



A Report
to the
Board of
Supervisors

*Maricopa County
Internal Audit
Department*

Ross L. Tate
County Auditor

Information Technology Audit

Court Technology Services

*Review of the Integrated Court
Information System (iCIS)*

September ■ 2007

Executive Summary	1
Introduction	2
Detailed Information	6
Department Response	16

The **County Auditor** is appointed by the Board of Supervisors. The mission of the Internal Audit Department is to provide objective, accurate, and meaningful information about County operations so the Board of Supervisors can make informed decisions to better serve County citizens.

The mission of Maricopa County is to provide regional leadership and fiscally responsible, necessary public services so that residents can enjoy living in a healthy and safe community.

Audit Team Members

**Eve Murillo, Deputy County Auditor
Toni Sage, IT Audit Supervisor
Susan Adams, Senior IT Auditor
KPMG LLP**

Copies of the County Auditor's reports are available by request.
Please contact us at:

**Maricopa County Internal Audit
301 W. Jefferson, Suite 660 ♦ Phoenix, AZ 85003 ♦ (602) 506-1585**

Many of our reports can be found in electronic format at:

www.maricopa.gov/internal_audit



Maricopa County

Internal Audit Department

301 West Jefferson St
Suite 660
Phx, AZ 85003-2143
Phone: 602-506-1585
Fax: 602-506-8957
www.maricopa.gov

September 14, 2007

Fulton Brock, Chairman, Board of Supervisors
Don Stapley, Supervisor, District II
Andrew Kunasek, Supervisor, District III
Max Wilson, Supervisor, District IV
Mary Rose Wilcox, Supervisor, District V

We have completed our review of the Integrated Court Information System, which was performed in accordance with the annual audit plan approved by the Board of Supervisors. The specific areas reviewed were selected through a risk-assessment process.

We found that Court Technology Services has a well-defined information technology strategic plan and established governance and operational practices. However, information technology controls should be strengthened in the following areas to ensure data integrity and validity, prevent unauthorized transactions, and ensure business requirements are adequately addressed.

- IT staff access to the production environment
- User access and password management
- Project management, change management, and testing

This report contains an executive summary, specific information on the areas reviewed, and Court Technology Services' responses to our recommendations. We reviewed this information with the Chief Information Officer and appreciate the cooperation provided by management and staff. If you have any questions, or wish to discuss the information presented in this report, please contact Eve Murillo at 506-7245.

Sincerely,

A handwritten signature in cursive script that reads "Ross L. Tate".

Ross L. Tate
County Auditor

(Blank Page)

Table of Contents

Executive Summary	1
Introduction	2
Detailed Information	6
Department Response	16

Executive Summary

Application Controls (Page 6)

Application security controls should provide reasonable assurance that information integrity is maintained and IT assets are protected. We found several application control weaknesses specifically related to end-user access functions. IT staff should not have the ability to access end-user functions. CTS should review user access rights and segregation of duties to remove any unauthorized or inappropriate user accounts and access rights.

Systems Access (Page 8)

System access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. We found weaknesses in three management areas: user account, password, and access review. CTS should develop appropriate policies and procedures, and stronger password standards.

Systems Change Management (Page 11)

Systems changes should be managed through established policies and procedures to mitigate risks of negatively impacting the stability or integrity of Judicial Branch operations and ensure alignment to business requirements. We found weaknesses with CTS concerning project management, change management, and testing. CTS should develop formal change management policies and procedures for all applications, operating systems, databases, and hardware changes. Further, CTS should establish formal project management policies and procedures for data conversion and testing.

Data Center Operations (Page 13)

Computer Operations controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. We determined that CTS appears to have adequate controls over computer operations, including help desk, backup and recovery, disaster recovery, and job scheduling. However, we found weaknesses in computer access authorization and review. CTS should develop appropriate policies and procedures for granting access to the computer room.

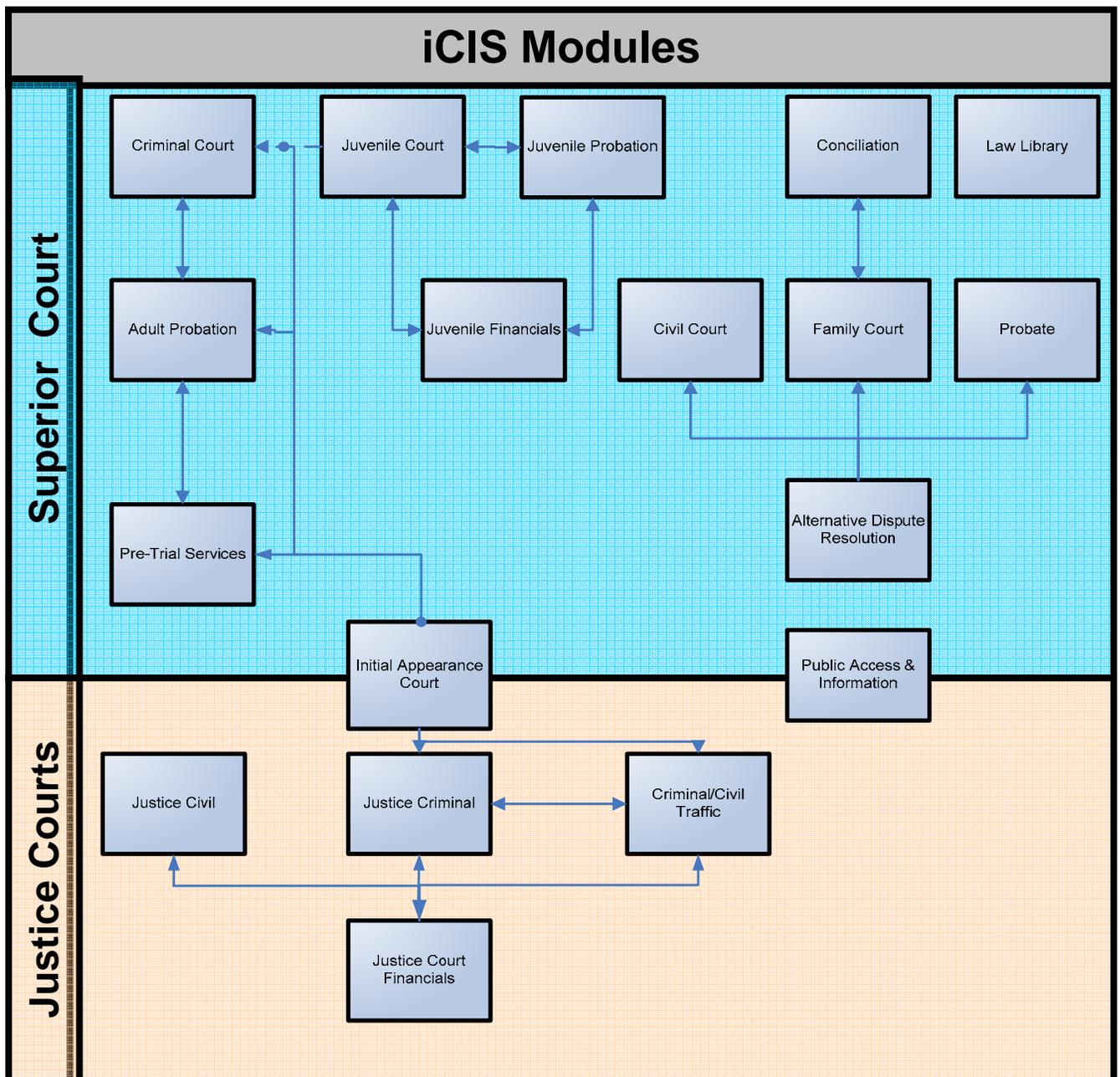
IT Governance (Page 14)

IT Governance ensures that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives. CTS has established IT Governance controls, such as a Judicial Branch IT steering committee and IT strategic plan. However, CTS lacks a risk assessment framework. CTS should document formal procedures for evaluating and monitoring risk of all projects.

Introduction

Background

The Court Technology Services (CTS) department, under the Maricopa County Judicial Branch, serves the Superior Court, Adult Probation, Juvenile Probation, and 23 Justice Courts at over 50 locations. CTS develops, maintains, and supports the Judicial Branch's IT infrastructure and application environment and the primary case management system, which is referred to as the Integrated Court Information System (iCIS). The iCIS application handles all aspects of case management and encompasses the functions shown below.



Source: CTS

The iCIS underlying architecture is based upon Microsoft Windows Server operating system and Structured Query Language (SQL) relational database management system. The entire iCIS application was internally developed. Public access to case history is available on the Superior Court's website. This on-line information is a separate database which is a mirror image of the information contained within iCIS.

During fiscal year (FY) 2007, CTS moved the Juvenile Probation and Juvenile Court Systems from the AS400 legacy platform to iCIS. Juvenile Probation is scheduled for an Internal Audit review during FY 2008.

Additionally, the Adult Probation Enterprise Tracking System (APETS) is a state-wide system developed and implemented by the Administrative Office of the Courts (AOC), Arizona Supreme Court. CTS' responsibility for this system is limited to overseeing the personal computers (PC) that run the APETS and updating the PC-based client software when AOC releases an update and when directed to do so by the Adult Probation Department (APD). The August 2006 Auditor General's review found that "...APETS development had closely adhered to AOC's project management framework." However, in July 2007, AOC released a new version of APETS and problems were encountered by Maricopa County Adult Probation, specifically with the Case Plan and Drug Court modules. Internal Audit was notified of this issue after field work was concluded.

Mission, Goals, and Performance Measures

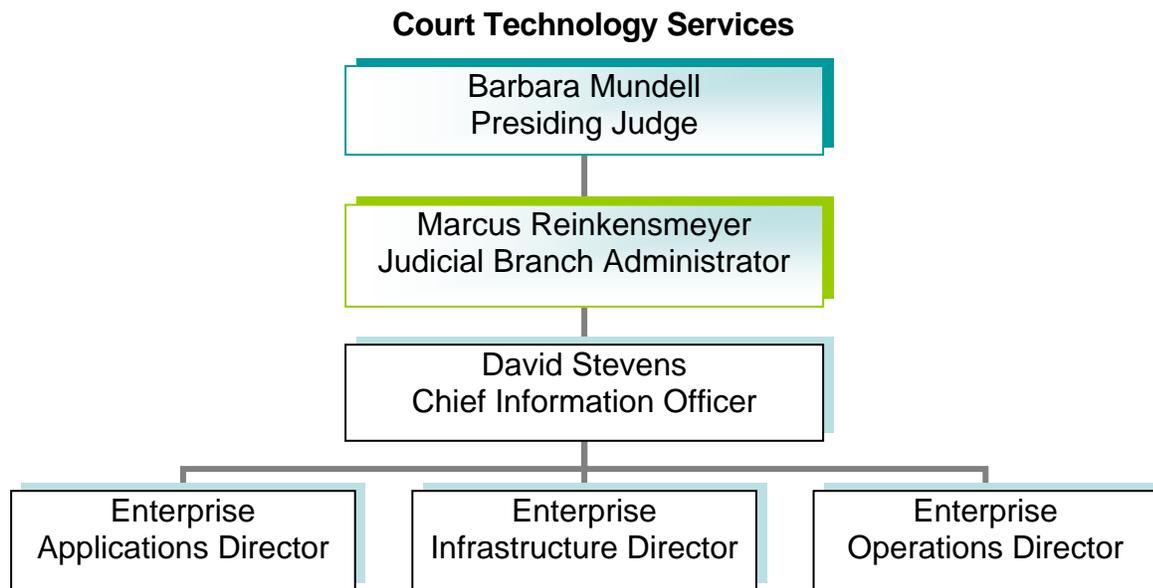
CTS' mission is to provide information technology that strengthens the Judicial Branch through stewardship, timeliness, and collaboration. CTS' purpose is to provide IT leadership and services to the Judicial Branch (Superior Court, Justice Courts, Adult Probation, and Juvenile Probation) so that management can obtain maximum benefit from the IT resource.

As stated in the CTS IT Strategic Plan, its goals are to:

1. *Transform the CTS service approach from operational support to fostering innovation*
 - 1.1. The decision making paradigm within the Judicial branch will acknowledge technology as an essential part of core court business
 - 1.2. A consistent Business Process Reengineering methodology will be used to implement new processes and solutions in the court
 - 1.3. Technology will generate revenue where appropriate
2. *Provide an effective technology infrastructure to meet both present and future needs*
 - 2.1. The Judicial Branch will use best practices and standards in support of core competencies
 - 2.2. There will be support across the Judicial Branch for proactive and timely refresh cycles for mission-critical hardware and software
 - 2.3. CTS will continue to leverage to the best use of the Judicial Branch infrastructure and services provided by the County
 - 2.4. There will be on-going investment in research and development that supports both CTS and Judicial Branch goals and objectives

3. *Foster collaborative and strategic alignment among justice partners in order to leverage resources*
 - 3.1. There will be collaboration between County and other justice partners in order to create mutually beneficial results
 - 3.2. Formal agreements with our justice partners, such as Service Level Agreements (SLA), Intergovernmental Agreements (IGA), and Memorandums of Understanding (MOU), will be thoroughly reviewed and implemented
4. *Implement a service delivery strategy that embraces an agile centralized administration and regional customer support model*
 - 4.1. CTS will continue to participate in Judicial Branch strategic planning
 - 4.2. CTS will have increased visibility and participation in initial project planning
 - 4.3. CTS will be a key stakeholder in Court facilities planning

Organizational Structure



In addition to CTS supporting iCIS, the Adult Probation Department oversees APETS and acts as the liaison to AOC.

Operating Budget

In FY07 CTS had 92 budgeted full-time employees and its projected expenditure budget was \$6.08M. The FY08 expenditure budget is \$6.93M. The increase is primarily associated with business development activities, including upgrading the case management system and the court automation system, hardware upgrades, and consultant expenditures for these projects.

Additionally, Adult Probation’s FY07 projected and FY 08 expenditure budget for IT programs are \$1.62M and \$1.65M, respectively.

Scope and Methodology

The objectives of this audit were to determine that adequate controls exist within the following areas:

- iCIS security (including programs and data access, and procedures for overseeing network access to the State's Adult Probation Enterprise Tracking System)
- iCIS program development and program changes (authorization, approval, and testing of system development and change activities)
- Computer operations
- Justice Courts financial system security
- IT Governance (including IT strategic planning and priorities)

We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Issue 1 Application Controls

Summary

Application security controls should provide reasonable assurance that information integrity is maintained and IT assets are protected. We found several application control weaknesses specifically related to end-user access functions. IT staff should not have the ability to access end-user functions. CTS should review user access rights and segregation of duties to remove any unauthorized or inappropriate user accounts and access rights.

Application Controls

Application controls ensure the completeness, accuracy, timeliness, and authorization of the entries made within a software application. Strong application controls include separating application development functions from end-user functions. For example, a programmer should not be able to perform cashier functions—because he has the ability to input unauthorized financial transactions.

Internal Audit uses the IT Governance Institute’s Control Objectives for Information and related Technology (COBIT) as a framework for IT best practices.

iCIS Application Control Weaknesses

We found several application control weaknesses specifically related to information technology staff having the ability to access end-user functions within the iCIS Justice Courts financial system module. Our testing revealed the following weaknesses:

- Nine developers have access to set and reset the receipt number. Manipulation of receipt numbers could result in understated revenue or compromised data integrity.
- Twelve CTS employees have access to void receipts and checks. Inappropriately voided receipts and checks may result in understated fees collected or delinquent payments.
- Payment information such as payer name, payee name and payment types can be changed after the receipt or check has been authorized. This enables unauthorized payments to occur.
- Ten CTS employees have access to the end-user (production) database. Data integrity can be compromised through the unauthorized deletion, addition, or modification of transactions. Unauthorized or incorrect changes could result in loss of data or incorrect transaction processing.
- Seventeen CTS employees have access to the fines and fees end-user functions within iCIS.
- A terminated employee (July 2006) still has access to set or reset receipt numbers and has end-user database access.

Recommendations

CTS should:

- A.** Revoke developer access to the end-user “production” functions
- B.** Restrict developer access to production database to query only
- C.** Review user access and disable any accounts belonging to terminated users. Determine whether any terminated user accounts have been accessed since the termination date.
- D.** Restrict access to modify receipt or check transactions after authorization
- E.** Perform regular reviews of user access rights and segregation of duties to remove any unauthorized or inappropriate user accounts or access rights

Issue 2 Systems Access

Summary

System access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. We found weaknesses in three management areas: user account, password, and access review. CTS should develop appropriate policies and procedures, and stronger password standards.

System Access Controls

Internal Audit uses the IT Governance Institute's Control Objectives for Information and related Technology (COBIT) as a framework for IT best practices. IT system access controls refer to policies, procedures, organizational structure, and electronic access controls designed to restrict access to computer software and data files. System access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment.

User Account Management

User account management entails requesting, establishing, modifying, and closing user accounts. There should be written procedures outlining the approval process as it applies to all internal and external users, and normal and emergency cases. Additionally, regular management reviews should be conducted of all accounts and related privileges.

Establishing or Modifying User Access

CTS does not have adequate formal policies and procedures for authorizing, establishing, or modifying user accounts on the network, iCIS, or the database. Furthermore, we found instances where CTS does not maintain adequate evidence of approval for user access currently established on the network, iCIS, and remotely. Formal standards should include:

- Procedure for requesting or modifying access
- Procedure for obtaining approval
- Procedure creating unique user accounts
- Procedure for maintaining evidence of approval

Terminating User Access

When terminated, an individual's access should be closed to prevent unauthorized change or deletion of data. CTS has not established formal policies and procedures for user access termination to iCIS and the database. We found one of eight (13%) terminated employees had access to iCIS. Furthermore, CTS did not retain appropriate user authorization forms for all terminated employees tested. Access termination procedures should include:

- Who is responsible for requesting user access termination
- Proper notification from the Court's Human Resources to CTS
- Who is responsible for terminating access

- Procedures for terminating user accounts

We also found that five of ten (50%) terminated employees still had active access to APETS. As a result, Adult Probation took corrective action during the course of this audit.

Password Management

Passwords are a system access control used to authenticate a computer user to a computer system. Passwords should be designed to restrict legitimate users to the specific systems, programs, and files they need. Passwords also prevent others, such as hackers, from entering the system at all. In addition, passwords identify the person responsible for a transaction, creating accountability for that transaction. Strong password controls, such as minimum length, periodic change, and encryption of password files, help reduce the potential for guessing or copying a user's password and using that password to gain unauthorized access to the system.

CTS' network password standards are inadequate. Current network password standards require a minimum of eight characters and expire every 180 days. CTS also lacks formal password policies for the iCIS application and database. Strong password standards should include:

- Minimum length of 8 characters
- Expiration every 90 days
- Minimum complexity (e.g., upper and lower case, special characters, alpha and numeric)
- Account lockout after three invalid access attempts
- Limiting the reuse of prior passwords

Access Security Management

Ensuring system security includes performing security monitoring and periodic testing, and implementing corrective actions for identified weaknesses to minimize the business impact of security vulnerabilities. Implementing a division of roles and responsibilities to reduce the possibility for a single individual to compromise a critical process strengthens system security. Personnel should only perform authorized duties relevant to their respective jobs and positions.

User Access and Duty Segregation Reviews

CTS has not established formal policies and procedures requiring reviews necessary to ensure that data is only accessible to those who require it for their job responsibilities (user access reviews, system and application segregation of duties reviews). Policies and procedures should include:

- Preparing a matrix identifying potential duty segregation conflicts
- Procedures for performing access and duty segregation reviews
- Frequency for performing access and duty segregation conflict reviews

Audit Log Reviews

Proactive security monitoring is essential to ensure data integrity. Logging and monitoring enables the early prevention, detection, and reporting of unusual activity. CTS does not have formal policies and procedures for monitoring auditing logs. Policies and procedures should

include maintaining evidence of the review, and should be performed by an individual that does not have privileged access to the system for which they are performing the review.

Recommendations

CTS management should:

- A.** Document formal policies and procedure for requesting new or modified access to the network, operating system, database, and application
- B.** Document formal policies and procedures for terminating user access within iCIS and the database
- C.** Ensure user access request forms are maintained for an appropriate period in order to provide an audit trail of additions, changes, and terminations to all user accounts
- D.** Strengthen network, operating system, iCIS, and database password standards
- E.** Document formal policies and procedures for reviewing user access and segregation of duty conflicts and perform reviews accordingly.
- F.** Document formal policies and procedures for monitoring audit logs for unauthorized activities
- G.** Ensure that Adult Probation reviews all active APETS users to determine if access is appropriate and required. Periodic user account reviews should be performed.

Issue 3 Systems Change Management

Summary

Systems changes should be managed through established policies and procedures to mitigate risks of negatively impacting the stability or integrity of Judicial Branch operations and ensure alignment to business requirements. We found weaknesses with CTS concerning project management, change management, and testing. CTS should develop formal change management policies and procedures for all applications, operating systems, databases and hardware changes. Further, CTS should establish formal project management policies and procedures for data conversion and testing.

Moving Systems Changes from Development to Operations

According to COBIT guidelines, all changes, including emergency maintenance and patches, should be formally managed. Changes (including those to procedures, processes, system, and service parameters) should be logged, assessed, and authorized prior to implementation, and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

We found the following control weaknesses:

- Inconsistency in the maintenance of approvals, prioritization, testing, and test results
- Lack of formal project management policies and procedures
- Lack of documented emergency change management procedures

Project management weaknesses may affect application, operational efficiency and effectiveness, and can increase the risk of unauthorized changes.

Data Conversion

Once development is complete, new systems and program changes should be thoroughly tested in a controlled environment to mitigate problems once the changes are operational. As stated in COBIT, this requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, and a post-implementation review. This ensures that operational systems are in line with the agreed-upon expectations and outcomes.

We found that CTS has not established formal data conversion policies and procedures. This may impact the implementation of applications such as the Juvenile Probation case management and financial system.

Recommendations

CTS should:

- A. Develop formal change management policies and procedures for all applications, operating systems, databases, and hardware changes, including:

1. Evaluation of the use of a project management office which should include business representation
 2. Management approval matrices for all levels of changes
 3. Change type definitions based on complexity and development time; (i.e. Major, Minor, Project)
 4. Priority definitions (i.e., Urgent, High, Medium, Low)
 5. Business case
 6. Documentation requirements for testing
 7. Maintaining evidence of successful testing by the business and IT
 8. Required approvals prior to migration into production
 9. Emergency change request procedures
- B.** Establish and document formal project management guidelines for data conversions which should include participation from IT and business end-users

Issue 4 Data Center Operations

Summary

Computer Operations controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. We determined that CTS appears to have adequate controls over computer operations, including help desk, backup and recovery, disaster recovery, and job scheduling. However, we found weaknesses in computer access authorization and review. CTS should develop appropriate policy and procedures for granting access to the computer room.

Access to Data Center

Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. We found that CTS lacked:

- Evidence that the computer room access was authorized
- Periodic user access reviews
- Formal policies and procedures for terminating user access to the data center

Weak controls over physical security could compromise the servers, the investment, and the data.

Recommendation

CTS management should establish formal procedures for granting and terminating access to the data center and for performing periodic reviews.

Issue 5 IT Governance

Summary

IT Governance ensures that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives. CTS has established IT Governance controls, such as a Judicial Branch IT steering committee and an IT strategic plan. However, CTS lacks a risk assessment framework. CTS should document formal procedures for evaluating and monitoring risk of all projects.

IT Governance Controls

IT governance involves defining organizational structures, processes, leadership, roles and responsibilities.

CTS has established several IT governance controls, including:

- A Judicial Branch IT steering committee that meets biweekly to review alignment of IT to business strategy and includes Juvenile Probation, Adult Probation, Justice Courts, Superior Courts, and Administration directors
- A three to five year IT strategic plan

However, we found that CTS lacks a risk assessment framework to ensure consistent risk analysis for each project and across departments.

Recommendation

CTS management should document formal procedures for evaluating and monitoring risk of all IT projects.

(Blank Page)

Department Response

AUDIT RESPONSE

Issue 1 - Application Controls

Response: Concur in process. During the first year in office, the CIO has been reviewing and revising CTS policies and procedures and best practices. We will incorporate these recommendations where appropriate.

Recommendation A: Revoke developer access to the end-user “production” functions.

Response: Concur in process. CTS will revoke unnecessary developer access to “production” functions and is developing a formalized access procedure. Further, CTS is cognizant of appropriate developer access rights as the rewrite of the iCIS application in the new architecture is being solidified.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation B: Restrict developer access to production database to query only.

Response: Concur in process. CTS will develop a policy that limits access to the production database to individuals in specific and appropriate positions for such actions.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation C: Review user access and disable any accounts belonging to terminated users. Determine whether any terminated user accounts have been accessed since the termination date.

Response: Concur in process. CTS is finalizing drafted policies related to this recommendation and will implement finalized versions.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation D: Restrict access to modify receipt or check transactions after authorization

Response: Concur – will implement with modifications. CTS requires additional business practice discussions with Justice Court Administration regarding this recommendation and will make changes accordingly.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation E: Perform regular reviews of user access rights and segregation of duties to remove any unauthorized or inappropriate user accounts or access rights.

Response: Concur in process. CTS is currently reviewing user access rights and establishing appropriate segregation of duties. Additionally, CTS is working on streamlined procedures, and associated policies, that tie into similar systems that are outside the scope of this audit. This involves working with Judicial Branch Administration to further define business practices affecting user access rights, and appropriate segregation of duties.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Issue 2 - System Access

Response: Concur in process. During the first year in office, the CIO has been reviewing and revising CTS policies and procedures and best practices as related to System Access. We will incorporate these recommendations where appropriate.

Recommendation A: Document formal policies and procedures for requesting new or modified access to the network, operating system, database, and application.

Response: Concur in process. Please refer to the response to Issue 1 – Recommendation E.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation B: Document formal policies and procedures for terminating user access within iCIS and the database

Response: Concur in process. Please refer to the response to Issue 1 – Recommendation E.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation C: Ensure user access request forms are maintained for an appropriate period in order to provide an audit trail of additions, changes, and terminations to all user accounts

Response: Concur in process. CTS will continue to develop this procedure in conjunction with appropriate Judicial Branch departments to allow for the necessary retention of user access request forms.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation D: Strengthen network, operating system, iCIS, and database password standards.

Response: Concur – will implement with modifications. CTS will continue to work with Judicial Branch Administration in establishing an acceptable password standard policy according to industry best practices.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation E: Document formal policies and procedures for reviewing user access and segregation of duty conflicts and perform reviews accordingly.

Response: Concur in process. Please refer to the response to Issue 1 – Recommendation E.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation F: Document formal policies and procedures for monitoring audit logs for unauthorized activities.

Response: Concur in process. Please refer to the response to Issue 1 – Recommendation E.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation G: Ensure that Adult Probation reviews all active APETS users to determine if access is appropriate and required. Periodic user account reviews should be performed.

Response: Concur with restrictions. CTS concurs with the recommendation. However, CTS cannot control these activities as they are completed by staff that works under the direction of the Adult Probation Department (APD). CTS will share this recommendation with appropriate APD staff and will collaborate with them to create an effective policy.

Target Completion Date: Investigate options - 12/31/2007
Implement solution - 01/30/2008

Benefits/Costs: Increased control and accountability.

Issue 3 - System Change Management

Response: Concur in process. During the first year in office, the CIO has been reviewing and revising CTS policies and procedures and best practices. We will incorporate these recommendations where

appropriate. Additionally with the pending rewrite of the Enterprise Case Management System it is anticipated that many of these recommendations can be more readily implemented.

Recommendation A: Develop formal change management policies and procedures for all applications, operating systems, databases, and hardware changes, including:

1. Evaluation of the use of a project management office which should include business representation
2. Management approval matrices for all levels of changes
3. Change type definitions based on complexity and development time; (i.e. Major, Minor, Project)
4. Priority definitions (i.e., Urgent, High, Medium, Low)
5. Business case
6. Documentation requirements for testing
7. Maintaining evidence of successful testing by the business and IT
8. Required approvals prior to migration into production
9. Emergency change request procedures.

Response: Concur in process. CTS will continue to develop and formalize existing policies and procedures, as well as those that have not been documented according to audit suggestions and industry best practices.

Target Completion Date: Investigate options - 03/30/2008
Implement solution - 05/30/2008

Benefits/Costs: Increased control and accountability.

Recommendation B: Establish and document formal project management guidelines for data conversions which should include participation from IT and business end users.

Response: Concur in process. CTS will formalize existing procedures that governs data conversions.

Target Completion Date: Investigate options - 03/30/2008
Implement solution - 05/30/2008

Benefits/Costs: Increased control and accountability.

Issue 4 - Data Center Operations

Response: Concur in process. During the first year in office, the CIO has been reviewing and revising CTS policies and procedures and best practices. We will incorporate these recommendations where appropriate. This has been an area that has been strengthened with the move to the new building.

Recommendation: CTS management should establish formal procedures for granting and terminating access to the data center and for performing periodic reviews.

Response: Concur – completed. CTS has established appropriate policy and procedures for granting access to the computer room/data center and for performing periodic reviews.

Target Completion Date: n/a

Benefits/Costs: Increased control and accountability.

Issue 5 - IT Governance

Response: Concur in process. During the first year in office, the CIO has been reviewing and revising CTS policies and procedures and best practices as related to IT Governance. We will incorporate these recommendations where appropriate. IT Governance continues to be an area of growth and importance for us.

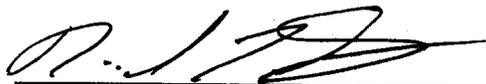
Recommendation: CTS management should document formal procedures for evaluating and monitoring risk of all IT projects.

Response: Concur in process. CTS will formalize existing risk assessment procedures.

Target Completion Date: Investigate options - 03/30/2008
Implement solution - 05/30/2008

Benefits/Costs: Increased control and accountability.

Approved By:



David L. Stevens, Chief Information Officer

8/29/07

Date



Marcus W. Reinkensmeyer, Court Administrator

9/7/07

Date



FOR JUDGE MUNDRELL

Honorable Barbara R. Mundell, Presiding Judge

9/7/07

Date