank staff from the Department of IT, Performance and Analytics Department, and Office of the City Clerk for their assistance and cooperation during this audit. All their valuable time and efforts spent on providing us information is greatly appreciated. The audit staff members responsible for this audit report are Wendy Minnaert, Steve Gomez, Danielle Knighten, and Andy Hanau.

Respectfully submitted,

Kyle Elser

Kyle Elser
Interim City Auditor

cc: Honorable City Attorney Mara Elliott
Kris Michell, Chief Operating Officer
Jeff Sturak, Assistant Chief Operating Officer
Jonathan Behnke, Chief Information Officer
Elizabeth Maland, City Clerk
Kirby Brady, Director of Performance and Analytics
Andrea Tevlin, Independent Budget Analyst

This Page Intentionally Left Blank

Table of Contents

Results in Brief

The City of San Diego relies on and generates significant amounts of data on a daily basis to plan, execute, and improve their operations. A Comprehensive Data Management program is essential to enable the City to appropriately protect and leverage its data resources to maximize the usefulness of this data to the City and the public while balancing appropriate access and security.

Recognizing the importance of its data management, the City has moved proactively to manage, inventory, and classify its data through several independent data management projects. The Performance and Analytics Department (PandA) has inventoried and classified significant amounts of City data based on and focused around their open data initiative. The Department of Information Technology (DoIT) has created a data classification policy focused on security, and is working to inventory the City's data based on this classification, and has appropriately addressed compliance with regulations in their initial project phase. The Office of the City Clerk (City Clerk) maintains a comprehensive records management program which covers a very specific type of data (records) in line with their City Charter defined role and authority. They are currently working with departments to implement the Citywide records management and retention schedule.

We found that while each of these groups have made significant progress through their individual focuses, these efforts require stronger coordination to ensure their individual efforts benefit the City's data management objectives as a whole. Currently, each effort is headed by a different group with a different focus, resulting in potential redundancies in the City's data management approach.

The primary departments heading up distinct data management efforts are the Performance and Analytics Department (PandA), The Department of Information Technology (DoIT), and the Office of the City Clerk, in addition to the various departments that own the data. While these efforts have resulted in partial data inventories and various classifications, there isn't a central complete or comprehensive inventory of City data to manage.

Standards require that the City define a data governance model as a core component of its data management methodology, the first steps include defining an organization-wide classification methodology and developing a centralized inventory of the City's data.

The City requires an inventory of its data with enough information about it (meta data) to effectively protect and leverage it beyond its initial operational scope. While the current efforts may ultimately identify and develop this inventory and classification methodology, it will likely take significantly more resources and time to achieve it if it remains uncoordinated. From a cybersecurity perspective, this coordination is imperative to identify and secure the City's data to protect it from loss in the event of a breach or data loss event, which could result from an employee losing a USB drive or the theft of a laptop from a car or residence in today's remote work environment.

To address these issues mentioned above, we made five recommendations to mitigate these risks in our public report and issued a confidential report outlining additional risks. These recommendations include creating a centralized data management strategy to increase cooperation and coordination between the departments, establishing a classification scheme to meets the requirements of all the stakeholders to prevent redundancy, establishing a centralized inventory utilizing the established classification methodlogy, and create an Administrative Regulation defining a data governace model that includes the roles and responsibilities of the stakeholders.

Management agreed to implement all five of our recommendations and outlined several planned steps to improve internal controls related to the issues we identified.

We also issued a confidential report addressing IT security related concerns in accordance with Government Auditing Standards Section 7.61, Reporting Confidential and Sensitive Information. Management agreed to implement the recommendations from the confidential report.

Background

Data Governance and Management

Data has become an increasingly important commodity in our daily lives, whether it is performing an internet search to answer a question, looking at our emails, or paying our bills, we rely on instant and in many times, secure access to this data to go about our day. In the same way, but to a much larger degree, organizations, such as the City of San Diego (City), generate and consume immense amounts of data daily; whether it is developing the annual budget, determining what roads require repairs, or running trash routes throughout neighborhoods.

In order to both use and protect this data, organizations implement data management plans to ensure that they know what data they have, how they can use it, and also how they must protect it.

Data Inventory and Classification as Critical First Steps in Data Governance

The first step in any management strategy is to identify what you are managing and how it should be managed. To do this, the manager must gather enough information to accomplish these tasks. This is also true of data management.

The fundamental steps require that an organization identify their data through an inventory, and classify that data based on what it needs to know to manage it effectively.

Specifically, data classification is the process of organizing data into categories that make it easy to retrieve, sort and store for future use, as well as preserving data confidentiality, integrity, and availability. It is a foundational step in data as well as cybersecurity risk management and involves identifying the types of data that are being processed and stored in an information system owned or operated by an organization. It also involves making a determination regarding the sensitivity of the data and the likely impact arising from compromise, loss, or misuse.

Data classification has been used to help organizations safeguard sensitive or critical data with appropriate levels of protection. It is a starting point for maintaining the confidentiality (and potentially the integrity and availability) of data based on the data's risk impact level. Data classification allows organizations to think about data based on sensitivity and business impact which then helps the organization assess risks associated with different types of data. The International Standards Organization (ISO) and the National Institute of Standards and Technology (NIST) recommend data classification schemes so that information can be more effectively managed and secured according to its relative risk and criticality, advising against practices that treat all data equally.

City Organizations Involved in Data Governance

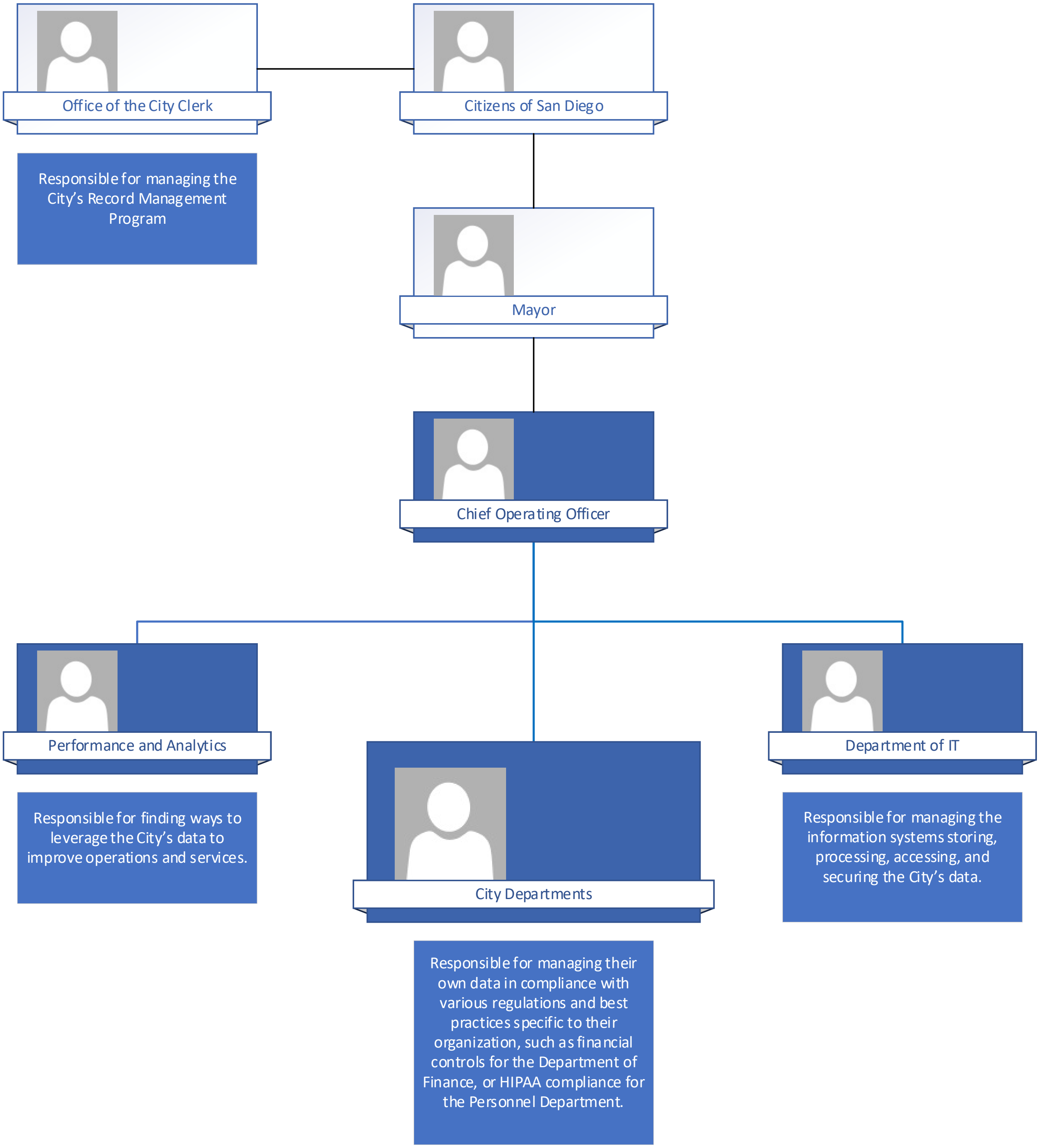
Throughout the City, departments collect, process, use, and own data to facilitate their operations and ultimately provide services to the residents of San Diego.

There are three primary departments that provide guidance to centrally manage segments of the City's data within the scope of their operations in addition to the individual department management of their own data. These departments, shown in **Exhibit 1**, include:

- Department of Information Technology to centrally manage information services and the data that flows through them;
- Department of Performance and Analytics to manage open data for the public and improve operations by leveraging data; and
- Office of the City Clerk as the custodian of the City's records.

Exhibit 1:

City's Current Data Management Organizational Structure


Office of the City Clerk
Responsible for managing the City's Record Management Program
Citizens of San Diego
Mayor
Chief Operating Officer
Performance and Analytics
Responsible for finding ways to leverage the City's data to improve operations and services.
City Departments
Responsible for managing their own data in compliance with various regulations and best practices specific to their organization, such as financial controls for the Department of Finance, or HIPAA compliance for the Personnel Department.
Department of IT
Responsible for managing the information systems storing, processing, accessing, and securing the City's data.

Source: Auditor Generated Based on City Organizational Charts.

The Department of Information Technology

The Department of Information Technology (DoIT) provides citywide strategic technology direction; operational support of application, infrastructure, and wireless technologies; enterprise application services; and manages IT services contracts and assets. Key areas of the department regarding data classification and encryption include:

- **IT Operations Management –** The IT Operations Group manages the network, data center, telecommunications, and departmental application portfolio for every location, server, departmental application, call center, and desktop phone in the City. Primarily operating through management of three IT service providers, the group sets the technology direction and innovation for the City's core infrastructure, resiliency, and data protection needs, and works with City departments to develop solutions to the challenges faced by the City; and
- **Cybersecurity Compliance and Risk Management** – The Cybersecurity Team provides the development, implementation and management of all citywide information security policies, standards, procedures, and internal controls.

DoIT's mission is to provide high quality technology and public safety wireless services while driving strategic innovation through collaboration and partnership with City and regional stakeholders.

Its vision is to be a national municipal leader and strategic business partner for innovative technology solutions.

To support the department's mission and vision, it has outlined four goals; only one of the goals is relevant to the security of the City's data and technology. The department plans to meet this goal by:

- Enhancing the automation of security with security information and event management;
- Creating an environment where security is a key decision point for all contracts, procurement processes, product selection, adoption, and use; and
- Modernizing, maintaining, and improving existing security tools in City infrastructure and in the cloud.

Another one of the goals is to deliver and support City technologies by optimizing the skills, training, and organizational structure of City staff to drive innovation and citywide best practices. Additionally, DoIT seeks to drive customer satisfaction through customer feedback and improvements.

The reader should note that DoIT's perspective of data management is focused within the spectrum of its mission and vision for providing and securing IT services to the City.

The Department of Performance & Analytics

The Performance and Analytics Department (PandA) is the City's internal consultant, driven by the following purposes:

- Simplify the customer experience to make it easy to communicate with and receive services from the City;
- Implement data-informed decision-making, migrating from reactive to predictive solutions; and
- Adopt a culture of continuous improvement and accountability to optimize the delivery of services.

PandA works across departments to eliminate silos, empower employees as problem solvers, instill a culture of data-informed decision making, and continuously improve processes and accountability.

The department's mission is to challenge the status quo. Its vision is to exceed expectations.

To support the department's mission and vision, it has outlined three goals; only one of the goals is relevant to the City's data management, which is to champion data-informed decision-making. However, it's related to open data. This kind of data is readily available to the public on the City's open government website and datasets. The department plans to meet this goal by:

- Expanding predictive analytics projects;
- Deploying point of service measurement tools; and
- Developing data analytics tools to improve City processes.

PandA's fiscal year (FY)2018 and FY2019 goals related to the City's data management were to increase data-enabled decision-making and transparency by (1) facilitating comprehensive data collection, management, and use; and (2) sharing data internally and publish externally.

Office of The City Clerk

The Office of the City Clerk (City Clerk) plays a vital role in municipal operations. The 1931 City Charter outlined the duties of the City Clerk, and the core functions remain: supporting the legislative body, coordinating municipal elections, and managing the City's Records Management Program. Key areas of the department regarding data classification and encryption is managing the City's records management program.

The department's mission is to provide accurate information and maximize access to municipal government, while its vision is to enhance access to local government.

To support the department's mission and vision, it has outlined four goals; only one of the goals is relevant to the security of the City's data and technology. This goal is to adhere to state and local mandates and deadlines related to City government. The department plans to meet this goal by providing records and information management guidance; resources and mandated training to City departments so that they can keep their retention file plans up-to-date and comply with records retention requirements; and vital records identification to ensure continuity after a disruption or disaster.

The City Clerk also provides records management training to departments, records coordinators, council staff, and mayoral staff on best practices to expedite legislative and regulatory compliance of City records.

The City Clerk's FY2019 goal was to continue to coordinate the City's Records Management Program by (1) providing records management training to departments, records coordinators, council staff, and mayoral staff on best practices to expedite legislative and regulatory compliance of City records; (2) establishing guidelines, training, and resources for departments to maintain vital records to ensure continuity after a disruption or disaster; and (3) providing greater accessibility to the historical records of San Diego and preserving extremely fragile books, maps, and documents using proven conservation methods and materials.

In FY2018, the City Clerk's goal was to adhere to state and local mandates and deadlines related to city government by (1) ensuring transparency and accessibility to public records in a timely manner; (2) complying with Brown Act noticing requirements and making SB343 (late-arriving) documents readily available; and (3) providing guidance and training to City departments to comply with record retention guidelines.

Organizations Providing Guidance for Data Governance

Three major organizations provide requirements and guidance for data and records management from the different perspectives embodied by the City's three departments:

- The National Institute of Standards and Technology (NIST) provides federal standards, requirements, and guidelines for securing information systems;
- The Data Management Association International (DAMA) provides guidance to data management professionals;
- The International Organization for Standardization (ISO)[1] is a worldwide federation of national standards[2] that provide standards and best practices across industries.

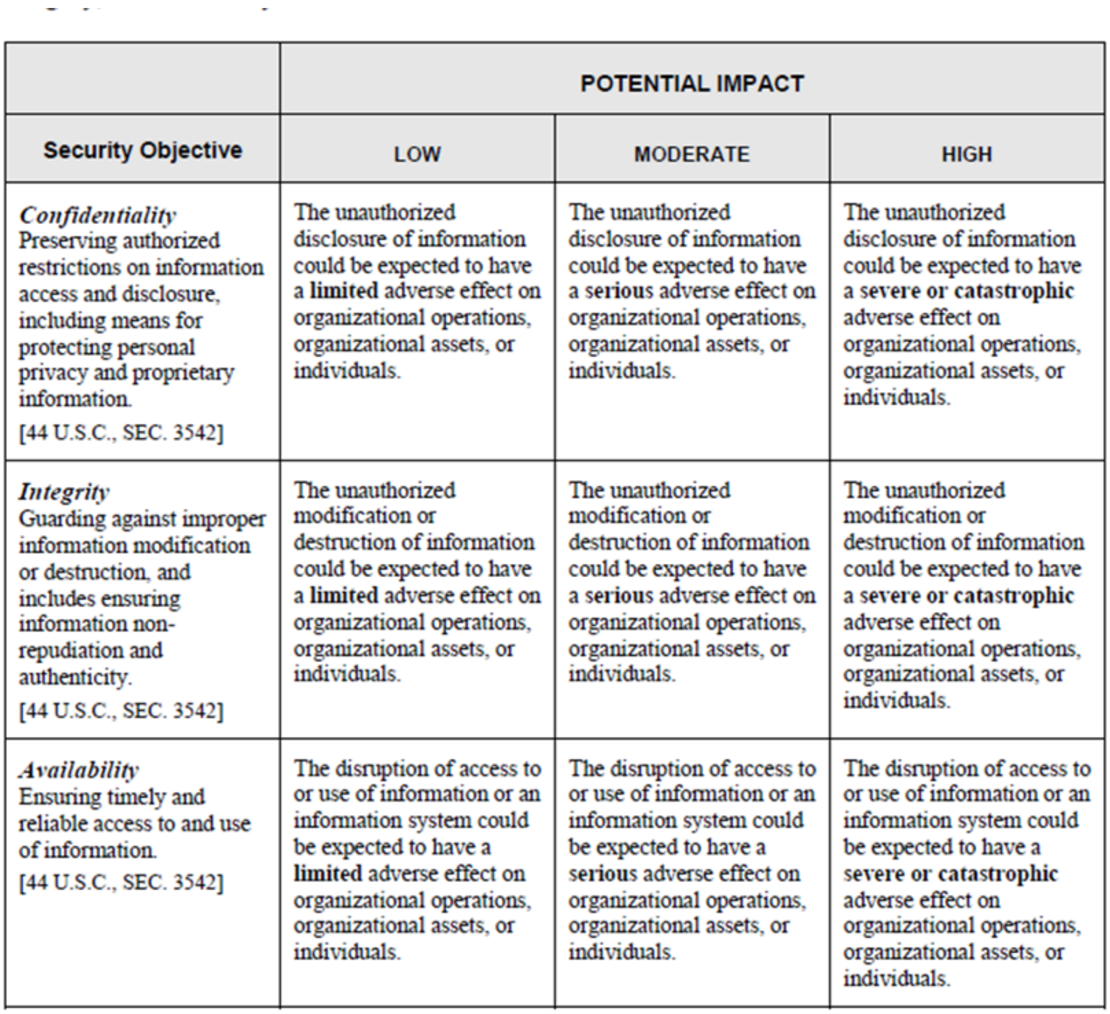
Exhibit 2 demonstrates NIST's potential security classification impact definitions.

[1] ISO 15489-1:2016 defines the concepts and principles from which approaches to the creation, capture, and management of records are developed < https://www.iso.org/standard/62542.html>.

[2] The City Clerk also follows the National Association of Government Archives & Records Administrators, the Association of Records Manager and Administrators, and the National Archives and Records Administrations to provide guidance for records management.

Exhibit 2:

Data Security Classification Definition Table



	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Source: National Institute of Standards and Technology (NIST)

Many of the controls provided by these agencies overlap with each other by providing similar control direction; however, the difference primarily lies in the perspective and detail of the guidance.

NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurements and standards infrastructure. NIST's Federal Information Processing Standards Publication Series is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act of 2002.

NIST's framework provides guidelines for the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry (PCI), and the Gramm–Leach–Bliley Act (GLBA), etc.

DAMA is a global association promoting the understanding, development, and practice of managing data and information as a key enterprise asset to support the organization.

ISO is a worldwide federation of national standards. ISO's International Standard 15489 defines the concepts and principles from which approaches to the creation, capture and management of records are developed.

Audit Results

Finding 1: The City Requires Stronger Coordination and Definition of Roles Between the Groups Responsible for Data Management to Ensure Availability and Security of the City's Data Resources

Data management is essential to ensure the City of San Diego (City) is aware of the data it has, maximize its usefulness for operations, and provide the public with appropriate access while balancing this access with appropriate security.

The City has undertaken several data management initiatives to better secure, manage, and leverage its data resources; however, with better coordination these initiatives could leverage the work performed by the different spearheading groups resulting in greater efficiency and stronger consistency.

Industry standards call for centralized data management for enabling business use of this data as well as appropriately securing it to prevent its misuse. Fundamental requirements include a data management strategy with a common set of directions for the effort, a centralized and comprehensive data inventory, and a centralized data classification methodology to enable full use and security.

The City has begun some centralization of data management efforts under several City departments:

- The Performance and Analytics Department (PandA), under the City's Chief Data Officer (CDO);
- The Department of Information Technology (DoIT), under the Chief Information Security Officer (CISO); and
- The Office of the City Clerk (City Clerk).

However, these efforts require additional definition of roles and responsibilities between the groups to better focus their efforts.

The City will likely achieve its goals regarding securing and leveraging City data under its current programs; however, it will likely take longer with numerous uncoordinated efforts to achieve it without developing a strategic plan and implementing a governance structure to achieve it.

The City's Data Management Parties Require Further Coordination

Centralized data management is critical for enacting smart City initiatives, such as energy saving smart features, like the City's smart street lights program or leveraging data for predictive analysis applied to targeting City services such as street repair or the implementation of safety features.

The City has undertaken several efforts to enact data management efforts; however, these efforts are divided among three groups without a clear plan that integrates the effort of the three. This results in duplication of efforts in some areas of data management, and other areas that require additional resources.

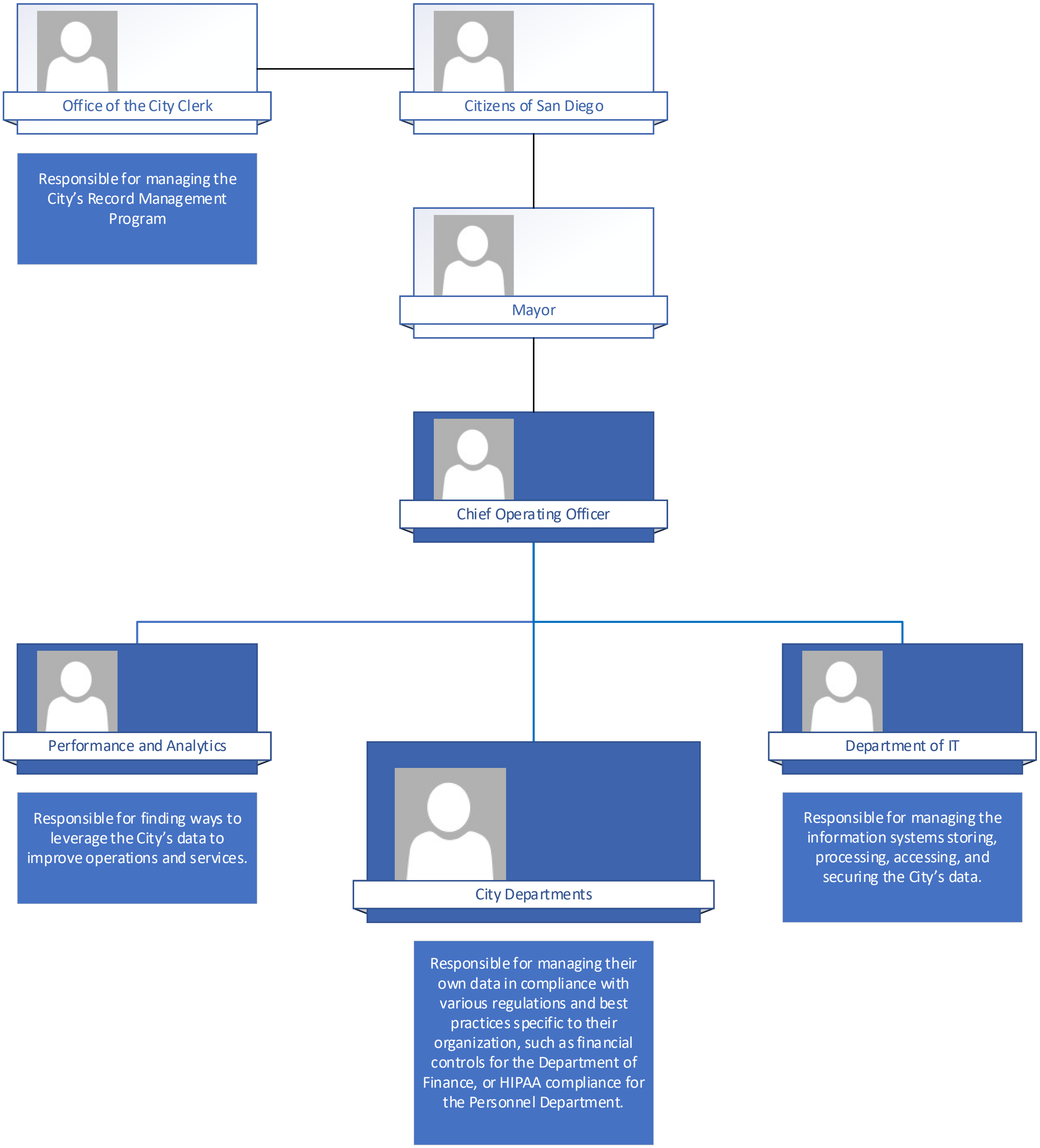
While each department in the City plays a role in data management for their data, PandA, DoIT, and the City Clerk play organizing roles in providing data management direction for the entire City for each of their unique focuses.

Each group, shown in **Exhibit 3**, is developing data management strategies, compliance requirements, and outcome objectives based on their unique roles.

The City has made significant progress with its open data project, IT classification effort, and record retention initiative. Still, each department is independently working toward the completion of several fundamental data management steps for their objectives.

Exhibit 3:

City's Current Data Management Organizational Structure


Office of the City Clerk
Responsible for managing the City's Record Management Program
Citizens of San Diego
Mayor
Chief Operating Officer
Performance and Analytics
Responsible for finding ways to leverage the City's data to improve operations and services.
City Departments
Responsible for managing their own data in compliance with various regulations and best practices specific to their organization, such as financial controls for the Department of Finance, or HIPAA compliance for the Personnel Department.
Department of IT
Responsible for managing the information systems storing, processing, accessing, and securing the City's data.

Source: Auditor Generated based on City Organizational Charts.

Performance and Analytics Data Management Initiatives

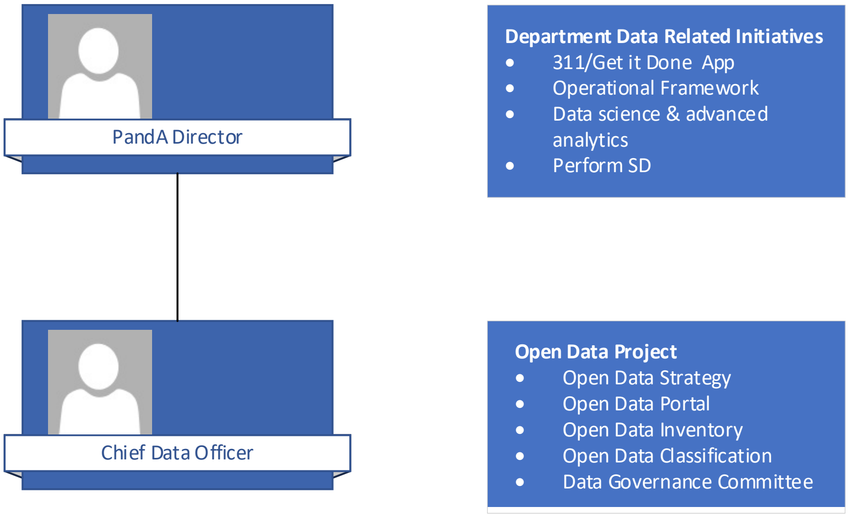
Open Data Initiative

The Performance and Analytics Department (PandA) is charged with making City services simplified for the City's customers and acts as both a consumer and manager of citywide data. The City created the role of the Chief Data Officer (CDO) as a program manager within PandA in 2015 to manage and facilitate the City's open data project through the City Council-approved Open Data Policy. In most private sector organizations, the CDO is responsible for managing the organization's data program. Within this scope, the CDO would oversee the data inventory and management of the City's data strategy. However, the CDO's current scope is defined by an internal PandA policy as a program manager over the open data project. Further, within municipal entities, other data management roles must be considered, such as the City Clerk and its City Charter-defined role, when identifying the appropriate role for a municipal CDO.

PandA's CDO inventoried data citywide as a deliverable of the Open Data Policy to determine information appropriate for an open data portal, which provides the public with access to City data. In this regard, the CDO has a partial inventory, categorization, and view of the City's data position, but a role typically responsible for leading the governance of data management activities in private sector organizations. The CDO views her future role as the leader of citywide data governance instead of only the City's open data, as shown in **Exhibit 4.**

Exhibit 4:

Performance and Analytics Data Management Projects



PandA Director

Chief Data Officer

Department Data Related Initiatives

- 311/Get it Done App
- Operational Framework
- Data science & advanced analytics
- Perform SD

Open Data Project

- Open Data Strategy
- Open Data Portal
- Open Data Inventory
- Open Data Classification
- Data Governance Committee

Source: Auditor Generated Based on Performance and Analytics Department (PandA) Documentation.

The Department of Information Technology's Data Management Indicatives

Data Classification & Regulatory Compliance

The Department of Information Technology's (DoIT) Cybersecurity Division is responsible for securing the City's information resources. Within this scope, the Cybersecurity Division is responsible for ensuring that the City's data is appropriately secured based on its classification. The Cybersecurity Division released data classification requirements in its June 2019 revision of the IT Standards and Guidelines Document. In spite of this, each City department follows their own categorization standards. During our discussions with the Cybersecurity Team, we found most departments believe that the categorization only applies to DoIT processes, which impacts DoIT's ability to determine exactly what data resides on the City's systems.

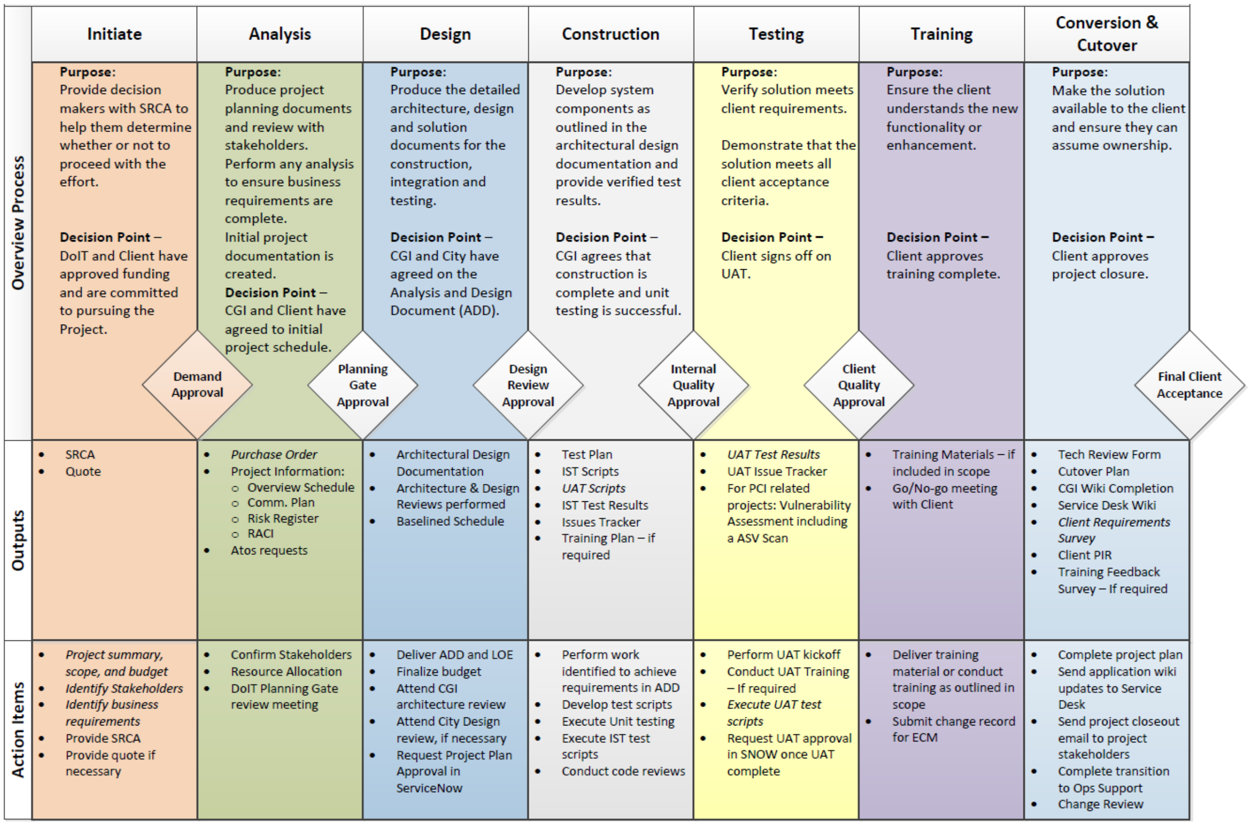
While it may seem counterintuitive, IT personnel rarely see the business data that organizations use in their operations and primarily focus on maintaining and securing the systems that house this data with very little perspective of how the business uses them and what is important to business. As a result, DoIT must work closely with departments to gain an understanding of what data is important and where it lives.

The City also has a less specific Administrative Regulation (AR) addressing data categorization, which the departments leverage to create their individual classification schema. Centralization will ensure that all users of the data can leverage the appropriate classification scheme for ensuring that the data is properly managed, used, distributed, and secured.

DoIT has recently begun a classification effort using its data classification for new data/information starting with a demand process to initiate an IT project, including to procure a new system or update an existing one. Initiating a new IT project through a demand, shown in **Exhibit 5**, is the beginning of the IT governance process, which includes classifying and approving the data.

Exhibit 5:

Department of IT Software Implementation/Demand Process



	Initiate	Analysis	Design	Construction	Testing	Training	Conversion & Cutover
Overview Process	**Purpose:** Provide decision makers with SRCA to help them determine whether or not to proceed with the effort. **Decision Point** – DoIT and Client have approved funding and are committed to pursuing the Project.	**Purpose:** Produce project planning documents and review with stakeholders. Perform any analysis to ensure business requirements are complete. Initial project documentation is created. **Decision Point** – CGI and Client have agreed to initial project schedule.	**Purpose:** Produce the detailed architecture, design and solution documents for the construction, integration and testing. **Decision Point** – CGI and City have agreed on the Analysis and Design Document (ADD).	**Purpose:** Develop system components as outlined in the architectural design documentation and provide verified test results. **Decision Point** – CGI agrees that construction is complete and unit testing is successful.	**Purpose:** Verify solution meets client requirements. Demonstrate that the solution meets all client acceptance criteria. **Decision Point –** Client signs off on UAT.	**Purpose:** Ensure the client understands the new functionality or enhancement. **Decision Point –** Client approves training complete.	**Purpose:** Make the solution available to the client and ensure they can assume ownership. **Decision Point –** Client approves project closure.
Outputs	• SRCA • Quote	• *Purchase Order* • Project Information: ○ Overview Schedule ○ Comm. Plan ○ Risk Register ○ RACI • Atos requests	• Architectural Design Documentation • Architecture & Design Reviews performed • Baselined Schedule	• Test Plan • IST Scripts • *UAT Scripts* • IST Test Results • Issues Tracker • Training Plan – if required	• *UAT Test Results* • UAT Issue Tracker • For PCI related projects: Vulnerability Assessment including a ASV Scan	• Training Materials – if included in scope • Go/No-go meeting with Client	• Tech Review Form • Cutover Plan • CGI Wiki Completion • Service Desk Wiki • *Client Requirements Survey* • Client PIR • Training Feedback Survey – If required
Action Items	• *Project summary, scope, and budget* • *Identify Stakeholders* • *Identify business requirements* • Provide SRCA • Provide quote if necessary	• Confirm Stakeholders • Resource Allocation • DoIT Planning Gate review meeting	• Deliver ADD and LOE • Finalize budget • Attend CGI architecture review • Attend City Design review, if necessary • Request Project Plan Approval in ServiceNow	• Perform work identified to achieve requirements in ADD • Develop test scripts • Execute Unit testing • Execute IST test scripts • Conduct code reviews	• Perform UAT kickoff • Conduct UAT Training – If required • *Execute UAT test scripts* • Request UAT approval in SNOW once UAT complete	• Deliver training material or conduct training as outlined in scope • Submit change record for ECM	• Complete project plan • Send application wiki updates to Service Desk • Send project closeout email to project stakeholders • Complete transition to Ops Support • Change Review

Source: Department of Information Technology.

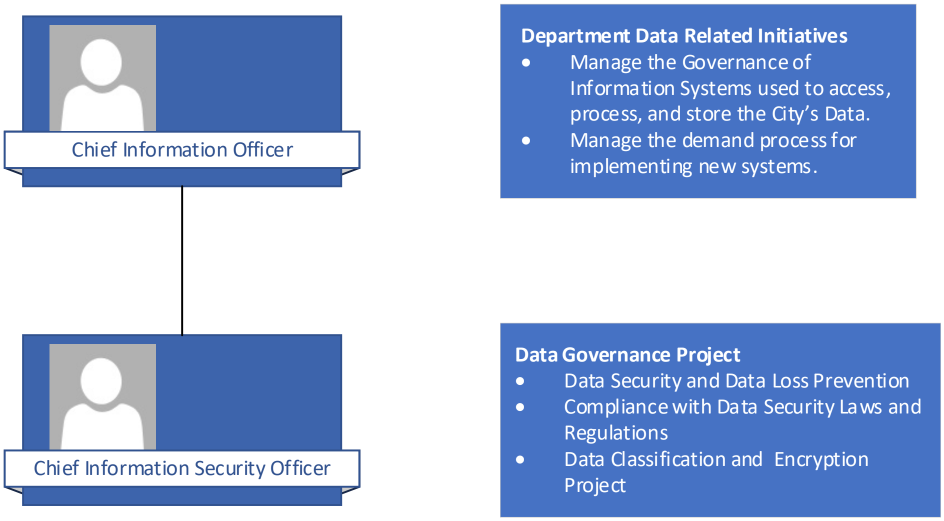
DoIT also conducts other activities that provide partial inventories of City data, such as maintaining a list of all City applications, including the general business use of those applications. Additionally, it ensures compliance with regulations, such as the Payment Card Industry Data Security Standard, resulting in a comprehensive security focused inventory of compliance related data.

As a result, DoIT maintains an IT-focused list of citywide data stored in applications with an IT-specific classification for newer systems or those under regulatory compliance. Even so, large segments of the City's data require departmental coordination to effectively classify it for IT purposes.

Furthermore, the IT classification requires additional attributes for other consumers of that data to leverage, and additional attributes to better manage a comprehensive security as discussed in our confidential report, as shown in **Exhibit 6.**

Exhibit 6:

Department of IT's Data Management Initiatives



Department Data Related Initiatives

- Manage the Governance of Information Systems used to access, process, and store the City's Data.
- Manage the demand process for implementing new systems.

Data Governance Project

- Data Security and Data Loss Prevention
- Compliance with Data Security Laws and Regulations
- Data Classification and Encryption Project

Source: Auditor Generated from Department of Information Technology Documentation.

Office of City Clerk Data Management Initiatives

The Office of the City Clerk (City Clerk) is an independent office created by the City Charter, and acts as the custodian of the City's records.

Record Management/ Retention Schedule

The City Clerk is responsible for the administration of a uniform Records Management Program assisting all City departments. The City Clerk's Records Management Division develops and circulates policies and procedures pertinent to the Records Management Program and works in conjunction with the City Attorney to ensure records retention compliance with local, state, and federal laws; and regulations relating to the retention and full disposition of public records.

Key components of the program include maintenance and oversight of the Master Records Schedule and Department Retention File Plans, mandated records and information training for all designated Department records coordinators, council and mayoral staff.

Under its Charter authority, the City Clerk first initiated a Records Management Program in 1959.

Records are a specific type of data. According to the City Clerk, a record is recorded information of any kind and in any form, created or received by the City that is evidence of its operation. Records include paper and electronic documents, electronic databases, electronic mail, correspondence forms, photographs, film, sound recordings, maps, and other documents that have administrative, legal, operational, fiscal, or historical value requiring retention of the record for a specified period of time.

Vital records are crucial in assisting departments to get back to business as soon as possible after a disaster. Normally, vital records make up only two to five percent of an organization's total volume of records.

Vital records that contain static information are kept permanently. However, some vital records that have short-term retention such as annual budget records, bank reconciliation files, and certificates of sale are kept until superseded by the new information.

The City's vital records include the City Charter, Municipal Code, tax and financial records, utility systems, land records, list of safety personnel and list of locations of emergency supplies, Articles of Incorporation, City Council resolutions, minutes and ordinances.

The City Clerk's definition of records is very similar to the International Standards Organization's[3] (ISO) definition, which defines records as evidence of business activity and information assets. Records can be distinguished from other information assets by their role as evidence in the transaction of business and by their reliance on raw data.

The City Clerk also maintains, preserves, and restores official City documents dating all the way back to the City's incorporation in 1850 and additional records as early as 1817.

Under these efforts, the City Clerk inventories and classifies data to identify vital records and to establish retention and disposition.

To facilitate this effort, the City Clerk maintains a recently released Master Record Schedule that contains a list of each record type within the City, its retention schedule, and the City department that owns the source version of that record. Department Retention File Plans are a list or record series derived from the Master Record Schedule applicable to each City department. The Records Management Program establishes policies and procedures for the retention and disposition of City records.

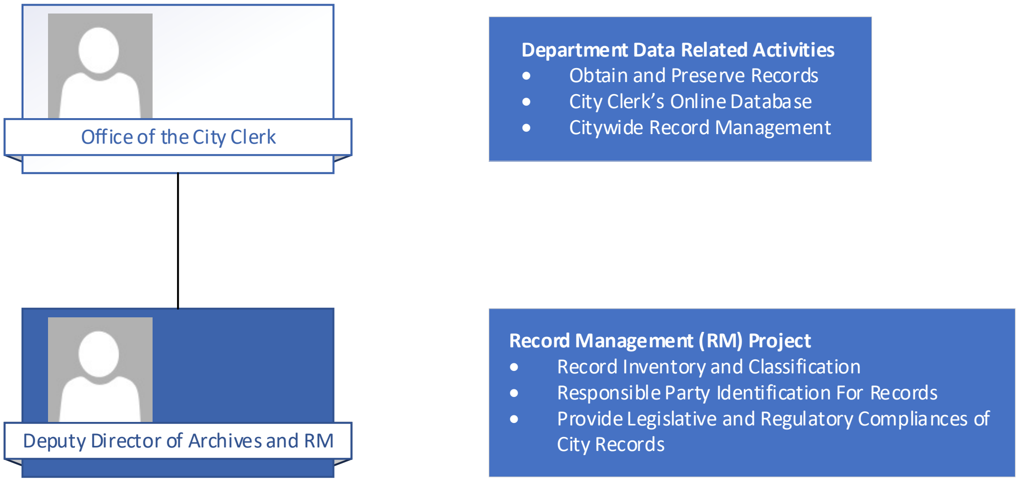
The City's Master Records Schedule classifies the records by six business functions. In this context, a record type is equal to a specific data category as used by the City Clerk, but not necessarily as other departments categorize their data. The City Clerk is currently in the process of implementing this schedule, which was approved by the City Council on October 18, 2018 and will take up to five years from the approval date for full adoption. As part of this process, the City Clerk is working closely with each City department to crosswalk their existing Records Disposition Schedule to the Master Records Disposition

[3] The International Standards Organization brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges <www.ISO.org>.

Schedule. As a result, the City Clerk has the most comprehensive list of City data associated with the department that owns the data, but in a format targeted toward their purpose, as shown in **Exhibit 7**.

Exhibit 7:

City Clerk Data Management Projects



Office of the City Clerk

Deputy Director of Archives and RM

Department Data Related Activities
- Obtain and Preserve Records
- City Clerk's Online Database
- Citywide Record Management

Record Management (RM) Project
- Record Inventory and Classification
- Responsible Party Identification For Records
- Provide Legislative and Regulatory Compliances of City Records

Source: Auditor Generated from City Clerk Documentation.

PandA, DoIT, and the City Clerk each require a comprehensive inventory of the City's data to effectively perform their functions and to ensure that the data is appropriately managed and secured; however, the City does not currently have a comprehensive data inventory, which is the first step in data management.

While each group has a portion of the City's data inventoried in different ways, no group appears to follow a single standard that facilitates its use by the other groups. Further, while individual departments inventory and classify the critical data they own, they also follow their own classification and management standards as defined by their individual business requirements. Additionally, there's no comprehensive citywide data owner list.

Administrative Regulation (AR) 90.64, Protection of Sensitive Information and Data, defines that City department heads assign the record coordinators for the record types they own, and the City Clerk is updating their list of record types owned by a specific department.

Additionally, the Chief Data Officer (CDO) also has a department contact list for personnel that they can work with to obtain data; however, this is an informal process and not part of their designated role. As a result, the CDO and Chief Information Officer (CIO) do not have a specific person to contact in each department that is responsible for the data management within that department.

Finally, each player is working to individually create their own master inventory and classification to complete their department's objectives without ensuring that other groups can leverage this inventory or classification for their objectives, resulting in redundant city efforts.

Data as a Critical Asset

Data is seen by many modern organizations in today's world as the crown jewel of the organization. In the private sector, data facilitates everyday services such as:

- Instant driving directions and traffic updates, such as Google Maps;
- Expedient online ordering and delivery, such as Amazon Prime; and
- Product intuitiveness and usability, such as the features found in smart phones and apps.

In cities, data facilitates services such as:

- Green efficiency initiatives, such as smart street lights, smart traffic lights to reduce congestion;
- Remote and online Services, such as the City's Get It Done app; determination/facilitation of online city services; and
- Data-driven city-planning, used to determine how a City can grow, infrastructure needs, and where resident services are most needed.

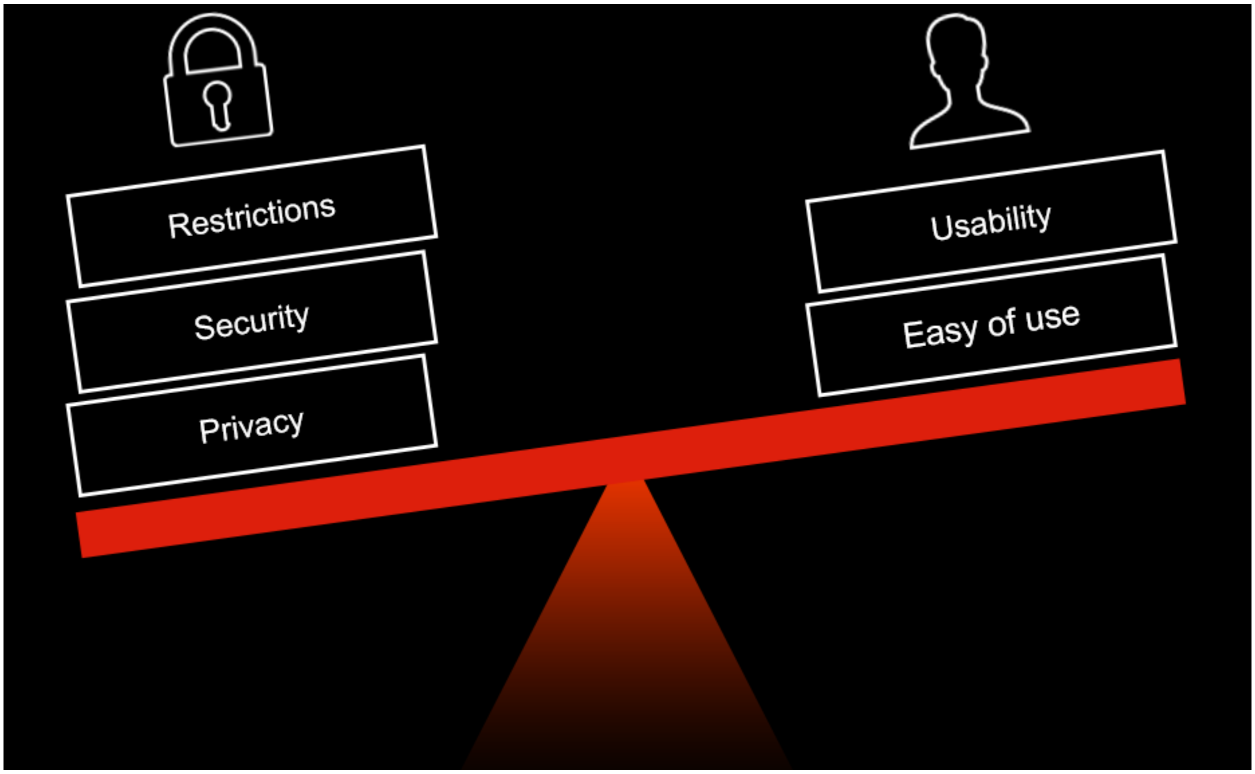
Data governance is critical to both enable the operational efficiencies and appropriate security of this crown jewel.

Security Is the Opposite of Data Usability, But Necessary to Protect Data Based on Its Classification, Or Sensitivity

The fundamental challenge between using and securing data is the balance between the two opposites of access, shown in **Exhibit 8**. The most usable data is completely available to everyone, while the most secure data is restricted to few, or unavailable for use.

Exhibit 8:

Security Verses Usability



Source: Kaymera Information Security.

Organizations must balance these requirements based on their needs and define the use of their data with the security needs based on the security classification of data. One critical aspect of data management is to define where in the spectrum of use vs. security that data should be placed and by whom it can be accessed. Additionally, this method for tracking the attributes would be managed in a standard manner through a data classification process.

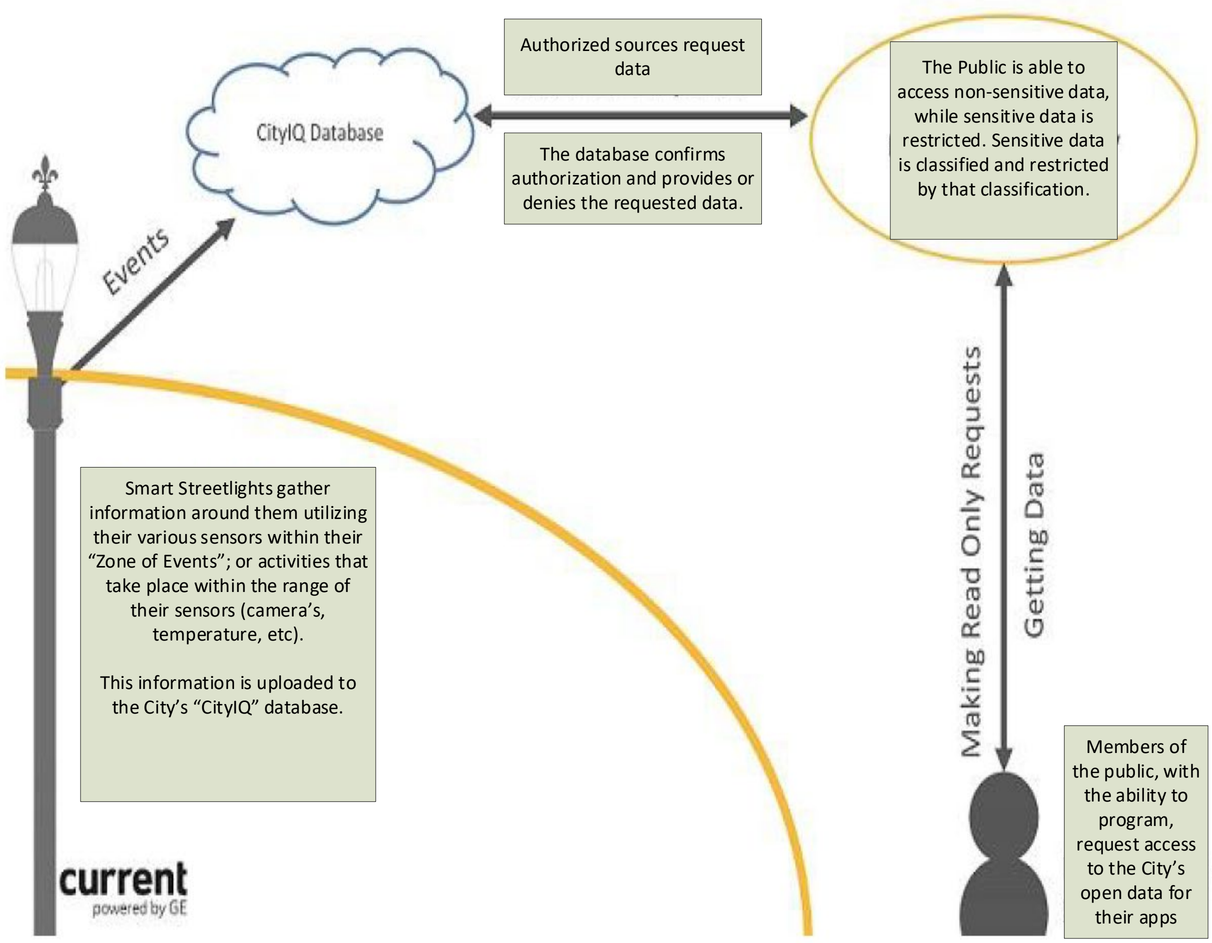
Recent Potential Applications:

Smart Streetlights

Cities and organizations have the opportunity to gather vast amounts of data from many sources. A recent example of data being collected and requiring governance is the Smart Streetlight Program, shown in **Exhibit 9**. This program has the opportunity to save City resources and collect useful information, but requires proper management to ensure the appropriate use and security of that data.

Exhibit 9:

Smart Streetlight Saving Power/Collecting Data



Authorized sources request data

The database confirms authorization and provides or denies the requested data.

The Public is able to access non-sensitive data, while sensitive data is restricted. Sensitive data is classified and restricted by that classification.

Smart Streetlights gather information around them utilizing their various sensors within their "Zone of Events"; or activities that take place within the range of their sensors (camera's, temperature, etc).

This information is uploaded to the City's "CityIQ" database.

Members of the public, with the ability to program, request access to the City's open data for their apps

Source: Auditor Generated from the City of San Diego's Sustainability Smart Streetlights Program.

Data, such as the information collected from the City's smart streetlight program, should be inventoried and classified to comply with data management best practices to ensure its appropriate use and security.

For example, according to the City's public site, anyone who would like to access open data from the smart street lights such as static data on parking, vehicle counts, pedestrian counts, temperature, humidity, or pressure, from the City's intelligent streetlight sensors may use the publicly available application programming interface key. However, raw video footage and images from these smart streetlights is restricted and only available to specific parties, such as the police department through specific procedures.

As in the case of the City's smart streetlights, a data inventory and classification process help to determine exactly what data is collected, and how that data should be treated.

Standards for Data Governance Facilitate Operational Efficiencies and Appropriate Security of Data

The Department of Information Technology (DoIT) secures the data and ensures the applications housing the data are properly managed; the City Clerk provides guidance for how long the records should exist and which formats are most appropriate to retain these records; and the Performance and Analytics Department (PandA) creates data access for open data and internal purposes, analyzes data to support decision-making and performance management, and improves data management practices when integrating departments into the Get It Done service request platform.

There are numerous definitions and guidance for managing data. However, the three most applicable guidance organizations for data management from the three data perspectives are:

- The Data Management Association International (DAMA) for overall data management and highly applicable to the CDO's role;
- The National Institute of Standards and Technology (NIST) for defining data security standards, highly applicable to the Chief Information Security Office (CISO); and
- The International Organization for Standardization (ISO) 15489[4] for records management as applicable to the City Clerk.

As a result, we are merging their guidance to focus on the same fundamental steps.

Data Governance and Management Initial Steps

Data governance[5] is the core component of data management, governing the availability, usability, integrity and security of data used in an enterprise. Data governance is about maximizing the value of data for operational effectiveness, decision-making, and regulatory requirements, as well as minimizing the risks associated with poor data management. Today's explosion of data is highly valuable to organizations from a strategic standpoint. It also presents challenges in storage, management, and adherence to regulatory and legal requirements. Developing an effective data governance program is essential to harness the data's potential and to help minimize risks.

[4] ISO 15489-1:2016 defines the concepts and principles from which approaches to the creation, capture and management of records are developed < https://www.iso.org/standard/62542.html>.

[5] According to DAMA, data governance is the core component of data management, tying together the other 9 disciplines, such as data architecture management, data quality management, reference & master data management <https://dama.org/>.

To unlock the value of an organization's data, the organization should develop and implement a clear data strategy. The data strategy can help organizations take a strategic view of data and use it more effectively to drive results. The best data strategies:

- Tailor to the organization's needs to engage necessary stakeholders;
- Plan for the future;
- Implement strategic projects;
- Develop partnerships across the organization; and
- Emphasize successes to drive a strategic mindset.

Data Inventory

A data inventory is a critical element of the City's information governance model, and the first step to managing data. If the inventory is set up correctly, it provides the City with not only what it has, but all the details about the data that it requires to fully manage and leverage it for operations. This information includes details about what it is, where it's located, who owns it, and who can access it. Organizations need to know the type and source of data collected, stored, and used—and how accurate and complete it is. Inventories should be risk-ranked to reflect inherent risk and quantify business needs for the data.

Building and maintaining a comprehensive data inventory can enhance overall data quality and help create a path to streamline the compliance efforts, which helps in the effort of reducing risk through the creation of an effective controls framework.

Data Classification

Data classification is a process of consistently categorizing data based on specific and pre-defined criteria so that this data can be efficiently and effectively protected and leveraged for operational requirements.

Data discovery is closely aligned with classification; before you can classify data, you have to find it. Data discovery needs to look at the endpoint, on network shares, in databases, and in the cloud.

Data classification is a foundational step in cybersecurity risk management. It involves identifying the types of data that are being processed and stored in an information system owned or operated by an organization. It also involves making a determination on the sensitivity of the data and the likely impact arising from compromise, loss, or misuse. The term—classification—as used in this document will imply the holistic approach of data categorization for confidentiality, integrity, and availability rather than the narrower scope of national security impact.

Data Classification as an Enabler

In effect, data classification enables a less restricted handling of most data by bringing clarity to the items requiring the elevated control.

According to standards, data classification is a foundational step in data management. It involves identifying the types of data that are being processed and stored in an information system owned or operated by an organization. It also involves making a determination on the sensitivity of the data and the likely impact arising from compromise, loss, or misuse.

For data classification process, the very first step is to conduct an inventory of the various data types that exist in the organization.

The second step is to conduct a risk assessment for each broad data type and assign a level of potential risk (low, moderate, or high) to each security objective—confidentiality, integrity and availability—with an associated risk matrix. And define data owners which are responsible for the correct classification and the data they own.

The third step is the security assessment and authorization. A data classification strategy must include a robust and effective means of authentication (making sure only the right people user data at a given level of sensitivity) and authorization (making sure they only use it in the right ways). The last step is continuous monitoring.

Data classification must be done by those who know the business needs of the organization and the importance and sensitivity of the data in relation to those needs with input from those with perspectives on individual privacy, regulatory requirements, public sentiment, and the legislative environment.

Insufficient Coordination Results in Redundant Efforts and Missed Opportunities to Increase the Efficiency of Implementing A Centralized Data Governance Program

A lack of coordination in the City's data management initiatives results in various duplicated efforts, and unnecessary barriers that could be reduced or removed though a centralized management approach.

For example, the Department of Information Technology (DoIT) rolled out a citywide security classification policy, which, when surveyed throughout the City, most departments considered it to be DoIT-specific and did not implement it. Without complete implementation from the departments, DoIT is hampered due to insufficient information on the departments' data.

Additionally, the Office of the City Clerk (City Clerk) is rolling out its record retention schedule and working with each department on the rollout for the management of their records, including electronic data. If the City Clerk coordinated this effort with the Performance and Analytics Department (PandA) and DoIT, it could potentially leverage the other's resources to obtain the information each require to complete their initiatives while creating a centralized inventory and classification.

While the City is moving toward centralized management of its data resources, it can reduce redundancies and improve the overall efficiency of its effort to maximize its smart-city efforts.

However, the City has not reached the initial stage of data management through the creation and classification of a comprehensive data inventory. The three managing groups have invested significant resources on this initiative, but only as it relates to their specific requirements.

Lack of data classification program maturity increases the risk of loss of data in the event of a breach or data loss, such as a lost USB drive or stolen laptop.

According to IT security standards for confidential data[6], the loss of data could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. For example, a severe or catastrophic adverse effect may result in:

- The loss of confidentiality, integrity, or availability might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
- Major damage to organizational assets,
- Major financial loss, or
- Severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

[6] Confidential data includes Health Insurance Portability and Accountability Act (HIPAA) data, Protected Health Information, California Law Enforcement Telecommunication System, attorney-client data, Payment Card Industry, and Personally Identifiable Information.

The City Has Not Created A Central Data Governance Strategy with Roles and Authority Divided Between Three Groups

The City has not implemented a centralized data management strategy that cleanly defines how the three involved parties manage data, their roles, and how they can standardize and enforce data management across City departments to facilitate success. As a result, each group and each department work toward their own measure of success.

This partially results from the fact that the City has three different groups managing three different aspects of data management/governance without coordination. Each one has their own strategies in various stages of development, deployment, and completion geared toward their individual objectives. For example, while DoIT has rolled out a data classification policy, the policy is not aligned to department business requirements and as a result, it is not followed by each department and viewed by departments as DoIT-specific, based on our survey results.

While each group has different compliance requirements, legal authority, and outcome objectives, there are common areas in which they can coordinate their efforts to minimize redundancies and achieve shared outcomes. However, each group's legal authority, core mission, regulatory, and compliance requirements must be incorporated into any centralized approach.

To reduce the duplication of efforts in data management, establish roles and responsibilities, and ensure consistency in data management across City departments, we recommend the following:

Recommendation #1: The three city data management authorities—the Chief Data Officer (CDO), Chief Information Officer (CIO), and City Clerk—should work collaboratively to create a centralized data management strategy based on a centralized data governance model. All three authorities should sign off on the policy and the City Attorney should conduct a legal review to ensure compliance with applicable laws and regulations.

Further, this strategy should incorporate the different roles of the CDO, CIO, and City Clerk to clarify their data management objectives and potential areas of collaboration (Priority 1).

Recommendation #2: The Chief Data Officer and Chief Information Officer should work with the City Clerk to create a citywide data classification of the various data types that leverage information gathered to create the Department Record File Plans, which outlines and classifies records and their retention requirements. This data classification should contain attributes required and usable by all involved parties in addition to incorporating the current classifications (Priority 1).

Recommendation #3: The Chief Data Officer (CDO) and Chief Information Officer (CIO) should work with the City Clerk to ensure departments coordinate efforts to create a data inventory containing the data/records, its location, owner, classification, and attributes. This effort can leverage the City Clerk’s Department Record File Plans to improve the efficiency of the effort.

Each department should define the person and position responsible in their department for data management that may mirror the records management representative to coordinate data management for the department in accordance with the City’s data strategy (Priority 1).

Finding 2: The Role of Chief Data Officer Requires Additional Definition to Facilitate Centralization of Citywide Data Management

In most private sector organizations, the Chief Data Officer (CDO) is the executive who holds the keys to help an organization both protect and unlock the full value of its data assets. The CDO builds and oversees a data strategy and set of competencies that work in concert to enable information sharing, collaboration, compliance and security, and efficient resource management to support such critical stakeholder objectives. The CDO takes an enterprise view of data, builds bridges, and knocks down walls as needed to enable data to flow expediently across departments and functions for better consumption and leverage. In addition, more than ever the CDO is the ambassador for the vision, business value, and resulting benefits of effective data management. However, the current CDO in the City of San Diego (City) builds and oversees strategies for open data and advanced analytics but does not have the authority to protect and unlock the full value of citywide data.

Within a municipal environment, such as the City, the CDO role must additionally take into account other roles, such as the Chief Information Officer (CIO) and City Clerk that have data management responsibilities and authority. The role definition should especially take into account the role of City Clerk, who has City Charter and municipal authority over City records management, which covers a specific type of data within the City.

We recommend the CDO, City Clerk, and CIO create an Administrative Regulation defining a citywide data governance model and the roles and responsibility of each of the City's data management entities within that model.

The City Has Not Defined CDO's Role and Authority for The Citywide Data Governance

The City has several partial data governance models in progress; however, it has not defined a centralized citywide data governance model to reduce redundancies. Additionally, the City has not defined the Chief Data Officer's (CDO) role and authority within that model. Currently, the CDO's role is only defined within the scope of the Performance and Analytics Department's (PandA) open data policy, resulting in insufficient authority to coordinate the City's data governance project. This policy was initially executed in 2015, within the scope of the City's Open Data Policy approved by the City Council.

In the City of San Diego, the CDO's job responsibility was initially to prepare an inventory of Open Data Sets owned or managed by the City. The CDO should build and oversee a data strategy and set of competencies that work in concert to enable information sharing, collaboration, compliance and security, and efficient resource management to support such critical stakeholder objectives. If the CDO lacks adequate resources or authority, he or she may need individual business units, back-office functions and IT departments to provide the extra resources.

Further, insufficient definition of roles in the City could result in a potential conflict with other data management roles in the City, such as the City Clerk or Chief Information Security (CISO).

The City Clerk classifies the data for record retention purposes and the CISO classifies data for security purposes. There is no citywide data management and data classification standard. The CDO, City Clerk and CISO follow different data management policies and procedures. Further, noncentralized roles with better-defined authority manage their data according to their individual department's needs, contributing to decentralized data management challenges.

Insufficient authority and definition place unnecessary challenges coordinating efforts between the CDO, CISO, and City's Clerk's roles in addition to the City's departments.

Standards Require That CDO's Role Combines Data Management, Architecture, Governance, And Analytics

According to Gartner,[7] CDOs in the private sector bear responsibility for the firm's enterprise-wide data and information strategy, governance, control, policy development, and effective exploitation. The CDO's role combines accountability and responsibility for information protection and privacy, information governance, data quality and data life cycle management, along with the exploitation of data assets to create business value.

In the private sector, the Chief Information Officer (CIO), CISO, and CDO roles should be clearly defined to prevent any overlap in responsibilities. The CDO plays more of a risk, compliance, policy management, and business role; the CDO should drive the information and analytics strategy serving a business role. The CDO builds and oversees a data strategy and set of competencies that work in concert to enable information sharing, collaboration, compliance and security, and efficient resource management to support critical stakeholder objectives.

Within a municipal environment, other roles must also be taken into account, such as the City Clerk who has a Charter-defined responsibility to manage Citywide records, which are a specific type of data. As such, the role of the CDO must be defined in a manner that does not infringe on the Charter role and authority of the City Clerk.

The CIO's Role in Data Governance

Fostering a positive relationship between the CDO, City Clerk, and the CIO functions is imperative. Since the City's business functions traditionally have not had the resources or leader to engage in data-related agenda-setting, technologists have grown to own data dictionaries, analytics, etc. The CDO is increasingly assuming these responsibilities and this can create friction. With direction from the Chief Operating Officer (COO), the two positions can work collaboratively to create business value from the organization's technology and data resources.

[7] Gartner is a global research and advisory firm providing information, advice, and tools for leaders in IT, finance, human resources, customer service and support, communications, legal and compliance, marketing, sales, and supply chain functions.

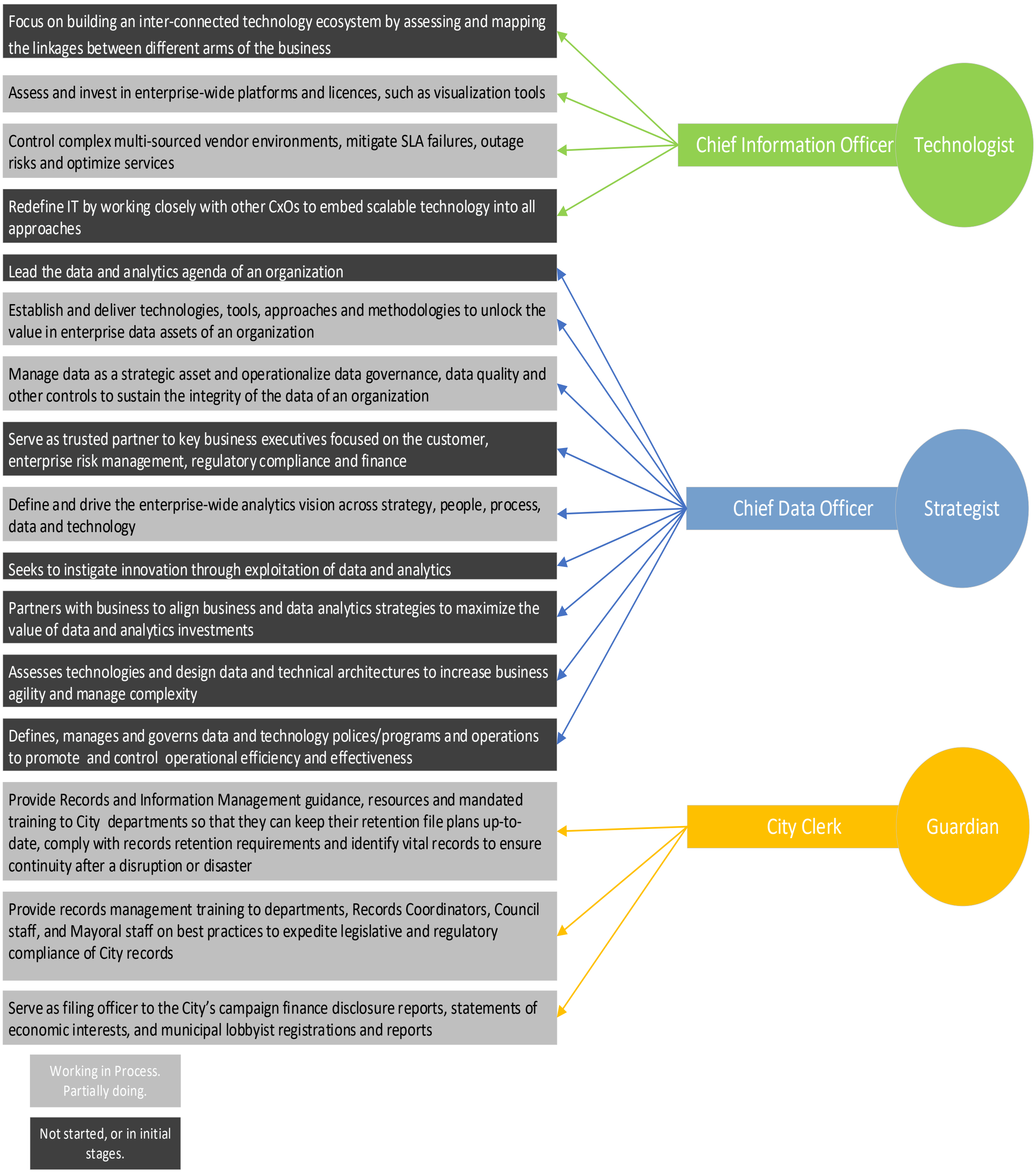
The Office of The City Clerk's Role in Data Governance

The City Clerk has a City Charter role codified in the Municipal Code and other City Administrative Regulations and guidelines to establish policy and procedures for the retention, disposition and preservation of City records regardless of format. City Clerk Records Management works with all City departments for identifying, classifying, archiving, and preserving City records. Its role in safeguarding the City's records includes electronic and paper forms of data. The City Clerk's tenure goes significantly further back than the CIO or the CDO, which are both relatively new roles and offices in comparison. As a result, any data management approach must incorporate the role of the City Clerk and include a definition of records and vital records in the data types classified, over which the City Clerk has a Charter responsibility.

Exhibit 10 shows a potential division of data management roles between the CIO, CDO, and City Clerk based on an analysis completed by Deloitte and adapted by the City Auditor to include the role of the City Clerk.

Exhibit 10:

Potential Data Management Role Assignments of CIO, CDO, and City Clerk



Focus on building an inter-connected technology ecosystem by assessing and mapping the linkages between different arms of the business

Assess and invest in enterprise-wide platforms and licences, such as visualization tools

Control complex multi-sourced vendor environments, mitigate SLA failures, outage risks and optimize services

Redefine IT by working closely with other CxOs to embed scalable technology into all approaches

Lead the data and analytics agenda of an organization

Establish and deliver technologies, tools, approaches and methodologies to unlock the value in enterprise data assets of an organization

Manage data as a strategic asset and operationalize data governance, data quality and other controls to sustain the integrity of the data of an organization

Serve as trusted partner to key business executives focused on the customer, enterprise risk management, regulatory compliance and finance

Define and drive the enterprise-wide analytics vision across strategy, people, process, data and technology

Seeks to instigate innovation through exploitation of data and analytics

Partners with business to align business and data analytics strategies to maximize the value of data and analytics investments

Assesses technologies and design data and technical architectures to increase business agility and manage complexity

Defines, manages and governs data and technology polices/programs and operations to promote and control operational efficiency and effectiveness

Provide Records and Information Management guidance, resources and mandated training to City departments so that they can keep their retention file plans up-to-date, comply with records retention requirements and identify vital records to ensure continuity after a disruption or disaster

Provide records management training to departments, Records Coordinators, Council staff, and Mayoral staff on best practices to expedite legislative and regulatory compliance of City records

Serve as filing officer to the City's campaign finance disclosure reports, statements of economic interests, and municipal lobbyist registrations and reports

Working in Process. Partially doing.

Not started, or in initial stages.

Source: Auditor Generated based on a Deloitte role analysis

Poor Definition of The CDO Role Results in Data Management Gaps, Potential Conflicts Over Responsibilities and Authority

The CDO's role was defined in the 2015 Open Data Policy Implementation Plan as a program manager geared toward implementing the open data program. The program was focused around making data available online to promote civic engagement, improve service delivery, allow for more effective communication with the public, and increase opportunities for economic development. The policy also recognized the limited resources devoted to the effort to accomplish their objective.

As a result, the CDO role is insufficiently defined in its current form to perform effective enterprise-wide data management, resulting in data management gaps and potential conflicts over responsibilities and authority.

The CDO’s Role is Insufficiently Defined to Manage the Citywide Data Program

The CDO’s role in the City was created with a very limited scope in mind for the purpose of spearheading the open data project. While this effort may have been a good start to begin a pilot data management program, it does not fulfill the current data needs of the City.

Without a business leader with authority established within a centralized model, taking into account other data management shareholders, the City’s individual departments perform uncoordinated redundant data management functions without ensuring other consumers of that data can leverage the same work the various departments are performing.

Further, the City’s data management approach requires clear delineation of authority and definition of roles between the CDO, City Clerk and CIO to prevent actual and perceived conflicts between their functions or charter authority and ensure there are no redundancies or undefined areas of responsibilities between their roles.

To ensure that the City’s data management effort is centralized, coordinated, and effective, we recommend the following:

Recommendation #4: The Chief Operating Officer should ensure appropriate resources are allocated to the City Clerk, Chief Information Officer, and Chief Data Officer to coordinate and execute the data management strategy based on that governance model (Priority 1).

Recommendation #5: The City Clerk, Chief Information Officer, and Chief Data Officer should create an Administrative Regulation defining a citywide data governance model and the roles and responsibility of each of the City’s data management entities. (Priority 1).

Conclusion

Data management, including creating a data inventory and classifying data, is a critical process to both fully leverage data for the City of San Diego's (City) operational needs, while appropriately granting members of the public access to that data, and implementing appropriate security over its sensitive data.

The City has been undertaking the effort to appropriately manage its data among several different departments; however, in order to facilitate the process, the City must formalize its data management strategy, define appropriate roles and responsibilities, and grant required authority to the roles to develop, centralize, and coordinate this data management program.

We made five recommendations to develop, centralize, and formalize the City's data management program. Management agreed with all five of our recommendations to better enable the City to both leverage and protect its data resources.

We also issued a confidential report addressing IT security related concerns in accordance with Government Auditing Standards Section 7.61, Reporting Confidential and Sensitive Information. Management agreed to implement the recommendations from the confidential report.

Recommendations

Recommendation #1: The three city data management authorities—the Chief Data Officer (CDO), Chief Information Officer (CIO), and City Clerk—should work collaboratively to create a centralized data management strategy based on a centralized data governance model. All three authorities should sign off on the policy and the City Attorney should conduct a legal review to ensure compliance with applicable laws and regulations.

Further, this strategy should incorporate the different roles of the CDO, CIO, and City Clerk to clarify their data management objectives and potential areas of collaboration (Priority 1).

Recommendation #2: The Chief Data Officer and Chief Information Officer should work with the City Clerk to create a citywide data classification of the various data types that leverage information gathered to create the Department Record File Plans, which outlines and classifies records and their retention requirements. This data classification should contain attributes required and usable by all involved parties in addition to incorporating the current classifications (Priority 1).

Recommendation #3: The Chief Data Officer (CDO) and Chief Information Officer (CIO) should work with the City Clerk to ensure departments coordinate efforts to create a data inventory containing the data/records, its location, owner, classification, and attributes. This effort can leverage the City Clerk’s Department Record File Plans to improve the efficiency of the effort.

Each department should define the person and position responsible in their department for data management that may mirror the records management representative to coordinate data management for the department in accordance with the City’s data strategy (Priority 1).

Recommendation #4: The Chief Operating Officer should ensure appropriate resources are allocated to the City Clerk, Chief Information Officer, and Chief Data Officer to coordinate and execute the data management strategy based on that governance model (Priority 1).

Recommendation #5: The City Clerk, Chief Information Officer, and Chief Data Officer should create an Administrative Regulation defining a citywide data governance model and the roles and responsibility of each of the City’s data management entities (Priority 1).

Appendix A: Definition of Audit Recommendation Priorities

DEFINITIONS OF PRIORITY 1, 2, AND 3

AUDIT RECOMMENDATIONS

The Office of the City Auditor maintains a priority classification scheme for audit recommendations based on the importance of each recommendation to the City, as described in the table below. While the City Auditor is responsible for providing a priority classification for recommendations, it is the City Administration's responsibility to establish a target date to implement each recommendation taking into consideration its priority. The City Auditor requests that target dates be included in the Administration's official response to the audit findings and recommendations.

Priority Class[8]	Description
1	Fraud or serious violations are being committed. Significant fiscal and/or equivalent non-fiscal losses are occurring. Costly and/or detrimental operational inefficiencies are taking place. A significant internal control weakness has been identified.
2	The potential for incurring significant fiscal and/or equivalent non-fiscal losses exists. The potential for costly and/or detrimental operational inefficiencies exists. The potential for strengthening or improving internal controls exists.
3	Operation or administrative process will be improved.

[8] The City Auditor is responsible for assigning audit recommendation priority class numbers. A recommendation which clearly fits the description for more than one priority class shall be assigned the higher priority.

Appendix B: Objectives, Scope, and Methodology

Audit Objectives

In accordance with the Office of the City Auditor's approved Fiscal Year (FY)2020 IT Audit Work Plan, we have completed an audit of the Citywide Data Classification and Sensitive Data Encryption Program. As stated in the work plan, the overall tentative objective of this audit was to assess the maturity of the City's sensitive data encryption and data classification process.

As a result of our preliminary research and initial program assessment, we defined our audit scope to focus on the period of FY2020 and to review the three objectives listed below:

- ***Objective 1:*** Assess the data classification process alignment and maturity.
- ***Objective 2:*** Assess the data classification and encryption process based on available classification.
- ***Objective 3:*** Assess the sufficiency of the City of San Diego's (City) Chief Data Officer role and authority to enact data governance including, classification

Scope and Methodology

Data Classification Process Alignment and Maturity

To assess the data classification process alignment and maturity, we requested and reviewed available data classification process documents, data governance documents, and relevant data management documents from the Department of Information Technology (DoIT), the Office of City Clerk (City Clerk), and the Performance and Analytics Department (PandA). These documents included available data classification policies and procedures, compliance with national best practices as defined in National Institute of Standards and Technology (NIST) SP800-X, and data owner lists and the available enterprise-wide data inventory components.

We also selected departments with sensitive data for review and assessed authentication and authorization methodology. Further, we interviewed department staff to determine the business requirements to determine sample size of data classification. Additionally, we performed a gap and alignment analysis of the data classification strategy alignment to the business requirements, the data governance alignment to the data classification policy and standards and the data classification strategy alignment to the national compliances, laws and regulations, and mapped the access controls to standards.

Data Classification and Encryption Process Based on Available Classification

To assess the data classification and encryption process based on available classification, we requested and reviewed data classification documents from the Department of Information Technology, Office of City Clerk, and the Performance and Analytics Department. We requested a sample of data classification enforcement and Standards for Data Classification tools. Additionally, we assessed the enforcement of data classification and relevant tool configuration for sufficiency based on standards, and we mapped configuration and data encryption to standards.

The Sufficiency of the City’s Chief Data Officer Role and Authority to Enact Data Governance

To assess the sufficiency of the City’s Chief Data Officer’s (CDO) role and authority to enact data governance including classification, we requested and reviewed data governance model and CDO's role and mission documentation. We performed a gap and alignment analysis of the data governance alignment to the CDO's role and mission of data classification.

We also issued a confidential report addressing IT related concerns in accordance with Government Auditing Standards Section 7.61, Reporting Confidential and Sensitive Information.

Internal Controls Testing

Our internal controls testing was limited to specific controls relevant to our audit objectives, including the controls to appropriately assess the maturity of the City's sensitive data encryption and data classification process and the sufficiency of the City's CDO's role and authority to enact data governance.

Compliance Statement

We conducted this performance audit in accordance with 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 the audit objective.

THE CITY OF SAN DIEGO

MEMORANDUM

DATE: May 28, 2020

TO: Kyle Elser, Interim City Auditor, Office of the City Auditor

FROM: Elizabeth Maland, City Clerk
Kirby Brady, Director, Performance and Analytics Department
Jonathan Behnke, Chief Information Officer, Department of Information Technology

SUBJECT: Management's Response to the IT Performance Audit of Citywide Data Classification and Sensitive Data Encryption

This memorandum provides background information and management's response regarding the IT Performance Audit of Citywide Data Classification and Sensitive Data Encryption. We would like to thank the Office of the City Auditor for their thorough review and feedback in their recommendations.

RECOMMENDATION #1

The three city data management authorities, comprised of the Chief Data Officer (CDO), Chief Information Officer (CIO), and City Clerk, should work collaboratively to create a Centralized Data Management Strategy based on a Centralized Data Governance Model. All three authorities will sign-off on the policy, and the City Attorney will conduct a legal review to ensure compliance with applicable laws and regulations.

Further, this strategy should incorporate the different roles of the CDO, CIO, and City Clerk to clarify their data management objectives and potential areas of collaboration (Priority 1).

Management Response: Agree with Recommendation.

The Chief Data Officer, Chief Information Officer, and City Clerk will create a Centralized Data Management Strategy based on a Centralized Data Governance Model that incorporates the roles of each department's data management objectives.

Target Date: July 1, 2022

RECOMMENDATION #2

The Chief Data Officer and Chief Information Officer should work with the City Clerk to create a Citywide Data Classification of the various data types that leverages information gathered to create the Department Record File Plans which outlines and classifies records and their retention requirements. This data classification should contain attributes required and usable by all involved parties in addition to incorporating the current classifications. (Priority 1).

Management Response: Agree with Recommendation.

The Chief Data Officer and Chief Information Officer will work with the City Clerk to create a Citywide Data Classification for data types created in the Department Record File Plans. The Citywide Data Classification will classify records and their associated retention requirements and contain attributes required and usable by all involved parties incorporating the roles of each department's data management objectives.

Target Date: July 1, 2023

RECOMMENDATION #3

The Chief Data Officer (CDO) and Chief Information Officer (CIO) should work with the City Clerk to ensure departments coordinate efforts to create a data inventory containing the data/records, its location, owner, classification, and attributes. This effort can leverage the City Clerk's Department Record File Plans to improve the efficiency of the effort.

Each department should define the person and position responsible in their department for data management that may mirror the records management representative to coordinate data management for the department in accordance with the City's data strategy (Priority 1).

Management Response: Agree with Recommendation.

The Chief Data Officer and Chief Information Officer will work with the City Clerk to ensure departments coordinate efforts to create a data inventory containing the data/records, its location, owner, classification, and attributes leveraging the City Clerk's Department Record File Plans.

A departmental data management coordinator will be designated to coordinate data management in accordance with the City's data strategy.

Target Date: July 1, 2021

RECOMMENDATION #4

The Chief Operating Officer should ensure appropriate resources are allocated to the City Clerk, Chief Information Officer, and Chief Data Officer to coordinate and execute the data management strategy based on that governance model (Priority 1).

Management Response: Agree with Recommendation.

Subject to the approved budget, the Chief Operating Officer, Assistant Chief Operating Officer, the City Clerk, Chief Information Officer, and Director of the Performance and Analytics Department will prioritize operational resources to coordinate and execute the data management strategy.

Target Date: July 1, 2021

RECOMMENDATION #5

The City Clerk, Chief Information Officer, and Chief Data Officer should create an Administrative Regulation defining a Citywide Data Governance Model and the roles and responsibility of each of the City's data management entities. (Priority 1).

Management Response: Agree with Recommendation.

The City Clerk, Chief Information Officer, and Chief Data Officer will create an Administrative Regulation defining a Citywide Data Governance Model and the roles and responsibility of each of the City's data management entities.

Target Date: July 1, 2023

Elizabeth Maland City Clerk	Kirby Brady Director Performance and Analytics	Jonathan Behnke Chief Information Officer Department of IT

JB/jl

cc: Kris Michell, Chief Operating Officer
Jeff Sturak, Assistant Chief Operating Officer
Rolando Charvel, Chief Financial Officer
Andrell Bower, Chief Data Officer, Performance and Analytics
Darren Bennett, Chief Information Security Officer, Department of Information Technology