Office of Internal Audit

UTSouthwestern
Medical Center

Decentralized Computing Audit

Internal Audit Report 19:22

January 13, 2019

Table of Contents

Executive Summary

Background

The information technology (IT) structure at the University of Texas Southwestern Medical Center (Medical Center) is decentralized with academic departments and other non-hospital related departments empowered to operate independently. Departments can make their own purchasing decisions within budgetary and policy requirements, including the decision to use the services of the centralized Information Resources (IR) department. This decentralized structure can present a higher risk to the Medical Center if departments elect to acquire and support their own decentralized computing environments and do not implement prudent IT security and operational controls typically present in a centrally managed IT organization. The major factor contributing to this risk is budgetary limitations through grant funding, which may not cover staffing costs for IT technical support resources.

An Internal Audit report in fiscal year 2015 highlighted this risk and, in response, management established the Embedded IT Program to provide an additional layer of support services available to departments. The diagram at Appendix B details the four layers of support. The Embedded IT Program is the highest level of support departments can purchase from IR. It offers a long-term arrangement with departments for continuous IT support using either a one-half or full-time support technician. Embedded IT technicians are employed and trained by Information Resources and office within the enrolled department. The Embedded IT program has focused on 70 departments in Academic Affairs, meeting with them to provide education and obtain sign-off that the departments understand their responsibilities for their decentralized IT system management. Currently, 12 Academic departments plus the Moncrief Cancer Institute are enrolled in the program.

Scope and Objectives

The Office of Internal Audit has completed its Decentralized Computing audit. This was a risk based audit and part of the fiscal year 2019 Audit Plan. The audit scope period was the beginning of fiscal year 2018 to current. As a follow-on to the fiscal year 2015 audit, the review included decentralized departmental computing environments, with a focus on services provided through the Embedded IT Program and a sample of departments, based on risk criteria, selected from Academic Affairs and Business Affairs. Audit procedures included interviews with stakeholders, review of policies and procedures and other documentation, substantive testing, and data analytics.

The overall objective of the audit was to evaluate the effectiveness of controls for managing IT resources for decentralized departmental computing environments to ensure key risk areas (i.e., change management, security patching, software licensing) are appropriately managed for effective data protection.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Executive Summary

Conclusion

Overall, the Embedded IT Program has been effective at improving the level of service available to departments to manage their computing environments. Opportunities for improvement observed in the three departments sampled without Embedded IT were not present in the one department sampled using Embedded IT. Accordingly, while grant funding limitations continue to be a major impediment to wide enrollment for academic departments, management should evaluate the cost/benefit of improving the decentralized control environment by: (1) enhancing the Embedded IT services offered with training on standards and tools available and providing backup personnel to attract additional departments and (2) expanding the reach of the program to other Medical Center departments. Standards for user account naming conventions should be created and monitoring established for unmanaged workstations. Monitoring is also needed to assess departmental compliance with Medical Center standards and procedures and gauge the effectiveness of current and any future expanded investment in the program.

Included in the table below is a summary of the observations noted, along with the respective disposition of these observations within the Medical Center internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

Priority (0)	**High (0)**	**Medium (3)**	**Low (0)**	**Total (3)**

Institutional strengths identified during the audit include:

- Implementation of the Embedded IT program has increased IT support and education in operational best practices provided to Academic Affairs departments

Institutional improvement opportunities are summarized below.

- **Enhance and Expand Embedded IT Program Service Offerings –** Opportunities exist to strengthen controls in decentralized computing environments by enhancing service offerings and expanding the reach of the Embedded IT program.
- **Standardize User Account Names for Unmanaged Workstations –** Policy ISR-111 Systems Access Management does not explicitly prohibit generic local user account names, which cannot be tied to the person using the account.
- **Implement Periodic Monitoring of Decentralized Computing Environments to Verify Compliance with Medical Center Policy and Standards –** Procedures are not in place to periodically verify compliance with relevant Medical Center policies in decentralized computing environments and assist in gauging the effectiveness of the Embedded IT program.

Executive Summary

Management has plans to address the issues identified in the report and in some cases have already implemented corrective actions. These responses, along with additional details for the improvement opportunities listed above are included in the Detailed Observations and Action Plans Matrix (Matrix) section of this report.

Opportunities for improvement noted for individual departments have been provided separately to their leadership and, in most cases, corrective action has already been completed.

We would like to take the opportunity to thank the departments and individuals included in this audit for the courtesies extended to us and for their cooperation during our review.

Sincerely,

Valla F. Wilson, Associate Vice President for Internal Audit, Chief Audit Executive, Interim Chief Compliance and HIPAA Privacy Officer

Audit Team:
Gabriel Samuel, Senior IT Auditor
Jeff Kromer, Director, IT & Specialty Audit Services

cc: Arnim E. Dontes, Executive Vice President, Business Affairs
Marc E. Milstein, Vice President, Information Resources & Chief Information Officer
Heather Mishra, Associate Vice President, Academic & Administrative Information Systems
Wade Radicioni, Director of Operations and Analytics, Academic Affairs
John Roe, Director, IR Client Services
Nathan Routen, Information Security Architect, Interim Chief Information Security Officer
David Russell, Ph.D., Vice Provost & Dean of Research
Cameron Slocum, Vice President and Chief Operating Officer, Academic Affairs
Joshua Spencer, Associate Vice President & Chief Technology Officer
Thomas Spencer, Ph.D., Assistant Vice President, IR Operations and Compliance
Dwain Thiele, M.D., Interim Executive Vice President Academic Affairs & Provost/Dean, UT Southwestern Medical School

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● 1. **Enhance and Expand Embedded IT Program Service Offerings** Opportunities exist to strengthen controls in decentralized computing environments by enhancing the services provided to departments through the Embedded IT program promoting the expansion of offerings to other Medical Center departments and providing the tools and processes used in the embedded program to other areas for improving department IT management. The departmental general computing control weaknesses noted in this report illustrate the need for increased awareness of available IR policies, standards and tools for use by departments to manage their decentralized computing operations. In addition, backup personnel are not currently available to provide services to a department in the event their Embedded IR technician is not available due to staff changes. For example, the one department audited was without a dedicated Embedded IR technician because the employee was promoted to another area of IR. This left the department without long-term support approximately 10 weeks with support needs serviced through the IR Service Desk, which is a less satisfactory level of service. A suitable replacement was hired as of December 21, 2018,	1. Re-emphasize available policies, standards and tools for use by departmental technicians. 2. If feasible, consider providing trained backup personnel for departments enrolled in this program to ensure service continuity in the event their regular technician leaves or is not available. 3. Evaluate the cost-benefit of implementing the Embedded IT program beyond Academic departments to other departments such as in Business Affairs. 4. After evaluation and as determined necessary, expand the Embedded IT Program sample monitoring beyond Academic departments to other institutional divisional departments including Business Affairs, Health Affairs and Institutional Advancement**.**	**Management Action Plans:** 1. Enhancing of training materials by April 2019. **Action Plan Owners:** Assistant Vice President IR Operations and Compliance **Target Completion Dates:** Enhance materials by April 28, 2019 2. Backup Embedded IT personnel will be designated and trained by July 2019. **Action Plan Owners:** Assistant Vice President IR Operations and Compliance Director, IR Client Services **Target Completion Dates:** July 31, 2019 3. Expansion of the Embedded IT program to be considered for funding of additional FTEs during FY 2020 budget cycle. If approved, proposed completion would be by August 31, 2020. If not approved, review the IR websites related to support and expand information for departments looking to explore embedded IT options. **Action Plan Owners:** Vice President and Chief Information Officer

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		Target Completion Dates: Budget proposal by April 30, 2019, completion by August 31, 2020 4. Monitoring a sample of departments as part of yearly departmental reviews subject to expansion of the program as noted in #3 above. This will be during the Fiscal Year 2020 cycle since the FY2019 cycle has already been completed. **Action Plan Owners:** Assistant Vice President IR Operations and Compliance **Target Completion Dates:** January 1, 2020

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 2. **Standardize User Account Names for Unmanaged Workstations** Review of the Kace report of unmanaged workstations (those not managed by Information Resources) revealed 2,968 instances of generic local user account names. Policy ISR-111 Systems Access Management does not explicitly prohibit generic local user account names. Generic account names cannot be tied to the person using the account to establish accountability for use. In addition, some well- known generic account names are attractive targets for intruders and could result in a security breach.	1. Evaluate the impact of changes to Policy ISR-111 Systems Access Management and educate on the policy provisions for requiring users to: (1), where practicable, join the UTSW domain and login using the Southwestern ID and (2) when not practicable, login using a Southwestern ID name for local accounts statically tied to a single UTSW user. Alternatively, address in a new policy. 2. Identify departments with workstations using generic local user account names and coordinate with department administrators to rename these accounts where practicable for compliance with the revised Information Resources standards as noted in #1 above.	<u>**Management Action Plans:**</u> 1. In consultation with the IR Technical Coordinators group and IR Team members, evaluate the problem and then implement policy changes and any feasible controls to address the risk. The evaluation will include addressing formal workstation naming conventions. <u>**Action Plan Owners:**</u> Associate Vice President and Chief Technology Officer <u>**Target Completion Dates:**</u> July 31, 2019 2. Coordinate with Chief Technology Officer to develop messaging and send request to departments to rename accounts by April 2019. Communicate any policy changes by September 1, 2019. <u>**Action Plan Owners:**</u> Assistant Vice President IR Operations and Compliance Associate Vice President and Chief Technology Officer <u>**Target Completion Dates:**</u> April 30, 2019 – department requests September 1, 2019 – communicate any policy changes

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● 3. **Implement Periodic Monitoring of Decentralized Computing Environments to Verify Compliance with Medical Center Policy and Standards** Procedures are not currently in place to periodically verify compliance in operations in decentralized computing environments to relevant Medical Center policies and standards. Current processes require academic departments to review and confirm they understand expectations. However, proactive monitoring for a larger audience, including additional spot-checks for compliance assists in promoting departmental accountability for protecting IT resources and data and provides perspective on the overall effectiveness and impact of the Embedded IR program.	Implement procedures for periodic monitoring and reporting of departmental compliance with relevant Medical Center policies and procedures for decentralized computing environments. The following are risk items that should be considered for monitoring: · Weak password controls · Terminated active users · User accounts with generic names · Servers with outdated operating system versions · Server security vulnerabilities not timely patched · Program changes without authorization documentation · Failed backup jobs not restarted · Software installed without documented proof of license · Antivirus status	**Management Action Plans:** Implement periodic monitoring of a sample of departments to ensure they not only understand responsibilities for compliance, but are indeed complying. Implementation will be subject to expansion of the Embedded IT program as recommended in Observation #1 and will be during the Fiscal Year 2020 cycle since the FY2019 cycle has already been completed. **Action Plan Owners:** Assistant Vice President IR Operations and Compliance **Target Completion Dates:** Approval of funding by September 1, 2019 Implementation by January 31, 2020

Appendix A – Risk Classifications and Definitions

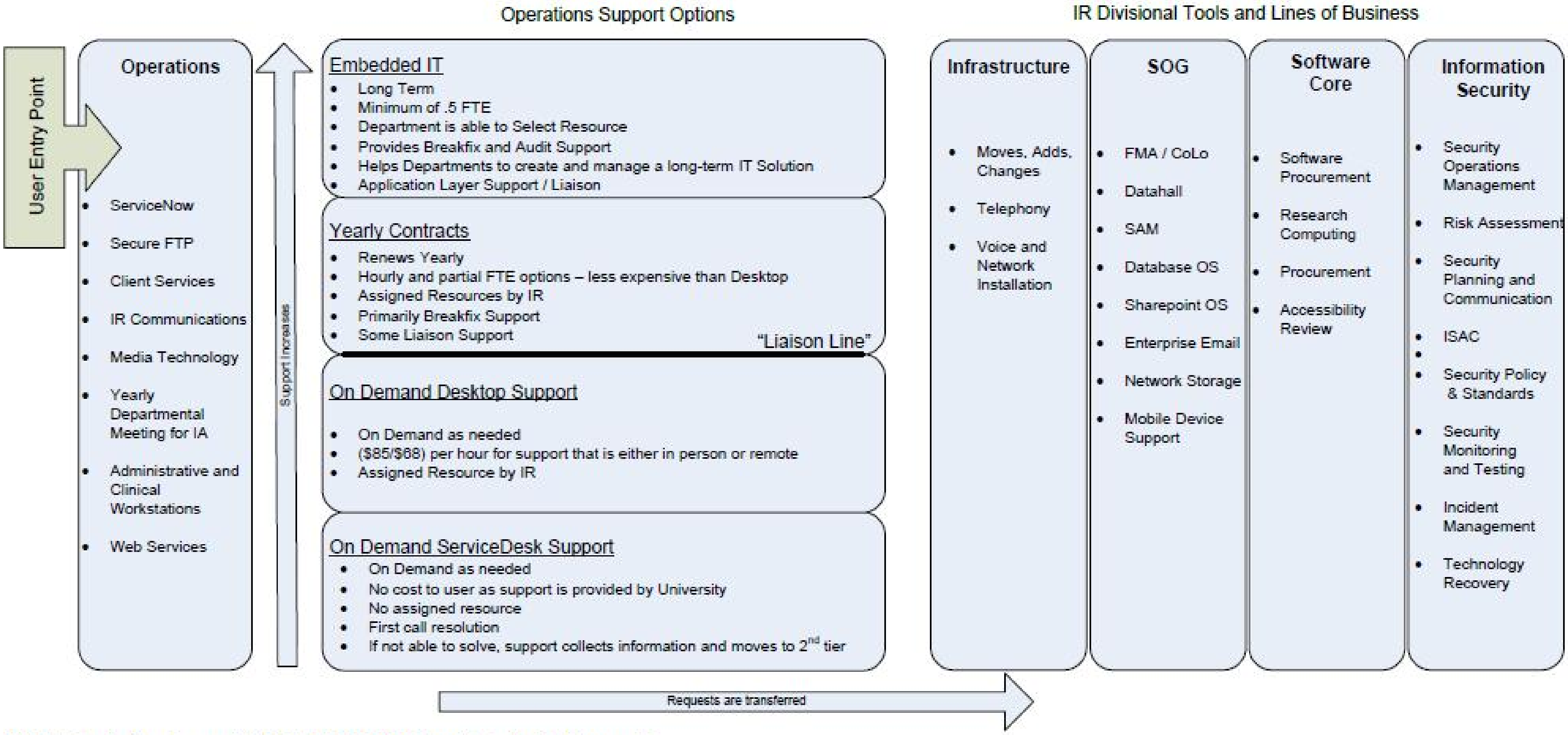
As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

	Degree of Risk and Priority of Action	
<u>Risk Definition</u>- The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Priority**	An issue identified by Internal Audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
	High	A finding identified by Internal Audit that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium	A finding identified by Internal Audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action is needed by management in order to address the noted concern and reduce the risk to a more desirable level.
	Low	A finding identified by Internal Audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Appendix B – IR Support for Users and Departments

The diagram below illustrates the layers of operations support Information Resources provides users and departments from the lowest level "On Demand ServiceDesk Support" to the highest level "Embedded IT."



Operations

- ServiceNow
- Secure FTP
- Client Services
- IR Communications
- Media Technology
- Yearly Departmental Meeting for IA
- Administrative and Clinical Workstations
- Web Services

Embedded IT

- Long Term
- Minimum of .5 FTE
- Department is able to Select Resource
- Provides Breakfix and Audit Support
- Helps Departments to create and manage a long-term IT Solution
- Application Layer Support / Liaison

Yearly Contracts

- Renews Yearly
- Hourly and partial FTE options – less expensive than Desktop
- Assigned Resources by IR
- Primarily Breakfix Support
- Some Liaison Support

On Demand Desktop Support

- On Demand as needed
- ($85/$68) per hour for support that is either in person or remote
- Assigned Resource by IR

On Demand ServiceDesk Support

- On Demand as needed
- No cost to user as support is provided by University
- No assigned resource
- First call resolution
- If not able to solve, support collects information and moves to 2nd tier

Infrastructure

- Moves, Adds, Changes
- Telephony
- Voice and Network Installation

SOG

- FMA / CoLo
- Datahall
- SAM
- Database OS
- Sharepoint OS
- Enterprise Email
- Network Storage
- Mobile Device Support

Software Core

- Software Procurement
- Research Computing
- Procurement
- Accessibility Review

Information Security

- Security Operations Management
- Risk Assessment
- Security Planning and Communication
- ISAC
- Security Policy & Standards
- Security Monitoring and Testing
- Incident Management
- Technology Recovery

NOTE: Application Support (HSIR / EDS / AAIR) is not included in this graphic
NOTE: Stakeholders and more senior customers may go directly to the IR division needed

Version 3