Reznick Group

ACCOUNTING • TAX • BUSINESS ADVISORY

MANAGEMENT LETTER

COUNTY OF SUTTER

JUNE 30, 2011

County of Sutter

TABLE OF CONTENTS

Reznick Group
ACCOUNTING • TAX • BUSINESS ADVISORY

Reznick Group, P.C.
400 Capitol Mall
Suite 900
Sacramento, CA 95814-4424
Tel: (916) 442-9100

May 31, 2012

To the Honorable Grand Jury and Board of Supervisors
County of Sutter, California

In planning and performing our audit of the financial statement of the County of Sutter (the County), we considered the County's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. We refer you to our Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards dated May 31, 2012, and our Report on Compliance and Requirements Applicable to Each Major and Nonmajor Program and Internal Control Over Compliance in Accordance with OMB Circular A-133 dated May 31, 2012. We did become aware of matters that are an opportunity for strengthening internal controls and operating efficiency.

Reznick Group offers the management report comments below for your review and consideration. We have already discussed these comments with various County personnel, and we will be pleased to discuss them in further detail at your convenience.

This letter is intended solely for the use of the Honorable Grand Jury and Board of Supervisors and management of the County of Sutter and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

Reznick Group, P.C.

Reznick Group, P.C.

County of Sutter

Management Report
Schedule of Current Year Recommendations

For the year ended June 30, 2011

POSTING OF AUDIT ADJUSTMENTS

Criteria

Monitoring of the ongoing financial condition of the County and efforts to budget properly require the accounting records to be accurately recorded.

Condition

At the time of our audit, we noted that the County was in the process of recording the prior year audit adjustments as part of their closing process.

Cause

There is no formal policy to record audit adjustments in a timely manner.

Effect of Condition

Without up to date accounting records it can be difficult to make timely management decisions, including budgeting efforts for subsequent years.

Recommendation

We recommend that the County adopt a policy to record audit adjustments in a timely manner from the date of the financial audit report.

Management Responses

Auditor-Controller's Response

The Auditor-Controller's Office strives to carry out its duties and provide services to taxpayers in a timely manner. Generally, whether this actually happens with regard to any specific task is a function of competing interests and the available resources to complete the task. The Auditor-Controller acknowledges that at the time of the audit, his office was in the process of recording the prior year audit adjustments as part of the closing process. Adopting a "formal policy to record audit adjustments in a timely manner" may have the effect of putting the emphasis on this task when instead it should be subrogated to another task with a higher priority. "Timely" without specific dates or requirements is a relative concept. Prioritizing work is a function of management. It is not clear how adopting the recommended formal policy would be of benefit to the County.

County Administrative Office’s Response

The County Administrative Office agrees with the Independent Auditor’s recommendation.

PAYROLL RECONCILIATIONS

Criteria

Good internal controls require timely payroll reconciliations.

Condition

At the time of our audit, we noted that the County of Sutter had not performed payroll reconciliations, and the reconciliations had to be completed during the performance of our audit procedures.

Cause

The County does not have policies and procedures to enforce payroll reconciliations to occur in a timely manner.

Effect of Condition

Not performing payroll reconciliations creates a weakness in internal control that could result in errors and irregularities not being detected in a timely manner.

Recommendation

We recommend that all payroll reconciliations be completed at the time that each payroll cycle is processed. These reconciliations include but are not limited to the following: Reconciling between the final payroll register and the approved departmental payroll time summary reports. Reconciling between the amounts disbursed from the payroll bank account and the payroll register. Reconciling between the payroll transactions posted to the general ledger and the payroll register.

Management Responses

Auditor-Controller's Response

Procedures have been put in place so that all payroll reconciliations will be completed at the time each payroll cycle is processed.

County of Sutter

Management Report
Schedule of Current Year Recommendations - Continued

For the year ended June 30, 2011

County Administrative Office’s Response

The County Administrative Office agrees with the Independent Auditor’s recommendation.

CAPITALIZATION POLICY

Status

This finding has not been implemented.

Criteria

Generally accepted accounting principles require that capital assets, that generally constitute the single largest asset of the County, be accurately recorded.

Condition

At the time of our audit, we noted that the County did not have a formal capitalization policy that addressed infrastructure assets or estimated useful asset lives. In fiscal year 2006, the County issued a memorandum revising the estimated life of a road from 15 to 30 years. However, this information, along with the details of a complete infrastructure accounting system, has never been formalized into a comprehensive infrastructure capitalization policy.

Cause

The County has not yet written a formal policy for the capitalization of infrastructure.

Effect of Condition

Without a written capitalization policy which addresses infrastructure and estimated useful asset lives, inconsistencies and misunderstandings regarding proper policy are likely to occur. In addition, misstatement of net capital assets as well as a lack of comparability between years can result when policies and procedures regarding capital assets are unclear.

Recommendation

We recommend that the County adopt a comprehensive updated capitalization policy which includes all required capital asset accounting elements including infrastructure and estimated useful asset life. This project will likely involve the combined efforts of the Auditor-Controller, County Administrative Officer and Public Works departments. This is a repeat of a prior year recommendation.

County of Sutter

Management Report
Schedule of Prior Auditor Comments - Continued

For the year ended June 30, 2011

Management Responses

Auditor-Controller’s Response

The Auditor-Controller agrees.

County Administrative Office’s Response

The County Administrative Office agrees with the Independent Auditor’s recommendation.

PERSONNEL BENEFITS TRUST

Status

This finding has not been implemented.

Criteria

Good internal control requires reconciliation of all trust funds.

Condition

We noted that the Personnel Benefits Revolving Trust fund (Fund 5226) had not been reconciled.

Cause

The staff assigned to reconcile the accounts does not have the appropriate training or expertise for such a task.

Effect of Condition

Without monthly trust account reconciliations of all payroll trusts, errors and irregularities could occur and not be detected in a timely manner.

Recommendation

We recommend that the unresolved differences be resolved and any inactive accounts be closed. This is a repeat of a prior year recommendation.

Management Response

Auditor-Controller's Response

The Auditor-Controller agrees.

County Administrative Office's Response

The County Administrative Office agrees with the Independent Auditor's recommendation. All benefits accounts will be reconciled as of June 30, 2012.

County of Sutter

Management Report
Schedule of Prior Auditor Comments - Continued

For the year ended June 30, 2011

The County contracted with a consultant to work with the Human Resources Department to reconcile the benefits accounts and to train staff. During Fiscal Year (FY) 2010-11 all inactive accounts were closed. No inactive accounts remained open in the financial system as of June 30, 2011. The reconciliation of the remaining active benefits accounts is still in progress and will be completed prior to June 30, 2012. Any identified unresolved differences will be brought to the Board of Supervisors prior to June 30, 2012. Additionally, the Human Resources Department has recently hired a new Benefits Manager. That individual is tasked with implementing policies and procedures to reconcile remaining active accounts on a monthly basis.

2011 Information Technology (IT) Observations

Access Controls

Observation

1. Available security settings on the Windows servers do not require users to change their passwords periodically, and passwords are not required to be complex; other parameters, such as password history and minimum age are not consistent with current security practices. On the AS400, users are also not required to change their passwords periodically, passwords are not required to be complex, and password length of only one character is required.

2. Although Reznick Group was informed that IT disables user IDs whenever they are notified of an employee termination, there is not an established, consistently followed mechanism to ensure IT is notified immediately of all personnel terminations (employees, temporary workers, volunteers, contractors, etc.). Reznick Group observed that several terminated employees had access to the IFAS Financial application.

3. User's access rights for the servers (Windows, Unix, and AS400) and applications are not reviewed periodically.

Risk

1. Passwords are the first line of defense to help protect unauthorized access to the County's servers, applications, and data. Without enforcing password changes, history, minimum age, and complexity, passwords can be more easily guessed and are more vulnerable to repeated password attempts from unauthorized individuals. The combination of these deficiencies increases the risk that passwords can be more easily compromised, resulting in unauthorized or inappropriate access to the County's computer resources and data.

2. Without a defined and consistently followed process to ensure computer access is revoked in a timely manner for terminated personnel, there is little or no assurance that terminated personnel do not have continuing access to the County's servers, applications, and data.

3. Without a periodic review of user's rights, there is an increased risk that a user might have access that is consistent with their current job responsibilities or that a terminated employee might continue to have server and application access.

Recommendation

1. Management should configure the security settings available on their existing servers and applications to at least the security level typically found on today's computer systems, including requiring periodic password changes, implementing a longer minimum password length, enforcing a minimum age, and requiring password complexity.

2. Management should establish, document, and implement a process to ensure timely notification and revocation of system access for all terminated personnel.

3. Management should implement a process to periodically review all users' access rights for the servers and applications. The review should be documented to provide evidence that it was performed, and to help ensure potential exceptions noted during the review are researched and resolved timely.

Management Response

County Administrative Office's Response

The County Administrative Office and the Information Technology Department appreciate the observations of the outside financial auditors, and will take the recommendations under advisement. In 2008, the Board of Supervisors commissioned a complete Management Audit of the Information Technology Department. The County has been following recommendations made during that audit; however, budgetary constraints subsequent to that time have limited the County's ability to take specific and/or broad action. Any action to be taken as a result of the 2008 management audit or the Reznick group's observations will be coordinated with the Information Technology Department and other County departments, and will be reported and recommended directly to the Board of Supervisors.

The Information Technology Department has responded to most of the Independent Auditor's observations in the paragraphs below. Responses to the observations regarding "Access Controls" and "Security Testing" have been omitted because making that information available for public disclosure could pose a severe security risk for the County. Nevertheless, the I.T. Department has reviewed the Independent Auditor's recommendations thoroughly and will take appropriate action.

Application Controls and Segregation of Duties

Observation

The Financial and Payroll applications have not been configured to enforced segregation of duties; all individuals in the Auditor-Controller's department have update access to all IFAS Financial application activities, and all Payroll individuals have access to perform all Payroll application activities.

Risk

Dividing responsibilities and activities within a process such that one person does not control all aspects of the process, referred to as segregation of duties, is one of the basic tenets of good control. The individuals with update access can perform all accounting activities in the application, as well as make changes to the application, all with no application enforced segregation of duties.

When job responsibilities and application access are assigned in such a way that all individuals have access to perform all aspects of a process or cycle, there is an increased risk of errors or omissions and automated controls and application workflows may not operate effectively. There is also an increased opportunity for unauthorized transactions or fraud to go undetected.

Recommendation

Management should establish roles within the County's applications that will help ensure individuals only have access to the application resources needed to perform their responsibilities and in such a manner so as to enforce appropriate segregation of duties.

Management Response

Information Technology Department Response

The IT Department will assist County Departments in reviewing access rights in their systems.

Security Testing

Observation

Independent IT security testing, including penetration tests of the County's firewalls, is not performed periodically.

Risk

A penetration test is a technique to identify potential hardware and software security vulnerabilities so that flaws and configuration weaknesses can be corrected. Without independent IT security testing being performed on a regular basis, it is difficult to know if the County's firewalls and other system security provisions are adequate and are configured to provide appropriate protection, or that data is secure from unauthorized access and possible modification.

Recommendation

Management should schedule external IT security testing, and once it has been performed address any identified issues in a timely manner to help ensure the protection and integrity of the County's systems and data.

Management Response

See County Administrative Office's response above.

IT Strategic Planning and Risk Management

Observation

1. The County does not have an IT strategic plan, and an active IT steering committee, or another IT planning and prioritizing process, has not been formally established.

2. IT risk assessments are not formally performed. As such, IT related risks are not formally documented, evaluated and addressed periodically.

Risk

1. Without establishing an IT strategic plan, and documenting the IT strategic planning and prioritizing function and activities, there is an increased risk that IT initiatives are not aligned with needs and priorities of the County. An IT Steering Committee is an approach that is commonly used to help ensure alignment and prioritization of IT and business strategies, priorities, expenditures, and activities.

2. Without performing formal periodic risk assessments, it is difficult to ensure that all relevant risks are being comprehensively identified, prioritized, and appropriately addressed in a timely manner. Various concerns and control deficiencies noted in this report might have been identified if the County was performing routine IT risk assessments.

Recommendation

1. Management should create and document an IT strategic planning and prioritizing function, and consider establishing an IT Steering Committee with a charter that defines membership, responsibilities, authorization, reporting, and accountability. This will help ensure that IT projects and future capabilities are in line with the current and future needs of the County's priorities and obligations.

2. Management should create and document a formal risk assessment process. A schedule should also be established to help ensure that comprehensive risk assessments are performed regularly with a process to ensure the risks are escalated and prioritized, and that corrective actions are completed timely to address identified risks.

Management Response

Information Technology Department Response

1. The IT Strategic Plan and IT Information Security plan have been drafted. The IT Steering Committee was established in 2008, but has not met in the recent past due to changes of representatives and the loss of the IT Department's management-level Deputy Director position, which was allocated time to lead the project. Revised plans and policies are currently being drafted, and the Steering Committee will be engaged in the review and finalization process once the plans and policies are complete.
2. Draft policies have been developed for business continuity and business resumption. These processes, along with risk assessment, must be driven by the business units of the County, where the IT component of their business should be formally assessed.

Change Management

Observation

1. A mechanism is not in place to ensure all application programming changes were authorized as IT personnel that make changes to application programs also move those changes into production.

2. Evidence of testing and user acceptance is not always obtained and maintained for changes to the County's applications.

3. Changes to information systems, including applications, servers, network, etc., are not consistently tracked in a centralized location.

Risk

1. Not restricting programmers from having the ability to make changes to application programs in production increases the risk of inappropriate or unauthorized changes, and of changes being made that have not gone through the appropriate testing and approval process that may compromise application and data integrity and availability.

2. Without evidence of testing and user acceptance, it is more difficult to demonstrate that testing was completed before changes were moved into production.

3. Without tracking changes it is more difficult to easily identify what changes were made, when, and who authorized and who made the changes.

Recommendation

1. The application development and programming activities should be segregated from operational activities, and programmers should not be granted access that allows them to make changes directly to the production environment, bypassing standard checks and balances (provisions should be made for emergency access that ensures accountability and oversight).

   If management determines that implementing traditional segregation of duties is not feasible, then management should implement independent logging of privileged access with independent review and monitoring to reduce the risk that the excess system access can be exploited.

2. Management should implement a process to ensure evidence of testing and user acceptance of all application changes is obtained and tracked.

3. Management should implement a process to track all changes. This could potentially be accomplished using the County's existing ticketing application.

Management Response

Information Technology Department Response

1. Due to extremely limited resources and reduced IT Department staffing levels, achieving the suggested separation of duties within the IT department is not currently possible. Departments are responsible for reviewing the results of changes and identifying any misunderstandings or errors that may occur as a result of the development process.
2. The IT Department tracks all activities through an on-line trouble ticket system. Each ticket sends a query to the requester regarding the work requested. The IT Department will add an additional question to the trouble-ticket system in order to document user acceptance.
3. This suggested process is already in place. Management will re-emphasize the importance of tracking activities with the existing system.

Disaster Recovery/Business Continuity Planning

Observation

1. Although some provisions have been made, the County does not have a documented disaster recovery/business continuity plan for its IT resources.

2. The County also does not have documented departmental disaster recovery/business continuity plans for resuming business operations.

3. Comprehensive tests of the County's disaster preparedness provisions are not performed periodically.

Risk

Without formally documented and tested disaster recovery/business continuity plans, there is only limited assurance that the County could resume normal operations in a timely manner, if at all, following a disaster or interruption in normal services.

Recommendation

1. Management should perform a business impact analysis to determine the risk of not having disaster recovery/business continuity plans, including establishing the maximum acceptable outage.

2. Based upon this analysis, the County should develop strategies and document a set of comprehensive disaster recovery and business continuity plans to help ensure the County is ready to resume an acceptable level of operations within an acceptable period of time following a disaster.

3. Once plans have been documented, they should be tested periodically and updated as needed.

Management Response

Information Technology Department Response

1. This task must be driven by the individual business units (County departments), with the IT Department's assistance. Technology is only one component of a Disaster Recovery/Business Continuity plan. Without specific departmental plans, the IT Department has no parameters around which to develop a comprehensive plan.
2. County-wide comprehensive plans fall outside the responsibility of the IT Department.
3. Agreed.

IT Policies and Procedures

Observation

Although some IT related policies and procedures have been drafted, most have not been finalized, approved, communicated, and implemented, and policies and procedures have not been formally addressed for many areas.

Risk

Documented policies and procedures help ensure consistent execution of management's intentions, help enforce compliance, facilitate training, serve as a daily reference, and can be used to help measure individual performance. Without documented policies and procedures there can be delay and loss of productivity in case of emergency or absence of staff. This risk is increased in smaller departments where the loss or unavailability of a single key employee can have catastrophic consequences.

Recommendation

Management should document IT policies and procedures, and implement a process to periodically review, update and disseminate them as needed. Some areas to consider when developing IT policies and procedures include:

- Appropriate computer, Internet and email use
- Control and custody of personally identifiable information
- Granting, monitoring, terminating and periodically reviewing system access
- Password administration and configuration requirements
- Security monitoring and incident escalation
- System administration activities
- System and application change controls
- Testing, authorizing, and applying system and application changes, upgrades and patches
- Scheduling, communicating and performing maintenance activities
- Periodic review of system parameters
- Capacity and performance monitoring and planning
- Data backup, archival and retention schedules
- Controls surrounding critical spreadsheets or other end-user computing

Management Response

Information Technology Department Response

Each of these areas will be addressed during the Department's next policy review.

Problem Reporting and Tracking

Observation

The County maintains a ticket tracking system to help track reported problems, requests for assistance, system enhancements, and other IT related activities. Reznick Group observed that some tickets classified as "Pending" in the tracking system date back to 2006, and was told that the Pending category is used to designate tickets that have not been fully resolved (such as a problem assigned to an analyst, work in process, problem reported to a vendor, holding due to lack of funding, future system enhancements, etc.).

Risk

With the number and age of tickets classified as Pending, it is difficult to determine which tickets are still current and potentially in need of more immediate attention or escalation, or to ensure that reported problems are being resolved in a timely manner.

Recommendation

Management should consider adding an additional ticket category to make is easier to determine which tickets should be given immediate attention.

Management Response

Information Technology Department Response

This recommendation has been implemented.