Risk Advisory Services
Information Technology Review Report

September 8, 2023

CARSON CITY – CLERK'S OFFICE

Submitted By:

Eide Bailly LLP
Richard McRae, CISM, CISA
Senior Manager, Risk Advisory Services

Ron Huffman, CMMC-RP
Associate, Risk Advisory Services

Eric Pulse, CISA, CISM, CRISC, CCSFP, CFSA
Principal, Director of Risk Advisory Services

EideBailly

CPAs & BUSINESS ADVISORS

Mr. Frank Abella, CIO
Carson City
201 North Carson Street, Suite 7
Carson City, Nevada 89701

We were engaged to perform information technology consulting services for Carson City – County Clerk's Office. This engagement was conducted in accordance with the terms of our engagement letter setting forth our involvement and scope of services. We have completed our work relating to Information Technology as of August 16, 2023, as outlined in our engagement letter dated May 12, 2023.

This letter and the accompanying attachment represent our report for the services provided and our observations. This report is intended for the information and use by Management of Carson City – County Clerk's Office in evaluating the adequacy of the procedures performed and the findings resulting from the performance of those procedures.

We would like to thank everyone at Carson City – County Clerk's Office for their cooperation and assistance during this engagement. We would like to also advise the Audit Committee that this review was completed using a combination of audit tracking and communication tools that included Suralink and Microsoft Teams Chat. These tools provided both the Eide Bailly consultants and Carson City team members an ongoing transparency into project status and communications, thereby promoting efficient document sharing plus question and issue resolution.

Please contact Rich McRae at 406.867.4163 if you have any questions regarding this report.

Sincerely,

Richard McRae

rmcrae@eidebailly.com

Project Background and Scope

Background

Eide Bailly completed an information technology consulting engagement focusing on information systems IT general controls within the County Clerk's Office (including the County Clerk, the County Recorder, and the Elections Department). Our approach to this engagement included information gathering such as documentation reviews, process reviews and interviews with key representatives to gain an understanding of the security posture of the IT environment. This approach also allowed us to better understand the IT operational functions that are critical to the protection of sensitive information and the continuation of business operations within the County Clerk's Office.

Objectives and Scope

The primary objective for this engagement was to obtain an understanding of the County Clerk's Office operations and security posture over the information technology general control environment. We completed an initial scoping survey to identify in-scope critical systems during the planning process. Based on management's input, the scope of procedures was limited to the Landmark-associated critical IT operations, processes, infrastructure, and systems activities as managed by the Clerk's Office and supported by the IT Department (*See Footnote 1). Landmark is used to record transactions within each of the departments such as deeds, mortgages, marriage licenses, and electoral candidate filings. The system provides public access to recorded documents, allowing the ability to search for and obtain document records. Landmark also processes the collection of associated filings and/or document request fees and taxes. In accordance with our work program, the scope of this engagement focused on the County Clerk's Office operations as follows:

- **General IT Administration and Governance**
  The IT environment physical, administrative, and technical controls are in place through an ongoing governance program and managed to acceptable levels within the organization. Administrative and governance controls are evaluated to ensure information safeguards are in place. Eide Bailly inspected IT policies and procedures for overall IT administration of the Information Security Program, including risk management; communication of security issues; onboarding/offboarding of personnel, and ongoing employee security awareness and training program.

- **Information Security**
  Information security policies and procedures are in place and address appropriate requirements and best practices. The City's security controls and practices are analyzed, including management of user access permissions, remote access, mobile device management, systems configurations, anti-malware and patch management, security maintenance and monitoring, incident response, and physical security over the IT asset infrastructure and electronic media. Eide Bailly's assessment of network and applications administration activities included inspection of WiFi configurations; user accounts and administrator security permissions; administration of user access and roles; security management practices and access control procedures; and overall monitoring procedures over Information Security.

- **Change Control, Development and Acquisition**
  Hardware and software are developed, acquired, and maintained with security as an integral part of the process. Acquisition and change management controls are evaluated including IT strategic planning processes, project risk assessment and implementation, applications and operating systems software upgrade control, and software integration and release documentation. Eide Bailly evaluated the in-house and external vendor procedures for ongoing maintenance of servers and applications software. Change ticketing, user permissions, testing vs. production environments, and change control test procedures were evaluated to ensure systems and applications software undergo controlled and authorized changes.

Objectives and Scope

- **Business Continuity and Disaster Recovery**

  Policies and processes provide reasonable assurance to recover from a disaster, minimize impact to customer service, and maintain security over customer information. Physical security and recovery procedures are evaluated including off site storage of electronic and hardcopy documentation, environmental controls within computer areas, business impact analysis, recovery procedures, and business interruption or special data processing risk insurance to cover costs of restoring operations in the event of a disaster. Eide Bailly evaluated the overall disaster recovery program to ensure that critical information systems are backed up and that restoration testing is completed at least annually.

***** Footnote 1**:** The Election Systems & Software for Carson City is administered by the Nevada Secretary of State's Office who is responsible for overseeing and auditing election systems and, therefore, was not included in the scope of this engagement.

Observations

The following table provides our observations from this IT consulting engagement for Management's consideration. We have provided subjective "Risk" and "Effort to Resolve" ratings, based on our professional judgement, to assist management in establishing mitigation priority.

General IT Administration & Governance
Observation 1: A formal risk management program is not in place over information technology. CISA's Cybersecurity Self-Assessment is an example of a formal risk assessment. A formal risk assessment that addresses risks, vulnerabilities, impact, likelihood, and response can help identify IT risk and priorities within the environment. Management noted they intend to complete a formal risk assessment at a future date. Eide Bailly advises the Carson City to continue with completing the IT risk assessment, as planned. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – IT currently has a monthly engagement with CISA. Who is Responsible? – Frank Abella, Andrew Rice, Andrew Kauble. Timeframe? – Current.

Information Security
Observation 2: LandMark password security settings and are not in compliance with industry best practices. Not having application-level password requirements increases the risk of compromised application accounts. Eide Bailly recommends that management considers working with the current vendor to enforce password requirements, or to finalize the current pursuit of a new application. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – Setup 90 Day Password Change process and appropriate user level access. Who is Responsible? – Scott Hoen, (Clerk), Linda Drake (Recorder), and Miguel Camacho (Marriage). Timeframe? – September 15, 2023.
Observation 3: Operating system and LandMark user access reviews are not performed and documented on a regular basis to verify appropriateness of permissions granted based on the user's job duties. Not performing user access reviews can lead to unintended access or privileges if other procedures (such as granting and terminating access) are missed, or if temporary access is not revoked. Eide Bailly recommends that management considers the completion of access reviews, at least annually, and the removal of the unused ADMIN, FORMS, and VERIFY accounts from LandMark. Risk – Medium. Effort to Resolve – High. **Management Response:** What to be Implemented? – Coordinate with Catalis/Landmark the removal of accounts not applicable. Create policy to immediately remove users when employment status changes. Who is Responsible? – Scott Hoen, (Clerk). Timeframe? – October 1, 2023.

Information Security
Observation 4: Administrator access for LandMark is not restricted to authorized and appropriate personnel. Not having the ability to utilize the principle of least privilege for the application can lead to the abuse of privileges, as well as increased risk in the case of a compromised account. Eide Bailly recommends that management considers working with the current vendor to allow for the utilization of least privilege, or to finalize the current pursuit of a new application. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – Work with Catalis/Landmark to define proper admin and user account access and continue to work on new application possibilities. Who is Responsible? – Scott Hoen (Clerk), Linda Drake (Recorder), and Miguel Camacho (Marriage). Timeframe? – October 1, 2023.
Observation 5: Firewall controls including monitoring appear in place. The Clerk-Recorder's Office should consider implementing an independent technical review of firewall rulesets by qualified service providers on an annual basis or as needed pending firewall ruleset firmware and ruleset changes. Not having an independent firewall ruleset increases risk that firmware updates and other necessary configuration changes may be incomplete, increasing risk of security breach. Eide Bailly recommends that management follows through with their scheduled firewall assessment. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – Will work with IT to perform their firewall assessment and updates to the platform on a minimum of an annual basis. Who is Responsible? – Scott Hoen, (Clerk), Linda Drake (Recorder), Miguel Camacho (Marriage). Timeframe? – October 1, 2023.

Information Security
Observation 6: Ongoing monitoring over network capacity and performance is not conducted. Not having a network capacity monitoring dashboard in place necessitates alternate procedures for monitoring performance conditions, capacity, and alerting functions. Eide Bailly recommends that management should continue evaluation and implement an ongoing capacity and performance utility over network. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – IT is currently looking to purchase the right tool. Who is Responsible? – Frank Abella, Andrew Rice, Andrew Kauble. Timeframe? – FY25 OPx.
Observation 7: Data loss prevention tools are in place, but a centralized preventative tool is not. A centralized data loss prevention tool allows IT to monitor critical file movements across the web, cloud, email, network, and endpoints from a single dashboard. Eide Bailly recommends that management finalizes the procurement of ForcePoint software that is currently in process. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – IT currently has implemented ForcePoint this August 2023. Who is Responsible? – Frank Abella, Andrew Rice, Andrew Kauble. Timeframe? – Current.

Change Control, Development and Acquisition
No Findings.

Architecture, Infrastructure, and Operations
Observation 8: Application restoration testing is not performed on a semi-annual basis. Not testing the ability to recover application data can lead to failures and RTO delays when Carson City experiences disasters or breaches. Eide Bailly recommends that management considers testing application restoration at least semi-annually. Risk – Medium. Effort to Resolve – Medium. **Management Response:** What to be Implemented? – IT is currently looking to purchase additional resources to conduct testing without business impact. Who is Responsible? – Frank Abella, Andrew Rice, Andrew Kauble. Timeframe? – FY25 CIP.
Observation 9: Due diligence is not performed to confirm that software vendors who support in-scope significant applications have established appropriate security - specifically over activities related to access control and software development lifecycle. Not performing some continued level of due diligence with the application vendor can lead to the vendor's issues becoming Clerk-Recorder's Office issues. Eide Bailly recommends that management considers semi-annual meetings with the vendor to ensure that the security practices, and operations of the vendor are up to the Clerk-Recorder's Office's expectations. Risk – Medium. Effort to Resolve – Low. **Management Response:** What to be Implemented? – Continue to pursue vendor alternatives and in the meantime, meet with Catalis/Landmark on a semi-annual basis. Have connected with Account Management and waiting on responses for most recent requests. Have connected with Catalis/Landmark IT about updates. Who is Responsible? – Scott Hoen, (Clerk), Linda Drake (Recorder), Miguel Camacho (Marriage). Timeframe? – FY25 CIP and utilize Technology Fund, December/June discussions.

Business Continuity and Disaster Recovery
Observation 10: The DR testing program is not sufficient to demonstrate the organization's ability to meet its continuity objectives. Not having the ability to test all systems for disaster recovery can lead to failures in achieving Carson City's RPO/RTO objectives. The current lack of documentation for DR testing can lead to less communication between IT and leadership, and decreased visibility on what went well and what did not. Eide Bailly recommends that management considers testing DR capabilities for all systems and documenting the process. Risk – Medium. Effort to Resolve – High. **Management Response:** What to be Implemented? – IT is currently looking to purchase additional resources to conduct testing without business impact. Who is Responsible? – Frank Abella, Andrew Rice, Andrew Kauble. Timeframe? – FY25 CIP.

Summary and Conclusion

This report includes specific observations to assist management in evaluating and improving the Information Technology general control environment. This engagement was designed to answer the following questions for management.

- **Did we identify any high-risk areas that deserve management's immediate attention?**

  No – During the consulting engagement, we did not identify issues warranting a high-risk rating. Examples would include deficiencies that might cause inability to maintain adequate levels of security or expose the organization to increased risk of compromise, downtime and / or loss of data.

- **Are controls over information technology and security consistent with the implementation of the Information Security Program?**

  Yes – The Information Security Program (policies, procedures, and guidelines) appears to be consistent with implemented internal control procedures in place at Carson City – County Clerk's Office.

- **What is our assessment of the Information Security Program and IT general controls?**

  Needs Improvement – Although overall general controls are functioning as intended as of the date of our work, improvements are needed to ensure and maintain a strong security posture within the IT environment. Within the IT environment, the Observations provided are intended to enhance procedures and improve overall security posture. At the program operations / application systems level, we advise management to prioritize mitigation over Observation 2, 3 and 4.

Any additional questions may be directed to members of our engagement team listed on the report cover.