



**The University of Texas Southwestern Medical Center  
Decentralized Computing Review - Biophysics**

**Internal Audit Report 15:26.01**

**March 2, 2015**

# Table of Contents

---

I. Executive Summary	3
• Background/Scope and Objectives	3
• Conclusion	4
II. Detailed Observations and Action Plans Matrix	7
III. Appendices	14
• Appendix A – Risk Classifications and Definitions	14
• Appendix B – Computer Security Related Observations Not Subject to Public Disclosure	15

## **Executive Summary**

---

### **Background**

The information technology (IT) structure at the University of Texas Southwestern Medical Center (Medical Center) empowers academic departments to operate independently. Departments can make their own purchasing decisions within budgetary and policy requirements, including whether or not 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. In addition, due to the lack of an accurate inventory of systems and hardware supporting these environments, the overall risk to the Medical Center regarding decentralized computing activities is unknown. Accordingly, as part of the annual audit plan, Internal Audit has included rotational audits of these computing environments, beginning with the department of Biophysics. This department was chosen due to the large number of computing devices it uses as well as a recent network security incident involving outsider intrusion into one of their web servers.

The faculty and staff in the Department of Biophysics at the Medical Center conduct research to discover the structural and energetic properties of molecules and their assemblies, and to relate these properties to biochemical and cellular function. They apply tools ranging from structural biology, including X-ray crystallography and Nuclear Magnetic Resonance (NMR) spectroscopy, to computational biology and modern imaging methods. Sponsored by the National Institutes of Health (NIH) and others, several Biophysics research projects are also conducted in collaboration with investigators across the United States and throughout the world.

The department is comprised of 13 computational or experimental labs that function independently from a financial and tactical management perspective. Twelve of the 13 labs are highly dependent on computing resources to conduct their research. They develop specialized software scripts to produce and analyze research data. Often, these data files can be massive (several terabytes) and the processing can run for several days. Accordingly, computing may also be performed on high-performance computing resources available on-campus (Bio-HPC) and externally at the Texas Advanced Computing Center (TACC). Two of the 13 labs are headed by Howard Hughes Investigators. Howard Hughes Investigators receive funds from the Howard Hughes Medical Institute (HHMI) which they may expend in any fashion on their research. Computing equipment purchased with HHMI funds is not owned by the Medical Center.

### **Scope and Objectives**

The Medical Center Office of Internal Audit has completed its audit of Decentralized Computing activities in the Department of Biophysics. This is a risk based audit as part of the fiscal year internal audit plan, which includes rotational audits of these computing environments, beginning with the department of Biophysics.

## **Executive Summary**

---

The audit scope period included computing activities of the Department of Biophysics from September 2013 to February 2015. Audit procedures included interviews with management, review of policies and procedures, substantive testing, physical inventory/observations and data analytics. The Bio-HPC computing facility was excluded from scope and will be reviewed separately in the future as support for this resource is shared among the Biophysics, Cell Biology and Neurology departments as well as the Green Center for Systems Biology. The computing equipment owned by HHMI was also excluded from scope regarding our testing of software license compliance and computer asset management.

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

The overall audit objective was to determine if adequate computing controls were in place for key IT-related risk areas, such as information security, IT general computer controls, application controls, and licensing inventory management. This audit is a part of the larger institutional objective to ensure an accurate and current inventory of applications and computing activities.

Areas of focus included, but were not limited to:

- Server environmental security: temperature, physical access, fire and water detection
- Data Backup
- User Access: Web, Server, Application, and Database level(s) (where applicable)
- Application change management
- Software patch management
- Software licensing
- IT Asset Management

### **Conclusion**

This review is the first department review performed to evaluate overall department management of decentralized IT computing risk areas. Issues identified in this review were either issues that may be consistent across all academic departments or issues specific to the Biophysics department. As it relates to issues common to other academic departments, the main opportunity is for Academic Administration, in coordination with Information Resources (IR), to assess and determine overall strategy for ensuring adequate IT resources are available to the academic departments and are held accountable for addressing the IT and security needs of academic departments and the Medical Center. In identifying the strategy, including IT resource organization structure and practices, the other academic issues noted below would also be addressed. We have coordinated with Academic Administration leadership and IR management in developing management action plans to address the issues. Due to immediate academic initiatives and the careful coordinated effort required to assess the current IT resources; develop an overall IT academic strategy; and restructure or hire resources, management action plan timelines are in phases with final completion by the end of the calendar year.

## Executive Summary

There were four significant (i.e. high or medium/high risk) issues identified as common issues across the academic departments listed below. Additionally, there was one medium risk and one low risk that can be found in the detailed section of the report. The significant issues were:

- Formal software licensing and computer asset management procedures are not in place to account for all computer hardware and software.
- Data backup requirements are not defined to ensure all data is protected and could be retrieved in the event of a disaster or data loss.
- Two other issues which regard computer security related information are not subject to public disclosure under Texas Government Code Section 552.139 *Exception: Government Information Related to Security Issues for Computers*. Details can be found at Appendix B, which is not included in the public version of this report.

In addition to the common academic department issues, there was one high and one medium risk observation specific to the Biophysics Department. The high risk observation is also not subject to public disclosure under Texas Government Code Section 552.139, but is detailed at Appendix B as explained above. The medium-risk observation regarded cabling safety and storage of flammable materials in two server rooms.

As a specific strength identified during the audit, the limited IT technical support personnel available to the Biophysics department are experienced and conscientious. They take their role seriously as they endeavor to support the IT needs of Biophysics and other departments' students, internal colleagues and external collaborators.

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.

### Common Issues Across Academic Departments

High (0)	Medium/High (4)	Medium (2)	Low (1)	Total (7)
----------	-----------------	------------	---------	-----------

### Issues Specific to the Biophysics Department

High (1)	Medium/High (0)	Medium (1)	Low (0)	Total (2)
----------	-----------------	------------	---------	-----------

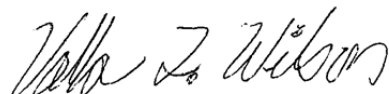
Management has plans to address the issues identified in the report and in some cases has already implemented corrective actions. These responses, along with additional details for the observations, are listed in the Detailed Observations and Action Plans Matrix section of this report.

## Executive Summary

---

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 Wilson, Assistant Vice President for Internal Audit

**Audit Team:**

John Maurer, Senior IT Auditor

Jeffrey Kromer, IT Audit Manager

Tim LaChiusa, Assistant Director of Internal Audit

Valla Wilson, Assistant Vice President for Internal Audit

Cc: Michael Rosen, Ph.D., Professor and Chairman of Biophysics  
J. Gregory Fitz, M.D., Dean of the Medical School, Provost and Executive Vice President for Academic Affairs  
Cameron Slocum, Vice President and Chief Operating Officer for Academic Affairs  
David Russell, Ph.D., Vice Provost and Dean of Basic Research  
Kirk Kirksey, Vice President and Chief Information Officer  
Joshua Spencer, Assistant Vice President and Chief Information Security Officer  
Arnim Dantes, Executive Vice President for Business Affairs  
Dipti Ranganathan, Associate Vice President for Information Resources

## **Detailed Observations and Action Plans Matrix**

---

### **COMMON ISSUES ACROSS ACADEMIC DEPARTMENTS**

The observations on the following pages were noted during our review of the Biophysics department. However, these are common issues across the schools and academic departments. They require the attention of Academic Administration management to implement the management actions plans.

## Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p><b>Risk Rating: Medium High</b> ●</p> <p><b>1. Implement software licensing and computer asset management procedures</b></p> <p>Formal software licensing and computer asset management procedures are not in place. Each Principal investigator is responsible for tracking computer assets and ensuring licensing compliance. Medical Center Policy ISR-252 requires every department to document its various software licenses in use and verify compliance with all financial and license renewal obligations.</p> <p>Without these procedures in place and personnel who are held accountable to perform procedures effectively, the risk of loss of assets, installation of unauthorized software (piracy risk) and violation of Medical center policy or licensed user agreements and copyright law is increased.</p> <p>Within the Biophysics Department:</p> <ul style="list-style-type: none"> <li>A current inventory of licensed software purchased is not documented for any of the 13 labs.</li> <li>Dell Kace, the inventory software required by IR for central reporting of installed software, was not installed on 13 of 40 (33%) workstations sampled for review. Waivers were not available for any of these 13 tested.</li> <li>Procedures are not in place to periodically reconcile Kace reports of installed software to documentation of purchased licenses to verify compliance with vendor licensing agreements and Policy ISR-252.</li> </ul>	<ol style="list-style-type: none"> <li>Identify personnel responsible for overall licensed software management or consider a dedicated IT resource. This ensures accountability and improves the ability to monitor compliance.</li> <li>Coordinate with IR to ensure Dell Kace and the appropriate Dell Kace key is installed on all computers and that those computers are reporting to the central Dell Kace server. Optionally, if Dell Kace cannot be installed, follow the process for submission of requests for waivers with Information Security on a machine-by-machine basis. This facilitates the reconciliation process to ensure proper management of software and computer assets.</li> <li>Document an inventory of all licensed software purchased. This increases the likelihood of license compliance.</li> <li>Implement procedures to periodically reconcile: (1) physical inventories of computers to PeopleSoft Asset Management records and (2) Dell Kace software reports to documentation of purchased licenses. This ensures compliance with Medical Center policy and vendor licensing requirements.</li> </ol>	<p><b><u>Management Action Plans:</u></b></p> <ol style="list-style-type: none"> <li>We agree with the recommendation. Personnel responsible for overall software management will be designated for all academic departments.</li> <li>Management will ensure Dell Kace is installed on academic department computers or will secure approved waivers for all academic departments.</li> <li>An inventory of all licensed software will be documented for all academic departments.</li> <li>Procedures to periodically reconcile Dell Kace hardware reports to PeopleSoft Asset Management and reconcile Dell Kace software reports to software license documentation will be implemented for all academic departments.</li> </ol> <p><b><u>Action Plan Owners:</u></b></p> <p>Vice President and Chief Operating Officer for Academic Affairs</p> <p>Associate Vice President for Information Resources</p> <p><b><u>Target Completion Dates:</u></b></p> <p>Once an infrastructure is established to address the issues in observation #1, we will be able to complete these actions as follows:</p> <ol style="list-style-type: none"> <li>September 30, 2015</li> <li>October 31, 2015</li> <li>November 30, 2015</li> <li>December 31, 2015</li> </ol>



## Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p><b>Risk Rating: Medium High</b> ●</p> <p><b>2. Develop and implement a standardized strategy and methodology to ensure data is protected</b></p> <p>There is not a standardized departmental policy defining the requirements for data backups. As a result, data could be compromised, lost, or not recoverable.</p> <p>In the Biophysics Department:</p> <ul style="list-style-type: none"> <li>Each PI has discretion for how data is backed up and stored. Data is typically backed up to a server or external drive stored in close proximity to the original data, risking loss of both the original and backup data in the event of a fire or other disaster.</li> </ul> <p>Specific issues identified were:</p> <ul style="list-style-type: none"> <li>One of 13 labs back up data to local "flash" drives.</li> <li>Two of 13 labs back up data to Bio-HPC servers located in a different building on the North Campus, which is still relatively close in proximity.</li> <li>Six of 13 labs back up data to local hard drives or servers located in the same lab or in another room in the Biophysics area.</li> <li>Backup frequency is not consistent, varying from "daily" to "infrequently".</li> <li>Backup media is not routinely tested for readability or completeness in 12 of the 13 labs.</li> </ul>	<p>1. Develop and implement a standardized data backup strategy for all departmental personnel to follow. Backup requirements defined should be based on risk factors. Consideration should be given to using a cloud solution that provides adequate storage. This will ensure that all institutional data is protected.</p> <p>Factors to include:</p> <ul style="list-style-type: none"> <li>Categorize data by value</li> <li>Consider grant stipulations</li> <li>Consider the Medical Center's Record Retention Schedule (seven years after close).</li> </ul> <p>Consider the following backup options:</p> <ul style="list-style-type: none"> <li>Storing data on shared network drives, which are backed up nightly by IR</li> <li>Using the Medical Center's new cloud-based data storage option</li> <li>Backup to computer disks or other media that is located or can be stored at a safe distance from the original data</li> <li>Periodic rotation to an offsite storage facility</li> </ul> <p>2. Periodically test backup media for readability. This will ensure it can be restored in the event of a disaster or other loss.</p>	<p><b><u>Management Action Plans:</u></b></p> <ol style="list-style-type: none"> <li>We agree and a standardized data backup strategy to ensure institutional data is protected for all academic departments based on risk will be developed. Individual departmental plans will then be documented.</li> <li>Procedures to periodically test backup media will be implemented for all academic departments.</li> </ol> <p><b><u>Action Plan Owners:</u></b></p> <p>Chief Information Officer</p> <p>Vice President and Chief Operating Officer for Academic Affairs</p> <p><b><u>Target Completion Dates:</u></b></p> <ol style="list-style-type: none"> <li>May 31, 2015</li> <li>August 31, 2015</li> </ol>

## Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p>Risk Rating: Medium ●</p> <p><b>3. Improve IT server operation management documentation</b></p> <p>IT server operation management documentation is missing, limited or inadequate. Without such documentation, personnel may lack the necessary instructions to maintain server availability. This could impact researchers and other customers in performing their functions.</p> <p>In the Biophysics department, opportunities exist in two labs to improve IT server procedural documentation, which will facilitate IT related support and ensure compliance with regulations and policies.</p>	<ol style="list-style-type: none"> <li>1. Develop thorough IT procedural documentation and make readily available to staff. Critical areas include server installation, security configuration, user setup and deletion, update monitoring and application, backup protocols and procedures. This will ensure continuity of departmental practices and a ready reference for training replacement staff.</li> <li>2. IR can provide a centralized SharePoint site for departments to store and share documentation. Management is encouraged to coordinate with IR to implement such a facility. This will enable standardized templates to be developed and made accessible to all departments, thus maintaining consistency.</li> </ol>	<p><b><u>Management Action Plans:</u></b></p> <ol style="list-style-type: none"> <li>1. Thorough IT procedural documentation will be developed and made readily available to staff including the areas recommended.</li> <li>2. Management will coordinate with IR to provide standardized procedure templates for all academic departments to facilitate documentation.</li> </ol> <p><b><u>Action Plan Owners:</u></b></p> <p>Vice President and Chief Operating Officer for Academic Affairs</p> <p>Associate Vice President for Information Resources</p> <p><b><u>Target Completion Dates:</u></b></p> <ol style="list-style-type: none"> <li>1. December 31, 2015</li> <li>2. December 31, 2015</li> </ol>

## Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p><b>Risk Rating: Low</b> ●</p> <p><b>4. Implement a standard user naming convention.</b></p> <p>There is not a standardized departmental policy for user account naming conventions. An inconsistent user naming convention prevents identification of the person using the account and obscures accountability for their actions.</p> <p>In the Biophysics department, a standard naming convention is not consistently used to set up new user accounts.</p>	<p>Adopt the Medical Center's naming convention policy as a departmental standard and require system administrators to follow this standard for all new user accounts. This will facilitate user identification and accountability.</p>	<p><b><u>Management Action Plans:</u></b></p> <p>The Medical Center's naming convention will be adopted as a standard for all academic departments and all system administrators will be required to follow this standard for all new user accounts.</p> <p><b><u>Action Plan Owners:</u></b></p> <p>Vice President and Chief Operating Officer for Academic Affairs</p> <p>Associate Vice President for Information Resources</p> <p><b><u>Target Completion Dates:</u></b></p> <p>December 31, 2015</p>

## **Detailed Observations and Action Plans Matrix**

---

### **ISSUES SPECIFIC TO THE BIOPHYSICS DEPARTMENT**

The observations on the following pages are specific to the Biophysics department. Management action plans will be addressed by the department management.

## Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p><b>Risk Rating: Medium</b> ●</p> <p><b>5. Safety and fire hazards exist in the server rooms</b></p> <p>During a walkthrough of the HHMI data center and the server closet in a certain lab, both located on the 10<sup>th</sup> floor of the ND building, the following safety hazards were served:</p> <ul style="list-style-type: none"> <li>• Network cabling is strung across the floor, including a main pathway through the HHMI data center. This poses a risk that someone could trip on the cables and fall. In addition, the cables are unnecessarily subjected to wear and possible breakage from foot traffic.</li> <li>• Flammable materials (cardboard boxes) are stored in proximity to the servers in both the HHMI data center and the server closet in another certain lab, posing a fire hazard and risking destruction of the server resulting in possible data lost.</li> </ul>	<ol style="list-style-type: none"> <li>1. Since the identified cables are not connected to the Medical Center network and support only HHMI equipment for which IR is not responsible, coordinate with Environmental Health and Safety and HHMI to identify a feasible solution for this safety hazard.</li> <li>2. Remove flammable materials from the data center and the server closet.</li> </ol>	<p><b><u>Management Action Plan:</u></b></p> <ol style="list-style-type: none"> <li>1. Management agrees with the recommendation. We are coordinating with Environmental Health and Safety and HHMI to identify a feasible solution for this safety hazard.</li> <li>2. The identified flammable materials have been removed from the HHMI data center and server closet.</li> </ol> <p><b><u>Action Plan Owners:</u></b></p> <ol style="list-style-type: none"> <li>1. Administrative Manager for Biophysics Manager of Administrative Services, HHMI</li> <li>2. Administrative Manager for Biophysics</li> </ol> <p><b><u>Target Completion Date:</u></b></p> <ol style="list-style-type: none"> <li>1. April 30, 2015</li> <li>2. Completed</li> </ol>

## 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:

<b>Risk Definition</b> - The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	Degree of Risk and Priority of Action	
	High	The degree of risk is unacceptable and either does or could pose a significant level of exposure to the organization. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium/High	The degree of risk is substantially undesirable and either does or could pose a moderate to significant level of exposure to the organization. As such, prompt action by management is essential in order to address the noted concern and reduce risks to the organization.
	Medium	The degree of risk is undesirable and either does or could pose a moderate level of exposure to the organization. As such, action is needed by management in order to address the noted concern and reduce risks to a more desirable level.
	Low	The degree of risk appears reasonable; however, opportunities exist to further reduce risks through improvement of existing policies, procedures, and/or operations. 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.