14 – 409 FIRE Program Assessment

Strategic Area: Information Technology, Clinical Analytics & Informatics
Risk Type: Compliance and Operational
Audit Manager: Mahmoud Sultan

Overview:

The Federated Institutional Reporting Environment (FIRE) Program is critical in creating a comprehensive, centralized clinical data repository to support clinical / institutional analytics, decision making, and business intelligence needs. This central repository houses historical clinical, research, and operational data within a data warehouse and is accessible to business users through reporting dashboards.

The FIRE Program is inclusive of several tier-three source systems and target dashboards with the FIRE data warehouse as the central repository of data. Operational, clinical, research, and genomic data is interfaced into the FIRE data warehouse from a variety of source applications. Individuals utilize this data to generate ad-hoc reports for analysis and decision-making purposes. The data is accessed via reporting dashboards, which includes: Pharmacy dashboards and Cohort Explorer. The Pharmacy dashboards provide users access to easily compare and analyze drug sales and dispense data. Cohort Explorer allows for ad-hoc exploration of patient populations which enables researchers to quickly answer patient population questions. It is utilized primarily by the Pharmacy, Genomic Medicine, and Clinical Analytics & Informatics (CAI) departments with approximately 70 users.

Audit Results Summary:

Internal Audit found that MD Anderson has established controls to support the FIRE data warehouse, with processes and procedures to evidence control design and operation. Through our procedures, we noted that Clinical Analytics & Informatics has a strong control environment with many control processes related to security, change management, and computer operations. Although we noted many effective control processes in place to manage the FIRE Program, we noted the following opportunities for improvement:

- All changes made to FIRE, including stored procedures, reports, objects, patches, routine maintenance, should be tracked and approved per the MD Anderson institutional policy through the change management system.
- Developer access to the production servers should be removed to limit the risk of ad-hoc / inappropriate changes to production.
- A formal user provisioning process should be followed to ensure manager approval is obtained prior to users gaining access to the system.
- A periodic review of user access, including high privileged accounts, should be performed at the dashboard, application, and database levels. Such review of users will
become especially critical as the user-base within the FIRE program increases over time.

- User guides and end user training manuals should be developed for the Pharmacy dashboards and distributed to business users to assist users in accessing and utilizing the dashboards appropriately.
- Risk Assessment questionnaires should be updated based on the application’s tier classification to remain in compliance with Institutional policy. Per institutional policy, Tier 3 systems must complete a risk assessment at least every two years

Management Summary Response:

Management’s action plans have been developed by the Clinical Analytics & Informatics team. The action plans that follow will be completed by 11/30/2014.

Number of Priority Findings to be monitored by UT System: None

A Priority Finding is defined as “an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.”

The courtesy and cooperation extended by the Clinical Analytics & Informatics was sincerely appreciated.

______________________________
Sherri Magnus

Sherri Magnus, CPA, CIA, CFE, CRMA
Vice President & Chief Audit Officer
September 17, 2014
Observation 1:  
**Change Management**

IA identified 3 changes that bypassed the institution’s change management process, which includes documenting any changes made to FIRE within a Change Management Notification Form (CMNF) ticket. Bypassing this process presents the risk of inappropriate changes made to FIRE’s functionality. This includes changes being potentially made without proper approvals or testing performed.

**Recommendation:**

IA recommends that any changes be tracked and approved through a CMNF ticket with the appropriate approvals retained and change testing documented. All system changes should follow the institutional change management process.

**Management’s Action Plan:**

Responsible EVP: Leon Leach  
Owner: Bryan Lari  
Observer: Melody Page  
Due Date: Completed

An overview of audit recommendations and the CMNF process was presented at the CAI department meeting on August 21, 2014. PowerPoint slides from the presentation are posted on the Internal Communications section of the CAI SharePoint. Links to pertinent Change Management policies, procedures and forms are included.

A follow up email was sent from Bryan Lari to all CAI workforce members. It reinforced the importance of following Change Management procedures, provided links to appropriate CMNF references, and discussed the penalties for non-compliance. The managers will also review the subject at team meetings. Additionally, CAI management has been charged with monitoring how consistently production system changes have been presented to the Change Management process. Any issues with further non-compliance with this important institutional policy will be addressed promptly by management.

Observation 2:  
**Developer Access**

IA noted that 4 developers were assigned high privileged production server access on the production server for FIRE. Access for these users was provided during the development phases of FIRE, which should have since been removed after go-live. Developer access to production increases the risk of inappropriate changes being made directly to the production environment by by-passing the program change controls. These users with their associated roles (developers) have the knowledge and expertise to make ad-hoc changes in production since access is not restricted.

As a follow-up, IA inspected the server audit log and noted the developers had not previously logged into the production server accounts and management has confirmed that access has since been removed. IA confirmed that no inappropriate activity occurred while this access was active.
Recommendation:
IA recommends the developer access to the production servers be removed to limit the risk of ad-hoc / inappropriate changes to production.

Management’s Action Plan:
Responsible EVP: Leon Leach
Owner: Bryan Lari
Observer: Melody Page
Due Date: Completed

CAI IT Project Managers will be responsible for including a task at the end of each applicable deliverable or project go-live to review production security access of developers with the Analytics Delivery Manager and have security provisions that might fall under this scenario revoked as appropriate.

It should be noted that it is possible for "developers" to hold dual roles as production support staff, and as such, they may appropriately have/require such access in order to accomplish the roles and responsibilities of their jobs. We recognize that segregation of duties is the ideal situation. CAI will also review server audit logs on a periodic basis to ensure that no inappropriate activity has occurred.

CAI believes that the audit recommendation has been successfully completed, pending final validation by Internal Audit.

Observation 3:
**User Provisioning**
Evidence of approval for access requests for FIRE was largely provided via email. Without following a strict user provisioning process, IA was unable to obtain approval for 1 account creation.

Additionally, IA was also unable to identify when user accounts were created in the FIRE data warehouse and associated reporting dashboards, which are used by individuals to generate ad-hoc reports. As such, IA was unable to gain comfort that approvals from management were provided prior to users gaining access to the FIRE environment.

Recommendation:
Management should develop a formalized user provisioning process which includes the identification of authorized approvers per business function (i.e. via ISARP) prior to users gaining access to the dashboards, application, and databases. Management should implement formal procedures to retain documentation and approval for user provisioning (new and modified users) so that access granted can be traced to the system. Additionally, management should either identify methods to obtain system generated listings for new/modified users (e.g. table logging), or system generated user listings should be obtained periodically to identify new and modified users for an audit period.
A formalized process has been put into place for granting access to FIRE resources. It is documented in the CAI Methodology Wiki on SharePoint.

Access to TRC Cohort Explorer and OBIEE Dashboards is requested and approved through ISARP. ISARP now generates a ticket in Cherwell to document the activity, so we should be able to report on this in the future (since we are unable to obtain reports from ISARP).

Database requests are now processed through Cherwell.

CAI believes that the audit recommendation has been successfully completed, pending final validation by Internal Audit.

Observation 4: User Recertification for Application, Databases, & Servers

The majority of users with access to the dashboards, databases, and servers are restricted to the FIRE project teams, who are developing the FIRE program. Upon notification of a user's termination or transfer, the user's account is locked, and subsequently removed; however, a formal user access review of the dashboard, database, and production server accounts is not performed. Lack of periodic monitoring increases the risk that user access is inappropriate.

Recommendation:
IA recommends that a review of users with access to the FIRE program, including high privileged accounts, should be performed at the dashboard, application, and database levels to ensure the continued appropriateness of users. Such a review of users will become especially critical as the user-base for FIRE increases over time.

Management’s Action Plan:
Responsible EVP: Leon Leach
Owner: Bryan Lari
Observer: Melody Page
Due Date: Completed

Access to TRC Cohort Explorer and OBI dashboards is controlled through ISARP, and therefore goes through the annual re-attestation process. Transfers are currently reviewed on a monthly basis in respect to access to TRC Cohort Explorer and OBI dashboards. Access to databases will now be reviewed on a monthly basis.

CAI believes that the audit recommendation has been successfully completed, pending final validation by Internal Audit.
Observation 5:

**User Guides**

The pharmacy dashboards do not currently have user guides available for end users. The user guides allow physicians in understanding the functionality of the system including helping the technology team troubleshoot. User guides will be very important for the institution in laying out the purpose, technologies, and functional support for the system.

**Recommendation**

IA recommends user guides be developed and provided to end users to assist them in accessing and utilizing the dashboards appropriately.

**Management’s Action Plan:**

Responsible EVP: Leon Leach  
Owner: Bryan Lari  
Observer: Melody Page  
Due Date: November 30, 2014

A user guide for the pharmacy dashboards will be developed during 1Q FY15.

Observation 6:

**Risk Assessment**

The Oracle Business Intelligence (OBI) risk assessment questionnaires had been completed in October 2011; however, updated Risk Assessments had not been completed as there have been no significant changes to the application or environment. Per institutional policy, Tier 3 applications are required to complete/update the risk assessment every two years after they have finished their initial assessment. IA noted that the OBI Risk Assessment had not been completed in October 2013, as required.

**Recommendation:**

IA recommends that OBI Risk Assessment questionnaires be updated to remain in compliance with Institutional policy.

**Management’s Action Plan:**

Responsible EVP: Leon Leach  
Owner: Bryan Lari  
Observer: Melody Page  
Due Date: Completed

The OBI risk assessment was completed in the new GRCv2 application as soon as the oversight was identified.

*CAI believes that the audit recommendation has been successfully completed, pending final validation by Internal Audit.*

Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.
Appendix A

Objective, Scope and Methodology:

The objective of this internal audit project was to assess FIRE’s compliance with Institutional policies and procedures which have been established by Information Services. This included gaining an understanding of the design and performing testing of the operating effectiveness of key IT general controls, such as security, change management, and computer operations.

The scope of this project was focused on evaluating the effectiveness of controls within MD Anderson’s environment during the testing period from 9/1/2013 through 3/24/2014. Internal Audit evaluated information technology general controls over the FIRE Program. This included assessing FIRE for Institutional Policies and Procedures over the following areas:

- Risk Assessment
- Access Security
- Data Classification
- Data Interfaces
- Change Management
- Computer Operations (Backup Recovery Procedures including Restorations)
- Disaster Recovery
- Reports / dashboards

Our procedures included the following:

- Interviewed key personnel in Clinical Analytics & Informatics department supporting the FIRE Program to obtain an understanding of the aforementioned areas.
- Corroborated to confirm the controls / processes that are in place with an adequate population to select samples for testing.
- Inspected supporting evidence to assess the in-scope areas against Institutional policies and procedures.

Our internal audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.