



CITY OF SAN ANTONIO

P.O. BOX 839966
SAN ANTONIO, TEXAS 78283-3966

March 21, 2005

Edward D. Garza
Mayor, City of San Antonio

Richard Perez
Councilman, District 4

Julian Castro
Councilman, District 7

Art Hall
Councilman, District 8

Carroll Schubert
Councilman, District 9

J. Rolando Bono
Interim City Manager

Andrew Martin
City Attorney

Richard Varn, Interim
Chief Information Officer

Gary Moeller
Director, ITSD

Gentlemen:

RE: Issue Final Report – Information Technology Services Application Change Controls Audit

The Application Change Controls Audit, which was approved by the Governance Committee as part of the FY2004-2005 Audit Plan, has been completed.

The scope of this audit was limited to reviewing application change controls for the various mainframe system programs and the SAP System. The report highlights nine audit findings that can be used as opportunities to improve internal controls within the application change lifecycle. At this time, the mainframe systems are the most vulnerable from a risk perspective based upon the issues identified. This seemed unusual to the audit team since the City has used and made changes to such applications for many years. The ERM Project SAP System presented fewer risk challenges to the City. To avoid the pitfalls commonly encountered, ITSD Staff should not delay completing the required documentation for the SAP System due to other priorities.

The following issues are detailed in the audit report:

Mainframe System Programs:

- Application development standards were not documented.
- Mainframe security guidelines and procedures did not exist.
- Mainframe application change procedures were not documented.
- Use of production data for test purposes was not documented.
- Version control occurred manually in some cases.

SAP System:

- The process for making changes directly to the production system was not documented.
- Operating system level security guidelines were not documented.
- Emergency change management procedures were not documented.
- Changes were not consistently documented in the issue-tracking database.

A conclusion was made on the effectiveness of internal controls for both the mainframe and SAP System. It was formed through performing generally accepted audit procedures and was based on a Risk Management Capability Matrix. Figure 1 in the audit report is a more detailed description of the capability matrix.

It was determined that the process capability stage for mainframe system programs application change controls was "Ad Hoc". In the general definition of this stage, it means that procedures do not formally exist, and that controls were either non-existent, or primarily reactionary. The "Ad Hoc" Stage usually indicates that there are no metrics/measurement or monitoring of performance. Through the formalization of change procedures, documentation of these, and with enhanced security, the mainframe system programs application change controls could improve from "Ad Hoc" to "Defined" Stage.

It was determined that the process capability stage for SAP System application change controls was "Defined". At the "Defined" Stage, procedures are usually well documented but not regularly updated to reflect changing business needs. Generally, at this stage both preventive and detective controls are used. However, there were no metrics stated for the change control process that could be used for measurement. With moderate effort, the City's SAP System application controls could be improved to the "Managed" Stage. This level could be achieved through the regular updates of documentation supporting the change cycle, and through implementing metrics to monitor the performance of each critical change function.

The current state of internal controls in the mainframe application programs environment will continue to pose a significant risk to data operations at the City of San Antonio. Several high profile and/or public safety related applications reside on the ITSD Mainframe System. These include the 9-1-1 Central Dispatching, Case Reporting System (used for EMS), and the Municipal Courts Warrants and Citations. The cumulative affect of the control weaknesses could present substantial difficulty recovering from a critical computer application system failure, or from the loss of key employees. Overall, current ITSD documentation does not meet any of the generally accepted standards. As such, it may not be reliable in training replacement personnel, or in a time of crisis when remote or recovery operations may be required.

The assistance provided by ITSD Personnel during this audit was extremely helpful and greatly appreciated. Department Management has provided specific corrective action and dates for completion. The Interim Chief Information Officer (CIO) has also reviewed and concurred with the issues raised by the audit, and with the actions planned by ITSD. It is also appropriate to thank the Interim City Manager, Mr. J. Rolando Bono, for this opportunity to review the City's information systems operations. While this particular audit project did not result in hard dollar cost recoveries, it did establish prospective benefits to the City through recommendations for improved effectiveness for these processes. It further provided the Interim City Manager and CIO with a critical status report on several key processes within ITSD.

Should you have any questions, a presentation on this audit will be scheduled for the next Governance Committee Meeting. We are also available for individual discussions or briefings if you would prefer.

Sincerely,



Patricia M. Major CPA, CIA, CTP, CGFM
City Internal Auditor
(210) 207-2853 Office, (210) 215-9455 Cell

cc: Troy Elliott – ERM Project Director
Rusty Phelps – Production Support Manager
Steve Bishop – Information Services Manager
Jim Bischoffberger – Information Services Manager
Hugh Miller – Information Services Manager
Mark Krisak – Assistant Information Services Manager



CITY OF SAN ANTONIO

INTERNAL AUDIT DEPARTMENT

**Audit of Application Change Controls
For the Mainframe and SAP Systems**

Project No. AU05-006

January 21, 2005

Prepared By:

Patricia Major CPA, CIA, CTP, CGFM
Mark Swann CPA, CIA, CISA
David Baumgartner CISA
Oscar Salazar

EXECUTIVE SUMMARY

Overview

Computer applications are continually changing to meet the demands of evolving business requirements. The internal controls that govern these changes are called application change controls. Application change controls play a critical role in protecting applications from the introduction of errors that could lead to disruption of work function, corruption of data, increased costs of maintenance or the inability of the City to provide timely response to citizens.

Properly applied change controls provide that, over time, application systems maintain the level of integrity and reliability intended at the point of inception.

A review of the City of San Antonio Information Technology Services Department's (ITSD) application change controls over the mainframe and the SAP System has been completed. Fieldwork for this review was conducted primarily during the period November 2004 through January 2005, with additional information being obtained thereafter.

This review was designed to provide reasonable but not absolute assurance that key internal controls within the application change management lifecycle for the mainframe and SAP System are operating effectively. The review included a study of internal controls based on discussion and reviews of selected documentation and would not necessarily reveal all internal control weaknesses.

Results In Brief

Based upon the work performed for this review, a number of issues and observations have been included in the report. Many of the issues are related to strengthening internal controls at ITSD.

Strengthening internal controls will help to ensure that mainframe and SAP application changes occur in a controlled and expected manner. In addition, the controls could provide documentation to be used as a baseline for ITSD operations requiring a well-controlled environment.

The control weaknesses identified were in following areas:

- Development of documented procedures for introducing change;
- Improvements in documenting actions taken to implement a change;
- Developing standard practices for application development; and
- Defining security parameters to limit application change capabilities.

Developing documented change procedures will help ensure a uniform process is followed for introducing change into an application system. Improving the use of Thread Manager to document actions performed for each specific application change will provide a single point to store and retrieve information supporting the need for and steps taken to implement each change. Developing standard practices for application development will help ensure that programming staff are using tools and techniques endorsed by ITSD Management when developing or changing applications. Improved application security standards will strengthen controls in place to permit or deny specific application change tasks.

For the most part, ITSD has agreed with the findings and has identified a course of action to implement corrective or mitigating measures.

The following pages provide an overview of the audit activities performed and the results obtained through the course of this project.

Background

Information Technology (IT) systems play a vital role in acquiring, processing, storing and distributing key financial, operational, and human resource related data at the City of San Antonio. Two key IT systems utilized by the City are SAP and the mainframe.

The mainframe environment plays a vital role in City operations by supporting many specialized business applications. Departments such as Municipal Courts, Health, Fire, EMS, Police, Alamodome, Aviation and Parks & Recreation process information through mainframe applications.

SAP is the primary system used for contract management, finance, inventory, purchasing, human resources and payroll. Future usage will also include budget preparation, work order processing and customer relationship management.

From October 2004 through December 2004, 770 changes were implemented in SAP alone through the transport management process. The volume of changes and the sensitivity of the data residing in both SAP and on the mainframe create increased concern about the integrity of internal controls over applying changes to these systems.

Objective

The objective of this audit project was to determine the adequacy and appropriateness of the internal control environment and risk management process used to manage changes to the SAP R/3 and mainframe computer applications.

Scope

The scope of this audit project was limited to the application change controls governing changes introduced into SAP and the mainframe application environment. The period under review includes any changes made during fiscal years 2004 and 2005 through the first quarter.

Criteria

This review was performed in compliance with Generally Accepted Government Auditing Standards (GAGAS) issued by the U.S. Government Accountability Office (GAO). To measure performance, audit staff used criteria based on City of San Antonio (COSA) policies and procedures, Control Objectives for Information and related Technology (CobiT) and sound practices developed outside of the COSA organization.

The IT Governance Institute (www.itgi.org) developed CobiT as an open standard using non-technical language to help focus information technology in support of overall business goals. CobiT was selected as criteria for measurement because it is aimed at addressing business objectives and is easy to understand. CobiT continues to gain acceptance internationally and is evolving due to support from the IT Governance Institute.

In addition to standards such as CobiT, there are other industry based or technology specific standards that can be used to measure an organizations control performance. The Center for Internet Security (CIS) and SANS (SysAdmin, Audit, Network, Security) Institute both provide guidance on baselines to be used for enhancing control at a more detailed level. The Capability Maturity Model for Software (SW-CMM) could be used to judge the maturity of the software process and for identifying key practices that are required to advance the maturity of these processes. Additionally, the Information Technology Infrastructure Library (ITIL) provides a cohesive set of best practices drawn from public and private sectors internationally.

It is important to note in reviewing the results of this audit that the City's Information Technology Services Department has not historically used these or other standards to measure control performance related to the application change cycle.

Methodology

This audit was performed in accordance with Internal Audit Department procedures based on GAGAS.

In order to perform the work required, audit staff used the following techniques:

- Reviewed documented policies and procedures provided by City ITSD management;
- Performed inquiries with City ITSD employees;
- Developed process maps (or flow charts) with concurrence from City ITSD staff;
- Conducted analysis of internal controls to identify key controls for testing; and
- Selected sample change requests for SAP and the mainframe to test the effectiveness of internal controls.

Conclusion

After the completion of audit procedures, a conclusion was made on the effectiveness of internal controls for both SAP and the mainframe. The conclusion was formed through performing generally accepted audit procedures and was based on a Risk Management Capability Matrix. The risk matrix provides information on characteristics of development stages for strategy capabilities, process capabilities, people capabilities, technology capabilities and information capabilities. For this project, the assessment was based specifically on process capabilities. A more detailed description of the process capability stages has been included as **Figure 1**.

It was determined that the process capability stage for SAP application change controls was "Defined". At the "Defined" stage, procedures were well documented but were not regularly updated to reflect changing business needs. Both preventive and detective controls were employed throughout the process. There were no metrics used for measurement.

With moderate effort, SAP application controls could be improved to the "Managed" stage within the next calendar year. This level could be obtained through the regular update of documentation supporting the change cycle and through implementing metrics to monitor the performance of each critical change function.

It was determined that the process capability stage for mainframe application change controls was "Ad Hoc". At the "Ad Hoc" stage, procedures did not formally exist and controls were either non-existent, or primarily reactionary in nature. There were no metrics or specific monitoring of performance.

Through the formalization of change procedures and documentation, along with enhanced mainframe security, the mainframe application change control stage could improve from "Ad Hoc" to "Defined" throughout the next calendar year.

Figure 1 – Process Capability Maturity Stages

<u>Stage</u>	<u>Procedures</u>	<u>Controls and Process Improvements</u>	<u>Metrics*</u>
Ad Hoc	<ul style="list-style-type: none"> No formal <i>procedures</i> exist. 	<ul style="list-style-type: none"> <i>Controls</i> are either non-existent, or are primarily reactionary after a “surprise” within the company. 	<ul style="list-style-type: none"> There are no <i>metrics</i> or monitoring of performance.
Repeatable	<ul style="list-style-type: none"> Some standard <i>procedures</i> exist. 	<ul style="list-style-type: none"> Detective <i>controls</i> are relied upon throughout the company. 	<ul style="list-style-type: none"> Few performance <i>metrics</i> exist, thus there is infrequent monitoring of performance.
Defined	<ul style="list-style-type: none"> <i>Procedures</i> are well documented, but are not regularly updated to reflect changing business needs. 	<ul style="list-style-type: none"> Both preventive and detective <i>controls</i> are employed throughout the company. 	<ul style="list-style-type: none"> Some <i>metrics</i> are used, but monitoring of performance is primarily manual.
Managed	<ul style="list-style-type: none"> <i>Procedures</i> and <i>controls</i> are well documented and kept current. 	<ul style="list-style-type: none"> Best practices and benchmarking are used to <i>improve</i> process in certain areas of the company. 	<ul style="list-style-type: none"> Many <i>metrics</i> are used, with a blend of automated and manual monitoring of performance.
Optimized	<ul style="list-style-type: none"> <i>Processes</i> and <i>controls</i> are continuously reviewed and <i>improved</i>. 	<ul style="list-style-type: none"> Extensive use of best practices and benchmarking throughout the company helps to continuously <i>improve</i> processes. 	<ul style="list-style-type: none"> Comprehensive, defined performance <i>metrics</i> exist, with extensive automated monitoring of performance employed.

*Metrics provide a means for measuring how well a control or process is performing.

Observations, Recommendations, and Responses

The following observations, recommendations and management responses were recorded as a result of work procedures performed. They are presented in order of significance beginning with mainframe issues followed by SAP issues.

Many mainframe applications exist to provide critical services to the City of San Antonio. Even after the Enterprise Resource Management (ERM) Project implementation is completed, mainframe applications will continue to play a vital role in supporting many City operations such as:

- Fire, EMS and Police Dispatching;
- Health Department Services;
- Municipal Court Services; and
- Development Services.

There are approximately seventy mainframe applications supported by twenty staff programmers in the Information Technology Services Department.

The Enterprise Resource Planning component of the ERM implementation uses SAP to provide an integrated environment for managing several critical processes at the City including:

- Financial – General Ledger, Accounts Payable, Payroll, Accounts Receivable, and Accounting
- Treasury - Funds Management
- Material Management – Purchasing, Contracts, Inventory Management
- Project Management – Capital Projects and Maintenance Orders
- Controlling - Budget Preparation and Cost Center Accounting
- Sales and Distribution – Revenue Billing and Accounting
- Human Resources – Organizational Management, Personnel, Benefits, Compensation, and Training

Mainframe Issue #1: Application Development Standards

Condition

Application development standards are not documented. As a result, there was no uniform procedure governing the use of development and productivity tools, library and data file naming conventions or program compiling procedures.

Criteria

CobiT control objective A14 - Develop and Maintain Procedures specifies that to ensure the proper use of the applications and the technological solutions put in place, a structured approach to the development of user and operations procedures manuals, service requirements and training materials should be developed.

Cause

Application development and productivity standards or procedures were neither defined nor documented.

Effect

Without documented procedures, there was an increased risk that nonstandard development tools and techniques could be used. In addition, it was more difficult to determine if changes were developed and implemented in accordance with an accepted process.

Recommendation

ITSD should develop and document mainframe programming standards and procedures. Contents should include, but not be limited to the following:

- Specific naming conventions for program development;
- Job Control Language standards for executing programs;
- Libraries for storing production source and object modules; and
- The use of data files in both test and production.

Management Response – February 8, 2005

ITSD concurs with the finding and recognizes the need to develop and document mainframe programming standards and procedures. As a result, ITSD's Business Information Support Manager will:

- *Develop programming standards for COBOL, CICS and Natural programming languages;*
- *Develop standards for storing Development and Production source and object modules;*
- *Develop standards for the use of Development and Production data files;*
- *Develop standards for the JCL execution of Development and Production programs; and*
- *Develop a list of all Development and Production source and object libraries.*

Expected completion date is December 2005.

Mainframe Issue #2: Mainframe Security

Condition

Mainframe security guidelines and procedures do not exist. Audit staff obtained and reviewed a list, provided by ITSD management, of system users authorized to perform changes to production applications. After comparing this list to the actual mainframe security settings, it was discovered that seven users were not on management's approved list but had access to perform changes to production. In addition it was discovered that two users, who were approved by management to perform changes to production, were authorized through special security privileges instead of specific authorizations.

In addition, security has not been configured to restrict access to powerful system utilities. Such utilities could override normal change controls by allowing the deletion and migration of code or direct configuration of program files.

Criteria

CobiT control objective DS5 - Ensure System Security specifies that information be safeguarded against unauthorized use, disclosure or modification, damage or loss by restricting to authorized users. In addition, CobiT control objective DS9 - Managing the Configuration indicates that to effectively manage the configuration the City needs to prevent unauthorized program alterations.

Cause

Mainframe security guidelines and procedures have not been documented; as such there are no formal procedures for periodically reviewing mainframe user access.

Effect

The lack of formal guidelines created an increased risk that unauthorized changes may have been made to production source and object libraries.

Recommendation

ITSD should develop mainframe security guidelines and distribute them to all appropriate staff. The guidelines should be based on mainframe security best practices and, at a minimum, include the following:

- Regular review of user access;
- Methods to assign special account privileges;
- Guidelines for granting access based on job requirements; and
- Guidelines for handling powerful system utilities.

Management Response – February 8, 2005

ITSD concurs with the findings and recognizes the need to document production source and object libraries. As a result, ITSD's Business Information Support Manager will:

- *Develop a list of all production source and object libraries;*
- *Develop a list of users that have access to each of these libraries;*
- *Review these lists quarterly to ensure appropriate access;*
- *Develop a list of all Non-Cancel users and review this list quarterly to ensure appropriate access.*

Expected completion date is April 2005.

ITSD also recognizes the need to secure access to sensitive utilities to prevent inadvertent damage to data. As a result, ITSD's Production Manager will:

- *Install, test and implement a security tool to secure powerful database utilities*
 - *Expected completion date is May 2005*
- *Install, test and implement a security tool to secure programming language utilities*
 - *Expected completion date is September-November 2005*

Mainframe Issue #3: Mainframe Application Change Procedures

Condition

Mainframe application change management procedures were not documented. All procedures currently followed were informal and were not consistently tracked to provide an appropriate level of documentation. There was not a method in place to determine if a potential change may have affected departments or operations outside of the intended scope.

Criteria

CobiT control objective A16 - Managing Changes specifies that unauthorized alterations, disruption, and errors can be minimized by a management system which provides for analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure.

CobiT control object DS10 - Managing Problems and Incidents states that a problem management system, to record incidents and actions taken, helps ensure that incidents are resolved and the cause investigated to prevent any recurrence.

Cause

Change management procedures were not documented.

Effect

Without a formal procedure, there was an increased risk that key components of the change management lifecycle would not be completed. In addition, the risk was also increased that unauthorized changes could be made to applications. Without a process in place to analyze the potential impact a change may have, risk of service delays was increased.

Recommendation

It is recommended that mainframe application change management procedures be documented and distributed to all appropriate personnel. Emergency and ad-hoc procedures should be included. Procedures should also include requirements for completing documentation throughout the change cycle where appropriate. The defined procedure should produce a consistent strategy for tracking changes from initiation through completion.

In addition, it was recommended that ITSD initiate a mainframe change management committee. Alternatively, a single enterprise-wide information technology change management committee could also provide an appropriate venue for assisting with mainframe change prioritization and risk mitigation.

Management Response – February 8, 2005

ITSD concurs with the findings and recognizes the need to develop and implement mainframe change management procedures. As a result, ITSD's Business Information Support Manager will:

- *Develop and implement a mainframe change management process based on the change management policies and procedures adopted for the Hansen and SAP Systems, which includes a change management control board.*

Expected completion date is December 2005.

Mainframe Issue #4: Production Data Used For Test Purposes

Condition

The City Information Technology Services Department lacked written procedures for using production data in a test environment. Current mainframe security privileges allowed programmers to copy data from production to a test environment for troubleshooting.

Criteria

CobiT control objective DS5 - Ensure System Security specifies that information be safeguarded against unauthorized use, disclosure, modification, damage or loss by restricting access to authorized users.

Cause

Management has not provided documented guidelines on the use of sensitive or confidential production data for testing purposes.

Effect

Production data used in a test environment inherently increased the potential for unauthorized disclosure of sensitive and confidential data.

Recommendation

ITSD should develop a written procedure to govern the use of production data for test purposes by department programmers.

Management Response – February 8, 2005

ITSD concurs with the findings and recognizes the need to define procedures for the use of development and production data. As a result, ITSD's Business Information Support Manager will:

- *Develop procedures for the use of development and production data.*

Expected completion date is April 2005.

Mainframe Issue #5: Version Control For Mainframe Programs

Condition

Version control was handled manually for certain mainframe programs. There were three workgroups and each was responsible for certain applications. Application source code and objects were maintained in multiple locations, and each workgroup administered version control using their own professional judgment.

Criteria

CobiT control objective A16 - Managing Changes indicates that effective management of change should include a system, which provides for release management and identification of changes.

Cause

The current version control procedure accounts for only Natural program language-based applications.

Effect

Due to the manual process, the risk of incorrect program versions being modified or migrated to production was increased.

Recommendation

Internal controls can be improved by extending the current Source Program Library Management (SPLM) scheme for non-Natural Programs to include uniform version management controls. In addition, the current change management system for Natural programs and objects has an optional feature that allows for automatic version control of non-Natural programs. This would allow for complete integration of non-Natural source and objects into a single version control system.

ITSD should conduct a feasibility study to determine the cost and effectiveness of this option to provide version management controls.

Management Response – February 8, 2005

ITSD concurs with the finding and recognizes the need to implement uniform version management control for non-Natural programs. As a result, ITSD's Business Information Support Manager will:

- *Perform a trial usage of a product add-on feature to extend their current version management application for use with non-Natural programs in an effort to verify compatibility; and*
- *If successful, procure the feature to enable its use beginning in July 2005.*

Expected completion date is July 2005.

SAP Issue #1: Changes Made Directly To SAP Production

Condition

SAP was configured to allow changes to be made directly to the production version of the software. On November 4, 2004 it was determined that the City's SAP System settings allowed for direct change to the production environment. The settings were then updated to "no changes allowed" on December 9, 2004; however, on December 16, 2004, the settings were updated again. This indicated that the system had been opened up to allow a change to be made directly to production on multiple occasions.

Criteria

CobiT control objective DS9 – Manage the Configuration indicates that to effectively manage the configuration the City needs to prevent unauthorized program alterations. In addition, COSA SAP security architecture was built around the understanding that the production client should be locked for changes.

Cause

The process to open SAP for a direct change to production was not documented.

Effect

When the production system was opened for changes, there was an increased risk that unauthorized modifications could occur because application security was not functioning as designed.

Recommendation

The process for applying change directly to production should be documented and include, at a minimum, steps to be taken to account for the following:

- Approval to open the production client;
- Tracking the actual changes/corrections made vs. intended;
- Closing the production system;
- Developing and retaining documentation of the event;
- Synchronizing the appropriate development and quality assurance environments; and
- Providing notification to the appropriate level of management.

Management Response – February 8, 2005

ITSD concurs with the finding. However, in doing so, they recognized that the procedures for opening the production system were understood by Project Team Members. Requests for opening the production system are documented and approved only at the Project Management Office level. E-mail is used to document when the system is opened and when it is closed. Safeguards, such as opening the system well outside of normal business hours in order to lessen the chance of inadvertent changes, are strictly maintained. As a result, ITSD's ERM Production Support Manager will:

- *Document the process for applying changes directly to production by including the process as part of the Transport Management System (TMS) procedures document.*

Expected completion date is May 2005.

SAP Issue #2: Operating System Level Security

Condition

Unix Solaris security guidelines were not documented. Solaris is the underlying operating system utilized for the SAP R/3 application. While some security logs are being produced to track the use of powerful authorizations within Solaris, the logs are not currently being monitored.

Criteria

The SANS (SysAdmin, Audit, Network, Security) Institute's publication on securing Solaris 8 & 9 using the Center for Internet Security benchmark encourages the use of logs to provide audit trails and usage accounting.

Cause

Unix Solaris security guidelines and procedures were neither defined nor documented.

Effect

Without a defined strategy for Solaris security implementation, there was an increased risk that unauthorized changes to SAP may not be discovered. Powerful commands can be issued at the operating system level to introduce modifications directly into the SAP production system. These modifications would be difficult to identify through SAP and would introduce inconsistencies between the development, quality assurance and production environments.

Recommendation

The City ITSD should develop a defined strategy for implementing security across all Unix platforms. The strategy should, at a minimum, provide a benchmark for:

- Running only the services and applications needed for the system to function as intended;
- Applying appropriate operating system, security and application patches; and
- Defining system access strategy, special account usage, and system backup procedures.

Management Response – February 8, 2005

ITSD concurs with the findings and recognizes the need to implement a UNIX security strategy. As a result, ITSD's Infrastructure Support Manager will develop documented UNIX security standards to include the following considerations:

- *Hardening the Solaris operating system using guidelines recommended by Sun Microsystems;*
- *Implementing the Solaris Security Toolkit; and*
- *Creating a documented patch management policy.*

In developing UNIX security standards, ITSD will:

- *Develop a baseline security process for Solaris including:*
 - *Unix security standards document;*
 - *Host-based controls;*
 - *An assessment process; and*
 - *A security baseline.*

Expected completion date is June 2005.

SAP Issue #3: Emergency Correction or Transport Procedures

Condition

Emergency change management procedures were not documented. The Transport Management System (TMS) Procedures document did not identify a separate process for emergency change requests. In addition, audit staff was unable to validate that staff was actually using the TMS Procedures document or that they were aware of its existence. When discussing this document with the SAP Development Team, it was evident that they were aware it existed but were not relying on it to perform their portion of the change process.

In addition, change back-out procedures were not documented to provide a method for reversing a change that produced unintended results. On December 15, 2004, four transport requests were erroneously migrated into the SAP production system due to a miscommunication of test results within the Production Support Organization. On December 16, 2004, an analysis was performed by Production Support to determine the impact that the transports would have on production data if not corrected. As a precaution, opening the production system and changing the production data back to the original value reversed the effects of one of the transports.

Criteria

The existing Production Support Organization guidelines state: "There will be two possible procedures for correction and transport into the production environment. These procedures include regular post go-live correction and transport procedure as well as an emergency correction and transport procedure."

CobiT control objective AI6 – Manage Changes indicates that effective management of change should include a system which provides for the implementation and follow-up of all change requests to include emergency procedures. In addition, CobiT control objective DS4 – Ensure Continuous Services indicates that fallback plans are an integral component to ensure continuous service.

Cause

Transport Management System Procedures have not been updated to reflect the currently accepted methods of processing emergency changes and have not been effectively communicated to all involved persons. In addition, the existing procedures do not provide a methodology for reversing the effects of a change to the production environment.

Effect

The lack of a documented process increases the difficulty in defining which requests should be handled as "emergency" and which should follow the standard transport process. Additionally, the lack of formal back-out procedures increased the risk that an unintended or incorrect change or transport may not be reversed appropriately.

Recommendation

It is recommended that the TMS Procedures document be updated and made available to all team members involved in the change process. Emergency change procedures should be formally defined, documented and included in the TMS Procedures document. Emergency procedures should include requirements for complete documentation of the conditions requiring the change, all test results prior to migration to production, update of end-user documentation where appropriate, steps to be taken if emergency access to make the change directly in production is required (such as logging of user actions or witness sign-off that only the intended change was made) and providing routine notification of emergency changes to the change control board.

Additionally, back-out procedures should be developed to support the process of reversing an unintended or incorrect change or transport.

Management Response – February 8, 2005

ITSD concurs with the finding that Emergency Change Management procedures are not documented. ITSD believes these procedures are understood by the project team, but agrees that they should be documented in the Transport Management System (TMS) procedures. As a result, ITSD's ERM Production Support Manager will:

- *Update TMS procedures to include the emergency change process;*
- *Gather input from the Basis team to use in updating the TMS procedure document; and*
- *Train all appropriate staff on the use of the TMS procedures.*

Expected completion date is May 2005.

ITSD concurs with the finding that back-out procedures are not documented; however, they recognize that Project Team members understood the emergency back-out procedures. As a result, ITSD's ERM Production Support Manager will:

- *Update the TMS procedures to include emergency back-out procedures.*

Expected completion is May 2005.

SAP Issue #4: Change Documentation

Condition

Changes to SAP are not consistently documented in the City's issue tracking database, which is known as Thread Manager. Upon reviewing the history of changes, it was discovered that there were 174 transports (changes) to SAP between December 1st and 21st, 2004. Thirty-six transports were vendor-required updates leaving 138 transports to analyze for the purpose of audit testing. Out of 138 requests, 111 did not include a Thread Manager issue number in the short text description of the transport as required. Of the 27 transports containing a Thread Manager issue number, 18 appeared to need an update of various degrees ranging from a change in status to an indication that a transport was submitted to correct the issue. Nine of the 138 appeared to be well documented with the correct actions and status included in the details of the Thread Manager issue.

In addition, documentation supporting the testing of changes was not available for all transports. Through review of sample production transports, it was determined that notification of test completion was communicated verbally at times. Draft documentation indicates that the notification should be performed through email communication.

Criteria

COSA standard naming convention for requests created in SAP provides that the Thread Manager issue number should be included in the short description of the transport request.

Sound change documentation practices also contribute to an improvement in CobiT control objective AI6 – Manage Changes. Objective AI6 indicates that changes are more effectively managed through a system that provides for the analysis, implementation, and follow-up of all changes requested and made to the IT environment. In addition, CobiT control objective DS10 – Manage Problems and Incidents indicates that both accessibility of configuration information and audit trails of problems and resolutions assist in the managing of problems and incidents.

Cause

The requirement to document all changes through creation and update of a Thread Manager issue was not being followed.

Effect

Without proper documentation it was difficult to determine the validity of changes made to the SAP System.

Recommendation

It was recommended that each change be documented by using Thread Manager as a tracking mechanism. The Thread Manager issue should accurately capture the details of the change to include reference to any related transports. In addition, all evidence supporting the testing of changes prior to migration to the production system should be retained in electronic form.

Management Response – February 8, 2005

ITSD concurs with the finding that each change should be documented using Thread Manager. ITSD's ERM Production Support Manager has already instructed the ERM project teams to include the Thread Manager issue number as part of the transport request short description where applicable and the transport number as part of the issue solution documented in Thread Manager.

ITSD concurs with the finding that all evidence supporting the testing of changes should be retained. ITSD's ERM Production Support Manager has implemented a "Transport Request Form" to document request creation and approvals.