DEPARTMENT OF INSPECTOR GENERAL

OKALOOSA COUNTY, FLORIDA

JD PEACOCK II, CLERK OF CIRCUIT COURT AND COMPTROLLER

December 14, 2021

JD Peacock, Clerk of Circuit Court and Comptroller
101 E James Lee Blvd
Crestview, FL 32536

Clerk Peacock,

Please find attached the report on our audit of the Clerk's Information Systems Department.

Our work served as a review of the department's internal controls, policies, and general governance

I want to thank Mike McKillips and his staff for the cooperation and accommodation they afforded us. Should you have any questions in the interim please do not hesitate to call me at (850) 689-5000 Ext. 3424.

Respectfully,

B. Embry

Brad E. Embry, Inspector General

CC: Meribeth Poole, Chief Deputy of Administration
Mike McKillips, Information Systems Director

Okaloosa County
Clerk Of Circuit Court

Department of Inspector General

Report on the Audit of Clerk Information Systems Department

REPORT NO. COC 21-01

REPORT ISSUED DECEMBER 14, 2021

ISSUED BY: BRAD E. EMBRY, INSPECTOR GENERAL

Contents

Executive Summary

We conducted a governance audit of the Clerk of Court Information Systems Department. We examined the processes, procedures, policies, and controls in used by the Department for their conformance with law and best practices and to verify their effectiveness in ensuring the Department meets its objectives. We looked at Department staffing, customer service, data backups, security, and policies.

At the conclusion of our audit, we found the Department to be well-managed, well-controlled, and effective at achieving its objectives. The Department has a successful organizational culture and complies with all applicable laws and Clerk policies. As a result of our audit procedures, we have reported one finding and recommendation, but this relates to a program over which the Information System Department does not have control.

Background

The Clerk-wide risk assessment released by the Department of Inspector General (IG) in October 2020 identified the Information Systems (IS) department as being the highest risk. Our Office's audit work plan for 2021 included an audit of the Information Systems department governance.

Objective

The objective of our governance audit was to examine the department's administrative policies, processes, and procedures to determine efficiency and effectiveness; evaluate the design of, and test the implementation and effectiveness of, internal control within the department; and evaluate the department's assessment of, and response to, risk.

Scope & Methodology

The scope of our audit included all processes in place during our work and all policies and procedures as of the date of this report. Audit methodology included interviews with leadership and staff, process walkthroughs, policy examination, and documenting controls.

Management is responsible for ensuring compliance and adequate safeguarding of public resources from fraud, waste, or abuse. This includes the design, implementation, and maintenance of internal controls relevant to these objectives. This review was conducted in compliance with The International Professional Practices Framework issued by the Institute of Internal Auditors and Principles & Standards for Offices of Inspector General issued by the Association of Inspectors General.

Department Overview

Staffing

The IS department is currently staffed by 8 personnel: A Director, two System Engineers, a Database Administrator, a Software Developer, a Systems Analyst, a Systems Technician, and a Computer Specialist. Each department member has responsibility for specific programs and functions. However, there is significant crossover in duties, creating effective operational redundancy within the department. The director holds weekly staff meetings, and every staff member indicated that they feel departmental leadership is effective and that they receive the support they need.

The Director noted that open positions within the department are often hard to fill, due to both competition with nearby federal government/contractor employers and the frequent ultra-specialization with the IT field that makes hiring a generalist difficult.

Customer Service

The IS department maintains a "help desk" portal that allows Clerk employees to submit tickets for assistance with IT programs and equipment. The Computer Specialist is the primary provider of services based on help desk tickets, but tickets can be worked by any member (often multiple members) of the department if the assistance requested relates to a function or program for which they are responsible.

The help desk portal allows the IS department to communicate directly with the person seeking assistance within the ticket. This enables the department to document all support provided. Additionally, if a department provides assistance to a clerk employee, they may ask the employee to submit a ticket after the fact (or may open and close the ticket themselves) to ensure the work is documented. Because of this, help desk metrics provide both the IS director and Clerk administration the ability to track the performance of the department's customer service function. These metrics can also be used to identify training opportunities and potentially underserved areas within the Clerk's office.

Backups

The IS department utilizes three types of backups: On site, off site, and cloud based. On site backups are maintained at the two courthouse locations. Offsite backups are maintained at a data center in Georgia. Cloud based backups are maintained through Microsoft Azure. The Azure backup is currently not a complete backup, but the department expects the migration to be complete within 1 year. Additionally, the department is currently working to make data backups more in line with statutory and policy retention requirements. This will reduce both the overall volume of data stored as well as the Clerk's legal liability for old data.

Security

Much of the security for the Clerk's general IT systems comes from the procedures and controls native to Microsoft's architecture. Security for other systems is based on industry controls and best practices or is the responsibility of a vendor. All equipment is hardware encrypted, and all off the shelf encryption is evaluated against the department's standards to ensure it meets specified levels of protection.

The IS department is in the process of implementing Center for Internet Security (CIS) Critical Security Controls Version 8. These controls, as described by their issuer, are designed to mitigate the most prevalent cyber-attacks against systems and networks. The expected timeline for full implementation is approximately 1 year from the date of this report.

The department recently obtained a new vendor for organization-wide cybersecurity training. The vendor will provide monthly video training to all Clerk employees. Additionally, the IS department regularly communicates information on threats or specific items of concern to Clerk employees.

Policy

The department's patch management policy states that all patches will be applied in accordance with a defined schedule. The director sends out biweekly emails reminding all users of the policy and the need to log out of systems; the department receives a list of any missed patches and updates and coordinates with those users to ensure the necessary updates are received.

The department also has policies for:

- Elevated Privileges Accounts
- Data Security & Risk Categorization
- Change Management
- Data Encryption

Testing

During our governance audit, we conducted interviews with the Department director and all Department Staff. We examined policies, documented processes, and verified controls. We found no instances of noncompliance with Department or Clerk policy, statutory requirements, or best practices.

Conclusion

In our opinion, the Information Systems Department is well managed, well controlled, and effective at meeting its objectives. The changes that have been made over the past several years since the current department director was hired have been successful at enhancing efficiency and ensuring conformity with industry best practices.

Organizational culture is an important part of both governance and internal control. The IS department director has demonstrated appropriate "tone at the top," and has acknowledged his responsibility for the development and maintenance of internal control. The majority of current department staff has been hired since the current director took over, which has led to significant staff buy-in of the department's culture. The director encourages staff to engage candidly and holds weekly team meetings. Communication, both within the department and with the overall Clerk's office, is effective.

The department should work toward creating formal contingency plans. Though we acknowledge the difficulty of this given the format of some mission-critical programs, it is important to have a formalized, executable plan for both malicious action response and disaster recovery. Because the department has effective backups and restoration capability, we do not feel that this rises to the level of a finding.

Our office will conduct follow-up checks of CIS control progress throughout the implementation process.

The County's external auditors are planning to conduct IT security testing during the current fiscal year. We will review any report produced to determine what effect it has on our office's future consideration of risk.

While the finding presented below relates to a program that is not controlled by the IS Department, the associated recommendation would require IS Department action.

Finding: The lack of administrative independence and inappropriate access levels within Pentamation presents a deficiency in internal control

Risk Factors: The program used by the Clerk's Office for all Clerk and BCC financial transactions and reporting, Pentamation, is controlled completely within the Clerk Finance department. The Finance Director, who reports directly to the CFO, is the system administrator, and possess all system rights and privileges. Additionally, we found that one non-supervisory, staff-level accountant possesses administrative-level, total system access in Pentamation. The finance director is not aware of any transaction logs that would detail the actions of specific users, and the User Documentation provided by Pentamation's vendor does not indicate that any such logs exist. Additionally, the Clerk IS Department has no control or authority over Pentamation.

Mitigation: By design, the system does not allow any user, even one with system administrator rights, to delete individual transactions. The data within Pentamation is regularly backed up as part of the IS department's overall backup process. The IS department is required to create user accounts for the server on which Pentamation is hosted, before a Pentamation user account can be created.

Recommendation: Finance Department and Information Systems Department leadership should work together to strengthen controls over Pentamation and the County's financial reporting. Having full system administration and control over financial processing exist within the Finance Department is an ineffective segregation of duties and creates an internal control deficiency. Administrative permissions over Pentamation should be limited to senior-level management. Allowing staff-level personnel to have administrative access to Pentamation creates an unnecessary risk to the organization. Ensuring proper user-rights and roles are assigned in Pentamation should be considered a high-priority issue.

Management Response

The Information Systems Department is working in conjunction with the Finance Department to implement policies and procedures that are more closely aligned with the security practices of the Clerk's Office. One of the first steps implemented is the revision of the Pentamation access approval workflow and having someone outside of the Finance Department add/modify/remove access rights for users. The Information Systems Department is also working with CentralSquare, the vendor for Pentamation/Finance Plus, to implement relevant security and auditing features for the existing Pentamation installation, as well as the new Finance Plus 5.2 installation, when that project begins. In the interim, existing user account access is being reviewed and modified to more closely reflect the actual access required by the user to complete their work in Pentamation.

Received by email, December 7th, 2021