
IT PERFORMANCE AUDIT OF LEGACY APPLICATIONS

**Office of the
City Auditor**

City of San Diego



The City should improve controls to identify, track, and monitor its use of legacy IT systems and to prioritize their replacement.



THE CITY OF SAN DIEGO

December 23, 2020

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

Transmitted herewith is an IT performance audit report of Legacy Systems. This report was conducted in accordance with the City Auditor's Fiscal Year 2021 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 39 of this report. We also issued a confidential report addressing IT related concerns in accordance with Government Auditing Standards Section 9.61, Reporting Confidential and Sensitive Information.

We would like to thank staff from the Department of IT 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 Kyle Elser.

Respectfully submitted,

Andy Hanau
City Auditor

cc: Honorable City Attorney Mara Elliott
Jay Goldstone, Chief Operating Officer
Matthew Vespi, Chief Financial Officer
Jeff Sturak, Deputy Chief Operating Officer
Jonathan Behnke, Chief Information Officer
Matthew Helm, Chief Compliance Officer
Andrea Tevlin, Independent Budget Analyst
Darren Bennett, Chief Information Security Officer
Chris Bennett, Application Sourcing Manager
Ken So, Deputy City Attorney

OFFICE OF THE CITY AUDITOR
600 B STREET, SUITE 1350 • SAN DIEGO, CA 92101
PHONE (619) 533-3165 • FAX (619) 533-3036

TO REPORT FRAUD, WASTE, OR ABUSE, CALL OUR FRAUD HOTLINE (866) 809-3500



Table of Contents

| | |
|--|-----------|
| Results in Brief | 1 |
| Background..... | 4 |
| Audit Results..... | 12 |
| <i>Finding 1: The Department of Information Technology Should Improve How It Tracks and Prioritizes Replacement of True Legacy Systems.....</i> | |
| | <i>12</i> |
| <i>Finding 2: The City Does Not Centrally Track the Full Cost of Their Legacy Information Systems, and Thus Cannot Perform Return on Investment Calculations to Aid in Justifying and Prioritizing Legacy System Replacement</i> | |
| | <i>25</i> |
| Conclusion..... | 33 |
| Recommendations | 34 |
| Appendix A: Definition of Audit Recommendation Priorities | 36 |
| Appendix B: Objectives, Scope, and Methodology..... | 37 |

Results in Brief

IT legacy systems are systems which are outdated, no longer effectively support modern operational needs, and carry increased maintenance costs. Despite these flaws, Legacy systems persist within the IT infrastructure of many organizations, including local, state, and federal government. A 2019 report found that the federal government spends approximately 90 billion dollars per year on information systems, of which 80 percent goes to support legacy systems.

Like the federal government, the City of San Diego (City) has a significant number of older systems that may be legacy; however, we found that the City does not sufficiently define what constitutes a legacy system in order to identify a complete picture of how many actual legacy systems the City has, where these true legacy systems are used, how much the City spends to maintain them, and consequently, how to best determine which systems should be prioritized for replacement.

Finding 1: The Department of Information Technology Should Improve How It Tracks and Prioritizes Replacement of True Legacy Systems

In order to determine the City's inventory of legacy systems, Department of Information Technology (DoIT) must first define what characteristics qualify a system as legacy. DoIT does not currently define true legacy systems, but tracks the applications and supporting architecture versions as their primary legacy metric. DoIT maintains over 250 systems in the City; of those systems, 170 are flagged as out of compliance with DoIT's software version policy, which is currently the closest metric DoIT has to tracking legacy systems. However, while this number is large, it fails to capture the actual number of legacy systems as the software version is only one component of a legacy systems definition. Additionally, many of these 170 applications only require an update to be current and are not truly legacy applications. As a result, the City cannot identify or track its true legacy systems and prioritize their replacement.

While the objective of DoIT is to ensure applications are within one version of the current commercial release version (N-1), this objective relies on the system-owning department to drive the updates and works best where there is a current commercially designed system, known as commercial-off-the-shelf (COTS)

system.¹ In cases where the application was custom designed for the City, DoIT can only ensure the supporting architecture, such as the database meets their standards; however, this does not capture the other potential risk areas of insufficiently supporting operations and the potential for increased costs to maintain the system.

Finding 2: The City Does Not Centrally Track the Full Cost of Its Legacy Information Systems, and Thus Cannot Perform Return on Investment Calculations to Aid in Justifying and Prioritizing Legacy System Replacement

The costs and benefits of replacing legacy systems vary widely from system to system, making comprehensive cost-benefit analysis essential to efficiently managing the City's legacy systems inventory. However, the City does not centrally track the cost of their applications using a method that allows a cost benefit analysis of keeping a legacy system versus replacing it. This information is spread out in multiple locations within each department and within the DoIT. While the City tracks costs of applications between the DoIT, outsourced contracts, and other department sources.

However, this information is not centrally tracked and used to help determine when an information system could be replaced for less than the legacy system is to maintain and prioritize their replacements by cost and risk. As a result, the City may unnecessarily be allocating additional funds to manage outdated systems and not replacing them in the most effective order.

In order to facilitate a cost benefit analysis of the City's legacy systems, we recommend that the City coordinate this effort between DoIT, and system owning departments to collect, analyze, and use this information to prioritize the replacement of legacy systems.

While the City gathers much of this information through various existing processes, they do not document and centralize it in a manner to allow an analysis to determine which systems should be prioritized for replacement based on both operational and technical risks to the City's mission of providing services to the residents of San Diego.

¹ Commercial off-the-shelf (COTS) products are packaged solutions which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.

We made 11 recommendations to improve how the City identifies, tracks, and prioritizes the replacement of legacy systems. The City and DoIT agreed to implement all 11 recommendations, we also issued a confidential report addressing certain IT related concerns in accordance with Government Auditing Standards Section 9.61, Reporting Confidential and Sensitive Information.

Background

Legacy System Definition

Legacy systems persist within the IT infrastructure of many organizations, including local, state, and federal government, despite no longer effectively supporting modern operational needs and increasing maintenance costs.

Most organizations define legacy systems as business-critical systems that demonstrate one or more of the following characteristics: old age, obsolete programming languages, inadequate data management, a degraded structure, limited support capability and capacity, no longer meets business needs, increasing maintenance costs, and lacking the necessary architecture to evolve. Legacy systems also often increase maintenance costs due to specialized needs that are no longer common or must be custom supported.

Federal Legacy System Management

The federal government, like its local government counterparts, has struggled with managing and replacing its legacy systems.

According to a 2019 Department of Energy report, the federal government invests close to \$90 billion on IT annually, with approximately 80 percent of these funds dedicated to maintaining legacy IT that is outdated or obsolete. The Government Accountability Office (GAO) goes on to state that given the magnitude of these investments, it is important that agencies effectively manage the operations and maintenance (O&M) of these systems. According to the Office of Management and Budget (OMB), overall IT investments in these older assets have increased in each year since 2003. During this same period, investments in development, modernization, and enhancements have trended downward, likely resulting from the additional funding required to support the legacy systems. According to the GAO report, federal legacy systems are IT investments that have become increasingly obsolete; many use outdated software languages and hardware parts that are unsupported. Given the magnitude of legacy system IT investments, it is important that agencies effectively manage them.

The San Diego Data Processing Corporation's Replacement and Current Impact on Legacy Systems

Many of the City of San Diego's (City) current legacy systems were designed by the former San Diego Data Processing Corporation (SDDPC) that supported the City's IT operations from 1979 to their replacement, starting with the outsourcing project in 2010. SDDPC was owned by the City, with appointed board members, but acted as a quasi-independent agency which created challenges in its IT service delivery model for the City.

The City began the bid process to replace SDDPC in 2010 that resulted in an award to three different vendors for the work SDDPC had been performing:

- Xerox was awarded the telecommunications component of the ongoing work, and was later acquired by ATOS;
- ATOS was awarded the data center component; and
- CGI was awarded the applications development and maintenance component.

The move away from SDDPC to improve overall management of the City's IT systems also resulted in the loss of some institutional knowledge of the City's systems SDDPC had custom developed, implemented, or managed.

The City then substantially increased the Department of Information Technology (DoIT) staff to manage these three vendors and move to a more centralized IT management model. These awards resulted in the decision to close SDDPC on or about December 31, 2013. However, many of the systems designed to support City operations during this time are still in use today.

**Parties Involved in
Legacy System
Management for City
of San Diego**

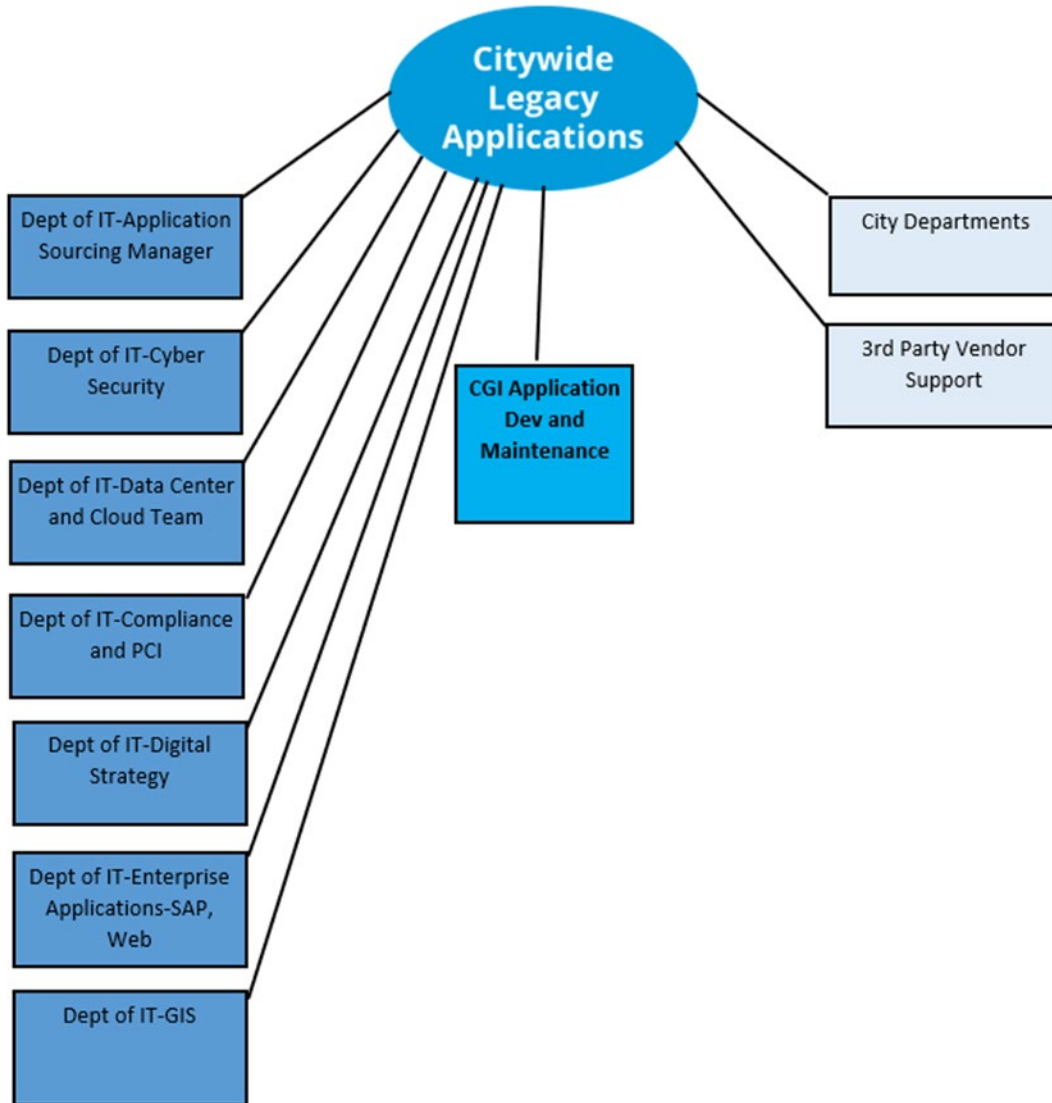
Currently, DoIT manages the vendors that replaced SDDPC and have centralized several IT functions under its purview. Centralized functions that oversee aspects of legacy systems are Cyber Security, Contract Management, Applications Sourcing Management, and others shown in **Exhibit 1**.

DoIT defines legacy applications as the applications that have one or more technologies that are not within one version of the current version (or 'N-1'). The applications are owned by the departments and the modernization of the legacy applications is up to the departments to fund. While DoIT can recommend funding for the modernization of the legacy applications, it cannot order the departments to take this action.

DoIT, CGI, other 3rd party vendors, and all City departments are responsible for Legacy Application Management as shown in **Exhibit 1**. CGI is an IT and business consulting services firm the City uses to provide application management services. However, there is no formal Legacy Application Management Strategy Policy which lists all related parties' responsibilities for Legacy Application Management.

Exhibit 1:

Vendors, DoIT, and City Departments All Have a Role in Legacy Application Management



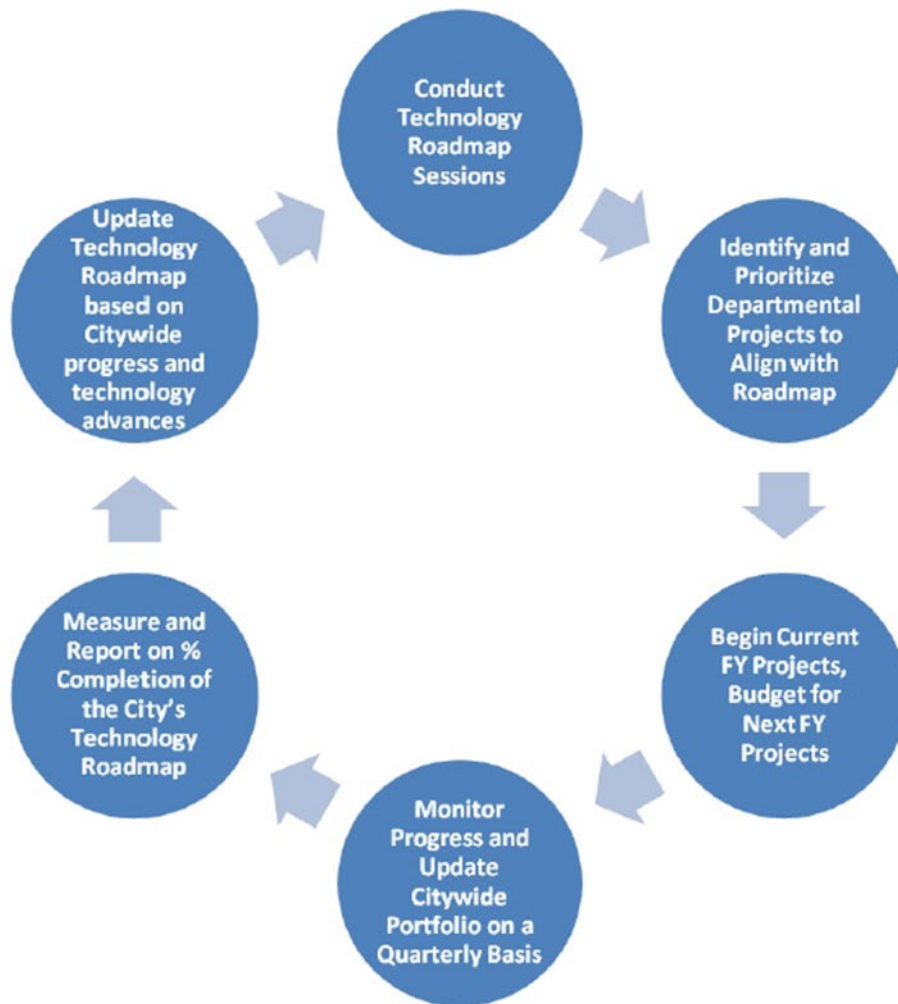
Source: Department of Information Technology.

The City Plans and Tracks the Replacement of IT Systems Through Its Technology Roadmap

DoIT created the roadmap implementation process which includes strategic planning sessions with the operational departments, Department of IT, and technical vendors and begins with conducting the technology roadmap sessions as shown in **Exhibit 2**. The City's technology roadmap is actively managed and measured on a quarterly basis and updated annually to drive the technology project planning and budget projections.

Exhibit 2:

City of San Diego Technology Roadmap



Source: Department of Information Technology.

The application roadmap contains a listing of the City's application portfolio (i.e., a listing of City systems) and is developed with the Application Development and Maintenance Support vendor, DoIT, and City departments. The roadmap contains information about the application, department, technology architecture, risk-based score, technology that is out of support, hosting location, date implemented, developer, and technical activities for the fiscal year.

The centralized process to track City systems is for each application demand (enhancement to current application or request for new application) to be entered into the Application Portfolio. The Application Portfolio is updated at a minimum of once per year after meetings with the departments or during any request for changes or additions to the portfolio. The tool to track and identify legacy systems based on the supporting architecture version is stored in the Application Portfolio. The Application Inventory list is generated from the List that is kept for the Application Portfolio. A generic example is shown in **Exhibit 3** below.

Exhibit 3:

Example Application Portfolio

| AppId | AppName | Architecture | Department | Score | Out of Support Tech | Hosting | Date Implemented | Age* (In Years) | Original Developer | Fy Activities |
|-------|-------------------|--------------|-------------------|-------------|-------------------------|----------|------------------|-----------------|--------------------|--|
| 0001 | Web Payments | Web Based | City Department 1 | Light Green | Scripting language 2 | in-House | 6/7/2012 | 9 | City/DPC | Apply Current Update to Scripting Language |
| 0002 | Desktop Permits | Thin Client | City Department 2 | Yellow | Application Out of Date | in-House | 7/7/2012 | 8 | City/DPC | Not started |
| 0003 | Payment Processor | Thick Client | City Department 3 | Red | Unsupported Database | in-House | 7/7/2012 | 8 | City/DPC | Work with department to update database |

Source: Auditor Generated Example from Department of Information Technology Information.

The third phase of the City's technology roadmap implementation process above begins with the standard System Development Lifecycle (SDLC) for the operational department's current fiscal year (FY). CGI/SDLC process includes Initiate, Analysis, Design, Construction, Testing, Training and Conversion & Cutover processes, as shown in **Exhibit 4** below.

Exhibit 4:

CGI/SDLC Process

| CGI / SDLC Version 3.3 | | | | | | | Legend: <i>Italics</i> - City owned item |
|------------------------|--|---|---|---|--|--|---|
| | Initiate | Analysis | Design | Construction | Testing | Training | Conversion & Cutover |
| Overview Process | <p>Purpose: Provide decision makers with SRCA to help them determine whether or not to proceed with the effort.</p> <p>Decision Point – DoIT and Client have approved funding and are committed to pursuing the Project.</p> | <p>Purpose: Produce project planning documents and review with stakeholders. Perform any analysis to ensure business requirements are complete. Initial project documentation is created.</p> <p>Decision Point – CGI and Client have agreed to initial project schedule.</p> | <p>Purpose: Produce the detailed architecture, design and solution documents for the construction, integration and testing.</p> <p>Decision Point – CGI and City have agreed on the Analysis and Design Document (ADD).</p> | <p>Purpose: Develop system components as outlined in the architectural design documentation and provide verified test results.</p> <p>Decision Point – CGI agrees that construction is complete and unit testing is successful.</p> | <p>Purpose: Verify solution meets client requirements. Demonstrate that the solution meets all client acceptance criteria.</p> <p>Decision Point – Client signs off on UAT.</p> | <p>Purpose: Ensure the client understands the new functionality or enhancement.</p> <p>Decision Point – Client approves training complete.</p> | <p>Purpose: Make the solution available to the client and ensure they can assume ownership.</p> <p>Decision Point – Client approves project closure.</p> |
| | | Demand Approval | Planning Gate Approval | Design Review Approval | Internal Quality Approval | Client Quality Approval | Final Client Acceptance |
| Outputs | <ul style="list-style-type: none"> SRCA Quote | <ul style="list-style-type: none"> <i>Purchase Order</i> Project Information: <ul style="list-style-type: none"> Overview Schedule Comm. Plan Risk Register RACI Atos requests | <ul style="list-style-type: none"> Architectural Design Documentation Architecture & Design Reviews performed Baselined Schedule | <ul style="list-style-type: none"> Test Plan IST Scripts <i>UAT Scripts</i> IST Test Results Issues Tracker Training Plan – if required | <ul style="list-style-type: none"> <i>UAT Test Results</i> UAT Issue Tracker For PCI related projects: Vulnerability Assessment including a ASV Scan | <ul style="list-style-type: none"> Training Materials – if included in scope Go/No-go meeting with Client | <ul style="list-style-type: none"> Tech Review Form Cutover Plan CGI Wiki Completion Service Desk Wiki <i>Client Requirements Survey</i> Client PIR Training Feedback Survey – If required |
| Action Items | <ul style="list-style-type: none"> <i>Project summary, scope, and budget</i> <i>Identify Stakeholders</i> <i>Identify business requirements</i> Provide SRCA Provide quote if necessary | <ul style="list-style-type: none"> Confirm Stakeholders Resource Allocation DoIT Planning Gate review meeting | <ul style="list-style-type: none"> Deliver ADD and LOE Finalize budget Attend CGI architecture review Attend City Design review, if necessary Request Project Plan Approval in ServiceNow | <ul style="list-style-type: none"> Perform work identified to achieve requirements in ADD Develop test scripts Execute Unit testing Execute IST test scripts Conduct code reviews | <ul style="list-style-type: none"> Perform UAT kickoff Conduct UAT Training – If required <i>Execute UAT test scripts</i> Request UAT approval in SNOW once UAT complete | <ul style="list-style-type: none"> Deliver training material or conduct training as outlined in scope Submit change record for ECM | <ul style="list-style-type: none"> 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.

**Organizations
Providing Guidance for
Data Governance and
Security**

COBIT 5 is the overarching business and management framework for governance and management of enterprise IT. It was created by ISACA, an independent, nonprofit, global association, engaged in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. COBIT 5 provides guidance for classifying data inputs and outputs according to enterprise architecture standards.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Audit Results

Finding 1: The Department of Information Technology Should Improve How It Tracks and Prioritizes Replacement of True Legacy Systems.

Finding Summary

In order to determine the City's inventory of legacy systems, the Department of Information Technology (DoIT) must first define what characteristics qualify a system as legacy. DoIT does not currently define true legacy systems, but tracks the applications and supporting architecture versions as their primary legacy metric. DoIT maintains over 250 systems in the City; of those systems, 170 are flagged as out of compliance with DoIT's software version policy, which is currently the closest metric DoIT has to tracking legacy systems. However, while this number is large, it fails to capture the actual number of legacy systems as the software version is only one component of a legacy systems definition. Additionally, many of these 170 applications only require an update to be current and are not truly legacy applications. As a result, the City cannot identify or track its true legacy systems and prioritize their replacement.

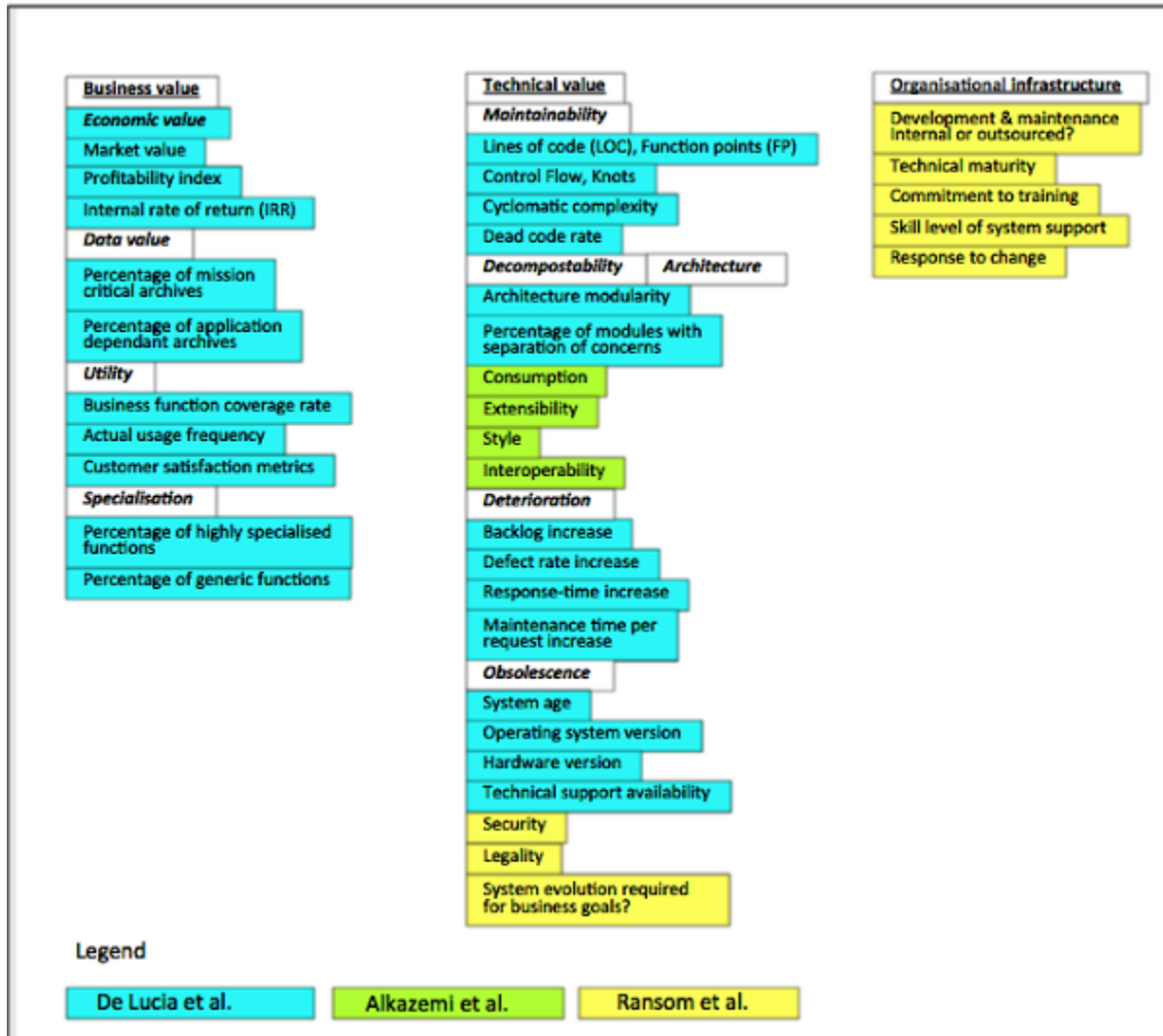
While the objective of DoIT is to ensure applications are within one version of the current commercial release version (N-1), this objective relies on the system-owning department to drive the updates and works best where there is a current commercially designed system, known as commercial-off-the-shelf (COTS) system.² In the case where the application was custom designed for the City, DoIT can only ensure the supporting architecture, such as the database meets their standards; however, this does not capture the other potential risk areas of insufficiently supporting operations and the potential for increased costs to maintain the system.

² Commercial off-the-shelf (COTS) products are packaged solutions which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.

DoIT's focus on technical architecture allows it to focus on the areas it better controls through contracts with the vendor, while it ultimately must rely on the City departments that own the systems to inform it that they would like to replace their applications, allocate funds, and ultimately drive the replacement process. However, the individual department often requires additional technical information to create the business case likely resulting in taking longer to prioritize the replacement of these systems. The missing component is a comprehensive risk assessment of these systems that captures the business and technical arguments for prioritizing the replacement of these legacy systems. **Exhibit 5** provides an example legacy systems assessment model that incorporates business, technical, and organizational components that should be incorporated into this risk assessment.

Exhibit 5

Legacy System Assessment Model



Source: PNR, A Model to Identify Solutions to Legacy Systems Increasing Maintenance Costs.

According to the Chief Information Officer (CIO), the annual review with departments includes documentation and discussions about both the business and technical risk considerations for systems that are identified in the application inventory as needing updates, which is currently the best list to identify legacy systems the City has. However, these are not specifically included in a formal annual legacy system report to help drive the prioritization of system replacement in the City. Additionally, systems that may be identified as legacy by business functionality, but with current architecture would not be identified in the current process.

Standards require that organizations sufficiently define their legacy systems based on criteria that captures the technical risks, as well as operational risks to these systems and perform risk assessments on these criteria to prioritize their replacement.

Systems that are maintained significantly beyond their useful life can negatively impact the operations they support, providing insufficient features expected of modern systems, increasing costs through specialized support needs and contracts. The security-related findings for legacy systems are addressed in a confidential memorandum.

We recommend that DoIT work with City departments to adopt a fully inclusive definition of legacy systems that captures the critical aspects of legacy applications, even those under the system-owning departments control. Additionally, DoIT should work with the departments to prioritize the replacement of systems based on the risks presented by these systems.

DoIT Tracks the Technical Supportability of an Application and Its Supporting Infrastructure, But Does Not Track Other Critical Legacy Indicators That Are Essential to Create A Business Case for a Prioritized Replacement

The Department of Information Technology (DoIT) tracks and maintains an application portfolio through their application support vendor. This portfolio tracks important information about the systems, such as their general business uses, the supportability of their components, and components that no longer meet DoIT's policy of maintaining applications that are within one version of the current release.

However, this application portfolio is missing critical information of the applications, such as a legacy system indicator, an accurate system age and expected lifespan, and other critical information to assess the viability and operational risks to the City's operations.

Additionally, this application portfolio does not include all the applications used throughout the City, including many owned or managed by other departments resulting in additional unknown legacy systems. Some City departments do not have a full inventory of their information systems, which presents further challenges for DoIT to maintain a comprehensive list.

DoIT's Legacy System Definition Limits Its Ability to Identify Legacy Systems Citywide

One of the primary limitations to tracking all legacy systems in the City is DoIT's definition of legacy systems. Specifically, DoIT defines legacy systems as those that have one or more components that are not within one version of the current version (N-1) of the application or its supporting architecture. While DoIT has developed and documented a standard definition for a legacy system this definition only focuses on the obsolescence of the technical architecture of the application and does not address other critical factors such as the age and expected lifespan of the application or how well it supports the system-owning department's operations. This definition especially falls short with homegrown applications that lack standardized version release information to gauge the obsolescence of the application.

Legacy definitions should address business and mission critical systems that exhibit old age, obsolete language design, inadequate data management, a degraded structure, limited support capability or capacity, inability to meet business needs, increased maintenance costs, and insufficient architecture to evolve. The definition helps an organization to identify systems

that do not meet these standards and ultimately to help ensure applications are maintainable, secure, and fully support business operations.

Additionally, the appropriate definition of legacy system addresses business, technical, architectural and organizational factors that can impact legacy systems assessment. This definition would allow DoIT to manage all factors, and help departments identify where they require additional functionality or service. It is important to remember that the assessment of legacy systems and the subsequent decisions of what needs to be done must be taken and supported by a broad range of stakeholders within City departments and DoIT. It is also essential to consider organizational factors such as resistance to change and internal capabilities before implementing the solutions.

The current process focuses on DoIT's IT roadmap, as shown in **Exhibit 2** on page 8, to determine how to ensure all the applications and supporting infrastructure are current and more easily managed. However, it only addresses the obsolescence attribute of the technical attributes but does not address the business, architectural, organizational and other technical attributes.

As a result, DoIT has not developed and documented a standard definition for a legacy system. When the auditor discussed the term legacy system with other departments, individuals had their own interpretation of what the term meant. Other agencies have experienced similar challenges. In an audit conducted by the Office of the Inspector General, they found points of contact for two different systems that reside on the same platform had different views as to whether their systems were legacy. One considered the system to be in its infancy even though it has been around for over eight years. The other individual considered their system as legacy due to how old the system was, and the technology used. Without a standard definition of a legacy system, it may be difficult for the individuals to come to the same conclusion that these systems are legacy and need replacing. Additionally, different systems have different useful life expectancies, which must be accounted for in the legacy definition.

Many Older Applications Have Unknown or Inaccurate System Ages Due to the Transition from SDDPC to a Contracted Services Model

As tracking a systems age and expected lifespan has not been critical to DoIT's legacy methodology, DoIT has not developed a comprehensive process to track these metrics to help determine when a system is past its useful life. For 170 of 267 systems that DoIT manages, they could only estimate the age of the system but could not confirm the exact age, or determine how long those systems should remain in production. Additionally, we noted that the age of the systems was not documented correctly in DoIT's application list, with many defaulting to a creation date of 2012, when CGI took over application support for the City from the now defunct San Diego Data Processing Corporation (SDDPC).³

Further complicating this process, many of these applications were custom designed many years earlier by SDDPC through direct requests from departments without DoIT's direct involvement. As a result, these home-grown systems pose unknown risks to the City's IT environment and likely do not support standard functionality expected today to support operations.

As this process has been outside of their scope of control, DoIT does not track and document the life expectancy of these legacy systems.⁴ DoIT informed us that they assess the realistic lifespan and ability to support legacy systems in developing the IT roadmap, but do not document this information outside the inferred supportability and lifespan tracked by the software version information.

³ CGI Inc., more commonly known as CGI, is a Canadian global information technology (IT) consulting, systems integration, outsourcing, and solutions company headquartered in Montreal, Quebec, Canada. Services provided to the City by CGI are application development and maintenance. San Diego Data Processing Corporation (SDDPC) was created by the City of San Diego in 1979 to manage all aspects of data infrastructure including voice and data communications, programs and processes, and coordination of activities that impacted the applications that the various City departments used.

⁴ According to the CIO, systems in the app inventory are tracked to prioritize updates and maintain current versions and future life expectancy based on the commercial version released; however, this may not capture or address legacy issues within the large number of homegrown systems at the City.

**Some Legacy Systems
Are Not Tracked in
DoIT's Application
Portfolio**

DoIT manages its application portfolio based on the systems that CGI, the external vendor, supports as well as the procurement process, and reporting by departments. However, some systems in the past have slipped through this methodology and are not included in the IT portfolio. As a result, there are legacy systems that are not included on DoIT's list.

During a limited review, the auditors discovered 34 systems that were not on the IT portfolio list, which included 15 legacy systems, due to City departments not reporting the data to DoIT or reporting incomplete and potentially erroneous data to DoIT.

**The STAC Committee
Approves the Legacy
Systems for
Replacement in its
Annual Meeting**

The Strategic Technology Advisory Committee (STAC) was formed as an evolution of the City's IT Business Leadership Group and governance process. The mission of STAC is to provide business value with each approved City technology initiative, and provide transparency and citywide prioritization of technology requests, including legacy system replacements and mitigation, in the City's annual budget process. The STAC is comprised of all the City's mayoral department directors and invite non-mayoral departments to the full committee and breaks into subcommittees to conduct various IT tasks.

**Legacy Systems
Reviewed During the
Annual STAC Meeting
are Based on the N-1
Model**

The STAC reviews the N-1 defined list of systems and architecture requiring updates annually as part of the IT budgeting process meeting to plan for the funding of upgrades or system replacements.

However, assessing the risk by version number does not account for system effectiveness, cost/benefit analysis, or the vulnerabilities or legacy design weaknesses specific to the application itself, only the version information of the application and its supporting architecture.

These factors are normally seen as belonging to the department to manage; however, these components require both department and IT knowledge to analyze and lend itself to discussion at the STAC meeting to aid in the prioritization of system replacement. Additionally, a comprehensive formal legacy risk assessment report is not currently part of the process and cannot be taking into account for the STAC meeting.

Previous STAC agendas reviewed by the auditor focused on educating the committee on the IT roadmap for updating and implementing IT systems for the fiscal year and into the next. However, STAC could also be used to discuss the risks presented by the current application portfolio based on a legacy application risk assessment, and help to identify systems to prioritize replacements based on these risks and to ultimately prioritize systems for replacement in the IT roadmap. Currently, STAC subcommittees review all IT funding requests submitted by departments, and address risk factors at that stage; while this helps take into account application risks when a department is looking to update their applications, it does not ensure that the applications that pose the highest citywide risk are prioritized for replacement.

Standards Require Legacy Systems are Adequately Defined, Identified, and Managed Due to the Risks They Present

According to the GAO's Green Book, "Management should design the entity's information system and related control activities to achieve objectives and respond to risks."⁵

Legacy definitions should address business and mission critical systems that exhibit old age, obsolete language design, inadequate data management, a degraded structure, limited support capability or capacity, unable to meet business needs, increased maintenance costs, and insufficient architecture to evolve. The definition helps an organization to identify systems that do not meet these standards and ultimately to help ensure applications are maintainable, secure, and fully support business operations.

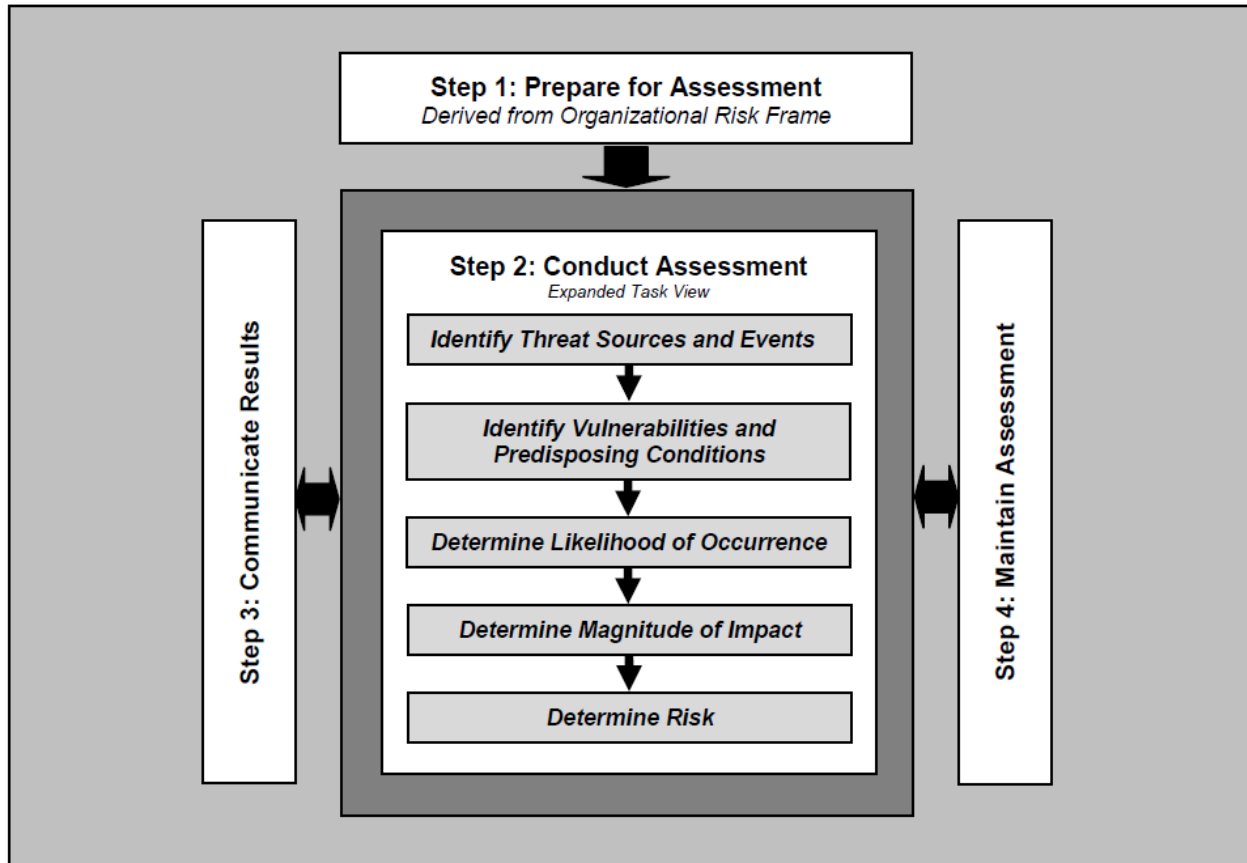
Establishing the definition of a legacy system should be based on an assessment of the risks these systems pose to the City. According to NIST 800-30 Revision 1 risk assessment is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other

⁵ Standards for Internal Control in the Federal Government, known as the "Green Book," sets the standards for an effective internal control system for federal agencies <<https://www.gao.gov/greenbook/overview>>.

organizations such as the City of San Diego, resulting from the operation of an information system as shown in **Exhibit 6**.⁶

Exhibit 6

Risk Assessment Process



Source: NIST Guide for Conducting Risk Assessments

⁶ The National Institute of Standards and Technology (NIST) announces the release of the final version of its updated risk assessment guideline, Special Publication 800-30, Revision 1. <<https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>>. The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations. This document provides guidance for carrying out each of the three steps in the risk assessment process (i.e., prepare for the assessment, conduct the assessment, and maintain the assessment) and how risk assessments and other organizational risk management processes complement and inform each other.

The City Has Traditionally Relied on DoIT to Manage Upgrades to the IT Architecture while the Department Manages Upgrades for the Applications It Owns

The City has traditionally relied on DoIT to manage upgrades to the IT architecture while the department manages upgrades for the applications they own. As a result, DoIT's focus on technical architecture allows it to focus on the areas it better controls through contracts with the vendor, while it ultimately must rely on the City departments who own the systems to inform it that they would like to replace their applications, allocate funds, and drive the replacement process; however, the individual departments may require additional technical information to justify these processes potentially resulting in taking longer to prioritize the replacement of these systems. The missing component is a comprehensive risk assessment of these systems that captures the business and technical arguments for replacing these legacy systems.

Other City departments do not rely on DoIT to do the upgrades and maintenance for all of the applications. Not every City department has maintained the application list for the department. Some of them are not aware of how many systems in the department. Some applications are on not on DoIT's application inventory list and they are not aware of any upgrades or maintenance cost. Additionally, other departments do not know the true cost of all systems, they do not know how legacy systems are identified, tracked and monitored (use and maintenance), and they do not work with DoIT to manage all systems.

DoIT also lacks information about some older custom-designed applications ordered by departments prior to 2012, when departments used to work directly with the San Diego Data Processing Corporation (SDDPC) without the inclusion of DoIT. DoIT learned about many systems after they were procured when they then were requested to support them.

When the City moved its application support to CGI from SDDPC, CGI began tracking the City's applications based on the ones they were asked to support and procured after that date when DoIT was included in the procurement process.

DoIT should be aware of applications procured after they were included in the procurement process in 2010 for IT applications; and of the applications maintained by CGI. However, DoIT does not have information on unreported departmental legacy applications prior to these periods, nor does it track information about the systems that don't focus on its limited definition of legacy systems. DoIT manages the replacement of legacy systems through the STAC process and the IT roadmap documenting the replacement plan for budgeted replacement of systems. However, the STAC meeting does not address legacy systems based on their meeting agenda and presentation.

The IT roadmap focuses on systems budgeted for replacement and to determine how to ensure all the applications and supporting infrastructure are current and reduce the City's risks from an IT architecture perspective, but it does not address the reason why customer departments own and maintain the applications and how effectively the legacy systems meet those requirements.

For the City to implement adequate and effective internal and management controls to track and monitor its legacy systems, we recommend the following:

Recommendation #1: The Department of Information Technology (DoIT) should develop and document a standard definition for a legacy system that incorporates the critical factors necessary to identify systems that no longer efficiently and effectively meet operational needs of the department (Priority 2).

Recommendation #2: In coordination with other City departments, The Department of Information Technology (DoIT) should create a policy and procedure to document when each legacy system was put into production where possible, and document the current life expectancy of each system. Further, DoIT should track and update the life expectancies as systems are updated and work with the department to prioritize their replacement as the systems near the end of their life expectancy (Priority 2).

- Recommendation #3:** The Department of Information Technology (DoIT) should create a centralized process to track legacy systems, listing their detailed deficiencies, and update this information on an annual basis for discussion with the department during the annual Strategic Technology Advisory Committee meeting (Priority 2).
- Recommendation #4:** The Chief Information Officer should create and impliment a policy and procedures that ensure risk assessments and risk assessment reports are completed and/or reviewed annually and updated according for all legacy systems (Priority 2).
- Recommendation #5:** The Chief Information Officer should include the results of the risks assessment for legacy systems as a significant discussion item on the agenda in the annual Strategic Technology Advisory Committee meeting with mayoral department directors to help determine which systems should be prioritized for replacement among departments (Priority 2).

Finding 2: The City Does Not Centrally Track the Full Cost of Their Legacy Information Systems, and Thus Cannot Perform Return on Investment Calculations to Aid in Justifying and Prioritizing Legacy System Replacement

Finding Summary

The costs and benefits of replacing legacy systems vary widely from system to system, making comprehensive cost-benefit analysis essential to efficiently managing the City of San Diego's (City) legacy systems inventory. However, the City does not centrally track the cost of their applications using a method that allows a cost benefit analysis of keeping a legacy system verses replacing it. This information is spread out in multiple locations within each department and within the Department of Information Technology (DoIT). While the City tracks costs of applications between the DoIT, outsourced contracts, and other department sources.

However, this information is not centrally tracked and used to help determine when an information system could be replaced for less than the legacy system is to maintain and prioritize their replacements by cost and risk. As a result, the City may unnecessarily be allocating additional funds to manage outdated systems and not replacing them in the most effective order.

In order to facilitate a cost benefit analysis of the City's legacy systems, we recommend that the City coordinate this effort between DoIT, and system owning departments to collect, analyze, and use this information to prioritize the replacement of legacy systems.

The City Does Not Centrally Track the Actual Cost of Legacy Systems

DoIT tracks the overall spending of an application based on the allocation estimate on an annual basis for the applications they manage through the vendors. This excludes applications managed by the other City departments. However, DoIT does not know the exact actual cost to maintain each individual application because most application are lumped together in one contract and the blended hourly rate is used. One application could be taking up the majority of the contractor's time and needs higher hourly pay for the labor thus cost more to maintain, which is a critical factor in building a business case to replace the application.

Additionally, DoIT indicated they do not track who maintains or provides oversight for some of these legacy systems.

DoIT does not know how much the contract cost for the systems managed by the other City departments. The cost of a capital asset is its full life-cycle cost (see section below), including all direct and indirect costs for planning, procurement (purchasing price and all other costs incurred to bring it to a form and location suitable for its intended use), operation and maintenance (including service contracts), and disposal. However, this information is tracked in various locations, some by DoIT and some by the departments, such as cost of licenses and maintenance, etc. Specific departments can spend their own discretionary funds to upgrade/enhance their existing applications, so those funds do not come out of DoIT's budget and are thus not tracked by it. As a result, the City may be maintaining legacy systems that could be replaced with cost savings and more modern business capabilities.

The City Cannot Evaluate the Cost and Benefits of IT Investments and Perform Operational Analysis Due to Insufficient Tracking of Application Costs

Traditionally, City departments have managed non-IT vendor portions of the IT cost, while DoIT manages the allocated City IT vendor costs of IT. As a result, DoIT polices do not require the cost and benefits of each alternative and operational analysis to be documented and reviewed.

While departments may provide some of this information in a narrative section of their IT budget request to update systems it is not documented as a standard or for systems departments are not currently requesting updates for. As a result, the Strategic Technology Advisory Committee (STAC) may not have

all of the necessary information to determine the investment alternative that is in the best interest of the City.

The City also runs the risk of managing large dollar acquisitions that may result in cost and schedule overruns, that fall short of meeting a user's needs. Until the City updates the STAC process, they run the risk of continuing to maintain systems that are past their effectiveness and are consuming more resources than the benefits they may provide.

Standards Require Organizations Document the Actual Cost to Operate and Maintain Each System and Track the Costs and Benefits of Each Alternative

According to the OMB A-11 (Office of Management and Budget Circular A-11) Capital Programming Guide, the cost of a capital asset is its full life-cycle cost, including all direct and indirect costs for planning, procurement (purchasing price and all other costs incurred to bring it to a form and location suitable for its intended use), operation and maintenance (including service contracts), and disposal.⁷

The OMB and government code further define the responsibilities of a chief information officer (CIO) to include monitoring the performance of information technology programs within their organization, including evaluating the performance of those programs on the basis of the applicable performance measurements, and advising the head of the City regarding where to continue, modify, or terminate a program or project.

In order to assess these systems, the CIO must create criteria that defines the return on investment for applications and systems. This calculation should take into account total cost to manage, maintain, or replace the system in addition to weighing risks posed by keeping outdated systems in the organization and costs associated with managing these additional risks.

⁷ OMB Circular A-11 ("Preparation, Submission, and Execution of the Budget") is a United States government circular that addresses budget preparation for federal agencies and is "the primary document that instructs agencies how to prepare and submit budget requests for OMB review and approval".

**The City May
Unnecessarily Be
Allocating Additional
Funds to Manage
Outdated Systems**

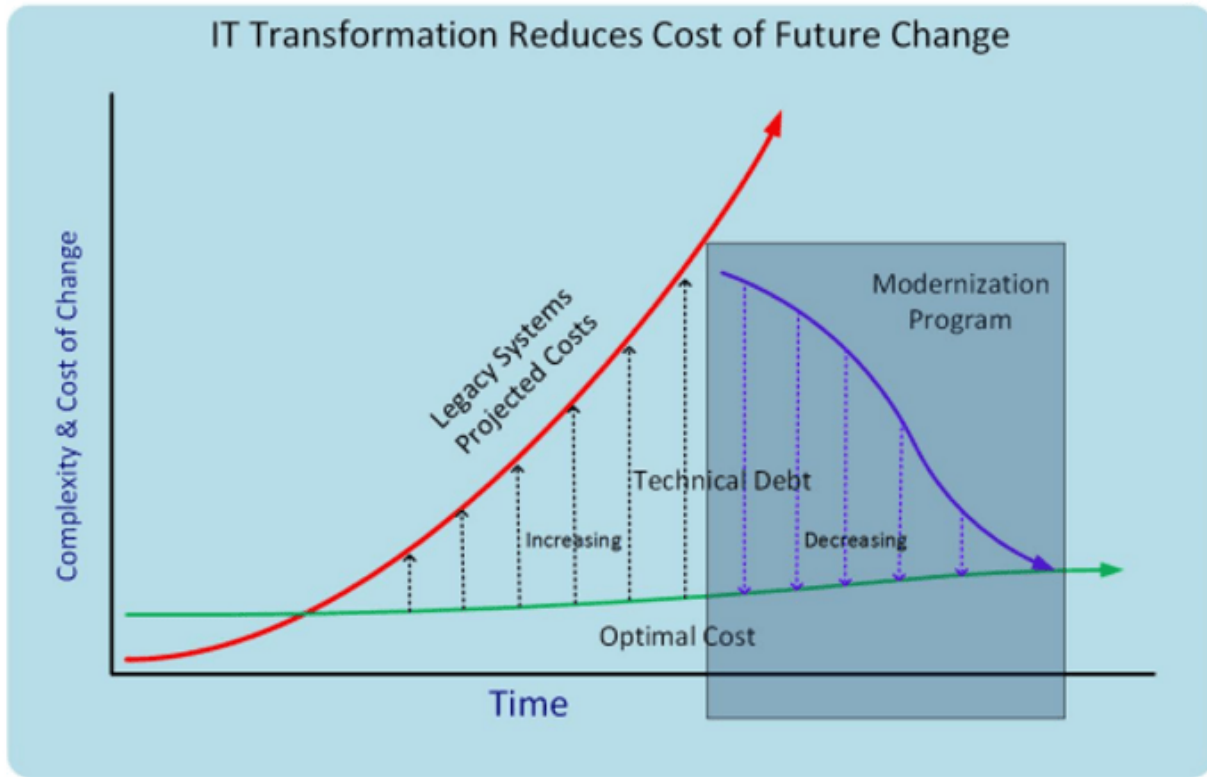
Not tracking costs increases the risk that the City is continuing to use and maintain systems that could be replaced with cheaper systems. By tracking costs and performing cost-benefit analysis, organizations can identify cost savings that could be realized through system replacements.

Further, without insight into systems managed by business departments, IT may be constrained in their ability to monitor and evaluate the performance of the legacy systems, and advice regarding whether to continue, modify, or terminate a program or project.

To illustrate this, the Social Security Administration's (SSA) IT Modernization Plan describes the framework to return the agency to one having a healthy IT foundation. In this example, the costs of change are significant, but show positive cost benefits relatively quickly as shown in **Exhibit 7**. This is because most of the SSA's core systems are over 30 years old, so their return on investment is high due to their high technical deficit and the cost increases the agency would incur by continuing to rely on legacy systems. By calculating the costs of legacy systems and performing a cost-benefit analysis, the agency was able to identify the cost savings it could realize by modernizing and replacing its legacy IT.

Exhibit 7

SSA's IT Modernization Framework



Source: Social Security IT Modernization Plan Framework

Contrary to the SSA's incremental work over the last 30 to 40 years, the IT Modernization Plan is a plan to replace SSA's core systems with new components and platforms, engineered for maximum usability, innate interoperability, and future adaptability.

A Cost / Benefit Analysis is Essential to Prioritizing the Replacement of Legacy Systems to Ensure the City is not Spending More Resources on Legacy Systems than the Cost of Their Replacement

The SSA is currently working to correct a long history of kicking the can down the road. While the City is not in as significant a technology deficit, the City does not currently have policies that require departments to perform a cost/benefit analysis for legacy systems that incorporate the cost of the legacy application to the cost of its replacement. While these activities may occur on an ad-hoc basis, they do not occur regularly to help identify and determine when a system should be replaced. As a result, the STAC may not have all of the necessary information to determine the investment alternative that is in the best interest of the City. Until the City updates the STAC process, they run the risk of continuing to maintain systems that are past their effectiveness and are consuming more resources than the benefits they may provide.

At the federal level, legacy systems significantly increase costs of maintaining legacy systems, which carries over to the local level as well as on a smaller scale.

The U.S. government planned to spend close to \$90 billion annually on information technology. Most of that will be used to operate and maintain existing systems, including aging (also called legacy) systems. These systems can be costlier to maintain.

Additionally, the National Archives and Records Administration (NARA) continues to spend unappropriated funds to operate and maintain legacy systems whose functionality should be subsumed by the original Electronic Records Archives (ERA). As a result, NARA has already spent approximately \$33 million to operate and maintain these systems as of 2019. Until NARA integrates the functionality for these systems into ERA 2.0 or other systems, NARA will continue to accrue approximately \$5 million per year on operation and maintenance of legacy systems that could be put to better use.

The City Has Not Traditionally Centralized the Management of Legacy Systems, Including the Responsibility of Conducting a Cost/Benefit Analysis

The City has not evaluated the replacement of their legacy information systems using a cost/benefit analysis primarily due to the varying roles of the departments managing the costs directly related to the applications they own, and the responsibility of DoIT to manage the supporting infrastructure and support the applications as needed from a technical perspective. As a result, there has not been a directive to track the true cost of managing applications and centralize this information for analysis, or utilize this information to help evaluate the replacement of systems.

As this information has not been a requirement, DoIT does not track the exact actual cost to maintain each individual application because most application are lumped together in one contract and the blended hourly rate is used. Further, departments that own more management of information technology, such as enterprise departments, do not track all of their applications and provide that information to DoIT resulting in unknown legacy applications to evaluate.

To ensure that the City spend appropriate fund to operate and maintain legacy systems, we recommend the following:

Recommendation #6:

The Chief Operating Officer should work with the Department of Information Technology (DoIT) and City departments to create a policy and procedure for centrally tracking all actual IT costs associated with legacy applications to facilitate replacement prioritization based on cost. DoIT should ensure that this information is updated annually (Priority 2).

Recommendation #7:

The Chief Operating Officer should ensure coordination between all City departments and the Department of Information Technology (DoIT) to develop, document, and implement a policy to require all City departments to annually report all information systems under their perview to DoIT as well as the total operation and maintenance costs managed outside of DoIT for each system (Priority 2).

Recommendation #8: The Department of Information Technology should develop a metric for identifying high cost legacy systems and work with departments to prioritize and phase out these systems (Priority 2).

Recommendation #9: The Chief Operating Officer should work with the Chief Information Officer to develop a policy and corresponding procedures to require that each legacy application has a current calculation weighing the costs and benefits of each alternative and is documented for, and reviewed during the annual Strategic Technology Advisory Committee process (Priority 2).

Recommendation #10: The Chief Information Officer should develop and implement an operational analysis policy, and coordinate with each City department to conduct and document an operational analysis for IT investments currently in production in accordance with this policy (Priority 2).

Recommendation #11: The Chief Operating Officer, working with the Chief Information Officer, should provide a confidential report annually to the City Council containing high risk legacy applications that should be prioritized for replacement. This report should include the risks impacting information technology operations, business operations, return on investment calculation available, and security considerations in appropriate detail for the City Council to make a decision whether to prioritize funding for application replacement (Priority 2).

Conclusion

Legacy systems are prevalent in numerous organizations, including the City of San Diego. Often, these systems can negatively impact the operations and return on investment we receive from these systems. It is important to identify legacy systems leveraging a robust definition, and evaluate which ones should be prioritized for replacement to provide the strongest return on investment for the City and the services we provide using these systems to the public.

The City currently tracks a limited scope of legacy system attributes that may prevent it from assessing these systems and properly prioritizing their replacement. Additionally, the City does not centrally track the total cost of these systems, further impacting its ability to determine which systems present the strongest return through replacement.

We made eleven recommendations to identify, monitor, assess, and prioritize the replacement of the City's legacy systems based on a risk assessment that includes critical criteria to make these decisions. Management agreed with all eleven of our recommendations.

We also issued a confidential report addressing IT-related concerns in accordance with Government Auditing Standards Section 9.61, Reporting Confidential and Sensitive Information. Management agreed to implement the recommendations from the confidential report.

Recommendations

Recommendation #1: The Department of Information Technology (DoIT) should develop and document a standard definition for a legacy system that incorporates the critical factors necessary to identify systems that no longer efficiently and effectively meet operational needs of the department (Priority 2).

Recommendation #2: In coordination with other City departments, the Department of Information Technology (DoIT) should create a policy and procedure to document when each legacy system was put into production where possible, and document the current life expectancy of each system. Further, DoIT should track and update the life expectancies as systems are updated and work with the department to prioritize their replacement as the systems near the end of their life expectancy (Priority 2).

Recommendation #3: The Department of Information Technology (DoIT) should create a centralized process to track legacy systems, listing their detailed deficiencies, and update this information on an annual basis for discussion with the department during the annual Strategic Technology Advisory Committee meeting (Priority 2).

Recommendation #4: The Chief Information Officer should create and implement a policy and procedures that ensure risk assessments and risk assessment reports are completed and/or reviewed annually and updated according for all legacy systems (Priority 2).

Recommendation #5: The Chief Information Officer should include the results of the risks assessment for legacy systems as a significant discussion item on the agenda in the annual Strategic Technology Advisory Committee meeting with mayoral department directors to help determine which systems should be prioritized for replacement among departments (Priority 2).

Recommendation #6: The Chief Operating Officer should work with the Department of Information Technology (DoIT) and City departments to create a policy and procedure for centrally tracking all actual IT costs associated with legacy applications to facilitate replacement

prioritization based on cost. DoIT should ensure that this information is updated annually (Priority 2).

Recommendation #7:

The Chief Operating Officer should ensure coordination between all City departments and the Department of Information Technology (DoIT) to develop, document, and implement a policy to require all City departments to annually report all information systems under their purview to DoIT as well as the total operation and maintenance costs managed outside of DoIT for each system (Priority 2).

Recommendation #8:

The Department of Information Technology should develop a metric for identifying high cost legacy systems and work with departments to prioritize and phase out these systems (Priority 2).

Recommendation #9:

The Chief Operating Officer should work with the Chief Information Officer to develop a policy and corresponding procedures to require that each legacy application has a current calculation weighing the costs and benefits of each alternative and is documented for, and reviewed during the annual Strategic Technology Advisory Committee process (Priority 2).

Recommendation #10:

The Chief Information Officer should develop and implement an operational analysis policy, and coordinate with each City department to conduct and document an operational analysis for IT investments currently in production in accordance with this policy (Priority 2).

Recommendation #11:

The Chief Operating Officer, working with the Chief Information Officer, should provide a confidential report annually to the City Council containing high risk legacy applications that should be prioritized for replacement. This report should include the risks impacting information technology operations, business operations, return on investment calculation available, and security considerations in appropriate detail for the City Council to make a decision whether to prioritize funding for application replacement (Priority 2).

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

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 2020 Audit Work Plan, we have initiated the IT Performance Audit of Legacy Applications. As stated in the Work Plan, the overall objective of the audit is to assess the impact of the legacy applications to the City’s IT security posture and assess additional impacts.

As a result of our preliminary research and initial program assessment, we have defined our audit scope to include the three objectives listed below:

- Objective 1: Assess the controls in place to identify, track, and monitor its use and maintenance of legacy IT systems.
- Objective 2: Assess funds to operate and maintain legacy systems and the legacy system evaluation processes.
- Objective 3: Review the effectiveness of the risk assessment process for legacy systems.

Scope and Methodology **Controls to Identify, Track, and Monitor Legacy Systems**

To assess the controls in place to identify, track, and monitor its use and maintenance of legacy IT systems we first assessed the definition used by the City to identify legacy system by reviewing policies, procedures, and working with IT Department staff to clarify the definition, use, and process to identify legacy systems. We further reviewed the process the City uses to track critical system legacy criteria, such as the age and corresponding expected lifespan, how centralized the process is to track this information, and assessed the internal controls over monitoring these systems through reviewing available centrally tracked information, relevant policies and procedures, and conducting inquiries with IT and City department staff.

Controls over Tracking Funds to Operate and Maintain Legacy Systems

To assess the controls over tracking funds to operate and maintain legacy systems and the legacy system evaluation processes we first reviewed relevant policies, processes, and procedures over tracking the total cost of ownership for legacy systems. We then reviewed the process, policies, and procedures for monitoring and evaluating the cost performance of legacy systems, their cost and benefit analysis, and operational analysis and conducted inquiries with IT and City department staff to clarify our understanding of these processes and assessed the controls over tracking funds to operate and maintain legacy system.

Effectiveness of the Legacy Systems Risk Assessment Process

To review the effectiveness of the risk assessment process for legacy systems we reviewed all relevant policies, procedures, process documents, and requested current risk assessments for the City's application portfolio. We reviewed these documents and met or corresponded with department staff to clarify our understanding of the City's current processes and compared those to NIST's risk assessment standards.

We also issued a confidential report addressing IT related concerns in accordance with Government Auditing Standards Section 9.61, 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 controls over identifying, tracking, and monitoring legacy systems, their risk assessment process, and the monitoring controls over the maintenance and replacement costs of legacy systems.

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

M E M O R A N D U M

DATE: December 4, 2020

TO: Andy Hanau, City Auditor, Office of the City Auditor

FROM: Jonathan Behnke, Chief Information Officer, Department of Information Technology

SUBJECT: Management's Response to the IT Performance Audit of Legacy Applications

This memorandum provides background information and management's response regarding the IT Performance Audit of Legacy Applications. We would like to thank the Office of the City Auditor for their thorough review and being receptive to our feedback on their recommendations.

If no City budget or resource constraints existed, the risk of the City's legacy application portfolio would be minimized. To address challenges associated with these constraints the Department of Information Technology develops annual plans with City departments outlining risks, technology changes, and opportunities for improvements to prioritize replacement or updates to legacy applications and include requests in departmental budgets for the upcoming fiscal year. As industry standards and best practices change, the Department of IT will continue to update the application portfolio appropriately.

The Department of Information Technology manages a portfolio of nearly 300 applications that provide technology solutions for essential City operations and services to our residents and businesses. A comprehensive review of each application is completed annually using industry technology and security roadmaps for databases, operating systems, programming languages, and application updates. Each application and its components are scored based on the useful life and supportability of the underlying technology. An annual plan is developed with each City department to update any out-of-support technology components to bring them to a current state.

Many of the City's applications require only minor updates to remain current while more complex applications may require a contract solicitation and a multi-year replacement plan.

While there is no formal flag for legacy systems in the application inventory, a risk-based scoring model prioritizes application updates and true legacy applications are scored with the highest priority for update or replacement.

Page 2
Andy Hanau, City Auditor
December 4, 2020

The audit report highlights that some of the systems that were managed by SDDPC and turned over to the City in 2012 may not have included a true system age. The age of each system is tracked with the best information available, but the age of a system is not a clear indicator of a legacy application. Applications like SAP, Salesforce, and Microsoft Office 365 are updated regularly and, while they may have been implemented years ago, they still remain current due to regular updates and enhancements to the functionality and underlying technology.

The City's Strategic Technology Advisory Committee membership includes every department director to provide unified oversight and direction to align the City's business needs with technology solutions. All new budget requests are scored and ranked for alignment with the City's strategic goals, risks, cost efficiencies, and technology alignment. The scoring system ensures that City budget requests are prioritized appropriately for available funding in the upcoming budget year.

The audit recommendations include developing a standard definition for true legacy systems and a requirement for City departments to report all applications and related costs to the Department of IT. This information will be leveraged along with the annual application portfolio review to provide a formal annual report outlining risks and costs that will deliver increased visibility in prioritizing the replacement of legacy systems.

Since many of the recommendations are minor adjustments to existing processes, the majority of the recommendations will be completed in FY21.

RECOMMENDATION #1

The Department of Information Technology (DoIT) should develop and document a standard definition for a legacy system that incorporates the critical factors necessary to identify systems that no longer efficiently and effectively meet operational needs of the department (Priority 2).

Management Response: Agree with Recommendation.

The Department of Information Technology will develop and document a standard definition for a legacy system using the critical factors required to identify systems that may no longer meet operational needs of the department efficiently and effectively.

Target Date: March 31, 2021

RECOMMENDATION #2

In coordination with other City departments, the Department of Information Technology (DoIT) should create a policy and procedure to document when each legacy system was put into production, where possible, and document the current life expectancy of each system. Further, DoIT should track and update the life expectancies as systems are updated and work with the department to prioritize their replacement as the systems near the end of their life expectancy (Priority 2).

Management Response: Agree with Recommendation.

Page 3
Andy Hanau, City Auditor
December 4, 2020

The Department of Information Technology will create a policy and procedure to document when each legacy system was put into production, where possible, and document the current life expectancy of the system and work with the department(s) to prioritize their replacement as the systems near end-of-life.

Target Date: June 30, 2021

RECOMMENDATION #3

The Department of Information Technology (DoIT) should create a centralized process to track legacy systems, listing their detailed deficiencies, and update this information on an annual basis for discussion with the department during the annual Strategic Technology Advisory Committee meeting (Priority 2).

Management Response: Agree with Recommendation.

The Department of Information Technology will update the existing centralized application portfolio process to update and track legacy systems on an annual basis including details on any deficiencies. The annual legacy system assessment will be included on the agenda for discussion during the annual Strategic Technology Advisory Committee meeting.

Target Date: June 30, 2021

RECOMMENDATION #4

The Chief Information Officer should create and implement a policy and procedures that ensure risk assessments and risk assessment reports are completed and/or reviewed annually and updated according for all legacy systems (Priority 2).

Management Response: Agree with Recommendation.

The Department of Information Technology, under the direction of the CIO, will create and implement a policy and procedures for annual risk assessment reports for all legacy systems.

Target Date: June 30, 2021

RECOMMENDATION #5

The Chief Information Officer should include the results of the risks assessment for legacy systems as a significant discussion item on the agenda in the annual Strategic Technology Advisory Committee meeting with mayoral department directors to help determine which systems should be prioritized for replacement among departments (Priority 2).

Management Response: Agree with Recommendation.

Page 4
Andy Hanau, City Auditor
December 4, 2020

The Chief Information Officer will include the results of the risks assessment for legacy systems as a significant discussion item on the agenda in the annual Strategic Technology Advisory Committee meeting to help determine which systems should be prioritized for replacement among departments.

Target Date: September 1, 2021

RECOMMENDATION #6

The Chief Operating Officer should work with the Department of Information Technology and City departments to create a policy and procedure for centrally tracking all actual IT costs associated with legacy applications to facilitate replacement prioritization based on cost. DoIT should ensure that this information is updated annually (Priority 2).

Management Response: Agree with Recommendation.

The Chief Operating Officer will work with the Department of Information Technology and City departments to create a policy and procedure for centrally tracking all legacy application IT costs to facilitate replacement prioritization based on cost. The Department of Information Technology will update this information annually.

Target Date: September 1, 2021

RECOMMENDATION #7

The Chief Operating Officer should ensure coordination between all City departments and the Department of Information Technology (DoIT) to develop, document, and implement a policy to require all City departments to annually report all information systems under their purview to DoIT as well as the total operation and maintenance costs managed outside DoIT for each system (Priority 2).

Management Response: Agree with Recommendation.

The Chief Operating Officer will ensure coordination between all City departments and the Department of Information Technology (DoIT) to develop, document, and implement a policy to require all City departments to annually report all information systems under their purview to DoIT as well as the total operation and maintenance costs managed outside DoIT for each system.

Target Date: June 30, 2021

RECOMMENDATION #8

The Department of Information Technology should develop a metric for identifying high cost legacy systems and work with departments to prioritize and phase out these systems. (Priority 2)

Page 5
Andy Hanau, City Auditor
December 4, 2020

Management Response: Agree with Recommendation.

The Department of Information Technology will develop a metric for identifying high-cost legacy systems and include this information in the annual application review with City departments to prioritize the replacement of these systems.

Target Date: June 30, 2021

RECOMMENDATION #9

The Chief Operating Officer should work with the Chief Information Officer to develop a policy and corresponding procedures to require that each legacy application has a current calculation, weighing the costs and benefits of each alternative, and is documented for and reviewed during the annual STAC process (Priority 2).

Management Response: Agree with Recommendation.

The Chief Operating Officer will work with the Chief Information Officer to develop a policy and corresponding procedures to require that each legacy application has a current calculation, weighing the costs and benefits of each alternative, and is documented for and reviewed during the annual STAC process.

Target Date: September 1, 2021

RECOMMENDATION #10

The Chief Information Officer should develop and implement an operational analysis policy and coordinate with each City department to conduct and document an operational analysis for IT investments currently in production in accordance with this policy (Priority 2).

Management Response: Agree with Recommendation.

The Chief Information Officer will develop and implement an operational analysis policy and coordinate with each City department to conduct and document an operational analysis for IT investments currently in production in accordance with this policy.

Target Date: June 30, 2021

RECOMMENDATION #11

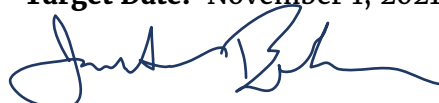
The Chief Operating Officer, working with the Chief Information Officer, should provide a confidential report annually to the City Council containing high-risk legacy applications that should be prioritized for replacement. This report should include the risks impacting information technology operations, business operations, return on investment calculation available, and security considerations, in appropriate detail for the City Council to make a decision whether to prioritize funding for application replacement (Priority 2).

Page 6
Andy Hanau, City Auditor
December 4, 2020

Management Response: Agree with Recommendation.

The Chief Operating Officer will work with the Chief Information Officer to provide a confidential report annually to the City Council containing high-risk legacy applications that should be prioritized for replacement including the risks impacting information technology operations, business operations, return on investment calculation available, and security considerations, in appropriate detail for the City Council to make a decision whether to prioritize funding for application replacement.

Target Date: November 1, 2021



Jonathan Behnke
Chief Information Officer
Department of IT

JB/jl

cc: Aimee Faucett, Interim Chief Operating Officer
Almis Udrys, Assistant Chief Operating Officer (Policy)
Jeff Sturak, Assistant Chief Operating Officer (Operations)
Rolando Charvel, Chief Financial Officer
Matthew Helm, Chief Compliance officer
Darren Bennett, Chief Information Security Officer, Department of Information Technology
Chris Bennett, Application Sourcing Manager, Department of Information Technology