



Internal Audit Report

**Advantage Application Review
May 2005**



Audit Team Members

Susan Adams, Senior IT Auditor

Thomas Fraser, IT Auditor

KPMG LLP



Maricopa County

Internal Audit Department

301 West Jefferson St
Suite 1090
Phx, AZ 85003-2143
Phone: 602-506-1585
Fax: 602-506-8957
www.maricopa.gov

May 20, 2005

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

We have completed our review of Advantage, the County's financial reporting application. This audit was performed in accordance with the annual audit plan approved by the Board of Supervisors. The specific areas reviewed were selected through a formal risk-assessment process.

In general, we found the internal control environment of the Advantage system to be effectively established and operating appropriately.

The following areas need improvement:

- User access permissions and segregation of job duties
- Controls governing outsourced data center operations
- Disaster recovery planning
- Procedures related to data extraction, data validity, and annual financial reporting

Within this report you will find an executive summary, specific information on the areas reviewed, and departmental responses to our recommendations. We have reviewed this information with the Director of Materials Management, the Chief Information Officer, and the Chief Financial Officer, and appreciate the excellent cooperation provided by management and staff.

If you have any questions, or wish to discuss the information presented in this report, please contact Tom Fraser at 506-6079.

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
Department Accomplishments	4
Detailed Information	5
Department Response	18

Executive Summary

Advantage Security (Page 5)

Overall, the Department of Finance (DOF) utilizes documented procedures and established security roles to control user access to the Advantage application. However, our review identified segregation of duties conflicts and excessive user-access permissions. Inadequate user-access controls diminish the reliability of data and increase the risk of destruction or inappropriate disclosure of data. DOF should correct user access issues and develop procedures to monitor and periodically review user access levels and controls.

Data Center Operations (Page 8)

Control deficiencies were identified with the vendor's management of outsourced data center operations that, if not corrected, could have an adverse effect on County operations. The Chief Information Officer should strengthen internal controls to reduce the County's risk of system failures, business interruptions, unauthorized access, and corruption of critical financial data.

Disaster Recovery (Page 11)

The Office of the Chief Information Officer (OCIO) has not developed a disaster recovery plan to address the issues associated with the County's outsourcing of data center operations. Inadequate disaster recovery planning increases the risk of business interruptions and data loss or corruption. The OCIO should develop an effective disaster recovery plan that is regularly updated and tested.

Network Access (Page 12)

Several internal control weaknesses exist related to County network user access and password parameters. These issues could give unauthorized users the ability to discover confidential information and tamper with the County's financial system. The Chief Information Officer should strengthen internal controls over network user access and password parameters to reduce these risks.

System Development (Page 14)

The OCIO has not established formal mainframe application development policies and procedures. Without clearly defined application development policies and procedures, future projects are at risk of project delays, inadequate and incorrect system functionality, and budgetary overruns. The OCIO should develop formal policies and procedures for application development.

Financial Reporting (Page 16)

The Department of Finance (DOF) developed and manages the database used to support the County's Comprehensive Annual Financial Reporting (CAFR) process. Several control weaknesses exist within the procedures over Advantage data extraction, data validity, and CAFR assembly. This lack of control increases the risk of data inaccuracies within the CAFR. DOF should strengthen these controls.

Introduction

Background

The County's Department of Finance (DOF) is the primary owner of the Advantage financial application. Advantage is an off-the-shelf, integrated financial system that has been customized for the County, and has been used since 1992. The system runs on an IBM mainframe managed by Infocrossing Inc. and physically located in Brea, CA. Users input data interactively (online) and processing occurs in batches nightly. User security profiles that limit access to job-required system resources and functions are established and maintained by DOF. DOF processes invoices for all County entities including the Maricopa Managed Care System as of January 1, 2005.

The office of the County's Chief Information Officer (OCIO) provides technology support for the Advantage system. The office supports the base system, inventory, fixed assets, and the extended purchasing applications that are run in the mainframe environment. Most Advantage program changes are made annually through a release from the application vendor, American Management Systems. The OCIO programming staff makes some custom program changes as requested by end-users.

Materials Management is a key user of the Advantage financial application and utilizes the Advantage system to manage the County's procurement activities, manage established vendor accounts, and track approved contract expenditures.

Data Center Operations

In 2004 the County elected to outsource data center operations, and awarded a contract to Infocrossing, Inc. (IFOX). The vendor assumed responsibility for the operation and management of the County's mainframe processing environment in September 2004. Additionally, IFOX performs all processing operations functions to run the system software, including upgrades and substitutions, in support of the applications processed in the IFOX Data Center.

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers

IFOX recently contracted for a Statement on Accounting Standards (SAS) No. 70, Type 2 review of their internal controls to include control structure policies, operational policies and procedures, physical security, logical security, networks, backup provisions, disaster recovery planning, and contract provisions. Moore Stephens Smith Wallace LLC., an independent advisory and accounting firm located in St. Louis, Missouri, performed the SAS 70 review. The review was completed in October 2004 with the scope of work focused on the January 1, 2004 through September 30, 2004 time frame.

Initial Risk Assessment

This review was initiated because a recently completed Countywide Information Technology (IT) Risk Assessment performed by Internal Audit identified the Advantage system as the County's critical operational and financial application.

Scope and Methodology

The objectives of this audit were to determine if:

- General security and computing controls performed at Infocrossing and at the County are adequate to safeguard County data resources
- Security processes and configuration controls within the Advantage environment are established and user access is limited to required responsibilities
- Changes, enhancements, and modifications made to Advantage are properly authorized, approved, implemented, and documented
- Key end-user computing controls over the CAFR process are established and spreadsheets and databases are properly controlled

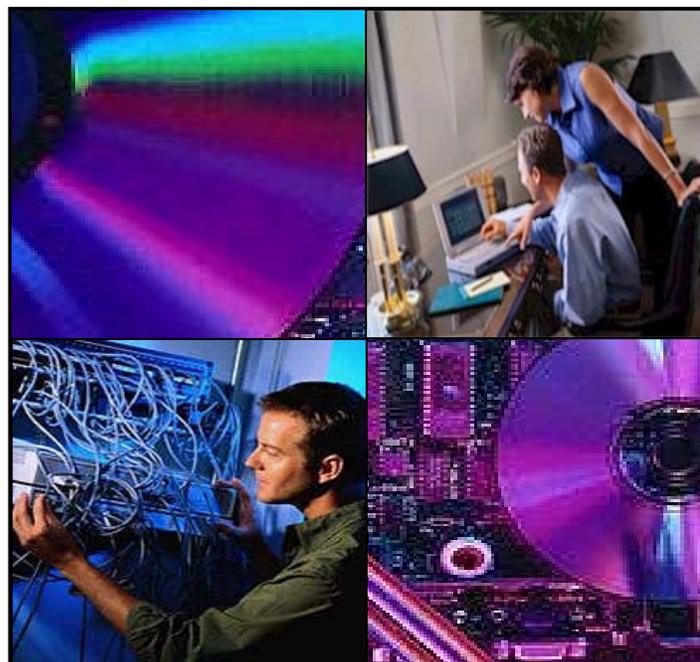
This audit was performed in accordance with generally accepted government auditing standards.

Department Reported Accomplishments

The Office of the Chief Information Officer (OCIO) has provided the following information for inclusion in this report.

Advantage Financial Systems

By the end of September 2004, County financial system mainframe operations were outsourced to Infocrossing of Brea, California. The outsourcing transition was implemented seamlessly as a result of the teamwork between the respective business areas, the interfacing systems, the OCIO, and Infocrossing. The estimated cost savings of the outsourcing are \$100,000 per year. A key benefit of the outsourcing involves disaster recovery. Since the processing of financial information is being done offsite in California, if a catastrophic event occurs in downtown Phoenix, Maricopa County financial data would not be at risk.



Issue 1 Advantage Security

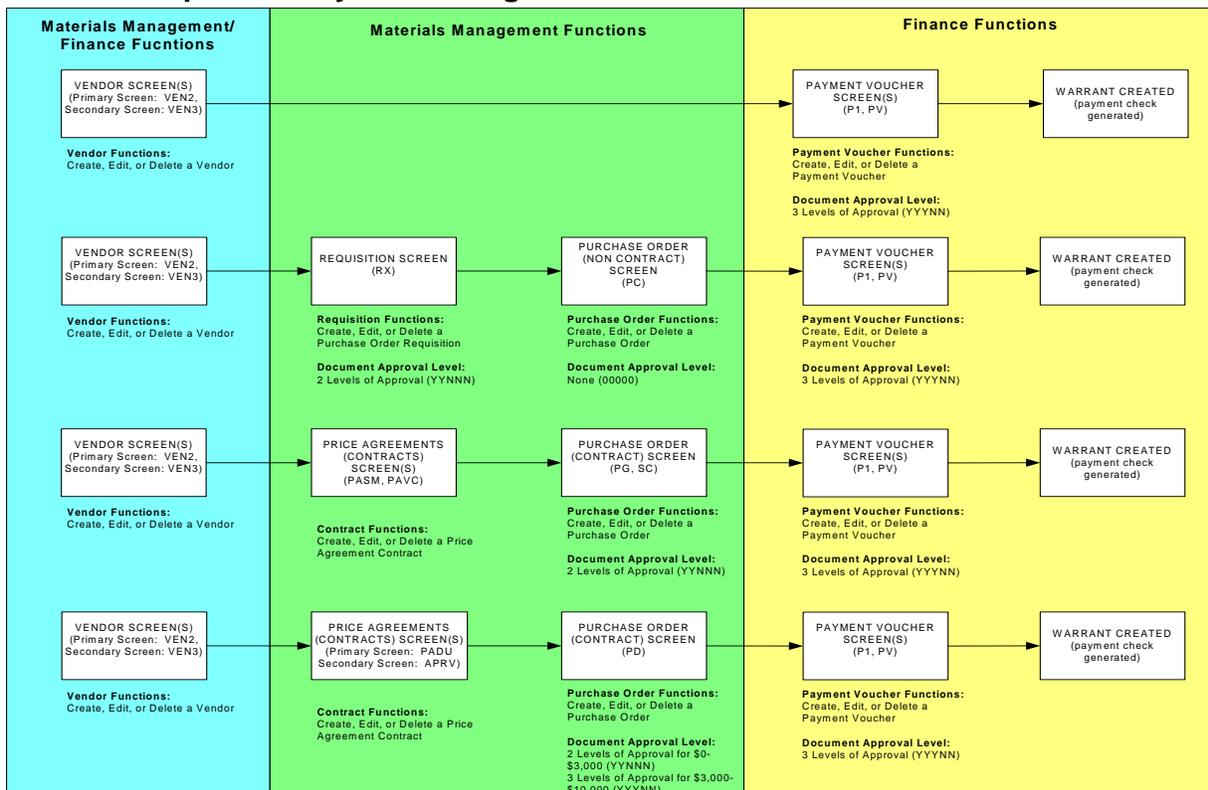
Summary

Overall, the Department of Finance (DOF) utilizes documented procedures and established security roles to control user access to the Advantage application. However, our review identified segregation of duties conflicts and excessive user-access permissions. Inadequate user-access controls diminish the reliability of data and increase the risk of destruction or inappropriate disclosure of data. DOF should correct user access issues and develop procedures to monitor and periodically review user access levels and controls.

Advantage Security

DOF is responsible for the management of general computer controls that support day-to-day transaction processing of the Advantage application. DOF manages user access and security over Advantage. Utilizing the knowledge of primary user departments (DOF, Materials Management) and the office of the Chief Information Officer we flowcharted the procurement process to identify key activity points. For each key activity point, we identified the associated Advantage screen menu as depicted in the following graphic.

Maricopa County Advantage Procurement Process Screen Flows



The above Advantage access controls points were compared to user profiles to identify users with possible segregation of duties issues

After obtaining user security profiles, we performed a detailed analysis to identify people that can perform two or more key activity points, which could allow them to bypass critical system segregation of duties controls. Our analysis noted security weaknesses in the following three areas:

Super User Access

Three Finance employees and one Materials Management employee have Super User access within Advantage. Super User access allows access to all Advantage tables and documents. This includes administering user security, modifying user profiles, creating financial documents, and modifying vendor information. Super User access is generally appropriate only for individuals who serve in a support or administration capacity and do not have transactional or functional responsibilities. A Super User often resides as an employee within the functional group and has hybrid IT/business support responsibilities (i.e., serving as front-line support for business users and as a liaison with IT). In functional groups where the Super User must also be assigned functional or transactional responsibilities due to business need, the activities of this individual must be monitored and validated by an appropriate supervising party. In general, this type of access should not be granted to employees noted in our review.

Segregation of Duties

The following system access segregation of duties conflicts exist within the County’s procurement process:

# of USERS	DEPARTMENT	INCOMPATIBLE DUTIES
4	Department of Finance	The ability to create vendors and create/approve payment vouchers
1	Materials Management	The ability to create vendors and create/approve payment vouchers through the use of multiple system user IDs
3	Materials Management	The ability to create Price Agreement Contracts and create/approve purchase orders up to \$3,000
3	Materials Management	The ability to create Price Agreement Contracts and create/approve purchase orders up to \$10,000
8	Materials Management	The ability to create Price Agreement Contracts and create/approve contract purchase orders
16	Materials Management	The ability to create and approve requisitions and create/approve non-contract purchase orders

These system access segregation of duties conflicts could lead to unauthorized or fraudulent vendor payments.

Appropriate Levels of Access

The ability to create vendors, create and approve payment vouchers and purchase orders, and create contracts and price agreements, appear to have been granted to employees not requiring these access permissions. There appear to be employees who have access to procurement

functions that are not needed for their job responsibilities. These functions include the following:

- Creating vendors
- Creating and approving payment vouchers and purchase orders
- Creating contracts and price agreements

Security Standards

The ISO/IEC 17799 International Security Standard states that care should be taken that no single person can perform unauthorized transactions in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization. The following controls should be considered:

- Segregation of activities that require collusion in order to defraud (e.g., creating a purchase order and verifying that the goods have been received).
- Requirement that two or more people be involved in activities with a risk of collusion, thereby lowering the possibility of unauthorized system activity.

Exposure

Inadequate user access controls diminish the reliability of data and increase the risk of destruction or inappropriate disclosure of data.

Recommendation

DOF should consider the following recommendations:

- A. Remove Super User access and limit system access to each employee's direct job responsibilities.
- B. Review the detailed security report and adjust security permissions to remediate these segregation of duties conflicts.
- C. Develop an Advantage security matrix to define required user roles and associated access permissions.
- D. Develop a formal Advantage security review process whereby actual system permissions are compared with authorized security permissions outlined in the Advantage security matrix.
- E. Perform the formal Advantage security review process at least annually, and require user management signoff.

Issue 2 Data Center Operations

Summary

Control deficiencies were identified with the vendor's management of the County's outsourced data center operations that, if not corrected, could have an adverse effect on County operations. The Chief Information Officer should address weak or missing internal controls to reduce the County's risk of system failures, business interruptions, and unauthorized access to or corruption of critical financial data.

Outsourcing Data Center Operations

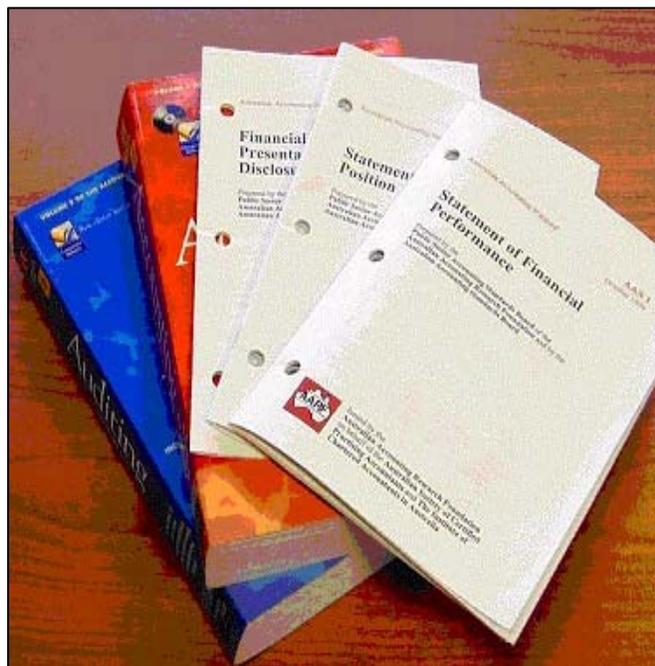
In 2004 the County elected to outsource data center operations, and awarded a contract to IFOX, who assumed responsibility for the operation and management of the County's mainframe processing environment in September 2004. Additionally, IFOX performs all processing operations functions necessary to run the system software, including upgrades and substitutions in support of applications processed in the IFOX Data Center.

SAS 70 Review

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

IFOX recently contracted for a SAS No.70 review. The review included an evaluation of their internal controls such as control structure policies, operational policies and procedures, physical security, logical security, networks, backup provisions, disaster recovery planning, and contract provisions.

Moore Stephens Smith Wallace LLC, an independent advisory and accounting firm located in St. Louis, Missouri, performed the SAS 70 review. The review was completed in October 2004 with the scope of work focused on the January 1, 2004 through September 30, 2004 time frame.



A SAS 70 review is an independent audit of an organization's IT controls and related processes

SAS 70 Review Testing

Auditing standards developed by the United States General Accounting Office state that sufficient, competent, and relevant evidence is to be obtained to afford a reasonable basis for the auditors' findings and conclusions.

Our audit procedures consisted of evaluating the tests performed by Moore Stephens Smith Wallace LLC to ensure there was an effective testing methodology supported by sufficient documentation to allow us to rely on the results of their testing. Additional clarity as to possible impact on County operations was obtained through interviews with IFOX management, the Office of the Chief Information Officer (OCIO), and with Moore Stephens Smith Wallace LLC.

Based on the issues noted in the SAS 70 report and inquiries with both Moore Stephens Smith Wallace LLC and IFOX, the following control and review deficiencies were identified.

Vendor Access

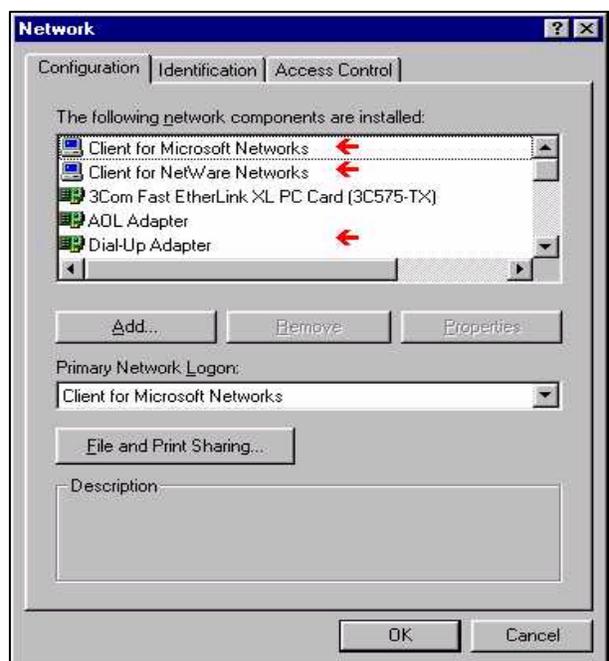
The only systems IFOX can connect to on the County network are the County's production, test, acceptance, education, and database environments physically located at IFOX. Additionally, this mainframe can connect to only a limited number of internal IP addresses. However, due to open firewall configurations, the mainframe can connect to any open network service on these internal IP addresses. These firewall configurations increase the risk of unauthorized access to County systems. The County should limit mainframe connectivity and network services to approved IP addresses.

Although the probability is relatively low, allowing IFOX to connect to all open network services on identified County internal IP addresses increases risk that an unauthorized user will gain access to other County resources.

The ISO/IEC 17799 International Security Standard states access control policy requirements for shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access policy and requirements of the business applications, and should be maintained and updated accordingly.

Exposure

Weak or missing internal controls increase the County's risk of system failures, business interruptions, and unauthorized access to or corruption of critical financial data.



Network User Access Configuration

Recommendations

The OCIO should:

- A.** Request annual SAS 70 reviews be performed and that the County be included in determining applicable samples and testing. Additional testing should be performed in cases where the external auditors experience high exception rates.
- B.** Limit IFOX mainframe connectivity of network services to approved IP addresses.

Issue 3 Disaster Recovery

Summary

The Office of the Chief Information Officer (OCIO) has not developed a disaster recovery plan to address the issues associated with the County's outsourcing of data center operations. Inadequate disaster recovery planning increases the risk of business interruptions and data loss or corruption. The OCIO should develop an effective disaster recovery plan that is regularly updated and tested.

Best Practices

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an organization's ability to accomplish its mission. For this reason, an organization should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions, (2) a plan to recover critical applications should interruptions occur, and (3) manual procedures for critical business processes.

Disaster Recovery Planning

In 2004 the County elected to outsource data center operations and awarded a contract to IFOX. IFOX assumed responsibility for the operation and management of the County's mainframe processing environment in September 2004.

A recently completed independent assessment of IFOX's internal controls identified Complementary User Controls that the County is required to establish and maintain under the IFOX service contract.

Each Complementary User Control was tested to identify any deficiencies. Additional detail on how the control deficiencies could possibly impact County operations was obtained through interviews with IFOX management, the OCIO, and Moore Stephens Smith Wallace L.L.C. who performed the IFOX SAS 70 review.

The OCIO has not developed a disaster recovery plan that incorporates the critical elements of IFOX's disaster recovery plan. The County has delayed development of their plan until IFOX has completed testing of their disaster recovery program to include a newly developed hot-site. If controls are not effective, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial information.

Recommendation

The OCIO should take proactive measures by ensuring an effective disaster recovery plan is established, tested, and updated periodically.

Issue 4 Network Access

Summary

Several internal control weaknesses exist related to County network user access and password parameters. These issues could give unauthorized users the ability to discover confidential information and tamper with the County's financial system. The Chief Information Officer should address weak or missing internal controls over network user access and password parameters to reduce the County's risk of unauthorized access to or corruption of critical financial data.

Review Results

Password Configurations

County network password parameters require passwords to contain between six and eight characters, however, the parameters do not require passwords to include a mix of both alpha and numeric characters. A sufficient level of password complexity decreases the risk of passwords being compromised. This could give unauthorized users access to confidential information leading to the ability to tamper with the County's financial system.

User Access

Current security settings allow batch jobs to run using universal access authority. Universal access authority grants batch jobs system permissions beyond their system requirements. This could give unauthorized users the ability to discover confidential information and tamper with the County's financial system.

User Status Notification

The County does not have a formal process to notify network administrators of users who have changed jobs or left the County. Without a formal process to notify network and Advantage Administrators about all terminated employees, there is an increased risk of unauthorized users having access to the mainframe and its applications (e.g., Advantage, Human Resources). This could give unauthorized users the ability to discover confidential information and tamper with the County's financial system.

The ISO/IEC 17799 International Security Standard states that access to information services should be controlled through a formal user registration process, which should dictate immediately removing access rights of users who have changed jobs or left the organization.

Password Resets

The helpdesk uses a common temporary password to reset network passwords. Individuals knowing the temporary password could attempt to access various mainframe user accounts using the common password. This could give unauthorized users access to confidential information leading to the ability to tamper with the County's financial system.

The ISO/IEC 17799 International Security Standard directs that users be provided with a secure temporary password that they are forced to change immediately. Temporary passwords provided

when users forget their password should only be supplied following positive identification of the user.

External/Vendor Access

The mainframe has a number of IFOX and County user accounts with system-wide access. System-wide access allows users to bypass critical network security functions such as logging. This could give unauthorized users the ability to tamper with the County's financial system without an audit trail.

The ISO/IEC 17799 International Security Standard states that privileges should be assigned to individuals on a need-to-use basis and on an event-by-event basis (i.e., the minimum requirement for their functional role only when needed).

Recommendation

The OCIO should consider:

- A. Establishing network password syntax rules to enforce a mix of alpha and numeric characters.
- B. Changing mainframe security practices by limiting security settings that allow batch jobs to run using universal access authority.
- C. Developing a formal communication process to promptly notify security administrators of all employee job changes and terminations.
- D. Requiring security administrators to regularly compare active user accounts with Human Resource records to confirm that all active user accounts are assigned to authorized personnel and do not pose segregation of duties conflicts.
- E. Requiring the helpdesk use a random password generator to create new passwords.
- F. Performing a review of all user IDs possessing system-wide access and removing system-wide access for user accounts not requiring it.
- G. Implementing a recurring certification process whereby management validates access rights within their areas of responsibility.

Issue 5 System Development

Summary

The Office of the Chief Information Officer (OCIO) has not established formal mainframe application development policies and procedures. Without clearly defined application development policies and procedures, future projects are at risk of project delays, inadequate and incorrect system functionality, and budgetary overruns. The OCIO should develop formal policies and procedures around application development.

Application Development

The County does not have formal mainframe application development policies and procedures to address the following:

- Defining business requirements, functional design, technical design, testing, and approvals
- Milestone signoff and approval
- Project documentation standards
- Segregation of duties between developers, testers, and implementers

Without clearly defined application development policies and procedures, future projects are at risk in the following areas:

- Unforeseen increases in scope
- Not meeting business requirements
- No Formal approval process
- Insufficient testing
- Inadequate project documentation and training materials

This could lead to project delays, inadequate and incorrect system functionality, and budgetary overruns. Additionally, the County does not use the required “Application Walk-Through” document to approve and migrate changes into the mainframe production environment. Without obtaining formal signoffs and approvals before migrating changes into production, there is an increased risk that unauthorized or untested changes will be made to the production environment that could cause data integrity issues.

Development Standards

The ISO/IEC 17799 International Security Standard states that in order to minimize the corruption of information systems, there should be strict control over implementation of changes. Formal change control procedures should be enforced. They should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary to perform their assigned tasks, and that formal agreement and approval for any change is obtained.

Recommendation

We recommend the OCIO develop formal policies and procedures around application development, at a minimum, to address the following:

- A.** Clear definition of business requirements, functional design, technical design, testing, and approvals
- B.** Milestone signoff and approval
- C.** Project documentation standards
- D.** Segregation of duties between developers, testers, and implementers
- E.** Utilization of the “Application Walk-Through” form to obtain documented signoffs and approvals before migrating changes into production.

Issue 6 Financial Reporting

Summary

The Department of Finance (DOF) developed and manages the database used to support the County's Comprehensive Annual Financial Reporting (CAFR) process. Several control weaknesses exist within the procedures over Advantage data extraction, data validity, and CAFR assembly. Due to the lack of formal controls over the DOF data main collection and CAFR development process, there is an increased risk of data inaccuracies within the CAFR. DOF should establish formal controls over the Access database and CAFR reporting process.

Review Results

Our review of DOF's procedures over Advantage data extraction, data management, and CAFR assembly procedures noted the following control weaknesses:

System Development

DOF does not use a formal change control process to make modifications to the Microsoft Access database used to support the CAFR reporting process. Without a formal change control process, there is an increased risk of unauthorized changes occurring. This could cause problems with the CAFR reporting process and lead to data inaccuracies within the CAFR.

Policies and Procedures

Although the Microsoft Access database has descriptions listed for each query and table, there is no formal documentation that describes in detail how to use the database and produce the CAFR. The CAFR reporting process is complex and requires significant knowledge and experience. If primary CAFR personnel are not available to assemble the CAFR, the County may encounter timeliness, accuracy, and completeness risks.

Segregation of Duties

The database owner and administrator for the CAFR SQL server is also the CAFR preparer. There is an increased risk that the data within the SQL Server database could be compromised and thus affect the validity of the CAFR.

User Access

Although the County maintains annual archives of the CAFR, the network folders housing the archives are not properly restricted. There is an increased risk that historical information could be altered. If the historical data is altered, the County may not be able to adequately respond to regulatory investigations and legal inquiries with accurate, valid data.

Recommended Standards

The ISO/IEC 17799 International Security Standard states in order to minimize information corruption, system controls should be established over change implementation procedures, facility operations, and critical business processes. In addition, important organizational records should be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities.

Recommendation

DOF should:

- A.** Implement a formal change control process.
- B.** Formally document the CAFR process and include separate SQL Server database administration and CAFR preparer responsibilities.
- C.** Set the CAFR network archive folders to read-only access.

Department Response

AUDIT RESPONSE
DEPARTMENT OF FINANCE APRIL 29, 2005

Issue #1:

Advantage Security - Overall, the Department of Finance (DOF) utilizes documented procedures and established security roles to control user access to the Advantage application. However, our review identified segregation of duties conflicts and excessive user-access permissions. Inadequate user-access controls diminish the reliability of data and increase the risk of destruction or inappropriate disclosure of data. DOF should correct user access issues and develop procedures to monitor and periodically review user access levels and controls.

Response: Concur. Processes are being put in place to reduce the risks that are detailed below.

Recommendation A: Remove Super User access and limit system access to each employee's direct job responsibilities.

Response: Concur—The Department of Finance will review Super User Access and system access and implement changes by 6/30/05. This will include removing at least one super user and considering the creation of a modified "Super User" profile which does not include all rights associated with a Super User Profile. A report will be created which documents all Super User activities on a weekly basis. This will be forwarded to the Finance Management Team weekly.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk of destruction or inappropriate disclosure of data.

Recommendation B: Review the detailed security report and adjust security permissions to remediate these segregation of duties conflicts.

Response: Concur – The Department of Finance will review the detailed security report and adjust security permissions by 6/30/05.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk of unauthorized or fraudulent vendor payments.

Recommendation C: Develop an Advantage security matrix to define required user roles and associated access permissions.

Response: Concur – The Department of Finance will create a detailed security matrix based on position description for Finance and Materials Management by 6/30/05.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk of improper functional or transactional responsibilities being assigned to the incorrect employees.

Recommendation D: Develop a formal Advantage security review process whereby actual system permissions are compared with authorized security permissions outlined in the Advantage security matrix.

Response: Concur – A procedure will be implemented which incorporates the review of the security matrix against the position description when assigning security rights. Exceptions to the Matrix requirements will be approved at a higher level.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk of improper functional or transactional responsibilities being assigned to the incorrect employees.

Recommendation E: Perform the formal Advantage security review process at least annually, and require user management signoff.

Response: Concur. A review process will be set up to review the security matrix and security assignment procedures.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk of improper functional or transactional responsibilities being assigned to the incorrect employees.

Issue #6:

Financial Reporting - The Department of Finance (DOF) developed and manages the database used to support the County's Annual Financial Reporting (CAFR) process. Several control weaknesses exist within the procedures over Advantage data extraction, data validity, and CAFR assembly. This lack of control increases the risk of data inaccuracies within the CAFR. DOF should strengthen these controls.

Response: Concur. Processes are being put in place to reduce the risks that are detailed below.

Recommendation A: DOF should implement a formal change control process.

Response: Concur—The Department of Finance has created a log to record all changes which must be initialed before changes are made to the Microsoft Access database used to support the CAFR reporting Process.

Target Completion Date: 4/26/05

Benefits/Costs: Reduction in the risk of unauthorized changes and the benefit of a historical record of all changes made to the database.

Recommendation B: Formally document the CAFR process and include separate SQL Server database administration and CAFR preparer responsibilities.

Response: Concur – The Department of Finance will document the CAFR preparation process and separate the SQL Server Administration and CAFR preparer responsibilities by 6/30/05 by assigning SQL and CAFR preparation to separate individuals.

Target Completion Date: 6/30/05

Benefits/Costs: Reduction in the risk that data in the SQL Server could be compromised and reduction in the risk of County encountering timeliness, accuracy and completeness problems.

Recommendation C: Set the CAFR network archive folders to read-only access.

Response: Concur. All historical CAFR network archive folders through 6/30/03 have been set to "read only" as of 3/9/05.

Target Completion Date: 3/9/05 - Completed

Benefits/Costs: Reduction in the risk that historical information can be altered.

Approved By :



Department Head/Elected Official

5/5/05
Date



Chief Officer

5/5/05
Date



County Administrative Officer

5/13/05
Date

AUDIT RESPONSE
OFFICE OF THE CHIEF INFORMATION OFFICER
MAY 10, 2005

ISSUE #2:

Control deficiencies were identified with the vendor's management of the County's outsourced data center operations that, if not corrected, could have an adverse effect on County operations. The Chief Information Officer should address weak or missing internal controls to reduce the County's risk of system failures, business interruptions, and unauthorized access to or corruption of critical financial data.

Response: Concur.

Recommendation A: Request annual SAS 70 reviews be performed and that the County be included in determining applicable samples and testing. Additional testing should be performed in cases where the external auditors experience high exception rates.

Response: Concur.

Target Completion Date: **December 31, 2005**

Benefits/Costs: Increased control over data center operations.

Recommendation B: Limit IFOX's production and mainframe connectivity of network services on approved IP address.

Response: Concur. Completed - Configured the IFOX connections through the County's firewall to allow traffic on only specific ports and specific services for the assigned IFOX IP address.

Target Completion Date: **Completed April 2005**

Benefits/Costs: Increased control over network security.

ISSUE #3:

The Office of the Chief Information Officer (OCIO) has not developed a business continuity plan to address the issues associated with the County's outsourcing of data center operations. Inadequate business continuity planning increased the risks of business interruptions and data loss or corruption. The OCIO should develop an effective business continuity plan that is regularly updated and tested.

Response: Concur.

Recommendation:

The OCIO should take proactive measures by ensuring an effective Business Continuity Plan is established, tested, and updated periodically.

Response: Concur.

Target Completion Date: **December 31, 2006**

Benefits/Costs: Increased controls to mitigate risks associated with disaster events.

ISSUE 4:

Several internal control weaknesses exist related to County network user access and password parameters. These issues could give unauthorized users the ability to discover confidential information and tamper with the County's financial system. The Chief Information Officer should address weak or missing internal controls over network user access and password parameters to reduce the County's risk of unauthorized access to or corruption of critical financial data.

Response: Concur.

Recommendation A:

Establishing network password syntax rules to enforce a mix of alpha and numeric characters.

Response: Concur.

Target Completion Date: **December 31, 2005**

Benefits/Costs: Increase control over access security.

Recommendation B:

Changing mainframe security practices by limiting security settings that allow batch jobs to run using universal access authority.

Response: Concur.

Target Completion Date: **December 31, 2005**

Benefits/Costs: Increase control over access security.

Recommendation C:

Develop a formal communication process to promptly notify security administrators of all employee job changes and terminations.

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over access security.

Recommendation D:

Require security administrators to regularly compare active user accounts with Human Resource records to confirm that all active user accounts are assigned to authorized personnel and do not pose segregation of duties conflicts.

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over access security.

Recommendation E:

Requiring the helpdesk use a random password generator to create new passwords.

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over access security.

Recommendation F:

Perform a review of all user IDs possessing system-wide access and removing system-wide access for user accounts not requiring it.

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over access security.

Recommendation G:

Implement a recurring certification process whereby management validates access rights within their areas of responsibility.

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over access security.

ISSUE 5 SYSTEM DEVELOPMENTS

Develop formal policies and procedures around application development, at a minimum, to address the following:

Response: Concur.

Recommendation A:

Clear definition of business requirements, functional design, technical design, testing, and approvals

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over system development processes.

Recommendation B:

Milestone signoff and approval

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over system development processes.

Recommendation C:

Project documentation standards

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over system development processes.

Recommendation D:

Segregation of duties between developers, testers, and implementers

Response: Concur.

Target Completion Date: **June 30, 2006**

Benefits/Costs: Increase control over system development processes.

Recommendation E:

Utilization of the "Application Walk-Through" form to obtain documented signoffs and approvals before migrating changes into production.

Response: Concur. Completed - To fulfill this recommendation, an Audit Trail Checklist has been developed to accompany each service request. Permission from the client to migrate to Acceptance or Production regions is obtained through email. The email is retained with other service request documentation.

Target Completion Date: **Completed April 2005**

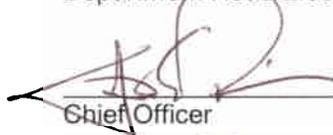
Benefits/Costs: The Audit Trail Checklist ensures that audit recommendations are being followed for migrating changes and closing the completed service request.

Approved By:

N/A

Department Head/Elected Official

Date



Chief Officer

5/11/2005
Date



County Administrative Officer

5/12/05
Date