Change Management Controls Compliance With The Sarbanes-Oxley Act Of 2002: An Example From Practice

Tim Kizirian, (E-mail: tkizirian@csuchico.edu), California State University, Chico
Wallace Leese, (E-mail: wleese@csuchico.edu), California State University, Chico
Nathan Heinze, (E-mail: nheinze@fau.edu), Florida Atlantic University

ABSTRACT

Publicly held firms and the assurance services industry are currently struggling with the implementation of standards set forth in the Sarbanes-Oxley Act of 2002 (SOX). How to meet and assess SOX standards is considered by professionals to be uncharted territory. This study reports the details of an actual SOX audit. An international computer component manufacturing corporation engaged information system auditors from a Big 4 firm to determine whether change management procedures in two areas in their Finance Department were compliant with SOX. Audit results indicated internal control deficiencies in the two areas audited. SOX compliance was thus determined to be weak and unreliable. In addition to reporting audit procedures actually used in practice to test SOX compliance, this case study presents key change management control procedures firms must have in place to be SOX compliant. We provide helpful practical guidance for corporations and audit firms involved with SOX compliance audits. In addition, this study has value for corporate internal control training sessions as well as general applicability for accounting information systems (AIS) and management information systems (MIS) courses.

1. INTRODUCTION

1.1 Background on the Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) was passed in response to well-publicized corporate accounting scandals, including Enron and WorldCom. SOX requires companies to reconsider their internal controls and financial reporting practices. Section 404 of the Act requires management to produce an internal control report that includes:

- A statement of management's responsibilities for establishing and maintaining adequate internal controls and procedures for financial reporting, and
- Conclusions about the effectiveness of the company's internal controls and procedures for financial reporting.

SOX frequently references three sources as providing the most generally accepted foundation for establishing a company's system of internal controls. These sources are:

- The Internal Control-Integrated Framework, produced by the Committee of Sponsoring Organizations (COSO). See http://www.coso.org.
- Control Objectives for Information and related Technology (COBIT) Version 3.1, © 2004, produced by the Information Systems Audit and Control Foundation (ISACF). See http://www.isaca.org.

- Consideration of the Internal Control Structure in a Financial Statement Audit – Statement on Auditing Standards, No. 55 (SAS 55). Produced by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). See http://www.aicpa.org.[1]

Firms working toward Section 404 compliance typically employ information system auditors to provide assurance that application program changes are performed in accordance with generally accepted professional standards (COBIT, COSO and SAS 55).

1.2 Background on Change Management Controls

It is anticipated that companies will need to produce detailed documentation to satisfy external auditors who will in turn attest to management's assertion on the sufficiency of internal controls. Section 404 compliance requires that internal controls are in place and operating effectively for key information system controls including the management of system changes made to an application. In the area of change management, the risk addressed is that unintended, unauthorized, or untested program changes are released to production. Key change management controls outlined in COSO, COBIT and SAS 55 include:

- Formal procedures as well as proper monitoring, documentation and approval exists at the following key stages in the change management process: overall request approval, categorization, prioritization, development, testing and production.
- All changes to production systems are initiated via a formal change control process and include documenting the program change request. Users provide input as to the categorization and prioritization of outstanding change requests.
- All changes to production systems are formally reviewed, tested, and authorized prior to release to production. User acceptance testing is performed, and the user accepts the change via sign-off, prior to implementation of the change into production.
- The changes are implemented into the production environment by personnel not responsible for making the changes (adequate segregation of duties).
- Separate environments exist for development, test, release, and production (adequate environment isolation).
- Changes to applications are processed as designed, completed in a timely manner, and meet the expectations of end users. Master production documentation should be updated concurrently with approved production changes.

2. CHANGE MANAGEMENT SOX ASSURANCE

Information system auditors from a Big 4 firm were engaged to conduct a change management SOX audit of two applications ("Trading" and "Investment") within the Finance Department of an international computer component manufacturing firm. The test steps below were performed by the information system auditors to verify that requests for changes were carried out in a manner consistent with COSO, COBIT and SAS 55:

- Conducted an interview with Tu Woo, Trading System Manager, and Neil Ng, Investment System Manager to obtain an understanding of the Trading and Investment processes. Documented the understanding of each of these processes in a narrative format with a supplemental flowchart.
- Documented any internal control deficiencies *in the design* of the Trading and Investment change management processes.
- Obtained a list of changes made during fiscal year 2004 from the System Mangers of the Trading and Investment applications.
- Selected a sample of 25 changes in the current year for both Trading and Investment using a random number generator.

[1] SAS 55 as amended by SAS 78 and SAS 94.

- Performed a walkthrough back to support tickets from the sampled changes to test that appropriate change management control procedures are operating effectively.
- Concluded on the effectiveness of the change management controls.

2.1 Obtaining an Understanding of the Trading System

The information system auditing firm conducted an interview with Tu Woo, Trading Systems Manager. The information system auditor's documentation, which is based on this interview, is detailed verbatim and unedited below:

Trading Program Changes

Request, Authorization, and Prioritization

Program change requests by users, in the form of bug fixes, enhancement requests, or additional functionality, are categorized into three different levels of approval requirement for implementation.

Level 1	New system projects or applications.	Requires FC (Finance Committee) approval consisting of: AT (Assistant Treasurer) Regional ATs, Systems Manager, key stakeholders, and on a need basis, Tax, and Legal managers.
Level 2	Modification to existing systems that affect: GL booking/recording, Authorization process, Access controls, and database structure	May or may not require FC, but at a minimum: AT, Systems Manager, key stakeholders, and on a need basis, Tax, and Legal managers.
Level 3	Modification to existing systems that does not affect areas listed in Level 2	Requires AT and Systems Manager.

Change requests are assigned a level of severity and priority to determine the order of implementation and production release.

Severity:	**Priority**:
1. Critical/System Crash 2. Major Error/Issue 3. Minor Error/Issue 4. Enhancement 5. Benign 6. Cosmetic	1. Resolve immediately 2. Fix in Next Major Release 3. Fix in Next Minor Release 4. Low Priority 5. Nice to have

A Trading user initiates a program bug or enhancement request via email to the Systems Staff. The Systems Staff personnel then logs the request for future review. Alternatively, the user can also submit the program change via the Bugs/Issues module of the Trading application. This module will generate an email to the Systems Staff after a program change request has been submitted.

The severity component is first established with the team. Bug fixes range from critical to minor or benign. Enhancements are generally considered to be non-critical changes (i.e. report formats, screen displays, etc.) and have lower priority than bug fixes. After determining the Severity, the Systems Manager uses the Priority scale to prioritize tasks.

Development

After prioritization, projects are assigned to programmers for analysis and development. There are programmers responsible for development of specific modules and these module assignments are based on the expertise of the programmers. Development is performed in a development environment, which is a mirror of the production environment. Data is refreshed from the Production environment based on the needs of testing for a Major project. Access to make changes is restricted to three developers who are registered in the Microsoft SourceSafe software to check out and check in Trading source code.

Weekly staff meetings are used to monitor the status of change requests -- what is completed, what is in process, and what is in the queue. Meeting minutes and progress updates are tracked via memos, documents, and flow charts, and stored in the System Repository. System project-related email correspondence is also archived.

Testing

Testing levels

- Unit Testing: done by the implementing developer. Only the unit or module being changed is tested to verify a bug is fixed or an enhancement is implemented to specification.
- Integration Testing: done by the implementing developer, after the units have been certified in unit tests. The purpose is to test whether different units that have been developed are working together properly. The test environment is a separate copy of the production environment.
- System Testing: done by Quality Assurance (QA) on the entire system. This takes an end-user view of the system and the test cases perform typical end-user actions as well as ascertain compatibility with the current production environment. The test environment is a separate copy of the production environment.

Depending on the types of changes made to the application, some or all of the following testing techniques will be employed:

- Regression Testing: to verify that the old functionality remains after changes have been introduced due to, for example, a bug fix.
- Stress Testing: where the extreme limits of the system are tested.
- Acceptance or Beta Testing: done by users ordering the changes as a validation check. The system is tested in its real or virtual environment (usually in parallel with a current system). When the testing is performed, the decision is made as to whether the product is to be accepted or not. Beta testing is used for program changes that are major in scope and functionality (Level 1 and 2).

Level 1 and 2 typically require all testing levels and techniques above.

After the original developer has fixed/developed the module and completed unit and integration testing, Systems QA performs system and regression testing and if successful, informs the Systems Manager. Test results are captured by QA staff and forwarded to Systems Manager and the AT for review and approval. Test results include:

- What was tested: bug/issue ID or description?
- Type of test: unit, integration, system, or Beta.
- Regression testing, load, and stress testing.
- Result: passed/not passed.

Once test results have been reviewed and approved by AT the process can move on to production release.

Transport

The Systems Manager conducts a final review and an overall test and communicates to the AT before releasing the program into production. Only the Systems Manager has the authority to move upgrade versions into production. In the event the Systems Manager is unavailable, a designated back-up (a senior developer) has the capability and knowledge to perform this function.

Upon the production release, release notes listing bug fixes and system enhancements are sent to the users via email. Information includes: bug/issue ID numbers traceable to the bug database (which contains the bug description, person logging the bug, and person fixing the bug).

For Level 1 and 2 changes, the production release timeline is determined by the FC or the Systems Manager. The general guidelines are:

- Avoid quarter end close
- Avoid month end close
- Friday evening is preferable if the release involves complex database changes so that the Systems Staff has the weekend to resolve issues and do a rollback if necessary.

The process of releasing a production upgrade is carried out by the Systems Manager as follows:

- Pre-advise users of the version upgrade via email; if necessary, notify users of system downtime and when system will back online.
- Update new application version in the database.
- Release software into production.

Documentation

- Email users notifying of new release (version number) with release notes (bugs/issues resolved and new enhancements).
- Make available user manual/documentation related to system changes.

The Trading front end resides on individual user's PCs. The Trading application checks the production directory for new updates each time a user logs in. Users are asked if they would like to update to the current version, and if they indicate "NO," users will not be allowed to access the system until they load the new version.

Change requests are tracked on a consistent basis through the Trading Bugs and Issues feature. Approval to the changes is done via the QA process. Microsoft's SourceSafe program is employed to store and maintain current and previous versions of all Trading applications.

Monitoring

For major projects, the FC holds regular meetings every 45 days to discuss the progress of the project in regards to the changes made, testing, and deadlines. In addition, the Trading System Administrator conducts weekly staff meetings with his development team to also discuss any changes made to the system or issues that may need to be resolved. On a monthly basis, the Assistant Treasurer conducts another staff meeting that includes any updates to the Trading system.

2.2 Obtaining an Understanding of the Trading System – Process Flowcharting

Based on the interview with Tu Woo, Trading Systems Manager, the information system auditor prepared a flowchart of the change management processes in Trading (Exhibit A). The flowchart is not intended to be detailed (i.e., capturing all events in Trading) but rather, portray change management in Trading at an overview level. The information system auditor highlighted, wherever possible, activities mentioned by COSO, COBIT and SAS 55 to be key areas of change management: overall request approval, categorization, prioritization, development, testing and production.

2.3 Obtaining an Understanding of the Investment System

The information system auditing firm conducted an interview with Neil Ng, Investment Systems Manager. The information system auditor's documentation, which is based on this interview, is detailed verbatim and unedited below:

Investment Program Changes

Initiation of Change Request:

Change requests are submitted to the Investment System via the "Feedback" button on the Investment System website, or a phone call or e-mail to systems personnel in Investment. Once a request is submitted through the Feedback tool, an automated email is sent to an Investment Support e-mail account, and specifically to technical leads notifying them that a support ticket has been submitted. If a request is made via phone call/email, an Investment System representative submits a support ticket using the Feedback tool on behalf of the customer/requestor.

Categorization:

Program changes are categorized into bug fixes, enhancements and showstoppers:

- Bug fixes - Bugs found in the production environment. End users create the bug ticket using the Feedback Tracker tool on the Investment System website. The bugs are reviewed by the Investment Administrator and then escalated to the Tech Leads for evaluation.
- Enhancements - Enhancements are improvements for the Investment application. They are submitted in the Feedback Tracker by the end users and reviewed by the IS team for prioritization. Minor enhancements are escalated to the development team for implementation. Major enhancements are collected for future releases.
- Showstoppers – Problems that prevent users from performing their daily job activities and require immediate fix.

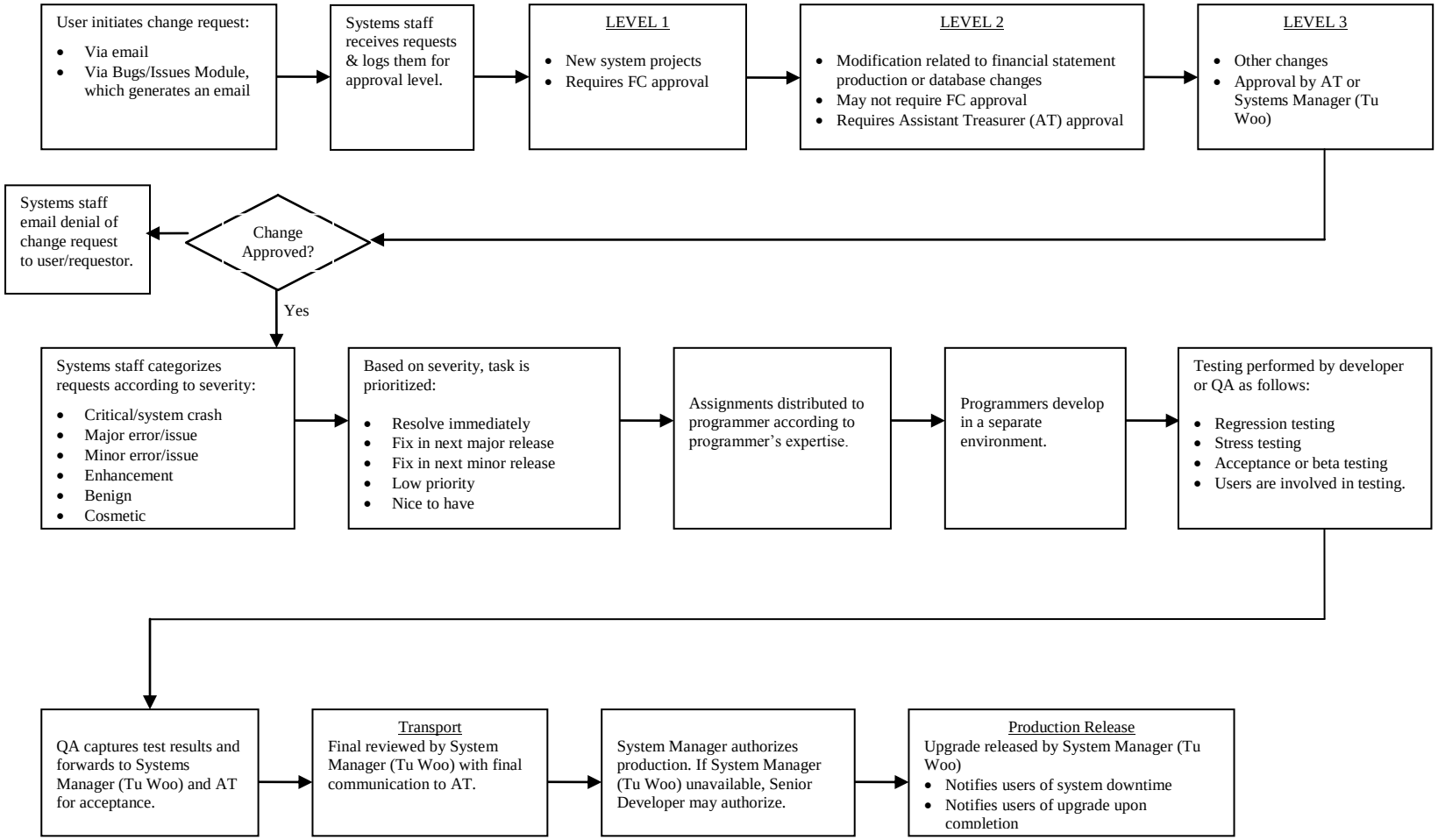
Classification of changes into Major and Minor

Only showstoppers are further categorized into Major and Minor changes.

Major changes:	Minor changes:
• Impact other areas of application. • Change core functionality. • Require >= 24 hours per work team to implement. • Are data model or process changes affecting more than one business area. • Changes affecting reports.	• Do not impact other areas of the application. • Do not change core functionality. • Add clarifying information that does not change the intent and/or meaning of the context. • Fix spelling or typographical errors. • Require <= 24 hours per work team to implement.

Exhibit A

The Information System Auditor's Flowchart of the Change Management Process Within the ***Trading*** Application of Finance



Change Request Disposition/Scheduling

- An Investment System member (Support desk, Business Analyst and Technical Lead) evaluates the input and engages other team members as necessary. Appropriate action is determined based on whether the request is a bug or an enhancement and if the change is major or minor. The Investment System member also estimates effort required, and based on resource availability, sets a target implementation date.
- An Investment System member contacts requestor to confirm requirements and acceptability of target implementation date.
- If a major change needs to be implemented earlier than target date, a stakeholder meeting is scheduled to review and prioritize change requests.
- If a minor change needs to be implemented earlier than the target date, priorities are discussed offline with requestor.
- Approved change request is scheduled and status is updated in the feedback tool record.

Implementation of Change Request

- Assigned developer codes and tests change according to change request details, clarifying details with requestor as needed.
- A Business Analyst, Quality Assurance member or Technical Lead will review the developer's tests of the change. The requestor has the opportunity to test change to ensure that the implementation adequately addresses the identified business need.
- Technical Leads will push code into production after the ticket is set to "QA passed."
- Once a change has been implemented Technical Leads will update the change request status in the feedback tool record.
- A new Application Version Number will be logged for each scheduled release.

Notification of Changes Implemented

- Auto email notification is generated once a support ticket is closed. The distribution list includes the entire Investment System and the originating user.
- For scheduled releases, an Investment System support also sends an email notification to impacted users and posts a summary of changes under the "What's New" page in the Investment System Homepage.

2.4 Obtaining an Understanding of the Investment System – Process Flowcharting

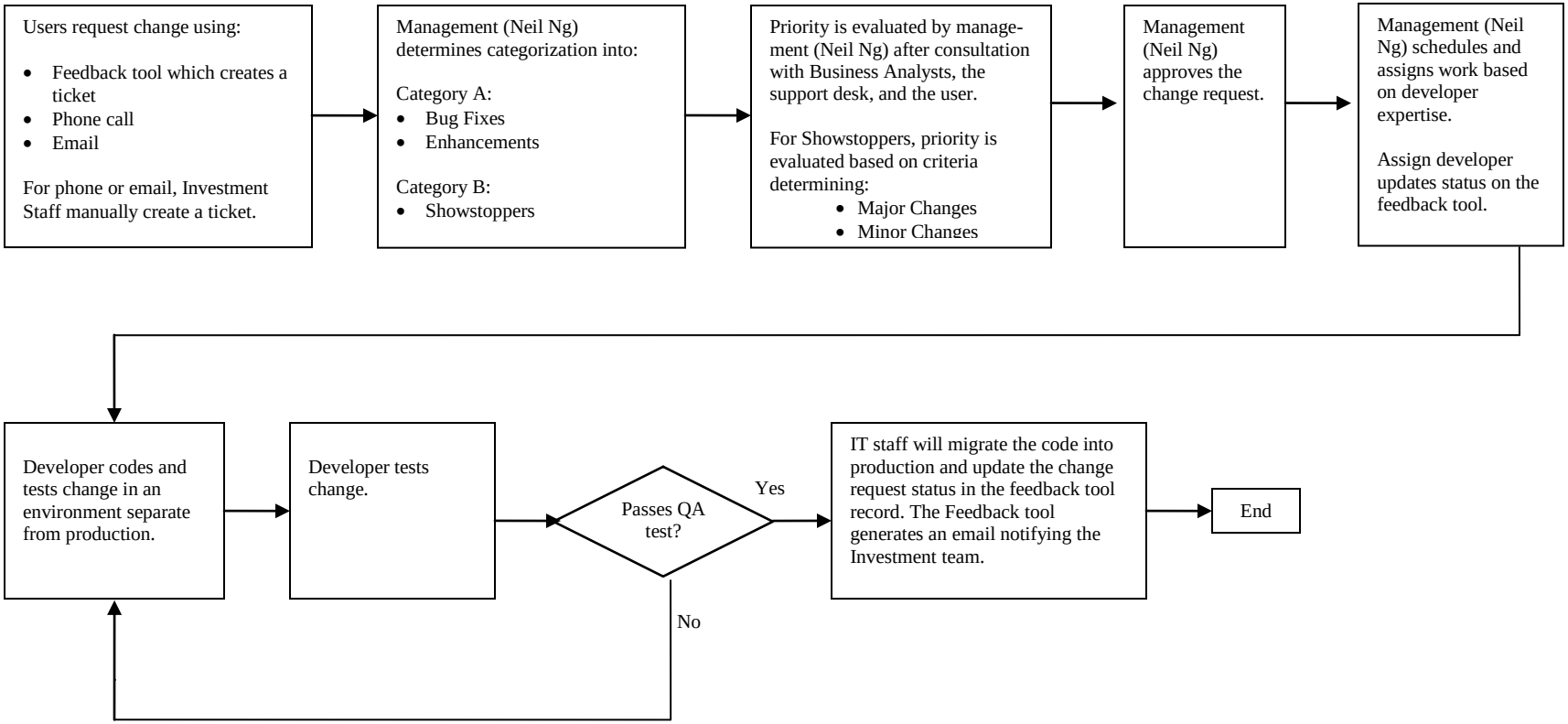
Based on the interview with Neil Ng, Investment Systems Manager, the information system auditor prepared a flowchart of the change management processes in Investment (Exhibit B). The flowchart is not intended to be detailed (i.e., capturing all events in Investment) but rather, portray change management at an overview level. The information system auditor highlighted, wherever possible, activities mentioned by COSO, COBIT and SAS 55 to be key areas of change management: overall request approval, categorization, prioritization, development, testing and production.

3. Audit Conclusions

The information system auditors performed all audit test steps including: understanding change management systems in Trading and Investment, noting deficiencies in the design of the change management processes, performing walkthroughs from sampled changes to support tickets to test that appropriate change management control procedures are operating effectively. The auditors' testing procedures exposed control deficiencies in Trading and Investment. The auditor's documented deficiencies follow verbatim and unedited.

Exhibit B

The Information System Auditor's Flowchart of the Change Management Process Within the ***Investment*** Application of Finance



3.1 Weaknesses in the Trading Application

- A support ticket not only initiates a change, but is also a conduit for documentation of approvals and work performance in accordance with management's intentions. Such an audit trail does not exist in the Trading application because a support ticket is never initiated. A unique support ticket number should be assigned to a change which would provide accountability for initiation, approval, testing and migration of changes into production.
- While rules of categorization and prioritization appear to be documented, there is no mention that the rules are shared with users. This contributes to poor user involvement.
- In some circumstances (unit and integration testing), the developer can test his own work. This is a segregation of duties deficiency.
- Users generally do not perform testing of changes. The only time user testing is mentioned is for Acceptance or Beta Testing, which is only one of several forms of testing.
- A statement that outlines organizational/overall change management standards cannot be found.

The Change Management Controls Reliability Assessment for the Trading Application

Based on the control deficiencies discovered, the overall change management controls reliability conclusion for Trading is *Weak/Don't Rely.*

3.2 Weaknesses in the Investment Application

- While support tickets are generated, they are not used as a conduit for documentation of approvals and work performance in accordance with management's intentions. Thus, while the support ticket does provide accountability for initiation of the change, it does not provide accountability for approval, testing and migration into production.
- While rules of categorization and prioritization appear to be documented, there is no mention that the rules are shared with users. This contributes to poor user involvement.
- No mention is made of the use of current (mirrored) production data when QA is testing development's changes. This may lead to an erroneous conclusion that the changes will work smoothly when pushed into production.
- Users do not perform user acceptance testing of changes.
- A statement that outlines organizational/overall change management standards cannot be found.
- The developer can test his own work. Further, the Business Analyst, Quality Assurance member or Technical Lead will merely *review* the developer's tests of the change as opposed to a more proper independent testing of the change. This is a serious segregation of duties deficiency.
- Development does not exist in an environment separate from testing and production. This is a serious segregation of environments deficiency.

The Change Management Controls Reliability Assessment for the Investment Application

Based on the control deficiencies discovered, the overall change management controls reliability conclusion for Investment is *Don't Rely.*

4. Summary and Conclusions: Measuring up to SOX Change Management Standards

Change management processes in Trading and Investment faired poorly when matched up to SOX standards. The information system auditors assessed that the risk that an unintended, unauthorized, or untested change could be released to production was *high*, as evidenced by the *Weak/Don't Rely* (Trading) and *Don't Rely* (Investment) assessments. We conclude with a useful summary of key change management controls outlined in SOX (see Section 1.2) along with related review procedures and compliance deficiencies discovered by the information systems auditor.

APPENDIX

Controls Outlined in SOX	Audit Procedures and Findings
Formal procedures as well as proper monitoring, documentation and approval exists at the following key stages in the change management process: overall request approval, categorization, prioritization, development, testing and production.	**Audit Procedure**: For the 25 randomly selected changes, note email evidence or note on the tracking tool that the System Manager approves, monitors, and maintains documentation of overall request approval, categorization, prioritization, development, testing and production. Obtain screen print evidence from the tracking tool or copies of the emails that that the System Manager approves, monitors, and maintains documentation of changes. **Audit Finding**: Monitoring, documentation and approval procedures are partial and incomplete. An overarching, consistent methodology that outlines change management standards does not exist. (Applies to both Trading and Investment).
All changes to production systems are initiated via a formal change control process and include documenting the program change request. Users provide input as to the categorization and prioritization of outstanding change requests.	**Audit Procedure**: For the 25 randomly selected changes, note that the tracking tool is utilized to create support tickets that identify change requests (use the tracking tool dropdown menu for request status), categorization (use the tracking tool dropdown menu for category), prioritization (use the tracking tool dropdown menu for priority). Obtain screen prints of these tracking tool dropdown menus. Obtain evidence via email or the tracking tool that rules of categorization and prioritization are documented and available to users, and that users initially suggest categorization and prioritization. **Audit Finding**: Support tickets are not initiated. (Trading). Support tickets initiate the change but do not carry that change request through a formal change control process, as tickets do not provide accountability for approval, testing and migration into production. (Investment). Users do not provide input as to the categorization and prioritization of changes. Rules of categorization and prioritization are not shared with users. (Applies to both Trading and Investment).
All changes to production systems are formally reviewed, tested, and authorized prior to release to production. User acceptance testing is performed, and the user accepts the change via sign-off, prior to implementation of the change into production.	**Audit Procedure**: For the 25 randomly selected changes, note email evidence or note in the tracking tool that changes may not be moved into production without passing QA. Note on the tracking tool that the System Manager approves, monitors, and maintains documentation of development (use the tracking tool dropdown menu noting assignment to developer), testing (use the tracking tool dropdown menus noting QA status and tester), and production (use the tracking tool dropdown menu noting staging QA status). Note email evidence in the tracking tool that user acceptance testing is formally performed and that users sign off on changes. **Audit Finding**: Users generally do not perform testing of changes. (Trading). The requestor has the *opportunity* to test change to ensure that the implementation adequately addresses the identified business need. However, users do not *consistently* perform user acceptance testing of changes. (Investment). Users do not sign off on changes prior to implementation into production. (Applies to both Trading and Investment).
Controls Outlined in SOX	**Audit Procedures and Findings**
Changes are implemented into the production environment by personnel not responsible for making the changes (adequate segregation of duties).	**Audit Procedure**: Obtain an access listing via email from System Managers listing out authorized users in the development, testing, QA and production environments. For each of these users, review listings to ensure that crossover duties do not exist. Select a user from each of these environments and attempt to access and operate in the remaining environments. **Audit Finding**: The developer can occasionally test his own work, creating a mild segregation of duties deficiency. (Trading). The developer tests his own work, which is then pushed into production, resulting in a serious segregation of duties deficiency. (Investment).
Separate environments exist for development, test, release, and production (adequate environment isolation).	**Audit Procedure**: Obtain an access listing via email from System Managers listing out authorized users in the development, testing, QA and production environments. For each of these areas, review listings to ensure that crossover duties do not exist. Select a user from each of these environments and attempted to access and operate in the remaining environments. **Audit Finding**: Development does not exist in an environment separate from testing and production, resulting in a serious segregation of environments deficiency. (Investment).
Changes to applications are processed as designed, completed in a timely manner, and meet the expectations of end users. Master production documentation should be updated concurrently with approved production changes.	**Audit Procedure**: For our 25 randomly selected changes, observe tickets, note the ticket date is consistent with the change request date. Note the length of time between the date submitted and the close date was not excessive. Confirmed job aides were available online. Obtain screen prints of those job aides. Note email announcement of pre-release training for current year change releases. **Audit Finding**: Procedures appear adequate. (Applies to both Trading and Investment).

5. SUGGESTIONS FOR FUTURE RESEARCH STUDIES

This case study can aid firms affected by SOX and information systems auditors working to provide SOX assurance. The primary focus of the Sarbanes-Oxley Act is data integrity. Data integrity cannot reasonably be achieved without strong change management controls. We presented key change management control procedures that firms must have in place to assure SOX compliance in this area. Additionally, we reported the details of an actual SOX compliance audit carried out by a Big 4 firm. The audit dealt exclusively with SOX compliance issues related to change management controls. However, compliance with SOX extends far beyond change management controls issues. SOX affects significant processes and significant applications that produce operational data to the firm's stakeholders. How to meet and assess SOX standards is for the most part uncharted territory. Additional research is needed to help remove this uncertainty. Additional research reporting implementation issues and solutions should provide guidance and insight for corporations and audit firms involved with SOX compliance audits of all types.

NOTES