



# OFFICE OF INTERNAL AUDIT

---

## REPORT TO THE BOARD OF SUPERVISORS

### Pinal County Information Technology General Controls Audit

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

August 17, 2010

## TABLE OF CONTENTS

Executive Summary	3
Audit Objectives	8
Scope and Methodology	9
Background	10
Audit Results	
Segregation of Duties	13
Super User Access	14
System Audit Journals	16
Employee Background Screening	19
Access Controls	21
Strong Password Policy	23
Security Duties	24
Asset Management	26
Disaster Recovery	29
IT Governance Strategy	32
Attachment: Management's Response and Action Plan	

# Executive Summary

---

The Office of Internal Audit has recently completed a general controls audit of the Pinal County Information Technology (IT) Department. Significant areas reviewed during the audit include:

- IT department internal controls
- System access controls
- Data security Controls
- Application, or Business Process, controls
- Resource protection controls

Overall we found the IT department has established controls over a majority of these functional areas and that most controls are working effectively; however, our audit testing revealed weaknesses in access and data security controls and significant deficiencies in equipment tracking. We also identified weaknesses in IT business contingency planning and countywide comprehensive IT governance. Specifically our findings include:

- ◆ Improper segregation of duties allows IT employees to gain excessive controls over critical processes.
- ◆ Super user profiles for systems supporting the Finance department and the Treasurer's office have not been reviewed to determine if user access is necessary and up to date.
- ◆ The security audit journal function in the JD Edwards<sup>1</sup> and Spillman systems has not been activated.
- ◆ Under current policies, super users with access to financial systems, and other employees with access to critical systems, are not required to submit to background screenings.
- ◆ Access controls for some systems are not adequate to prevent unauthorized users from gaining access to sensitive information.
- ◆ Pinal County employees are not required to practice uniform strong password policies for access to critical county systems.

---

<sup>1</sup> The audit journal function for the AS400 system was activated during the course of the audit

- ◆ Security duties for critical systems and functions are not specifically assigned or regularly monitored
- ◆ IT department employees could not locate some equipment identified in a test sample from the inventory control list and were not aware of current county software tracking policies.
- ◆ IT disaster recovery/continuity planning lacks critical details including an effective collaboration process with other county departments
- ◆ IT does not practice a county-wide governance approach for the use of IT resources, services, and investments.

We identified several recommendations for improvements including:

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.*

*The Finance Department and Treasurer's Office could also implement compensating manual controls including regular reviews of system values and super user profiles; and, zero-balance and maximum disbursement accounts.*

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:*
  - a. *Set to allow access to necessary functions only*
  - b. *Purged or disabled if they are no longer active*
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 require users with extraordinary access to sign on at certain workstations lessens the chance of unauthorized user access to sensitive information.*

- 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.*
- 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<sup>2</sup>. System values should be set at recommended levels/values.*
- 6. The Chief Information Officer should ensure all IT personnel with access to critical data immediately undergo background screenings, including criminal history checks.*
- 7. 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.*
- 8. The Chief Information Officer should require all system administrators to immediately review user lists and purge inactive and terminated employee user profiles.*

---

<sup>2</sup> Internal Audit verified the QAUDJRN value has been activated for the AS400 system

9. *The Chief Information Officer should develop a comprehensive county-wide password management policy and distribute to all systems personnel and Pinal County departments. Policies should follow National Institute of Standards and Technology (NIST) recommended guidelines.*
10. *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.*
11. *The Chief Information Officer should immediately assign duties to the SSO to work with all county departments to integrate IT solutions into ongoing Continuity of Operation Plans (COOP) including, but not limited to, identifying secure offsite storage for sensitive back up data.*
12. *The Chief Information Officer should develop comprehensive written policies for all inventory/fixed asset tracking procedures, including the new barcode tracking system process and appropriate staff training.*
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 maintain accurate information.*
14. *The Chief Information Officer should develop and implement a comprehensive software asset management<sup>3</sup> program.*

---

<sup>3</sup> <http://www.microsoft.com/sam/en/us/default.aspx>

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 all identified high-risk circumstances.*
  
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.*
  
17. *The Pinal County Board of Supervisors should adopt a county-wide IT governance policy that establishes an IT governance leadership committee to:*
  - a. *Establish An IT strategic master plan*
  - b. *Establish guidance on how IT resources will be collaboratively approved and managed.*
  - c. *Develop county-wide IT security policies.*

The following report provides additional details of our audit observations, findings, and recommendations for improvement. We would like to thank the management and staff of the Pinal County Information Technology department for their assistance and cooperation during the course of this audit.

Lori Stripling  
Pinal County Internal Audit Officer

## **Introduction**

The Office of Internal Audit has completed an audit of the Pinal County Information Technology (IT) department and internal controls over IT systems and functions. Our audit was planned and conducted in accordance with Generally Accepted Government Auditing Standards<sup>4</sup>. These standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. Information System audit standards require auditors to obtain a sufficient understanding of information system controls necessary to assess audit risk and plan the audit within the context of the audit objectives.<sup>5</sup>

## **Audit Objectives**

The primary objectives of this audit were to:

- Verify the Information Technology department has established adequate general internal controls, including comprehensive written policies and procedures for all IT processes
- Obtain an understanding of how physical access to IT systems is determined and restricted
- Evaluate the adequacy of policies and procedures Management has established for application controls to provide reasonable assurance data security objectives are achieved
- Determine if the Information Technology department has established policies and procedures to provide assurance assets are safeguarded against waste, loss, unauthorized use, and misappropriation

---

<sup>4</sup> <http://www.gao.gov/govaud/ybk01.htm>

<sup>5</sup> GAGAS 7.24

## **Audit Scope**

Determine if the Information Technology department has established internal control procedures to identify, measure, monitor and manage potential risks to system access, data security and asset protection. This would include:

- System and Application access controls
- Program change controls (changes to system are completed in a controlled environment)
- Physical security of assets
- Inventory control procedures
- Database and storage media protocols
- IT general operations controls

## **Audit Methodology**

Our audit included such tests of internal controls, procedures, and documentation as were necessary to accomplish audit objectives. Our methodologies included:

- Interviews with IT management and personnel
- Interviews with appropriate federal, state, and county staff
- Tours of facilities and observation of operational activities
- Review of IT Department written policies and procedures
- Examination of other relevant documentation and surveys
- Testing of system data and security controls
- Research of applicable laws and regulations including prior audit findings
- Review of relevant computer system information and interviews with vendor staff

## Background

According to the mission statement prepared by the Pinal County Chief Information Officer (CIO)<sup>6</sup> the Pinal County Information Technology (IT) Department provides, “technology solutions and system support to Pinal County elected officials and their staff so they can provide the highest level customer service to successfully serve the citizens of Pinal County.”<sup>7</sup> The department is divided into 11 divisions:

1. Application Development Service Activity
2. Application Support Activity
3. Citizen Contact Center\*
4. Desktop Support Services\*
5. Electronic Document Management \*
6. Enterprise Project Services\*
7. Geographic Information Services\*
8. Network Operations
9. Radio Technology\*
10. System Administration
11. Telecom & Audio/Visual Infrastructure (AVS)\*

\*This audit was limited to an examination of general operations and system security and **did not** include a detailed review of the functions within these divisions.

## Prior Audits

Audit standards<sup>8</sup> require auditors to evaluate corrective actions taken to address prior audit findings and recommendations. Prior Pinal County state audit reports<sup>9</sup> have discussed a lack of effective internal control over financial computer systems within the County and have declared this a material weakness in internal control over financial reporting. Audit reports issued from FYE June 30, 2007 to FYE June 30, 2009 assert:

---

<sup>6</sup> Richard R. Jones (Pinal County CIO) hired in October 2007

<sup>7</sup> <http://pinalcountyz.gov/Departments/BudgetOffice/Documents/Budget%20Book/2009-10%20Budget%20Book.pdf>

<sup>8</sup> GAGAS 7.36

<sup>9</sup> [http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Financial\\_Audits/ICC\\_09/Pinal\\_Cty\\_6\\_30\\_09\\_Rpt\\_on\\_ICC.pdf](http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Financial_Audits/ICC_09/Pinal_Cty_6_30_09_Rpt_on_ICC.pdf)

- The County did not monitor changes in users' responsibilities.
- The County could not identify when programs were changed.
- The County could not provide documentation that program changes were authorized.
- The County's servers, and other important hardware components, are accessible to many employees who had no legitimate system responsibilities.
- The County did not provide its employees with sufficient training.
- The County did not have a comprehensive disaster recovery plan.
- The County gave users access to unnecessary functions.
- The County gave some users unnecessary unlimited access.
- The County could not identify which users initiated transactions.
- The County Treasurer should strengthen controls over its computer system.

During the course of this audit we reviewed corrective actions taken to address these findings and determined many controls to address audit findings are in place and operating effectively.

Specifically, we reviewed current policies and procedures within the Information Technology department and found:

- The IT department has developed and implemented a "create new accounts" Standard Operating Procedure (SOP) and policy. To set up a new user on any application a department manager must send a completed System Security form to the IT Help Desk. The form defines the necessary parameters required for the User profile. Changes in User responsibilities and access are monitored by the requesting department and modified by IT when requested.
- The IT department has developed and implemented an effective Change Management Policy, SOP, and standard forms. The policy covers all changes to production systems. All change requests must be authorized and approved by department management.
- The IT department has secured all data centers and implemented a door access security program. The department is also in the process of transferring many

critical hardware components to a newly renovated data center. The center is secure and equipped with the latest environment-control technology.

- The IT department has developed and implemented extensive training for department employees.
- The IT department has developed a preliminary disaster recovery plan and has started to perform limited testing.

While Management, for the most part, is able to effectively manage many internal control issues some general control weaknesses persist and control failure impacts could still be severe.

The following report discusses general control weaknesses we identified during the course of this examination.

## Audit Findings and Recommendations

### A. Segregation of Duties

Improper segregation of duties allows IT employees to gain excessive controls over critical processes. Understanding and applying proper segregation of duties (SOD) controls are vital to maintaining information security. For example, when managing access controls a person should not be able to grant himself/herself access rights and then perform a transaction. Similarly, an individual should not be able to perform a transaction and then delete all the logs, or change system settings, tracking the activity. All system changes should be properly reviewed, and duties properly segregated, to reduce the risks associated with a process being compromised either maliciously or through human error.

The IT department is currently organized, and many employees are assigned, according to applications or systems (JDE, Web, etc.). System staff members perform a variety of functional duties, regardless of job descriptions. Because of the current organization and based on staff responses to internal control questions, it is apparent that current segregation of duties is not at the Information Systems Audit and Control Association (ISACA) recommended levels (see table below).

<b>Exhibit 2.9—Segregation of Duties Control Matrix</b>														
	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database Administrator	Network Administrator	Systems Administrator	Security Administrator	Systems Programmer	Quality Assurance	
Control Group		X	X	X		X	X	X	X	X		X		
Systems Analyst	X			X	X		X				X		X	
Application Programmer	X			X	X	X	X	X	X	X	X	X	X	
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X		
End User		X	X	X			X	X	X			X	X	
Data Entry	X		X	X			X	X	X	X	X	X		
Computer Operator	X	X	X		X	X		X	X	X	X	X		
Database Administrator	X		X	X	X	X	X		X	X		X		
Network Administrator	X		X	X	X	X	X	X						
System Administrator	X		X	X		X	X	X				X		
Security Administrator		X	X			X	X					X		
Systems Programmer	X		X	X	X	X	X	X		X	X		X	
Quality Assurance		X	X		X							X		

X—Combination of these functions may create a potential control weakness.

## Recommendation

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.*

*The Finance Department and Treasurer's Office could also implement compensating manual controls including regular reviews of system values and super user profiles; zero-balance and maximum disbursement accounts.*

## B. Super User Access

Super user profiles allowing extraordinary access to systems supporting the Finance department and the Treasurer's office have not been reviewed to determine if access is necessary and/or appropriate for current duties. Testing for this audit included a review of special authority and "super" settings for user profiles within the system supporting the Finance Department and the application used in the Treasurer's Office.

A special authority setting, for example, may grant users All Object (ALLOBJ) authority. ALLOBJ authority allows a user to manipulate any object on the system, with the exception of User Profiles, for which separate Security Administrator authority is required. With ALLOBJ authority, every file, program, data area, etc. on the system can be accessed, manipulated and even deleted.

We also examined special settings for user profiles. To maintain system security, a user profile is assigned an initial menu on start up that restricts a user to the options available on that menu. Some profiles are set to allow Menu Travel (MT) capabilities. These users can 'travel' to other menus allowing expanded menu options. User profiles can also be set to allow Fast Path (FP) capabilities. FP allows a user to enter menu commands and quickly

travel to custom menus (i.e., user security, queue security, etc.) greatly expanding menu options. Super user profiles set to allow Command Entry (CE) authority can break free of the menu entirely and can command or “tell” the system what to do.

A disgruntled employee assigned one of these profiles, or an unauthorized individual using a super profile and password, could gain access to the system and obtain confidential employee, vendor or taxpayer information, including social security numbers and bank accounts, and/or make unauthorized changes to data, like salaries or payment addresses.

We reviewed user profiles with these super settings within the QSECOFR (Security Officer), SYSOPR (System Operator) and PGMR (Programmer) groups and determined:

- 50 profiles<sup>10</sup> have \*ALLOBJ authority
- 55 profiles have SECADM authority
- 27 profiles have command entry (CE) capabilities
- 19 of the profiles with command entry capabilities are currently enabled
- 12 of these 19 enabled profiles are assigned to IT’s JDE staff, 1 to Finance Department staff, 3 to IT’s system maintenance and development staff, and 3 to Treasurer’s office staff

The County Treasurers office uses a computer system for all operations that is supported by the AS400 system. The application for the system was developed and programmed by one Treasurer’s office employee. The employee, and the department accountant, both have user profiles with unlimited authority. An additional Treasurer’s office super user profile we found could not be attributed to any current employee.

Internal Audit and IT staff worked with staff in the Treasurer’s office to restrict user profiles with excessive authority and disable the one unidentified user profile having excessive authority. A list of the above identified profiles has been submitted to IT department staff for review.

---

<sup>10</sup> Some profiles identified have more than one special authorities

## Recommendations

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<sup>11</sup>. System values and user profiles should be:
  - a. *Set to allow access to necessary functions only*
  - b. *Purged or disabled if they are no longer active**
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<sup>12</sup> to limit users with extraordinary access to sign on at a certain workstation lessens the chance of unauthorized user access to sensitive information.*
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.*

### C. System Audit Journals

The audit journal function in the J.D. Edwards and Spillman systems has not been activated. Layered security provides the best protection because it does not rely solely on the integrity of any one element. One critical security layer is the important function of documenting security related events using a system audit journal. We reviewed the use of system audit

---

<sup>11</sup> IT JDE system management has started to review and reset identified profiles

<sup>12</sup> <http://www.powertech.com/guides/Compliance/OLMTSECOFR.htm>

journals in two key Pinal County systems: the J. D. Edwards (JDE) system used by the Finance department and the Spillman system used by the Pinal County Sheriffs' office (PCSO).

The Spillman system is equipped with a security logging feature. The 'Sylog' function allows logging/auditing of various data access for all Spillman users and can be set to log any action by any user of the system. There are also a variety of other automated security related features in the Spillman system. At this time the IT department has not been instructed by the PCSO to activate the Spillman system audit functions.

We reviewed the JDE/AS400 system automated audit functions and tested security settings and found:

- Settings are set to capture security information; however, the audit journal log had never been activated. Turning the audit journal on would provide invaluable information should a department ever experience a negative security event. Journal logs can be set to control the amount of information captured and monitoring responsibilities can be periodic.
- Many of the security settings we tested were lower than IBM recommendations. (variances are highlighted in yellow on table below)

System value tested	Value description	Level of importance	Current setting of system value	IBM recommended setting of system value
QSECOFR	Master Security Officer profile	HIGH	9 profiles have security officer capabilities	Restrict security officer profiles
QSECURITY	Controls privileged instructions	HIGH	40	40 – 50
QINACTTV	Time-out system value	HIGH	None – Workstations never timeout	60 minutes Leaving a terminal unattended can allow system intrusion
QALWBJRST	Restore Security sensitive objects	HIGH	*ALL – A virus could be loaded into the system and bypass this value	*NONE - Prior to performing OS maintenance it will be necessary to change to *ALWPTF
QAUDCTL	System auditing control	HIGH	AUDLVL NOQTEMP	AUDLVL NOQTEMP
QAUDLVL (system audit level)	Determines which events are	HIGH	See Table Below	*SERVICE and *PGMFAIL are events

System value tested	Value description	Level of importance	Current setting of system value	IBM recommended setting of system value
	logged to the security audit journal			recommended beyond current settings
QCRTAUT	Create Default *Public	<b>HIGH</b>	*CHANGE	*USE and control at library level
QAUDENDACN	Auditing end action	<b>HIGH</b>	*NOTIFY	*NOTIFY sends message to System Operator if auditing is turned off
QCRTOBJAUD	Audit new objects	<b>HIGH</b>	Blank and *ALL	Blank and *ALL
QMAXSGNACN	Action when # of sign on attempts exceeds the maximum	<b>HIGH</b>	3- Disable device and profile (recommended by IBM)	2- a higher setting could assist a DOS attack knocking all devices off line
QMAXSIGN	Maximum # of sign-on attempts	<b>HIGH</b>	5	3-5
QPWDEXPTIV	# of days before a user must change password	<b>HIGH</b>	75	90
QPWDMINLEN	Password minimum length	<b>HIGH</b>	5	6
QPWDRQDDIF	Duplicate password control	<b>HIGH</b>	5	5
QRMTSIGN	Remote sign-on control	<b>HIGH</b>	*SAMEPRF	*FRCSIGNON Force sign-on each time system is accessed
QSCANFCTL	Scan file systems after restore	<b>HIGH</b>	*NOPOSTRST objects will not be scanned after a restore	*ERRFAIL
QVFYOBJRST	Verify object on restore	<b>MEDIUM</b>	1- Do not verify on restore	3- Verify on restore (prevents viruses from being downloaded)
QPWDRQDDGT	Require digit in password	<b>MEDIUM</b>	0 Not required	1 - Prevents dictionary attack against passwords
QDSPSGNINF	Display user sign-on information	<b>MEDIUM</b>	0	1- Provides users with sign on information

<b>(QAUDLVL) Audit Control features that may be set at the object level</b>			
<b>Set</b>	<b>Value</b>	<b>Rating</b>	<b>Description</b>
<b>X</b>	*AUTFAIL	<b>HIGH</b>	Log Authority failures
<b>X</b>	*DELETE	<b>HIGH</b>	Log deletion of objects
<b>X</b>	*OBJMGT	<b>HIGH</b>	Log object management changes
<b>X</b>	*SYSMGT	<b>HIGH</b>	Log changes to certain system management areas
<b>X</b>	*SAVRST	<b>HIGH</b>	Log restore actions to security sensitive objects
<b>X</b>	*SECURITY	<b>HIGH</b>	Log security related changes
<b>Not set</b>	*SERVICE	<b>HIGH</b>	Log usage of the system and hardware service tools
<b>Not set</b>	*PGMFAIL	<b>HIGH</b>	Log Program failures caused by security violations
<b>X</b>	*SECCFG	<b>HIGH</b>	Log changes to security configuration

**Recommendation**

- The Chief Information Officer should require all system personnel with security responsibilities to immediately activate the audit journal for all systems with these capabilities<sup>13</sup>. System values should be set at recommended levels/values.*

**D. Employee Background Screening**

Employees with super user capabilities and access to financial systems, and other users with access to critical systems, are not covered by current background screening policies. Pinal County Information Technology Policy 1.13 requires “All positions that this policy applies (to) shall have a background screening conducted within 30 days upon initial employment or assignment.” The policy applies to “PC Analysts, PC Technicians, Computer Network Specialists, IT Engineers, Senior IT Engineers, and any other position that has administrative access to configure or maintain data on the Arizona Criminal Justice Information System (ACJIS) or FBI Criminal Justice Information System (CJIS) network.”

<sup>13</sup> Internal Audit verified the QAUDJRN value has recently been activated for the JDE/AS400 system

The CJIS Security Policy 4.5.1, paragraph H requires employees who support computer systems within restricted areas “are subject to a state of residency and national fingerprint-based record check.” Additional procedures, such as a criminal history check, may be conducted. The Pinal County Sheriff Office (PCSO) ACJIS offices are considered restricted areas. We confirmed a Background Investigator had performed criminal history checks on some IT personnel.

Internal Audit requested a list from PCSO and the Arizona Department of Public Safety (DPS) of all IT employees who have been authorized to work for the Pinal County Sheriff’s Office. The list contained 36 employees. We tested the list to verify all of the authorized employees were current Pinal County IT employees and found one employee was terminated in October 2009.

We also requested a list from the IT department of all employees who have received background checks. The spreadsheet we received listed the names of all employees and a column titled “approval dates.” We requested documentation of approval dates and were told by the CIO<sup>14</sup> “The background checks from the ACJIS policy are located in the HR personnel files. Starting in 2008 the policy (ACJIS) went into effect and, prior to that, verbal approvals were given to IT when staff passed.” Sixty-two (62) employees are listed with approval dates ranging from 6/28/06 to 4/22/08. Sixteen (16) of the 62 employees are on the list provided by PCSO/DPS of authorized employees who have been screened and finger-printed.

We asked the Human Resources department if they had any information on IT personnel background checks. HR staff responded that prior to the new Pinal County background investigation policy implementation date<sup>15</sup> IT was responsible to conduct background checks on employees and maintain information in interview packets.

---

<sup>14</sup> Email message sent April 8, 2010

<sup>15</sup> December 9, 2009, Pinal County implemented a new personnel policy<sup>15</sup> for Background Investigations. The policy states, “A background investigation will be required for newly hired employees as a condition of employment.”

Thirteen (13) employees, including several super-users with access to sensitive financial systems, are not on any of the lists provided. We confirmed at least one super-user has not been asked to submit to a background screening.

While it is important to conduct pre-employment screenings for applicants considered for positions with access to sensitive information systems, it is also important to check individuals already working in these positions.

### **Recommendations**

- 6. The Chief Information Officer should require all IT personnel with access to critical data immediately undergo background screenings, including criminal history checks.*
  
- 7. 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.*

### **E. Access Controls**

Access controls for some systems are not adequate to prevent unauthorized users from gaining access to sensitive information. Inadequate implementation of access controls increases the possibility that unauthorized users can gain access to the computer systems. Internal Audit requested detailed information about current policies and procedures regarding data center door access and confirmed the IT department has developed thorough standard operating procedures to grant and monitor door access.

The IT department has also developed policies and procedures for setting up new user accounts and provided draft policies requiring system access be removed in a timely manner for terminated employees. The procedures did not include a requirement to review current user lists.

Internal audit requested user lists for two county systems, JD Edwards (Finance) and Spillman (Pinal County Sheriff Office) and reviewed the lists for current users.

To test the Spillman user list we randomly chose 25 of the first 2,000 user profiles listed and verified whether the users were still employed by Pinal County. Two (2) of the 25 users tested were terminated employees with currently active profiles. One employee was terminated in 2005 and one in 2009.

For the JD Edwards (JDE) User list we asked the IT department to provide the PRTUSRPRF (Print User Profile) report and tested the report for inactive users to determine if their profiles were enabled or disabled.

For purposes of this test, inactive Users were defined as user profiles that have not been used since January 2008. Of the 848 User profiles listed we found 338 (40%) had not been used since January 2008. Of these 338 profiles, 210 (62%) were still enabled. We were not able to determine if any of these profiles belonged to terminated employees, since employee names were not listed on the User Profile (USRPRF) list. Twenty-seven (27) profiles have not been used since the 1990's and may have been activated for one time system maintenance. We did not include training profiles (temporary profiles established for employee training in JD Edwards) in this test.

### **Recommendation**

8. *The Chief Information Officer should require all system administrators to immediately review user lists and purge inactive and terminated employees' user profiles.*

## **F. Strong Password Policy**

Pinal County departments do not practice uniform strong password policies for critical county systems. The National Institute of Standards and Technology (NIST) Computer Security Division recommends implementing a comprehensive enterprise password management<sup>16</sup> program that includes the following:

1. Create a policy that specifies all of the organization's password management-related requirements.
2. Protect passwords from attacks that capture passwords.
3. Configure passwords to reduce the likelihood of successful password guessing and cracking.
4. Determine requirements for password expiration based on balancing security needs and usability.

IBM, the vendor for the AS400 system used to maintain data for the Pinal County Finance department and the Treasurers office, supplies seven (7) user profiles for basic server/system setup and maintenance. All profiles have a default password that should be immediately changed. We tested the seven profiles to confirm default passwords had been changed and found all passwords had been changed from the default setting.

<b>Profile</b>	<b>User</b>	<b>Changed from default Y/N ?</b>
QSECOFR	Security Officer	Y
QSYSOPR	System Operator	Y
QPGMR	Programmer	Y
QSRVBAS	Service Base	Y
QUSE	User profile for system function	Y
QSRV	Service settings	Y
QDFTOWN	Default owner for system restore	Y

We also contacted System Administrators for a list of all computer systems in use in Pinal County and asked about password policies and procedures. The following questions were asked:

---

<sup>16</sup> <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

1. Does a login name and password uniquely identify user at sign on?
2. Does the application automatically force a periodic password change?
3. Are strong passwords required?

After receiving responses from a majority of System Administrators, we determined password policies and procedures for County applications are not uniform and strong password policies are not required for any reported systems.

### Recommendation

9. *The Chief Information Officer should develop a comprehensive county-wide password management policy and distribute to all systems personnel and Pinal County departments. Policies should follow National Institute of Standards and Technology (NIST) recommended guidelines.*

### G. Security Duties

Security duties for critical systems and functions are not specifically assigned or regularly monitored. Well developed security policies and procedures are a critical element of an integrated information technology governance strategy.

Many of the weaknesses identified in prior audit reports,<sup>17</sup> and during this audit, involve security control weaknesses including lack of security monitoring, inadequate security policies and procedures, and inadequate security for back up tapes.

Continued weakness in information system security controls increases the risk of unauthorized access or undetected misappropriation of equipment and sensitive data.

---

<sup>17</sup> [http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Pinal\\_County.htm](http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Pinal_County.htm)

After reviewing job descriptions for IT employees, we identified security duties specifically assigned to at least three IT positions; however, when we asked the CIO and other IT staff about security duties it was evident the responsibilities, as one employee stated, "...are shared amongst almost all IT personnel with varying degrees of involvement."

Allowing system and data security duties to be accomplished by numerous employees with no coordinated and comprehensive security oversight may increase the risk that security responsibilities will be missed or partially implemented.

There is a need for a designated system security officer (SSO) with specific job duties that include, but are not limited to:

- Identifying gaps or lapses in current security procedures
- Developing procedures to prevent or mitigate security lapses or gaps
- Maintaining system and data security processes throughout county departments, including ensuring new encryption software for data tape back up is comprehensively implemented and tapes are secured a significant distance away from main processing environments"<sup>18</sup>
- Monitoring current security procedures for compliance
- Helping county personnel identify IT risk and security considerations during development of department Continuity of Operation Plans (COOP)

### *Recommendations*

*10. 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.*

*11. The Chief Information Officer should assign immediate duties to the SSO to work with all county departments to integrate IT solutions into ongoing*

---

<sup>18</sup> <http://www.primode.com/glossary.html>

*Continuity of Operations Plans (COOP) including, but not limited to, identifying secure offsite storage for sensitive back-up data.*

## **H. Asset Management**

IT department employees could not locate some equipment on the inventory control list, and some identified IT equipment was not recorded on the list. Also, responsible IT department staff was not aware of the current county policy<sup>19</sup> for software tracking.

Pinal County has recently updated the County Capital Assets policy 8.8. The policy was updated to comply with Governmental Accounting Standards Board (GASB) Standard 51, *Accounting and Financial Reporting for Intangible Assets*. The standard requires capitalization of identifiable intangible assets and provides guidance for amortization of intangible assets. The new county policy adds the category of intangible assets with a depreciated useful life of more than 10 years and increases the capitalization thresholds for machinery and equipment to \$5000 and Buildings and Improvements to \$25,000. Additional policy changes included assigning primary responsibility for tracking IT equipment below the \$5,000 Capital Asset threshold to the IT department<sup>20</sup>, and instructing all departments to comply with IT Standard Operating Procedures (SOP).

The effective date of the policy is July 1, 2009; however, at the time fieldwork for this audit was conducted the policy had not been approved by the Board of Supervisors. Therefore, for purposes of this audit, Internal Audit determined the department's asset management should be evaluated using the prior policy as the controlling authority. Under this policy, prior capitalization thresholds for machinery and equipment were set at \$1,000, and the IT department was responsible to safeguard assets under the department's possession.

---

<sup>19</sup> Pinal County Policy 2.4 Computer Software Management

<sup>20</sup> Policy Section F

<u>Policy</u>	<u>Land</u>	<u>Machinery &amp; equipment</u>	<u>Buildings &amp; Improvements</u>	<u>Infrastructure</u>	<u>Intangible Assets (depreciated useful life of 10+yr.)</u>
<b>Prior</b>	All	\$1,000	\$5,000	\$100,000	N/A
<b>New July 1, 2010</b>	All	\$5,000	\$25,000	\$100,000	\$50,000

We discussed current asset tracking procedures with IT staff, and determined department staff responsible for software assets were not aware of Pinal County Policy 2.40 *Computer Software Management*. This policy requires the IT department to maintain a recordkeeping system for all county software and regularly review software for proper licensure. Department staff also confirmed they do not maintain a record keeping system for software and have not developed procedures to review licensure.

Not implementing software tracking procedures may have resulted in unnecessary and duplicate software purchases throughout county departments. Implementing a comprehensive software asset management program could reduce software and support costs, and the department could reallocate underutilized software licenses.

IT staff provided the department's 'Asset Tracking Equipment Changes' policy.<sup>21</sup> The stated purpose of the policy is, "To track changes in status, ownership and disposition of Pinal County owned computers, laptops, and servers for Telecom." The new process requires assets to be tagged when they are received in the shipping and receiving division, and added to an Asset Management Database. The department has started using a barcode system for asset tagging (WASP<sup>22</sup>).

To assess the current condition of IT department asset tracking, Internal Audit staff conducted testing using the IT department fixed asset list provided by the Finance department and the assets listed on the IT department tracking system and found:

---

<sup>21</sup> No policy number

<sup>22</sup> <http://www.wasbarcode.com/>

- We were able to locate 8 of 12 items selected from the fixed asset list. IT staff explained 3 of the 4 items we could not find had been salvaged and 1 had been stolen. The department could not provide copies of salvage forms. The stolen item was reported to authorities and the report was verified.
- 5 of 11 assets physically located in either the Administration office or the new data center were not recorded on the list.

It appears both the fixed asset list and IT asset tracking software are not up to date with current inventory.

We also visited County offices in the Casa Grande and Apache Junction complexes and randomly chose 20 assets to verify the chosen assets were appropriately tagged and listed on the inventory list provided by the Finance department. We found:

- 7 items were tagged and on the list
- 5 items were not recorded on the list
- 8 items were on the list but had no visible asset tag (items were identified by some other means. i.e. serial number, etc.)

As part of our testing, we also examined compliance with the recently developed IT department custodian agreement form. The form documents issuance of employee-assigned equipment (cell phone, laptops, etc.) and is used to identify equipment that needs to be returned when an employee voluntarily leaves county employment or is terminated. We found compliance with these procedures was well documented.

We reviewed IT department compliance with Pinal County Procurement Card policies and procedures.<sup>23</sup> We tested 7 of 66 procurement card transactions and reviewed all supporting documentation. We found procurement card procedures were working well and there were no instances of non-compliance.

---

<sup>23</sup> No policy number

## Recommendations

12. *The Chief Information Officer should develop comprehensive written policies for all inventory/fixed asset tracking procedures, including use of the new barcode tracking system process and appropriate staff training.*
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 maintain accurate information.*
14. *The Chief Information Officer should develop and implement a comprehensive software asset management<sup>24</sup> program.*

### I. Disaster Recovery

IT disaster recovery/continuity planning lacks critical details and does not include an effective collaboration process with other county departments. The lack of a comprehensive disaster recovery plan has been mentioned as a finding in the Auditor General's Pinal County Report on Internal Control and Compliance<sup>25</sup> for the past three years. Our audit procedures included a review of IT department disaster recovery planning.

To review the current level of the IT department disaster preparedness we requested access to disaster recovery planning information and testing documents, and researched recommendations from the National Institute of Standards and Technology (NIST) for

---

<sup>24</sup> <http://www.microsoft.com/sam/en/us/default.aspx>

<sup>25</sup> [http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Financial\\_Audits/ICC\\_09/Pinal\\_Cty\\_6\\_30\\_09\\_Rpt\\_on\\_ICC.pdf](http://www.auditorgen.state.az.us/Reports/Counties/Pinal/Financial_Audits/ICC_09/Pinal_Cty_6_30_09_Rpt_on_ICC.pdf)

contingency planning.<sup>26</sup> NIST is the federal technology agency that works with the technology industry to develop technology measurements and standards.<sup>27</sup>

We also contacted System Administrators for a list of all computer systems in use in Pinal County and asked about disaster recovery procedures. The following questions were asked:

1. Are system backups created and saved?
2. Is backup data stored offsite?
3. Is restoration of the system included in a Disaster Recovery Plan?

As a result of our review we determined:

- IT recently conducted a recovery test on the AS400 system and reported all subsystems were successfully recovered.
- Testing revealed several gaps/weaknesses with general Disaster Recovery procedures, including the availability of forms and stock, and transportation for needed personnel and equipment.
- Based on a comparison of IT disaster recovery planning documents and the NIST Seven Step Contingency Planning Process, it appears IT department personnel have started steps 1, 2, 3 and 4 (see seven step process below).
- Detailed contingency plans for all county IT platforms<sup>28</sup> and identified high risk situations, including disaster recovery, have not been developed.
- The documents provided did not discuss how IT disaster recovery/contingency planning collaborates with ongoing county Continuity of Operation planning (COOP) efforts.

---

<sup>26</sup> <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

<sup>27</sup> <http://www.nist.gov/index.html>

<sup>28</sup> PC, servers, web, mainframe, etc.

NIST SEVEN STEP CONTINGENCY PLANNING PROCESS		
STEP	TITLE	DESCRIPTION
1	Develop the contingency planning policy statement	A formal county/department policy provides the authority and guidance necessary to develop an effective contingency plan.
2	Conduct the Business Impact Analysis (BIA)	The BIA helps to identify and prioritize critical IT systems and components throughout the county.
3	Identify preventive controls	Measures taken to reduce the effects of system(s) disruptions can increase system(s) availability and reduce contingency life cycle costs
4	Develop recovery strategies	Thorough recovery strategies ensure that system(s) may be recovered quickly and effectively without disruption
5	Develop an IT contingency plan	The contingency plan should contain detailed guidance and procedures for restoring damaged system(s).
6	Plan testing, training, and exercises	Testing the plan identifies gaps, and training prepares recovery personnel for plan activation.
7	Plan maintenance	The plan should be a living document that is updated regularly to remain current with system(s) enhancements.

### Recommendations

*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<sup>29</sup>, etc.) to facilitate this effort.*

*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.*

<sup>29</sup> [http://csrc.nist.gov/groups/SMA/fasp/documents/contingency\\_planning/contingencyplan-template.doc](http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc)

## **J. IT Governance Strategy**

Pinal County lacks a comprehensive county-wide IT Governance strategy. The Pinal County Information Technology department does not practice a county-wide governance approach for the use of IT services and resources and, individual county department IT investments are not considered within the context of a county-wide strategic IT plan.

For example, during the course of this audit we reviewed an operations level agreement (OLA) the IT department recently<sup>30</sup> established with the Pinal County Attorneys office. The objective of the agreement was to document support services provided by Pinal County IT staff. Similar services, and in some cases more extensive services, are provided to other county departments with no OLA established. While there is nothing inappropriate in establishing an OLA, the practice raises the question of when a formal agreement should be established. The practice also emphasizes the need to determine if Pinal County government needs a more comprehensive enterprise-wide IT strategy.

In June 2009, after reviewing their county's efforts to establish an effective IT governance strategy, the Maricopa County Internal Audit Department issued a report<sup>31</sup> entitled *Countywide Information Technology Governance*.

In the report, governance was defined as, "...how (county) management formally decides to employ Information Technology in supervising, monitoring and directing an organization," and noted, "...IT governance is more crucial than ever during a recession and is a critical component of doing more with less."

The report cited an MIT Sloan School of Management study that estimated, "private firms with superior IT governance performance generate up to 40 percent higher return on investment (ROI)," and estimated Maricopa County could conservatively generate \$1 million more in ROI each year. In 2008 IT expenditures in Maricopa County were \$81,587,745.

---

<sup>30</sup> July 23, 2009

<sup>31</sup> [http://www.maricopa.gov/Internal\\_audit/PubDocuments/FY2009/ITGovReport.pdf](http://www.maricopa.gov/Internal_audit/PubDocuments/FY2009/ITGovReport.pdf)

The report recommended:

1. IT governance policies that include-
  - Ownership of IT governance
  - Alignment of IT strategy with County business strategy
  - Management of IT risks, resources, and performance measures
2. Ensuring the following best practices are part of the IT governance model –
  - IT investments align with County objectives and goals
  - IT projects align with business values
  - IT risks and resources are properly identified and managed
  - IT performance is measured and reported

Maricopa internal auditors found, “...the current IT governance structure is weak, having outdated and incomplete IT governance policies ...that do not address critical success factors” such as, prioritizing projects, aligning business and IT objectives, and identifying performance measures.

At this time Pinal County has not developed any formal comprehensive County IT governance policies and procedures.

### *Recommendation*

- 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:*
  - a. Establish a countywide IT strategic master plan*
  - b. Establish guidance on how IT resources will be collaboratively approved and managed.*
  - c. Develop county-wide IT security policies.*

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<p>1. <i>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.</i></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><b>Action Plan Deliverables:</b> SOP to review server log. Turn on JD Edwards application audit log. SOP to review key functions within the application log.</p>	December 31, 2010	<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>2. <i>The Chief Information Officer should require all system personnel with security responsibilities to immediately conduct a review of all user profiles and system values<sup>32</sup>. System values and user profiles should be:</i></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><b>Action Plan Deliverable:</b> A review of “super setting” AS400 accounts to ensure access to necessary functions only.</p>	December 31, 2010	<p>Jay Vargo – Review of “super setting” profiles.</p> <p>Doyle Johnson – Confirmation of “super settings” for application support staff.</p>

<sup>32</sup> IT JDE system management has started to review and reset identified profiles

**IT Department Audit Response and Action Plan**  
August 2010

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<p>3. <i>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<sup>33</sup> 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>	<p>Yes</p>	<p><b>Action Plan Deliverable:</b> Limit QSECOFR profile to only logon from AS400 console.</p>	<p>October 31, 2010</p>	<p>Rodney Banks</p>

<sup>33</sup> <http://www.powertech.com/guides/Compliance/QLMTSECOFR.htm>

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<p>4. <i>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><b>Action Plan Deliverable:</b> 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>	December 31, 2010	Richard Jones
<p>5. <i>The Chief Information Officer should require all system personnel with security responsibilities to immediately activate the audit journal for all systems with these capabilities<sup>34</sup>. 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><b>Action Plan Deliverable:</b> List of applications with journaling capability and specific events being journaled.</p>	December 31, 2010	Doyle Johnson Jay Vargo
<p>6. <i>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><b>Action Plan Deliverable:</b> NA</p>	TBD	Richard Jones

<sup>34</sup> Internal Audit verified the QAUDJRN value has recently been activated for the JDE/AS400 system

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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>	<p>Yes</p>	<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><b>Action Plan Deliverable:</b> Update current IT Policy 1.13 to include monitoring and updating PCSO when IT staff are terminated.</p>	<p>October 31, 2010</p>	<p>Jay Vargo Brian Kreklau</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>	<p>Yes</p>	<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><b>Action Plan Deliverable:</b> Purge terminated users from systems with unique usernames. SOP to notify system administrators when employees are terminated.</p>	<p>December 31, 2010</p>	<p>Jay Vargo Doyle Johnson</p>

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<p><i>9. 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>	<p>Yes</p>	<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><b>Action Plan Deliverable:</b> 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>	<p>December 31, 2010</p>	<p>Richard Jones</p>
<p><i>10. The Chief Information Officer should designate one System Security Officer responsible to ensure comprehensive security for county information systems and maintain regular monitoring of all IT security policies and procedures.</i></p>	<p>Yes</p>	<p>Currently Pinal County IT does not have the staff resources or in house skill set to designate a System Security Officer.</p> <p><b>Action Plan Deliverable:</b> Submit a request to County Manager for position.</p>	<p>TBD</p>	<p>Richard Jones</p>

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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>	<p>Yes</p>	<p>Currently Jay Vargo and Richard Jones are responsible for working with Departments and their COOP planning.</p> <p><b>Action Plan Deliverable:</b> Offsite data backup location SOP</p>	<p>October 31, 2010</p>	<p>Jay Vargo</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>	<p>Yes</p>	<p><b>Action Plan Deliverable:</b> Asset tracking SOP</p>	<p>October 31, 2010</p>	<p>Richard Jones Angie Woods</p>

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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>	<p>Yes</p>	<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><b>Action Plan Deliverable:</b>            Work with Finance to insure asset management program is followed.</p>	<p>July 1, 2011</p>	<p>Angie Woods</p>
<p><i>14. The Chief Information Officer should develop and implement a comprehensive software asset management<sup>35</sup> program.</i></p>	<p>Yes</p>	<p>Duties have been assigned to new staff member starting August 9, 2010</p> <p><b>Action Plan Deliverable:</b>            Software asset management program</p>	<p>July 1, 2011</p>	<p>Angie Woods</p>

<sup>35</sup> <http://www.microsoft.com/sam/en/us/default.aspx>

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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<sup>36</sup>, 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. Once department COOP plans are completed IT System Recovery Team will begin the task of contingency planning with all application owners.</p> <p><b>Action Plan Deliverable:</b>  IT Contingency Plan for County Systems</p>	<p>June 30, 2012</p>	<p>Richard Jones</p>

<sup>36</sup> [http://csrc.nist.gov/groups/SMA/fasp/documents/contingency\\_planning/contingencyplan-template.doc](http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc)

**IT Department Audit Response and Action Plan**  
**August 2010**

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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 hold 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><b>Action Plan Deliverable:</b> IT Contingency Plan for County Systems</p>	<p>June 30, 2012</p>	<p>Richard Jones</p>

**IT Department Audit Response and Action Plan**  
August 2010

Audit Recommendation	Concur Y/N	Action Plan	Target Date	Individual Responsible
<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> <p><i>a. Establish a countywide IT strategic master plan</i></p> <p><i>b. Establish guidance on how IT resources will be collaboratively approved and managed.</i></p> <p><i>c. Develop county-wide IT security policies.</i></p>	Yes	<p><b>Action Plan Deliverable:</b> Work with Assistant County Manager to develop IT Governance Policy</p>	July 1, 2011	Richard Jones