University of Texas Southwestern Medical Center

Internal Audit Report 14:21
User Access Approval Review
FY2014

September 2, 2014

Office of Internal Audit
5323 Harry Hines Boulevard
Dallas, Texas 75390-9017
(214) 648-6106

University of Texas Southwestern Medical Center
Internal Audit Report 14:21
Software Licensing Inventory Review Report
FY 2014

AUDIT REPORT
September 2, 2014

Daniel K. Podolsky, M.D., President
University of Texas Southwestern Medical Center
5323 Harry Hines Boulevard, MC 9002
Dallas, Texas 75390-9002

Dear Dr. Podolsky:

The University of Texas Southwestern Medical Center (Medical Center) Office of Internal Audit has completed its User Access Approval Review. This is a risk based audit and part of the FY 2014 Internal Audit Plan.

Executive Summary

Background

The Medical Center's Information Resources (IR) department manages access to numerous systems through the Systems Access Management (SAM) group. However, there are many other systems for which access is managed independently from IR. For the IR-managed systems, user access is obtained by an employee's Supervisor, Manager or other leader using the Institutional Access Request (IAR) form on the iAIM website. This IAR approach has become cumbersome and antiquated and the iAIM website will soon be retired since it has reached its end of life cycle. A new, more automated system was needed whereby application access requests would be processed more efficiently. The IR department selected the web-based Service Now (SN) system, which is supported 24x7 as the new User Access Approval application. Development began in March 2013, and the new system will be launched into production by September 30, 2014.

Objectives

Prior to the implementation of SN to the production environment, the overall audit objective is to evaluate the effectiveness of the internal process controls for the new SN User Access approval process.

Scope

The scope period is fiscal year 2014 through the present, i.e., September 1, 2013 – August 2014. Audit procedures included interviews with stakeholders, review of policies and procedures and other documentation and data analytics. Our examination was conducted according to guidelines set forth by the *Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing*.

Conclusion

The design of controls in the new SN system appears adequate. There are three reasonableness checkpoints regarding user access in the new system: 1) At the department approver level; 2) At the System Access Management (SAM) level; and, 3) At the Technical Services/application administrator level where the request, approvers, application owner, and department are all reviewed again. Additionally, with regard to the systems centrally-managed by IR, the risk of users being granted

inappropriate access will be lower in the centralized environment because, unlike the current system, the new application will prevent a user from approving their own access requests. Unknown risk of inappropriate user access still remains for the decentralized systems and will be reviewed in forthcoming internal audits of these environments. Finally, the new system will have increased system stability and will allow users to check the status of their request in real time, rather than interrupting Client Services staff. Overall, this new system and accompanying processes will lower risk to the organization by preventing the granting of inappropriate access.

The following opportunities to enhance system implementation were identified:

- Offer use of the SN system to departments with decentralized systems to prevent inappropriate access and possible segregation of duty conflicts.
- Implement controls to prevent department approvers from delegating approval authority without documented Management approval and specified duration. Similarly restrict SN System Administrators.
- Implement procedures for departments to periodically validate and re-certify their respective list of approvers.
- Implement an effective and efficient method to remove an approver from the system upon their termination or transfer.
- Evaluate span of responsibility and assist departments to address instances where there is a high risk of insufficient approver review.

Once the findings presented here are addressed, the application should go forward and move to Production as planned.

Management Response

Overall, management agrees with the findings and will implement procedures within the constraints of the SN system to address them with all management actions to be completed by March 31, 2015. Specifically:

- IR management will formulate a plan to integrate decentralized systems into the SN user access approval system.
- Although the SN system allows approvers to delegate approval authority, the written approval procedures and the training documents will state that approvers not delegate approval authority.
- In keeping with security best practices, all IAR approvers will be recertified annually.
- SN administrators will monitor for terminated and transferred approvers and remove them promptly.
- Client Services will determine appropriate criteria for span of control and provide reports to the departments to review instances where there is a high risk of insufficient approver review.

Detailed Results

1. Improve Security Access for Decentralized Systems

While we have an awareness of the number of systems in our decentralized environment, we don't have an account of all of the applications used within the departments. Each application typically requires creation of user accounts which are independent of centralized network access controls and therefore, there is a risk of inappropriate access including conflicts in segregation of duties.

Recommendations

Management should continue in its effort to ensure all decentralized systems are identified and there is appropriate management of risks. As part of the Business Continuity efforts, management is in the process of ensuring all applications are inventoried, risks are accessed and the systems are included in the Service now Application Registry. However, this effort does not ensure that all decentralized systems have sufficient user access. To lower the risk of inappropriate access in decentralized systems, management should:

- Centrally manage all of those systems classified as high risk systems.
- Require a security survey be completed for all systems managed by the IR PMO or are above $25K. Information Security approval of survey is required before the purchases can be made. This will ensure departments are using the Lightweight Directory Access Protocol (LDAP) for authentication.
- Given the risk of lack of management of user access controls for certain applications conduct the following;
    - Coordinate with department management to encourage or require the departments to manage user access via the SN system.
    - Where possible, offering user authentication to decentralized systems using the LDAP. This will ensure access to these decentralized systems is more appropriately managed when changes in user status such as terminations or transfers occur.

Management Response

This was not part of the original scope of the IAR migration but it is a good recommendation. Review of decentralized systems will begin immediately following implementation of the system in late September 2014 with planned completion by Q2 2015.

Target Implementation: March 31, 2015

2. Require and Document Management Approval When Approvers Delegate Authority

An approver can delegate their approval authority to someone else without management knowledge or management approval. This means a delegated approver could authorize the granting of access permissions for any employee in his/her department to files, databases, and/or applications, thus intentionally or unintentionally violating segregation of duty principles.

Similarly, SN Administrators can also add delegates without management knowledge or management approval.

Recommendations

Implement an approval workflow, or procedure, that first requires documented Management approval with a specified duration for each occurrence of approver delegation.

Management Response
SN has a built in delegation process that cannot be changed without customization from the vendor. The approval procedures and training documents will request that approvers forgo any additional delegation as each department has multiple approvers already listed.

Responsible Official: John Roe, Director of Information Resources Client Services

Target Implementation: September 30, 2014

3. Require Each User's Department Management to Periodically Re-Certify Approvers
At the time of the audit, procedures for all user departments to periodically validate and re-certify their respective list of approvers were not documented. Without this process, the list of approvers can grow through accretion and contain inaccurate data and/or unauthorized approvers. For example, Internal Audit's data analytics testing revealed the SN approvers table contains approvers that are no longer active in the PeopleSoft Human Capital Management (HCM) system in five departments.

Recommendations
Require, at least annually, each user department's management to re-certify and date document its approval of their SN access request approvers.

Management Response
Annual recertification will be conducted for all IAR approvers.

Responsible Official: John Roe, Director of Information Resources Client Services

Target Implementation: September 30, 2014

4. Promptly Remove Approvers from the Approver Table Upon Transfer or Termination
Editing of the approver table is a manual process and it was decided that each individual department would be responsible for requesting removal of approvers from their approval cycle in the event of a transfer or termination. There is low risk that a transferred approver can make approvals for his/her previous department because the department ID's will not match. However, reliance on department management to remember to request removal of an approver's name upon transfer or termination creates the risk this will not be done, thus resulting in accretion of inaccurate data.

Recommendations
A better alternative is for SN administrators, not department management, to delete transferring and terminated approvers. Whenever approver is terminated or transferred to another department, the SN administrators should timely remove the approver's name from the approver table, date document the approver's removal, and notify department management of the approver's removal. Further, include a daily Termination Report that captures the name of any approver who has a deactivated account from Active Directory. This daily Termination Report should go to the SN Administrator's Home Page. Thus, the SN administrators can maintain a current and accurate approver Table.

Management Response
For terminated approvers, the SN administrators will monitor for when the accounts for these employees have been flagged as inactive in Active Directory and a SN administrator will remove them from the approver list.

For transfers, the SAM group will create an approval group separate from SN. When approvers are transferred between departments their name is dropped from all SAM groups. This will serve as a flag to notify the SN administrator to remove the approver's name from their old department's IAR approval table. A secondary control to ensure the data is accurate will occur during the annual recertification process.

Responsible Official: John Roe, Director of Information Resources Client Services

Target Implementation: September 30, 2014

5. Monitor Approvers Span of Responsibility to Ensure Appropriate Levels

In evaluating designated departmental approvers in the SN system to the number of users assigned, data analytics revealed the top 168 approvers are assigned to approve over 100 users. The approver with the largest number was assigned 1779 users and the next four largest each has 1105 users. While the number of users to approver ratios and volume of approval requests may vary in terms of adequate management, the higher number of users or access requests may pose a risk that the approver may not have the ability to diligently review and evaluate the access requests for ensuring appropriate levels of security access.

Recommendations

Designation of approvers is the responsibility of departmental management. However, IR should monitor the risk levels as follows:

- Determine appropriate measures for approver span of responsibility and implement procedures to periodically evaluate approver volume of user access requests.
- Coordinate with and inform department management when access approval levels present a high risk of insufficient review. Obtain management's acknowledgement as to whether to continue or identify additional security access approver for managing volume levels appropriately.

Management Response

Client Services will work with Information Security to determine appropriate criteria for span of control. We will provide reports to the departments to review instances where user to approver ratios or user access request volumes exceed criteria. While this is not in the critical path of the project, we will begin the review immediately after go live of the new SN system. We will have the notification process operational by December 31, 2014.

Responsible Official: John Roe, Director of Information Resources Client Services

Target Implementation: December 31, 2014

Sincerely,

Valla F. Wilson, Assistant Vice President for Internal Audit

Audit Team:

John Maurer	- Senior IT Auditor
Jeffrey Kromer	- Manager of Internal Audit
Tim LaChiusa	- Assistant Director of Internal Audit

Valla Wilson - Assistant Vice President, Internal Audit

Cc: Arnim Dontes, Executive Vice President for Business Affairs
Kirk Kirksey, Vice President for Information Resources
Ed Ames, Assistant Vice President for Information Resources
Joshua Spencer, Assistant Vice President and Chief Information Security Officer
John Roe, Director of Information Resources Client Services
Mary Robles, IR Manager