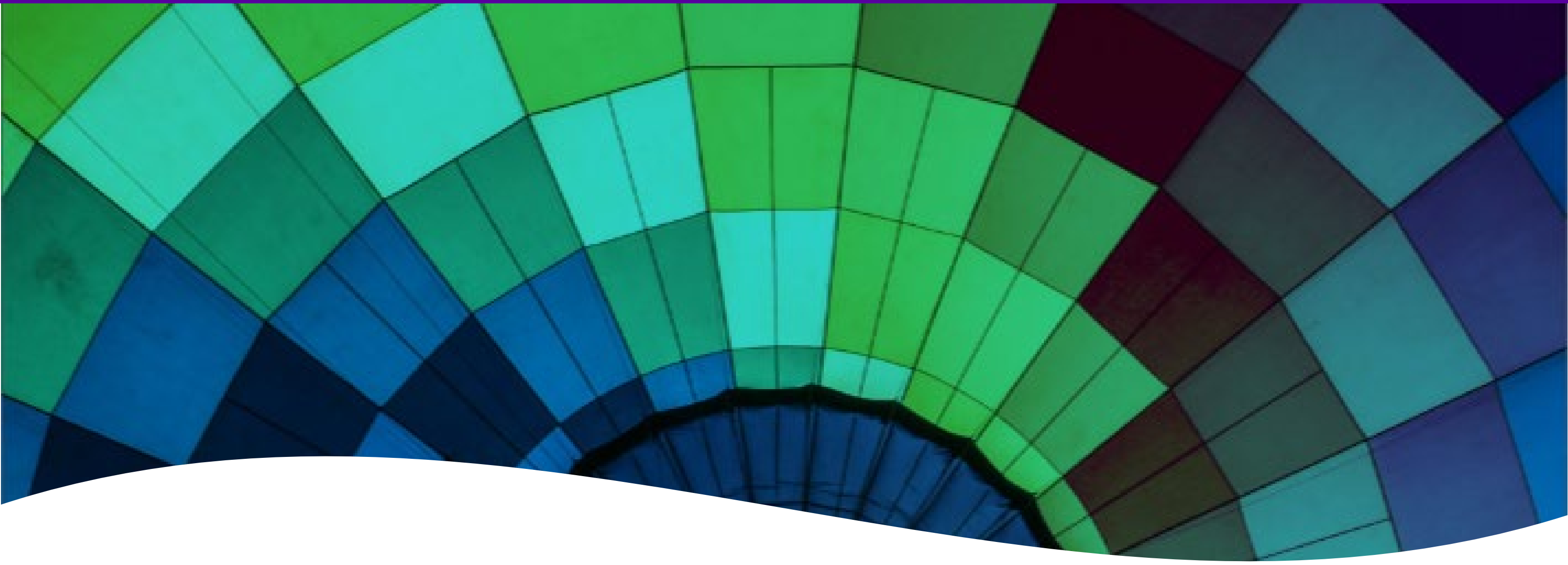
Internal Audit Division – Assurance Audit Report



Santa Clara County Library District

Performance Audit of Administrative and Information Technology Practices

October 19, 2023
Assignment #: 10367

Audit Staff
Robyn Rose, CPA, CICA, Internal Audit Manager
Hugo Lopez, Supervising Internal Auditor
Albert Beltran Jr., CIA, CISA, Internal Auditor-in-Charge

County of Santa Clara - Office of the County Executive

THIS PAGE LEFT BLANK

Executive Summary

Background

Internal Audit Division (IAD) performed an assurance audit of the Santa Clara County Library District's (Library District) administrative and information technology (IT) practices. The audit was selected through our Fiscal Year 2022-23 annual risk assessment and audit planning process.

The Library District's Services & Support Center provides centralized operations for its member libraries under a Joint Powers Authority (JPA) agreement. The JPA operates as a separate local government agency comprised of several cities and the County of Santa Clara (County). The role of the JPA Board is to provide policy direction and oversight to the Library District; however, the County serves as the Fiscal Agent and employer of Library staff.

Objective

The audit was performed to provide reasonable assurance that:

(1) IT systems meet minimum information security standards,
(2) Library District's approach towards addressing patron and staff safety aligns to management's mission and objectives, and
(3) Internal controls over administrative services follow best practices.

Scope

The audit scope included Library District's operations from July 1, 2021 to December 31, 2022 and was limited to the Administrative Services Office and IT practices not impacted by the new strategic plan adopted in October 2022.

What We Found

Library District provides a variety of services to County residents through flexible operating hours and 24/7 online access to library materials. Recently, the Library District participated in the County's Racial Equity training cohort to align with their vision of being an inclusive space where everyone feels welcomed. Their Strategic Plan was also updated to reflect their vision and priorities.

Libraries have a unique and changing role in communities and support our most vulnerable and marginalized populations. With the expanding services Library District provides to County residents coupled with the responsibility to protect patron data privacy, there is an increased need to ensure administrative and IT practices, including financial and non-financial resources, are managed effectively to address key operational risks.

Overall, we believe Library District could strengthen internal controls over IT and staff safety to enhance effectiveness in achieving organizational objectives.

The five improvements identified in the areas summarized below and detailed in the ***Findings and Recommendations*** section of this report will help management ensure internal controls are enhanced and potential risks are mitigated.

Information Security Controls requirements has the following four findings:

- An IT security framework and related policies and controls were not defined.
- IT vendor contracting and management best practices were not followed.
- Formal policies and procedures are needed to ensure sensitive information is fully protected.
- Continuity of Operations Plan/Continuity of Government were not fully developed.

Staff Training has the following one finding:

- Objectives and materials for safety-related training were not consistently provided to staff.

We also noted four "**Other Observations**" submitted for Library District management's consideration (See **Appendix 4**).

Executive Summary

The chart below summarizes risk categories for each audit area by priority ratings.

#	Area	Priority Ratings			Total
		High (1)	Medium (2)	Low (3)	
1	**Information Security Controls**	1	2	1	**4**
2	**Staff Training**	-	-	1	**1**
3	**Administrative Services Internal Controls**	-	-	-	**-**
Total Findings		**1**	**2**	**2**	**5**

See **Appendix 1** for definition of priority ratings.

Prior to issuance of this report, Library District management proactively addressed findings noted in this report and communicated their improvement plan to IAD. As a local government agency, Library District is not required to comply with all County polices unless requested by their JPA board. However, for purposes of this audit, Library District management agreed to be evaluated based on County and governmental best practices and relevant guidance.

Audit reports are designed to assist management and provide constructive recommendations for improving their operations. As a result, the report generally does not elaborate on activities that are functioning effectively. The draft report was discussed with Library District management prior to final issuance. A total of 15 recommendations were made for the five findings noted in the table above. Management agreed with 14 of the 15 recommendations and partially agreed with one (Recommendation 3.1). Attached herein is their formal response. In accordance with professional auditing standards, IAD intends to perform a follow-up audit on the recommendations presented.

We conducted the audit in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

It is anticipated that this report will be submitted to the Finance and Government Operations Committee in Winter 2023. This report is intended solely for the County and its stakeholders. However, this report is a matter of public record, and its distribution is not limited.

We would like to thank Library District management and staff for their time, cooperation, and assistance during this engagement. Additional support for this audit was provided by internal auditor Nadege Andjou, CPA along with Raydan Al-Shaibani, CISA and Yvonne Cabral from the County's Information Security Office (ISO) who assisted with findings and recommendations related to information security. We would also like to thank other County departments who provided feedback and guidance throughout the engagement.

Robyn B Rose

Robyn Rose, CPA, CICA
Internal Audit Manager
October 19, 2023

Table of Contents

EXECUTIVE SUMMARY 1-2

FINDINGS AND RECOMMENDATIONS

FINDING 1 - MANAGEMENT HAS NOT DEFINED AN INFORMATION SECURITY FRAMEWORK AND ESTABLISHED RELATED POLICIES AND CONTROLS. 4

FINDING 2 - IT VENDOR CONTRACTING AND MANAGEMENT BEST PRACTICES NOT FOLLOWED............ 5-7

FINDING 3 - MANAGEMENT DOES NOT HAVE POLICIES AND PROCEDURES TO ENSURE SENSITIVE INFORMATION IS SAFEGUARDED..8-9

FINDING 4 - CONTINUITY OF OPERATIONS PLAN/CONTINUITY OF GOVERNMENT IS NOT FULLY DEVELOPED. 10-11

FINDING 5 - OBJECTIVES AND MATERIALS FOR SAFETY-RELATED TRAINING WERE NOT CONSISTENTLY PROVIDED TO STAFF...12-14

APPENDIX 1: DEFINITION OF RISK CATEGORIES AND PRIORITY LEVELS.......................................15

APPENDIX 2: INTERNAL CONTROLS FRAMEWORK...16

APPENDIX 3: PROGRAM BACKGROUND, METHODOLOGY AND SCOPE LIMITATION..........................17-19

APPENDIX 4: OTHER OBSERVATIONS...20-22

MANAGEMENT'S FORMAL RESPONSES

Findings and Recommendations

INFORMATION SECURITY CONTROLS

FINDING 1: An IT security framework and related policies and controls were not defined.	
OBJECTIVE	To determine if a defined Information Security Framework with related policies and controls exist.
CRITERIA	County's Information Security Office (ISO) Handbook, Planning Section states "Information System Owners (SOs) and other personnel responsible for the protection of Santa Clara County information or information systems shall follow NIST [National Institute of Standards and Technology] guidance…" U. S. General Accountability Office "Green Book", Principle 11 states "Management should design the entity's information system and related control activities to achieve objectives and respond to risks."
CONDITION	During our review of the Joint Powers (JPA) Agreement dated August 9, 2001, we noted a party responsible for Library District IT security is not formally designated. Currently, Library District management assume responsibility for maintaining and operating a secure IT system. County ISO is responsible for providing integrated systems and cybersecurity support to protect the countywide networks, devices, programs, and data. ISO requirements are derived from NIST and satisfy the policy and procedure controls of NIST SP 800-53. We noted the Library District informally follows ISO policies; however, staff have difficulty accessing resources inside the County network due to domain name restrictions (sccld.org vs sccgov.org), which hinders their ability to keep current with County policies and county training. Based on inquiry, Library District management identified "technology issues" as a significant concern of operations. The Library District and County Technology Services and Solutions (TSS) finalized a Letter of Understanding (LOU) before issuance of the final audit report. The LOU assigns and clarifies technology roles and responsibilities between the two parties. ISO standards are mentioned when connecting to County networks; however, ISO is not explicitly a party to the agreement, thus some aspects of information security such as their policies and Handbooks are not addressed. When an information security framework is not established, there is an increased risk that management and monitoring of IT systems are not assessed and deployed in a consistent manner. Additionally, if staff consistently experience restrictions accessing critical resources, there is a chance of not obtaining guidance necessary for implementing or updating IT security controls.
RECOMMENDATION	**1.1** Library District management should adopt an information security framework for their technology infrastructure and update policies and procedures to reflect that framework.
PRIORITY/EXPECTED COMPLETION DATE	**High (1) – Within three months after issuance of the final audit report**
MANAGEMENT'S RESPONSE	Agreed – Library District initiated discussions with ISO to make progress in this area.

FINDING 2: IT vendor contracting and management best practices were not followed.	
OBJECTIVE	To determine if Library District follows best practices related to IT vendor management.
CRITERIA	Library District Procurement Policy states "...to the extent feasible, the Library shall follow the County's policies on soliciting and contracting." County Board Policy 5.4.5.5 states "Agencies/Departments are required to develop performance standards and implement a process that incorporates monitoring, administration and evaluation of contracts." ISO Handbook, Systems and Service Acquisition, Section 4.1.2 states “Require that contractors and vendors provide information describing the functional properties of the security controls to be employed as a part of the contracted information system or service in sufficient detail to permit analysis and testing.” ISO Solicitations and Procurement Security Guidance states “To further assist the solicitation and/or Request for Proposal process, the ISO has developed the following security requirements that should be included at the beginning of a solicitation and/or RFP process.” NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) states Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level (see Section 4.3 Security Controls).”
CONDITION	The cloud-hosted applications containing patron data used by the Library District are the Patron Incident Tracking System (PITS) and Horizon. PITS stores details related to patron behavior policy violations and suspensions. Horizon is an Integrated Library System that records historical information of circulated library material. Other applications collect data related to patron technology usage and Library service levels, but were not reviewed at this time. During the audit, we noted the below instances where best practices with the IT vendor contracting process were not followed: **<u>Security Risk Assessment</u>** We noted Security Risk Assessments (Assessment) for four of the five IT vendor solutions were not requested prior to contract finalization. County ISO conducted an Assessment of Horizon; however, the associated recommendations were not implemented. The Assessments are intended to identify, evaluate and provide recommendations that should be implemented to ensure potential threats, application security defects and vulnerabilities are mitigated. If Assessments are not performed for IT systems, potential security weaknesses in the vendors cloud infrastructure or services may go undetected increasing the risk of cyberattacks and other vulnerabilities.

FINDING 2: IT vendor contracting and management best practices were not followed.
(continued)

CONDITION
(continued)

Key Contract Language

We noted key provisions were not consistently included in the contracts reviewed such as scope of work, business needs requirements, information security reporting requirements, performance measures, monitoring of backup servers, and protection of PII Data.

Business needs requirements are expected to be communicated to the vendor before implementing new IT systems which ensures the needs of the organization are met. Additionally, performance measures are important for determining the effectiveness and efficiency of contract terms and should be regularly monitored for compliance with agreed upon deliverables to ensure services and goods are delivered timely and as intended.

While IT vendors are generally required to maintain their systems in a manner that protects client data, Library District is responsible for ensuring contract language includes vendors acknowledgement of their obligation to maintain the confidentiality, integrity, and availability of their information.

If important aspects of a vendor contract are not established and monitored, there is a risk of not obtaining the best value for contracted amount, compromised service quality, contractual breaches, and potential disruptions to critical business operations.

System Monitoring

Based on inquiry, we noted there were gaps in monitoring IT systems and applications containing sensitive information, which increases risks when vulnerabilities and necessary updates are not addressed timely. A primary reason was vacancy of the IT Manager position during the audit period. Although IT consultants were hired during the vacancy, there were limitations with the level of management and oversight provided.

Not regularly monitoring IT systems, could lead to external threats compromising personal information, potential data breaches and loss of data.

Required Vendor Documents

We further noted IT security documents were not obtained annually from the vendor such as System and Organization Controls (SOC) 2 Type II reports, Business Continuity Plans (BCP) and/or Disaster Recovery Plans (DRP), which hindered Library District management from receiving communication on the security posture of their technology systems. The SOC 2 Type II report is an examination by an independent auditor capturing how a service organization safeguards customer data, evaluates the effectiveness of internal controls and ensures deficiencies are timely addressed. The BCP/DRP identifies viable recovery strategies within the application service areas, outlines specific recovery methods and goals, and provides the maximum time required to restore services.

If critical security related documents are not requested and reviewed from vendors, there is a risk data is not recoverable due to cybersecurity breach or system failure.

Findings and Recommendations

FINDING 2: IT vendor contracting and management best practices were not followed.
(continued)

RECOMMENDATIONS	Library District management should ensure the following: **2.1** Key aspects are included in IT vendor contracts (e.g., business needs requirements, payment terms, scope of work, performance measures, PII data safeguards). **2.2** Performance standards within contracts are regularly monitored to ensure compliance with agreed upon deliverables. **2.3** Assessments for all technology systems are requested from County ISO during the initial contract phase or when undergoing amendments. Any recommendations should be timely addressed to ensure adequate security. **2.4** IT security reports such as SOC 2 Type II reports and BCP/DRPs are requested and reviewed annually. Any deficiencies noted should be timely addressed by the vendor. **2.5** Information systems with sensitive information are regularly monitored to prevent data compromise, which will ensure updates and vulnerabilities are timely addressed.
PRIORITY/EXPECTED COMPLETION DATE	**Medium (2) – Within three to six months after issuance of the final audit report**
MANAGEMENT'S RESPONSE	Agreed – Library District initiated discussions with ISO and is utilizing the County's TSS procurement process for appropriate IT contracts to make progress in these areas.

FINDING 3: Formal policies and procedures are needed to ensure sensitive information is fully protected.	
OBJECTIVE	To determine if Library District maintains controls for IT systems to ensure sensitive and confidential information is safeguarded.
CRITERIA	California Public Record Act (CPRA) (effective 2022, operative 2023), Section 7927.105(c) states in part "All patron use records of a library that is in whole or in part supported by public funds shall remain confidential." ISO Handbook, Planning, Section 3.1.1 states in part "Ensure the use of information systems is restricted to Santa Clara County approved users…" NIST Guide to Protecting the Confidentiality of [PII] references that organizations should apply the appropriate safeguards for PII based on the confidentiality impact level (see Section 4.3 Security Controls). Green Book, Principle 11.14 states "Management designs control activities to limit user access to information technology."
CONDITION	During the audit, we noted the following instances where controls over usage and protection of data captured in IT system could be improved: **User Access Controls** We determined a list of users assigned to specific roles and access levels within PITS and Horizon systems was not maintained or monitored, which helps limit unnecessary access to sensitive information. Instead, management assigns staff to general role groups based on their job classification. A description of those roles could not be easily determined to ensure the permission or access rights were adequately assigned. We further noted Single Sign-On (SSO) for the various IT applications used by staff was not implemented. Although not required, SSO is an authentication method that allows a user to log-in with a single ID to multiple applications and has become the leading practice as an efficient solution that streamlines the user experience and improves security. If user access controls are not properly assigned, there is a risk of potential unauthorized access, data breaches, and compromised data integrity that could lead to unreliable information maintained in IT system. Moreover, not implementing SSO creates an increased risk of an offboarded staff or other individuals having continued access into a system or applications without permission.

FINDING 3: Formal policies and procedures are needed to ensure sensitive information is fully protected. *(continued)*	
CONDITION *(continued)*	**<u>Data Protection</u>** We observed there were no formal guidelines or documented procedures for de-identifying and protecting potentially sensitive or confidential data collected from various sources used to submit required monthly and annual reports to the California (CA) State Library. While no instances of compromised data were found, the Library District's Data Administrator is the primary staff responsible for gathering information and possessing the institutional knowledge needed to complete the required state reports. The CA State Library provides detailed guidance on the data required from local library systems. The information captured is expected to include basic descriptive data such as number of hours each library branch is open and total library visits. While the information submitted to the state does not contain sensitive information, the source of the data is captured from IT systems containing potentially sensitive activities (e.g., data on virtual library program attendance, number of teen and adult volunteers and number of minors participating in children's programs). If there are no clear instruction on how to handle sensitive or confidential data, there is a risk personal information could be compromised. To mitigate this risk, the County's Privacy Office (PO) provides resources and guidance to help countywide departments develop customized procedures for capturing data based on a particular situation using best practices such as NIST.
RECOMMENDATIONS	**3.1** Library District management should formally establish policies and procedures for protecting personal information and patron privacy rights, specifically related to: • Collecting and processing data from various IT applications for the monthly and annual reporting to stakeholders, • Including a requirement to annually review the policy for potential updates, and • Working with the County PO to develop policies and procedures for de-identification of library data following data minimization principles and best practices to comply with current data privacy standards. **3.2** User access controls for IT systems should be properly assigned by Library District management to ensure sensitive information is safeguarded. Additional tasks to consider includes: • Reviewing and updating roles and permission matrix for software applications, • Conducting periodic User Access Reviews, and • Implementing SSO to each application and/or solution which supports this capability.
PRIORITY/EXPECTED COMPLETION DATE	**Medium (2) – Within three to six months after issuance of the final audit report**
MANAGEMENT'S RESPONSE	Partially Agreed – Library District will continuously update their privacy related policies and procedures along with roles and permissions for the integrated library system.

FINDING 4: Continuity of Operations Plan/Continuity of Government is not fully developed.	
OBJECTIVE	To determine if Library District maintains a current Continuity of Operations Plan/Continuity of (COOP/COG).
CRITERIA	CA Code of Regulations, Title 19, Section 2403 states “(c) Local government, operational area, regional, and state levels shall provide for all of the following functions within SEMS [Standardized Emergency Management System]: management, operations, planning/intelligence, logistics, and finance/administration." ISO Handbook, Contingency Planning Section states in part "The Information System Owner shall...Develop and maintain a contingency plan for all information systems, as a part of the System Security Plan, which includes the following: Essential mission and business functions despite the information system disruption, compromise, or failure..." ISO Policy on Cloud Service Providers, Section 16.0.4 states "Cloud Service Providers vendors...shall be required to have a viable risk management strategy...in conjunction with a formally documented [BCP] and [DRP].”
CONDITION	CA Code of Regulations, with guidance from the Governor's Office of Emergency Services, requires local governments to develop a viable COOP/COG document, which enables government agencies to continue their essential functions under a broad spectrum of circumstances that may disrupt normal government operations. The County’s Office of Emergency Management (OEM) is responsible for coordination among countywide departments and local governments within Santa Clara County, including the Library District, to ensure all key stakeholders’ roles and responsibilities are formally documented in preparedness for an emergency event. Based on review of the Library District's 2023 COOP/COG, we noted mission-critical IT systems and their evolving roles during emergency situations were absent from the document. Incorporating vital IT systems into the plan ensures essential functions and activities can be restored when an interruption occurs. County ISO provides guidance to departments that can be incorporated into the COOP/COG. Recently, Library District services were significantly impacted during height of the COVID-19 pandemic and staff were activated as disaster service workers to aid in the response efforts. Library branches also served as heating and cooling centers during extreme weather events. These situations were not included to ensure a full range of emergencies are addressed. Another area that should be reviewed in the document is the “orders of succession”, which is currently represented by an organizational chart conveying its internal structure and relationships by job title, but does not clearly identify delegation of authority by a sequence of specific positions. Without a comprehensive formal agreement detailing the level of cooperation among key stakeholders during emergencies, potential disruptions of service could result in confusion and untimely response for continuing operations for essential functions. Additionally, if technology systems are not included, there is an increased risk mission-critical systems are not adequately restored after a service disruption.

FINDING 4: Continuity of Operations Plan/Continuity of Government is not fully developed. ***(continued)***	
RECOMMENDATIONS	**4.1** Library District management should review federal, state and County guidance and revise the COOP/COG to include any missing components, such as: • Information on the critical technology systems used by staff and their role to ensure continuity of operations, • Roles and responsibilities of facilities during emergency situations, and • Order of Succession. **4.2** The COOP/COG should be regularly reviewed and updated to reflect County guidance (e.g., OEM and ISO) to ensure continued compliance with applicable standards and best practices. **4.3** Library District management should ensure successful coordination among stakeholders during various situations by training staff on their roles and responsibilities within the COOP/COG and on major updates.
PRIORITY/EXPECTED COMPLETION DATE	**Low (3) – Within six to 12 months after issuance of the final audit report**
MANAGEMENT'S RESPONSE	Agreed – Library District will update the COOP/COG based on our recommendations.

STAFF TRAINING

FINDING 5: Objectives and materials for safety-related training were not consistently provided to staff.

OBJECTIVE

To determine if patron behavior and staff training policies and practices aligned to management's objectives.

CRITERIA

Green Book, Principle 4 states "Management develops personnel to achieve the entity's objectives, including developing competencies and tailor training based on the needs of the role."

Green Book, Principle 6 states "Management should define objectives clearly to enable the identification of risks and define risk tolerances."

CONDITION

Providing a welcoming and open public space at library facilities and ensuring the safety of staff and patrons are the Library District's main priorities. One tool that helps them define this is their Behavior Standards (Standards), which are posted publicly online and in all library facilities. The Standards contain prohibited patron behaviors such as, "assaulting, harassing, stalking, staring, bullying or threatening the public or staff," and describe some actions that Library District staff may take in responding to prohibited patron behaviors. All staff are expected to be aware of the Standards and related prohibited patron behaviors.

During the audit, we identified the below instances where controls over safety-related training provided to staff could be improved to ensure consistent alignment with Library District priorities:

Staff Training Expectations Not Aligned to Library District Priorities

We found there were two specially trained safety officers assigned to all library facilities, yet other staff could engage with patrons who violated the Standards. Library District staff participate in various safety-related training to help identity and handle negative patron behaviors. The impact of these trainings on staff performance was not assessed or measured against the number and types of patron behavior incidents to ensure alignment with expected outcomes. Upon reviewing related training documents provided to staff, we noted management's objectives and expected performance were not mentioned.

For reference, below is a table of active incidents in PITS from January 1, 2022 to June 1, 2022. This data could be used to inform future patron behavior goals or staff training needs.

Branch Location	# Incidents
Campbell	5
Cupertino	7
Gilroy	12
Los Altos	7
Morgan Hill	3
Milpitas	14
Saratoga	8
Woodland	1
Total	**57**

Note: Data represents incidents ranging from damaging or stealing library property to threatening public or staff. Management noted a small percentage of these incidents involved a call to local authorities.

FINDING 5: Objectives and materials for safety-related training were not consistently provided to staff. *(continued)*

CONDITION *(continued)*

Without defined objectives, goals and related metrics for monitoring and improving staff performance, there is a risk of management and the governing body not having timely and accurate information to make informed operational decisions or enhance trainings.

<u>Safety Training</u>

We also found training on the Standards were not provided to all Library District staff. Typically, “in-charge” staff such as the Community Librarian or other senior level staff participate in the training and excludes front-line staff who also interact with patrons. Front-line staff receive training from the County’s Department of Facilities Security, who provides guidance on “Verbal De-Escalation” and “Active Shooter Response” trainings. These trainings cover basic skills needed to promote the safety and security of staff and patrons, but does not address all patron behavior violations included in the Standards.

If all staff do not receive trainings equipping them with appropriate knowledge and skills on appropriate response techniques related to patron behavior incidents, there is a risk that violations are not handled equitably resulting in unnecessary escalated patron behaviors.

<u>Emotional and Mental Health Training</u>

We further noted staff training materials do not currently address the Library District’s shifting role of providing trauma-informed responses to patrons and the emotional and mental health needs of staff who may experience trauma as a result of responding to the behavior incidents. Recent industry publications discuss the real and perceived shifts in Library staff responsibilities through the lens of first responders, not only in support of vulnerable and marginalized populations, but with other traumatic incidents such as drug overdoses and threats of violence. One article title sums up the idea of this relatively new industry-wide concern for Library operations, “Superheroes Need Help Too.”

If staff are not properly trained on how to handle traumatic situations, there is a risk of their mental health needs going unnoticed, resulting in burnout or compassion fatigue.

<u>Documenting Behavior Incidents and Receiving Feedback</u>

When reviewing training materials, we noted staff generally understood the Standards, but did not receive uniform guidance or consistent feedback on the violations requiring documentation in PITS and if the information met reporting expectations. For example, staff entered low stress or easily de-escalated behavior violations in PITS at their discretion as management generally focused on evaluating high-profile or extreme incidents. Additionally, feedback was not regularly provided regarding the quality and completeness of staff documentation entered in PITS.

If staff are not provided with guidance on documentation requirements based on management’s expectations, there is an increased risk of entering information inconsistently.

FINDING 5: Objectives and materials for safety-related training were not consistently provided to staff. *(continued)*	
RECOMMENDATIONS	**5.1** Library District management should establish objectives for patron/staff safety and include specific training content to achieve those objectives, such as: • Promoting consistency on how staff respond to patron behaviors at all library facilities, • Reporting PITS data to the JPA Board for increased transparency related to equity, public safety and workplace safety, • Establishing organizational objectives specifically addressing various aspects of personal safety with a focus on mental health and emotional well-being, and • Developing metrics and evaluation methods to measure and report on attainment of the objectives. **5.2** Training materials should explicitly outline staff performance expectations for responding to patron behavior incidents, such as including a document describing various patron behavior scenarios and expectations on how staff should document the incidents (e.g., a script with suggested phrases) to ensure alignment with management's objectives. **5.3** Library District management should provide all staff with sufficient guidance to ensure patron incident information is entered in PITS accurately and completely. **5.4** Library District management should implement a standardized process for reviewing staff's documented behavior incidents and follow-up actions to ensure responses align with their expectations.
PRIORITY/EXPECTED COMPLETION DATE	**Low (3) – Within six to 12 months after issuance of the final audit report**
MANAGEMENT'S RESPONSE	Agreed – Library District will update training related policies and procedures based on our recommendations, establish objectives for patron/staff safety and formalize a process for reviewing staff incident reports to provide consistent feedback.

Appendix

APPENDIX 1: DEFINITION OF PRIORITY RATINGS FOR AUDIT RECOMMENDATIONS

Priority Ratings	Definition of Priority Ratings and Suggested Implementation Timeframe
High / Priority One (1)	Priority One recommendations are assigned to the highest assessed level of risk. For these recommendations, internal controls are considered poor or insufficient, which results in the likelihood of financial loss, waste, misappropriation of assets, or errors for the area(s) evaluated. Priority One recommendations also include issues related to non-compliance with laws, regulations or policies and procedures. Management should urgently implement these recommendations within one to three months after issuance of the final audit report to avoid risk exposure.
Medium / Priority Two (2)	Priority Two recommendations are assigned to the moderately assessed level of risk. For these recommendations, internal controls provide reasonable assurance that the County program(s) or area(s) evaluated are protected from potential financial loss, waste, misappropriation of assets, or errors; however, additional action is needed to strengthen current practices. Management should promptly implement these recommendations within three to six months after issuance of the final audit report to improve internal control processes.
Low / Priority Three (3)	Priority Three recommendations are assigned to the lowest assessed level of risk. For these recommendations, internal controls are operating as designed to ensure the County program(s) or area(s) evaluated are protected from potential financial loss, waste, misappropriation of assets, or errors. These recommendations are desired actions to enhance current practices. Management should consider implementing these recommendations within six to 12 months after issuance of the final audit report to provide additional confidence in the internal control system.

APPENDIX 2: INTERNAL CONTROLS FRAMEWORK

We utilized guidance in the U.S. Government Accountability Office's *Standards of Internal Controls in the Federal Government* ("Green Book") to evaluate best practices for internal controls within government entities. Internal controls are processes used by management to help achieve their goals and objectives related to operations, reporting, and compliance.

Standards in the "Green Book" comprise of the following five internal control components and corresponding 17 principles that work together in an integrated framework:

Components	Principles
Control Environment	1. The oversight body and management should demonstrate a commitment to integrity and ethical values. 2. The oversight body should oversee the entity's internal control system. 3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve its objectives. 4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals. 5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.
Risk Assessment	6. Management should define objectives clearly to enable the identification of risks and define risk tolerances. 7. Management should identify, analyze, and respond to risks related to achieving the defined objectives. 8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks. 9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.
Control Activities	10. Management should design control activities (i.e., policies and procedures) to achieve objectives and respond to risks. 11. Management should design the information system and related control activities to achieve objectives and respond to risks. 12. Management should implement control activities through policies.
Information and Communication	13. Management should use quality information to achieve its objectives. 14. Management should internally communicate the necessary quality information to achieve its objectives. 15. Management should externally communicate the necessary quality information to achieve its objectives.
Monitoring Activities	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. 17. Management should remediate identified internal control deficiencies on a timely basis.

Source: https://www.gao.gov/greenbook

APPENDIX 3: PROGRAM BACKGROUND AND METHODOLOGY

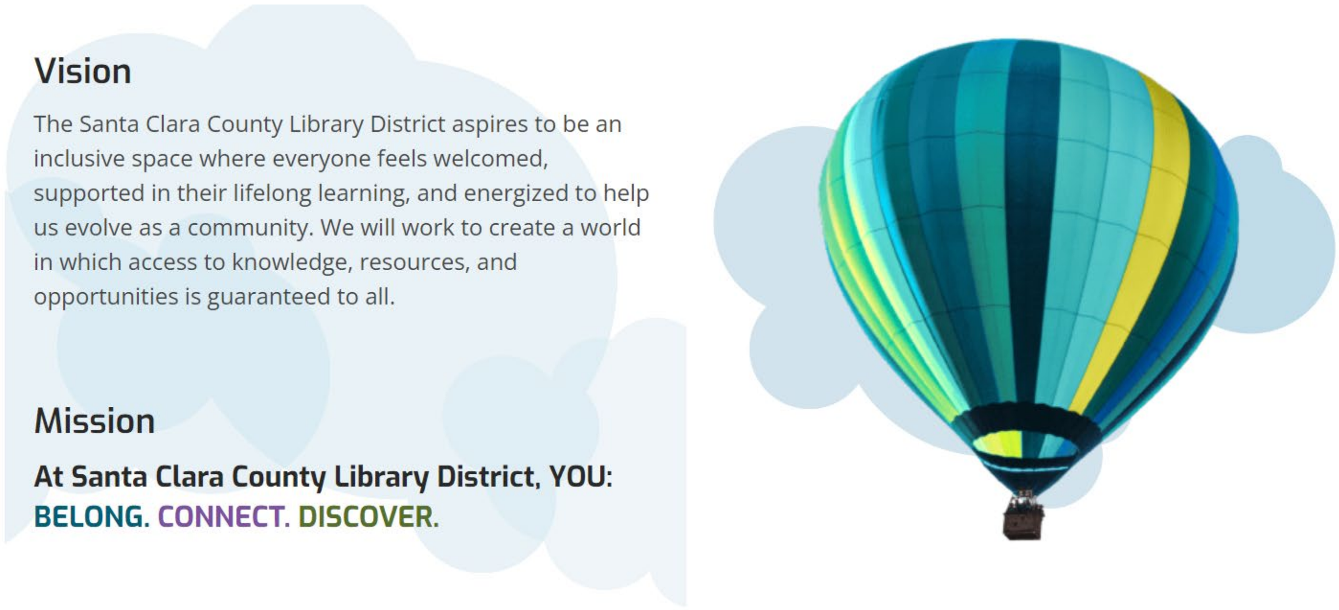
PROGRAM BACKGROUND [1]

Originally founded in 1914 as a County agency, the Library District is now a JPA operating as a separate "public entity"[2] authorized under CA Government Code Section 6500. The JPA is comprised of nine cities and the County, who acts as fiscal agent and official employer of Library District staff. The JPA's regulations are listed in CA Government Code Title 1, Div 7, CH 5, Article 1.

The Library District fulfills its service mission primarily through offering and lending a wide variety of material, which, as of FY2021-22, includes a collection of over two million books, videos, CDs, DVDs/Blu-rays, audiobooks, eBooks and extensive online resources accessible from anywhere with an internet connection. Library District also has two bookmobiles, and four "GoGoBiblio" electric outreach vehicles.

There are currently seven community libraries and one branch library serving the cities of Campbell, Cupertino, Gilroy, Los Altos, Milpitas, Monte Sereno, Morgan Hill, Saratoga, town of Los Altos Hills and unincorporated areas of the County.

The Library District recently underwent a 10-month long process of engaging staff, patrons, residents, commissioners, community leaders, JPA Board members and other stakeholders to create their new strategic plan, which was adopted in October 2022. The Library District's new vision, mission and four overarching operational priorities are as follows:



Vision

The Santa Clara County Library District aspires to be an inclusive space where everyone feels welcomed, supported in their lifelong learning, and energized to help us evolve as a community. We will work to create a world in which access to knowledge, resources, and opportunities is guaranteed to all.

Mission

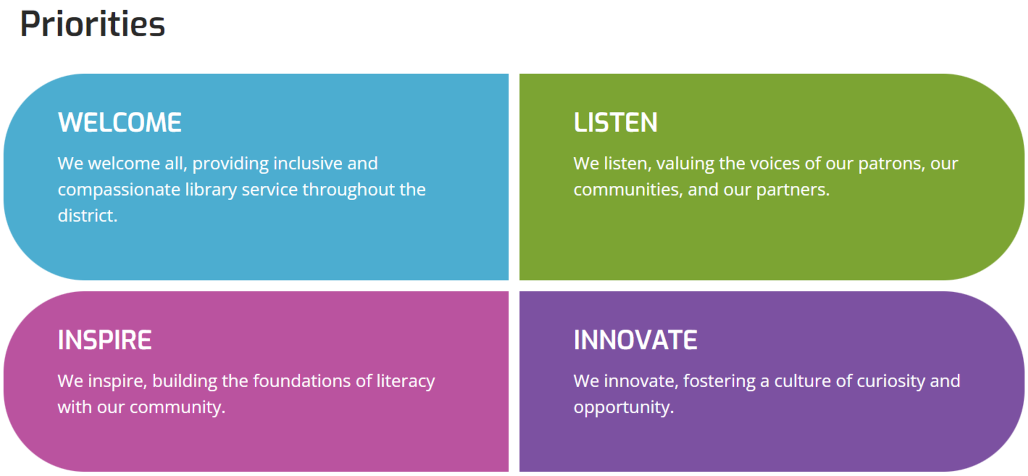
At Santa Clara County Library District, YOU:

BELONG. CONNECT. DISCOVER.

[1] E*xcerpts from Library District website, reports and strategic plan*

[2] CA GOV CODE Section 6507. "For the purposes of this article, the agency is a public entity separate from the parties to the agreement." https://leginfo.legislature.ca.gov/ accessed August 2022 - October 2023

Appendix



Priorities

WELCOME

We welcome all, providing inclusive and compassionate library service throughout the district.

LISTEN

We listen, valuing the voices of our patrons, our communities, and our partners.

INSPIRE

We inspire, building the foundations of literacy with our community.

INNOVATE

We innovate, fostering a culture of curiosity and opportunity.

Additionally, Library District received the following achievements:

- For 15 consecutive years, was rated one of America’s Star Libraries recognized by the Library Journal.
- In 2022, was rated as a 5-Star library in their Index of Public Library Service, which is one of only five library systems in the United States given this honor with expenditures over $30 million.
- In 2020, received the Innovative Project of the Year Award (for a Large District) from the California Special Districts Association.
- In 2019, received the Challenge Award from the California State Association of Counties.
- In 2014 and 2019, won Innovator Awards from the Urban Libraries Council.

Appendix

METHODOLOGY

To achieve our audit objectives, IAD performed the following procedures:

- Conducted meetings with management, staff, and industry representatives.
- Requested and reviewed Library District policies and procedures.
- Performed walkthroughs at two libraries.
- Provided management with internal control questionnaires.
- Consulted with County ISO to review IT security controls and best practices applicable to key library systems.
- Provided management a list of resources that were considered in developing our recommendations.
- Coordinated with management and County Counsel to determine the criteria used for evaluating audit objectives.

SCOPE CONSIDERATIONS AND LIMITATIONS

As fiscal agent of Library District, the County is responsible for financial policy oversight. Since the intent of the audit was to review internal controls over administrative and IT practices, most fiscal policy areas were considered out of scope during the risk assessment phase.

The County's Employee Services Agency is responsible for hiring and related human resources responsibilities as Library District staff are County employees, thus review of this area was also limited**.**

Additionally, as a separate local government agency, the Library District is not required to comply with all policies of its JPA members, such as the County. IAD coordinated with management and County Counsel on determining criteria for our audit objectives. To maintain independence and reduce audit risk to an acceptable level, we also reviewed County ordinances, County Board Policies, state and federal guidance for local governments and industry standards for criteria.

APPENDIX 4: OTHER OBSERVATIONS (OBS)

The following observations were developed for Library District management to address additional areas relevant to their operations and provide further transparency to the public. The observations were discussed with management before issuance of the formal report. IAD also provided resources to support each suggestion. Implementation of the suggestions noted below are at the discretion of Library District management as they were deemed lower priority.

OBS 1 – LINES OF AUTHORITY/ROLES AND RESPONSIBILITIES

Criteria: JPA Agreement, Sections 7.2 (Fiscal Agent), 7.4 (Employees) and 7.5 (Administrative Staffing).

Observation: The Library District is a local government agency where most aspects of their operations are at the discretion of management and JPA Board member approval; however, we noted the reporting structure and lines of authorities between the County and Library District were not defined for all administrative practices. For example, the JPA Agreement defined the County as responsible party for the following areas:

- Hiring of Library District staff who are employees of the County and subject to the labor agreements and personnel/merit system rules administered by ESA.
- Assigning County Counsel representation for legal matters.
- Serving as the Library District's Fiscal Agent and requiring adherence to fiscal-related policies within the Finance Agency.
- Providing purchasing, budgeting, payroll and treasury services to the Library District.
- Appointing of the County Librarian by the County Executive with functional reporting to the JPA Board.

Other administrative areas were not explicitly addressed in the JPA Agreement such as technology support as it is implied that Library District's Administrative Services Office assumes this responsibility. We also noted purchasing and other procurement functions (e.g., p-cards and contracting) are handled internally without County oversight. Additionally, the Library District staff cannot easily access many County resources and training materials for areas such as p-cards, IT, information security, and other non-fiscal policies for guidance.

As a result, it may be difficult to easily determine the roles and responsibilities over the administration and monitoring of Library District's operations. Without clearly defining the reporting structure between the Library District and County, there is a risk of operating inefficiently and ineffectively, resulting in not meeting organizational mission and objectives.

Suggestion: Library District management and the JPA Board should formalize language in the JPA Agreement or other legal document to ensure roles and responsibilities are clearly defined and consistently applied over critical areas of operations. A few key areas to consider include: Information Security (Finding 1), Surveillance Ordinance (OBS 2) and Emergency Operations and Business Continuity Planning (Finding 4).

OBS 2 – SURVEILLANCE ORDINANCE

Criteria: County Surveillance Ordinance (Ordinance) Sec. A40-3 – Information Required states "Unless it is not reasonably possible or feasible to do so...the department...must submit to the Board an Anticipated Surveillance Impact Report and a proposed Surveillance Use Policy before the public meeting."

Observation: Based on inquiry, we noted the Library District's Surveillance Policy addresses video camera usage around library facilities to capture patron activities, but does not include other aspects of surveillance addressed in the County Ordinance such as annual reporting requirements to a governing body and reference to radio frequency identification (RFID) systems. The Library District utilizes RFID technology to track circulated library materials, but they are not required to comply with the County Ordinance and related requirements.

We also reviewed city ordinances of JPA members for reference to data privacy, surveillance and protection rights of the community. The City of Morgan Hill has one of the only ordinances specifically protecting citizen rights related to surveillance.

If Library management does not submit annual surveillance reports and operates a surveillance device without approval or oversight, there may be potential for a lawsuit brought against the Library District, and the reputation of both the Library District and County may be perceived as having a lack of transparency.

Suggestion: Library District management and JPA Board should update the Surveillance Policy to align with more robust ordinances such as the County and City of Morgan Hill. Additionally, the San Francisco Public Library publishes an annual impact report on RFID technologies that can be referenced for best practices.

The updated Surveillance Policy should be communicated to internal and external stakeholders.

OBS 3: P-CARD MANAGEMENT AND OVERSIGHT

Criteria: Library Purchase Card (P-Card) Program Policies and Procedures

Observation: A P-Card is a form of charge card that allows goods and services to be procured without going through the traditional procurement process.

Based on review of the Library District's P-card practices, we noted the Administrative Services Office oversees all aspects of this area (e.g., card issuance, usage, allowable purchases, reporting and reconciliations); however, Sections 7.2 & 7.5 of the JPA Agreement appointed the County as Fiscal Agent and responsible party over purchasing and accounts payable functions.

Additionally, the County’s Procurement Department administers countywide P-Cards and procurement practices, but the Library District is not required to follow their policies and procedures. The County's Controller-Treasurer Department (CTD)-Claims Unit is responsible for issuing all warrants on behalf of countywide department. CTD-Claims Unit also performs annual "Payment-After-the-Fact" reviews of countywide purchasing transactions. We found the Library District P-Card transactions and other payments were excluded from the annual reviews; however, the official exclusion agreement could not be located by Library District or CTD management during the audit period.

We further noted cardholders received fraud alerts, which detects potential unauthorized activities on the P-Card, and also perform their own monthly reconciliations on transactions. Since cardholders receive fraud alert notifications and also reconcile their own information, there is risk of unauthorized activities going undetected caused by a lack of segregation of duties.

Suggestion: Library District management should coordinate with County’s Procurement Department and CTD to formally agree and document administration over the purchasing and accounts payable functions outlined in the JPA Agreement to ensure roles and responsibilities are clearly defined. Any exemption from County policies should also be documented.

OBS 4 – PERFORMANCE MEASURES FOR THE NEW STRATEGIC PLAN

Criteria: Green Book, Principle 13 states "Management should use quality information to achieve the entity's objectives. "

Observation: During the audit, we noted performance measures were not developed to align with the Library District's new Strategic Plan adopted in October 2022, including related data collection efforts for management to effectively measure progress in achieving their goals and objectives.

Through inquiry, we found Library District management is currently developing new goals and objectives to align with the Strategic Plan. As of the audit report issuance date, we noted data collected for performance measures were not established to determine if goals, the cost effectiveness, or systems efficiencies were achieved.

We provided management with example goals, objectives and measures from other similar agencies to consider, ranging from one-page overviews to comprehensive documents detailing the strategic planning processes and aligned measures reflective of progress towards their goals and objectives. Resources from the Government Alliance on Race Equity (GARE) were are also provided as context on how to incorporate equity practices when establishing objectives.

Suggestion: Library District management should ensure performance metrics align with the new strategic plan's goals and objectives. Management should consider expanding the data collected by the CEO's Measures of Success division to include pertinent information in line with the new strategic plan.

We also suggest Library management and the JPA board formalize their "risk tolerance" and "risk appetite" (i.e., ability and desire of the organization) for achieving results so quickly that progress outpaces available resources, and for not achieving results after investing JPA Board approved resources.

santa clara county library district

Santa Clara County Library District, Services & Support Center, 1370 Dell Ave, Campbell, CA 95008-6604| sccld.org

MEMORANDUM

DATE: November 1, 2023

TO: Internal Audit Division

FROM: Jennifer W. Weeks, County Librarian

SUBJECT: Library District Response to Internal Audit Report

Thank you for the opportunity to review and respond to the Internal Audit Report of the Library District's administrative and information technology practices. Following are the Library's responses to each of the recommendations.

Recommendation	**Response**
1.1 Library District management should adopt an information security framework for their technology infrastructure and update policies and procedures to reflect that framework.	The Library agrees with this recommendation and has finalized a formal Letter of Agreement with the County Technology Services and Solutions (TSS) for support, and also opened discussions with the County Information Security Office (CISO) to make progress in this area.
2.1 Library District management should ensure that key aspects are included in IT vendor contracts.	The Library agrees with this recommendation and is utilizing the County TSS procurement process for appropriate IT contracts.
2.2 Library District management should ensure that performance standards within contracts are regularly monitored to ensure	The Library agrees with this recommendation.

compliance with agreed upon deliverables.	
2.3 Library District management should ensure that assessments for all technology systems are requested from County ISO during the initial contract phase or when undergoing amendments.	The Library agrees with this recommendation and has opened discussions with the CISO to make progress in this area.
2.4 Library District management should ensure that IT security reports such as SOC 2 Type II reports and BCP/DRPs are requested and reviewed annually. Any deficiencies noted should be timely addressed by the vendor.	The Library agrees with this recommendation and has opened discussions with the CISO to make progress in this area.
2.5 Library District management should ensure that information systems with sensitive information are regularly monitored to prevent data compromise, which will ensure updates and vulnerabilities are timely addressed.	The Library agrees and will continue its practice of partnering with the CISO for annual vulnerability assessments and work proactively to remediate any issues and improve its overall information security posture.
3.1 Library District management should formally establish policies and procedures for protecting personal information and patron privacy rights, specifically related to IT applications for the monthly annual reporting, and procedures for de-identification of library data following data minimization principles and best practices	The Library partially agrees. The Library's mission and core policies support the values outlined in the American Library Association's Library Bill of Rights, which specifically maintains that privacy and confidentiality of patron data is of the utmost importance. The Library's updated privacy policy references California Government Code § 7927.100, and § 7927.105 which guarantees privacy in library use for all individuals. The Department will continue to build upon these existing policies and procedures to maintain patron privacy through best practices and current data privacy standards.

to comply with current data privacy standards.	
3.2 User access controls for IT systems should be properly assigned by Library District management to ensure sensitive information is safeguarded.	The Library agrees with this recommendation and is updating the roles and permissions for the integrated library system.
4.1 Library District management should review federal, state and County guidance and revise the COOP/COG to include any missing components.	The Library agrees with this recommendation and the current COOP will be revised to include more detailed information on the critical technology systems, roles and responsibilities of facilities during emergency situations, and an Order of Succession.
4.2 The COOP/COG should be regularly reviewed and updated to reflect County guidance (e.g., OEM and ISO) to ensure continued compliance with applicable standards and best practices.	The Library agrees with this recommendation and the current COOP will be revised with these elements.
4.3 Library District management should ensure successful coordination among stakeholders during various situations by training staff on their roles and responsibilities within the COOP/COG and on major updates.	The Library agrees with this recommendation and updates to the COOP will include this information.

5.1 Library District management should establish objectives for patron/staff safety and include specific training content to achieve those objectives.	The Library agrees with this recommendation and has established objectives for patron/staff safety in the current training documentation. Training has been reviewed to ensure those objectives are included.
5.2 Training materials should explicitly outline staff performance expectations for responding to patron behavior incidents, such as including a document describing various patron behavior scenarios and expectations on how staff should document the incidents (e.g., a script with suggested phrases) to ensure alignment with management's objectives.	The Library agrees with this recommendation and training materials will be updated to outline staff performance expectations regarding patron incidents.
5.3 Library District management should provide all staff with sufficient guidance to ensure patron incident information is entered in PITS accurately and completely.	The Library agrees with this recommendation and the PITS user guide will be updated to ensure incidents are entered in a more complete manner.
5.4 Library District management should implement a standardized process for reviewing staff's documented behavior incidents and follow-up actions to ensure responses align with their expectations.	The Library agrees with this recommendation and will formalize the process for reviewing staff incident reports to provide consistent feedback.