



OFFICE OF INTERNAL AUDIT

REPORT TO THE BOARD OF SUPERVISORS

Pinal County Information Technology

General Controls Audit

Follow-up Review

June 2011

Lori Stripling, Internal Audit Officer
Kate Witek, Internal Auditor
Jason Konrad, Internal Audit Analyst

In August, 2010, Pinal County Office of Internal Audit (Internal Audit) released the Information Technology (IT) Department General Controls audit and concluded the department had established controls over a majority of the areas tested and most controls were working effectively. Internal Audit identified weaknesses in access and security controls; equipment tracking; business contingency planning; and IT governance; and offered seventeen recommendations to reduce risks and improve business processes.

Internal Audit has completed a follow-up review of the Information Technology (IT) Department General Controls audit and determined the Information Technology Department made admirable progress in implementing prior report recommendations.

Of the seventeen (17) recommendations suggested, IT has completed nine (9) and partially completed six (6), with notable achievement in the following areas:

- Establishment of Standard Operating Procedures
- Review of user profiles and purging of Inactive AS/400 Accounts
- Implementation of Login restriction for Security Officer Profile with Super User Access
- Activation of application audit journals and standard security groups
- Implementation of offsite storage for sensitive back up data

According to the Chief Information Officer (CIO), recommendation number ten (10) could not be completed due to a lack of “staff resources or in-house skill set” and budget constraints on additional hiring. This recommendation proposed the CIO “designate one System Security Officer to ensure comprehensive security for county information systems and maintain regular monitoring of all IT security policies and procedures.” **These duties are of critical importance and Internal Audit recommends the Chief Information Officer consider additional security training for a current employee.**

The remaining recommendation (#6); *to require all IT personnel with access to critical data undergo background screenings*, will not be implemented. County Attorney staff have advised against “changing the terms and conditions of employment,” for these employees and stated it is not necessary, “...unless there is an articulable reason for requesting a background investigation after an employee has been working problem-free.” IT will continue to follow the Background Investigations policy for newly hired employees.

The following matrix provides details of management’s reported progress. We would like to thank the Information Technology Department for their assistance during our follow-up review.

Lori Stripling
Pinal County Internal Audit Officer

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p>1. The Chief Information Officer should implement compensating controls to offset improper segregation of duties for staff assigned to work with financial systems. Compensating controls should include regular review of system logs.</p>	Yes	<p>IT has hired Security Consultants to help evaluate Application security and AS400 Server security to create system logs and standard security groups.</p> <p>Action Plan Deliverables: SOP to review server log. Turn on JD Edwards application audit log. SOP to review key functions within the application log.</p>	12/31/10	<p>Doyle Johnson – JDE application audit logging. SOP for reviewing key functions as determined by best practices.</p> <p>Jay Vargo – Server log review for key functions as determined by best practices.</p>	<p style="text-align: center;">Complete</p> <p>Security logs have been turned on and SOP's have been created.</p>
<p>2. The Chief Information Officer should require all system personnel with security responsibilities to immediately conduct a review of all user profiles and system values. System values and user profiles should be:</p> <p><i>a. Set to allow access to necessary functions only</i></p> <p><i>b. Purged or disabled if they are no longer active</i></p>	Yes	<p>IT staff have purged user accounts that have never logged into and have not logged into for 180 days for the AS400/JDE.</p> <p>Action Plan Deliverable: A review of “super setting” AS400 accounts to ensure access to necessary functions only.</p>	12/31/10	<p>Jay Vargo – Review of “super setting” profiles.</p> <p>Doyle Johnson – Confirmation of “super settings” for application support staff.</p>	<p style="text-align: center;">Complete</p> <p>IT staff purged inactive user accounts, and SOP's have been created.</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>3. The Chief Information Officer should require individuals, who sign on to financial systems using a security officer profile with super user access, to sign on at one designated and monitored computer. Setting system controls to limit users with extraordinary access to sign on at a certain workstation lessens the chance of unauthorized user access to sensitive information.</i></p>	Yes	<p>Action Plan Deliverable: Limit QSECOFR profile to only logon from AS400 console.</p>	10/31/10	Rodney Banks	<p style="text-align: center;">Complete</p> <p>The QSECOFR profile (security officer profile with super user access) can only be used from the AS400 console.</p>
<p><i>4. The Chief Information Officer should ensure employees in all county departments are trained to lock personal computers when not in use (CTRL+ALT+DEL; select Lock Computer) to discourage unauthorized access to county computers.</i></p>	Yes	<p>Action Plan Deliverable: A "Lock Computer" section will be included in a County Password Policy for approval by the BOS. Rather than training end users this can be a system enforced policy. This may cause issues within business units which have users that share computers.</p>	12/31/10	Richard Jones	<p style="text-align: center;">Complete</p> <p>Per the CIO, as of Monday May 9th, 2011, computers in departments identified as high risk (Budget, HR, Finance, IT, and Treasurer) will automatically lock after 15 minutes of inactivity. The CIO should consider implementing this county-wide.</p>

Information Technology Follow-up
Management's Response and Action Plan
May 2010

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>5. The Chief Information Officer should require all system personnel with security responsibilities to immediately activate the audit journal for all systems with these capabilities. System values should be set at recommended levels/values.</i></p>	Yes	<p>Specific audit journaling for applications that have these capabilities will be turned on.</p> <p>Action Plan Deliverable: List of applications with journaling capability and specific events being journaled.</p>	12/31/10	Doyle Johnson Jay Vargo	<p style="text-align: center;">Complete</p> <p>Journals for all systems (with these capabilities) have been turned on.</p>
<p><i>6. The Chief Information Officer should require all IT personnel with access to critical data immediately undergo background screenings, including criminal history checks.</i></p>	Yes	<p>Draft policy will be developed once Human Resources and County Attorney advise.</p> <p>Action Plan Deliverable: NA</p>	TBD	Richard Jones	<p>The email, located in the row below, was sent from Wendy Peterson, Civil Division, County Attorney's Office, to Bob Calloway, Employee Relations Division, Human Resources, regarding this recommendation.</p>
<p><u>County Attorney's office advisory email -</u></p> <p><i>"I've reviewed Pinal County's policy on Background Investigations, 3.05. The policy states that a background investigation on current employees is appropriate in only limited circumstances. A background investigation will be conducted on a current staff employee if he/she is transferring into a position where a background investigation is required and if a background investigation was not done when the employee was hired initially. A background investigation will not be conducted for an employee transferring to the same classification (same duties, responsibilities) in the same unit. In my opinion, unless a current employee is transferring into a new position the policy does not apply. Additionally, if an employee was hired without a background check (and there hasn't been a problem with that employee) s/he doesn't have an expectation that s/he will be subject to a background investigation. In other words, we would be changing the terms and conditions of employment. Additionally, the purpose of running a background investigation seems to be to eliminate potential employee or security problems. Unless there is an "articulable" reason for requesting a background investigation after an employee has been working "problem free" I don't see a legitimate reason for conducting one (other than the stated reason for investigating a current employee [i.e., transferring into a new position]). In any event, in that situation it seems to me that there are other mechanisms in place for investigating a current employee (e.d., an Administrative Investigation). Let me know if you have any other questions."</i></p>					

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p>7. <i>The Chief Information Officer should develop a policy and procedure requiring accurate and comprehensive documentation and monitoring of the background screening process for all IT employees. This should include a requirement for immediately notifying PCSO when an IT employee with ACJIS authorization is terminated, so the employee can be removed from the ACJIS approved access list.</i></p>	Yes	<p>Current background checks are monitored by Pinal County Human Resources. If IT is required to have ongoing background checks for all staff a policy and procedure will need to be implemented.</p> <p>Action Plan Deliverable: Update current IT Policy 1.13 to include monitoring and updating PCSO when IT staff members are terminated.</p>	10/31/10	Jay Vargo Brian Kreklau	<p style="text-align: center;">Complete</p> <p>IT created a knowledge document/procedure and SOP for notifying PCSO when an IT employee is terminated.</p>
<p>8. <i>The Chief Information Officer should require all system administrators immediately review user lists and purge inactive user profiles and terminated employees' user profiles.</i></p>	Yes	<p>IT staff has purged user accounts that have never logged into and have not logged into for 180 days for the AS400/JDE. New Project Proposal is being developed by IT to implement electronic workflows.</p> <p>Action Plan Deliverable: Purge terminated users from systems with unique usernames. SOP to notify system administrators when employees are terminated.</p>	12/31/10	Jay Vargo Doyle Johnson	<p style="text-align: center;">Complete</p> <p>IT created a SOP and knowledge document/procedure on how to generate application lists.</p> <p>Verified AS/400 purged accounts.</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p>9. <i>The Chief Information Officer should develop a comprehensive enterprise password management policy and distribute to all systems personnel and Pinal County departments. Policies should follow NIST recommended guidelines.</i></p>	Yes	<p>A password policy should be formally written and approved. However, meeting all NIST recommendations will cause users to begin writing their passwords down in order to remember them.</p> <p>Action Plan Deliverable: A password policy that meets the needs of the County and follows best practices while working with all system password limitations for BOS approval.</p>	12/31/10	Richard Jones	<p style="text-align: center;">Partially Complete</p> <p>Per the CIO, the password policy and implementation should be rolled out within a few months to the high risk departments.</p> <p style="text-align: center;">Specific password criteria was provided.</p>
<p>10. <i>The Chief Information Officer should designate one System Security Officer (SSO) responsible to ensure comprehensive security for county information systems and maintain regular monitoring of all IT security policies and procedures.</i></p>	Yes	<p>Currently Pinal County IT does not have the staff resources or in house skill set to designate a System Security Officer.</p> <p>Action Plan Deliverable: Submit a request to County Manager for position.</p>	TBD	Richard Jones	<p style="text-align: center;">Incomplete</p> <p>The position was not funded for Fiscal Year 2011/2012.</p> <div style="text-align: center; border: 2px solid black; background-color: #92d050; padding: 5px; margin: 10px 0;"> <p>FOLLOW UP RECOMMENDATION</p> </div> <p>The Chief Information Officer should consider additional security training for a current employee</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>11. The Chief Information Officer should assign immediate duties to the SSO to work with all county departments to integrate IT solutions into ongoing COOP's including, but not limited to, identifying secure offsite storage for sensitive back up data.</i></p>	Yes	<p>Currently Jay Vargo and Richard Jones are responsible for working with Departments and their COOP planning.</p> <p>Action Plan Deliverable: Offsite data backup location SOP</p>	10/31/10	Jay Vargo	<p style="text-align: center;">Complete</p> <p>Although the SSO position was not funded for the upcoming Fiscal Year, secure offsite storage for sensitive back up data has been identified and is now being used. Further, a draft SOP is in the process of being finalized.</p>
<p><i>12. The Chief Information Officer should develop comprehensive written policies for all inventory/fixed asset tracking procedures, to include use of the new barcode tracking system process and ensuring appropriate staff training.</i></p>	Yes	<p>Action Plan Deliverable: Asset tracking SOP</p>	10/31/10	Richard Jones Angie Woods	<p style="text-align: center;">Complete</p> <p>IT created a SOP for IT Asset Tracking and Equipment Inventory Changes. They are also in the process of implementing software that tracks computers by serial number.</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>13. The Chief Information Officer should ensure the fixed asset list is complete and accurate. This should include preliminary communication with the Finance department to ensure lists are comprehensive and regular monitoring to ensure lists are accurate.</i></p>	Yes	<p>In the past, regular monitoring of fixed assets has not been possible due to Finance only providing asset information once a year. Duties have been assigned to new staff member starting August 9, 2010</p> <p>Action Plan Deliverable: Work with Finance to insure asset management program is followed.</p>	7/1/11	Angie Woods	<p>Partially Complete</p> <p>Fixed asset inventory is currently in process.</p>
<p><i>14. The Chief Information Officer should develop and implement a comprehensive software asset management program.</i></p>	Yes	<p>Duties have been assigned to new staff member starting August 9, 2010</p> <p>Action Plan Deliverable: Software asset management program</p>	7/1/11	Angie Woods	<p>Partially Complete</p> <p>Software License inventory is currently in process.</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>15. The Chief Information Officer should designate a team of IT security personnel, including members supporting all current platforms, and assign duties to develop detailed contingency plans for identified high-risk circumstances. NIST, and many other websites, provide guidance and tools (templates, etc.) to facilitate this effort.</i></p>	<p>Yes</p>	<p>System Recovery Team is in place and hold monthly meetings to discuss current system requirements for system recovery. NIST guidelines are being used.</p> <p>Once department COOP plans are completed IT System Recovery Team will begin the task of contingency planning with all application owners.</p> <p>Action Plan Deliverable: IT Contingency Plan for County Systems</p>	<p>6/30/12</p>	<p>Richard Jones</p>	<p>Partially Complete</p> <p>Future Target Date</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>16. The Chief Information Officer should assign IT security personnel to work with other county departments to ensure ongoing county-wide continuity of operations planning (COOP) includes collaborative and effective use of IT resources.</i></p>	<p>Yes</p>	<p>System Recovery Team is in place and holds monthly meetings to discuss current system requirements for system recovery. NIST guidelines are being used. Once department COOP plans are completed IT System Recovery Team will begin the task of contingency planning with application owners. Currently Jay Vargo and Richard Jones are responsible for working with County Departments and their COOP plans.</p> <p>Action Plan Deliverable: IT Contingency Plan for County Systems</p>	<p>6/30/12</p>	<p>Richard Jones</p>	<p>Partially Complete</p> <p>Future Target Date</p>

**Information Technology Follow-up
Management's Response and Action Plan
May 2010**

Audit Recommendation	Concur (Yes or No)	Management's Response and Action Plan	Target Date	Individual(s) Responsible	Internal Audit Assessment
<p><i>17. The Pinal County Board of Supervisors should adopt an IT governance policy that establishes a countywide IT governance leadership committee and directs the committee to:</i></p> <ul style="list-style-type: none"> <i>a. Establish a countywide IT strategic master plan</i> <i>b. Establish guidance on how IT resources will be collaboratively approved and managed.</i> <i>c. Develop county-wide IT security policies.</i> 	Yes	<p>Action Plan Deliverable: Work with Assistant County Manager to develop IT Governance Policy</p>	7/1/11	Richard Jones	<p>Partially Complete</p> <p>Future Target Date</p>