

**The Sutter County  
Board of Supervisors' Response to the  
ENDORSED FILED**

**2013-2014**

OCT 02 2014

SUPERIOR COURT OF CALIFORNIA  
COUNTY OF SUTTER  
CLERK OF THE COURT  
By JACKIE LASWELL Deputy

**Sutter County Grand Jury  
Final Report**



Ronald Sullenger	District No. 1
Stanley Cleveland, Jr.	District No. 2
Larry Munger	District No. 3
Jim Whiteaker	District No. 4
James Gallagher	District No. 5

*County of Sutter*  
*Office of the County Administrator*

*... established 1850*

September 30, 2014

The Honorable Susan E. Green  
Presiding Judge of the Sutter County Superior Court  
466 Second Street  
Yuba City, CA 95991

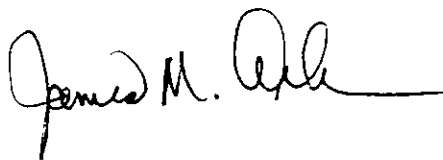
Dear Judge Green:

On behalf of the Sutter County Board of Supervisors, I am herewith submitting its response to the findings and recommendations of the 2013-2014 Grand Jury.

The Board of Supervisors appreciates the dedicated efforts of the 2013-2014 Grand Jury in the preparation of its report and the complimentary comments it made with respect to the County and its employees, and trusts that you will find the enclosed material responsive.

I would be happy to meet with the Grand Jury to discuss any or all of these issues.

Sincerely,



JAMES M. ARKENS  
County Administrative Officer

JMA/SMC/lb

**TABLE OF CONTENTS**

County Reorganization: Development and General Services Departments.....4  
Sutter County Information Technology Department.....5

## **County Reorganization Development and General Services Departments**

### **Discussion:**

*The Grand Jury conducted a review of Sutter County's reorganization of the Development Services and General Services Departments.*

*The Grand Jury interviewed nine Sutter county employees that were involved in the reorganization, and reviewed the initial written proposal made to the Board of Supervisors regarding the reorganization as well as all further proposals made regarding additional staff requests.*

*The Grand Jury reported that staff from both departments reported that communication between line staff and management has improved through the reorganization. They also reported that morale is improving. There is more access to the supervisors and upper management as staff are now housed together. By allowing staff more access to management, they are able to communicate more effectively.*

### **Response from the Board of Supervisors:**

**The Grand Jury did not issue Findings or Recommendations regarding the County reorganization of the Development Services and the General Services Departments.**

**The Board of Supervisors thanks the Grand Jury for its detailed review and comments.**

## **Sutter County Information Technology Department**

### **Grand Jury Finding #1:**

*The Information Technology Department is not in compliance with the 2011-2012 [sic] Audit Report.*

### **Response from the Board of Supervisors – Grand Jury Finding #1:**

The Board of Supervisors agrees in part with the finding. The County's former independent auditing firm issued an Information Technology Observations review as part of the 2010-11 Audit Report. The observations and recommendations were reprinted, with status updates, in the 2011-12 Audit Report. A copy of the original Observation Report from the 2011-12 Audit Report is attached to this response for reference.

The County's Information Technology Department was reorganized in 2013, and, effective July 1, 2013, became part of the newly organized General Services Department. The General Services Department Information Technology Division (General Services/IT) has made significant strides to address the observations and recommendations as laid out in the Grand Jury Report. The following is a summary response from General Services/IT indicating the Department's progress to date.

### **ACCESS CONTROLS**

In January of 2014, General Services/IT began implementation of a new password policy for all Sutter County Domain and AS/400 accounts. This policy has now been fully implemented. Account passwords must now be changed at routine intervals, and will need to adhere to password complexity criteria.

### **APPLICATION CONTROLS and SEGREGATION OF DUTIES**

Over the course of the last few months, IFAS (the County's financial system) security has been completely revamped. Every IFAS role and account has been re-evaluated and access to IFAS has been restricted based on the individual user. Our team continuously monitors and updates IFAS security, proactively.

### **SECURITY TESTING**

In May of 2014, Sutter County became an official member of the Multi-State Information Sharing & Analysis Center (MS-ISAC). The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, tribal and territorial governments. Collaboration and information sharing among members, private sector partners, and the U.S. Department of Homeland Security are the

keys to success. The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery. The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

## **IT STRATEGIC PLANNING AND RISK MANAGEMENT**

In May of 2014, General Services/IT worked with Curt Dodds (IT Strategy Consultant) to develop an IT Strategic Plan. The first draft and IT's response are already complete and the Department is awaiting a final draft. A Strengths/Weaknesses/Opportunities/Threat (SWOT) analysis was performed with IT staff, led by Mr. Dodds. Political/Economical/Social/Technological (PEST) analysis was used to help identify opportunities and threats within the SWOT analysis. Opportunities and threats were then prioritized based on input from the group. Using the prioritized opportunities and threats, Mr. Dodds produced a plan, drawing on his IT experience and using the Good Strategy/Bad Strategy approach of UCLA professor Dr. Richard Rumelt.

## **CHANGE MANAGEMENT**

General Services/IT has implemented change management systems for critical infrastructure (network and servers/clients).

### **Grand Jury Recommendation #1:**

*The Sutter County Grand Jury recommends that the IT Department request additional funding in order to comply with the 2011-2012 [sic] Audit Report.*

### **Response from the Board of Supervisors – Grand Jury Finding #1:**

The Board of Supervisors agrees in part with the recommendation.

The Board of Supervisors has committed additional resources to General Services/IT priorities, including the strategic planning efforts conducted over the past year. The Board has acknowledge the varied needs of the Department, and understands that those needs must also be balanced against the requirements for funding programs and functions within other areas of the County. Continued budget constraints and the competing priorities of the County are expected to continue for the foreseeable future, and will force the County to make difficult decisions regarding funding any new programs and efforts.

# Sutter County

---

## Prior Year Information Technology (IT) Observations

### Access Controls

#### Status

Based on inquiry with the IT department the access control observations and recommendations from the prior year are in process of implementation at June 30, 2012, however, they have not been fully implemented.

#### 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.

# Sutter County

---

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

### *Prior Year 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.

### *2012 County Administrative Office's Response*

Management response has not changed from the prior year.

## **Application Controls and Segregation of Duties**

### Status

Based on inquiry with the IT department the application controls and segregation of duties observations and recommendations are on hold pending migration to new systems at June 30, 2012.

### 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



# Sutter County

---

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

### ***Prior Year Information Technology Department Response***

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

### ***2012 Information Technology Department Response***

Management response has not changed from the prior year.

## **Security Testing**

### Status

The security testing observations and recommendations are on hold as there has been no budget allocated to address this item at June 30, 2012.

### 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.

# Sutter County

---

## IT Strategic Planning and Risk Management

### Status

Based on inquiry with the IT department the IT strategic planning and risk management observations and recommendations are in process of implementation at June 30, 2012, however, they have not been fully implemented.

### 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

#### ***Prior Year 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

# Sutter County

---

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.

## ***2012 Information Technology Department Response***

Management response has not changed from the prior year.

### **Change Management**

#### Status

Based on inquiry with the IT department the change management observations and recommendations 1 and 2 have not been implemented as of June 30, 2012. Observation and recommendation 3 has been implemented as of June 30, 2012.

#### 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).

# Sutter County

---

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

### *Prior Year 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.

### *2012 Information Technology Department Response*

Management response has not changed from the prior year.

## **Disaster Recovery/Business Continuity Planning**

### Status

Based on inquiry with the IT department the disaster recovery / business continuity planning observations and recommendations have not been implemented as of June 30, 2012.

### 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.

# Sutter County

---

## 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

### ***Prior Year 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.

### ***2012 Information Technology Department Response***

Management response has not changed from the prior year.

## **IT Policies and Procedures**

### Status

Based on inquiry with the IT department the IT policies and procedures observations and recommendations have not been implemented due to lack of staffing at June 30, 2012.

### 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

# Sutter County

---

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

### ***Prior Year Information Technology Department Response***

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

### ***2012 Information Technology Department Response***

Management response has not changed from the prior year.