

19-115 Departmental Review – Imaging Physics

EXECUTIVE SUMMARY

At management's request, Internal Audit conducted a review of key financial, administrative, and compliance functions, which was intended to provide a general assessment of related processes and controls.

The Department of Imaging Physics resides within the Division of Diagnostic Imaging. The department has three main mission focus areas: Patient Care Support, Research, and Education. The department's FY2018 operating expenses were \$15.9 million, with more than 120 faculty, staff, and trainees. Many in the department serve in various roles as they collaborate with others in the Diagnostic Imaging Division and throughout the Institution.

Overall, we identified deficiencies in the department's internal control system, including inadequate oversight and monitoring, lack of written policies and procedures, challenges in obtaining information, employee turnover, and inappropriate segregation of duties. As a result, we observed the following:

| Area | Key Issues Noted | Ranking |
|---------------------------|---|---------|
| Service Center Management | <ul style="list-style-type: none"> Inconsistent billing and collections Lack of controls over SAIF Lab activities | High |
| Asset Management | <ul style="list-style-type: none"> Unencrypted assets Inadequate reporting of missing and offsite assets Untimely certification of annual inventory | High |
| Personnel Management | <ul style="list-style-type: none"> Untimely approval of timecards in Kronos Inaccurate tracking and recording extramural leave | Medium |
| Grants Management | <ul style="list-style-type: none"> Untimely and inaccurate effort reporting Untimely closeouts for inactive projects | Medium |
| Financial Management | <ul style="list-style-type: none"> Outstanding account deficits of \$1.28 m Lack of controls over training course revenues Inappropriate procurement card expenditures Inadequate documentation and required approvals for Chairman's fund expenditures | Medium |
| System Access | <ul style="list-style-type: none"> Lack of a risk assessment Inadequate system access controls | Medium |

In fiscal year 2018, management hired a new Department Administrator (DA) and filled several key positions. The DA has been proactive in addressing issues noted within this report throughout the engagement. She developed standard operating procedures and initiated the close out of expired grants.

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.

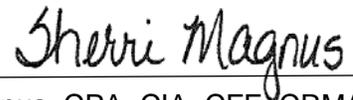
Additional details are outlined in the **Detailed Observations** section below. Additionally, we have provided our general concerns surrounding iLab and other service centers to Institutional Compliance for further consideration. Finally, certain issues have been communicated to management under separate cover.

Management's Summary Response:

Management agrees with the observations and recommendations and has developed action plans to be implemented on or before November 2019.

Appendix A outlines the methodology for this project.

The courtesy and cooperation extended by the personnel in the Department of Imaging Physics are sincerely appreciated.



Sherri Magnus, CPA, CIA, CFE, CRMA
Vice President & Chief Audit Officer
May 30, 2019

DETAILED OBSERVATIONS

Observation 1:**Improve Department's Internal Control System****RANKING: HIGH**

An effective internal control system provides the framework needed to ensure the integrity of financial and accounting information and to promote accountability. During our review, opportunities to improve or establish internal controls were identified in several areas, related to the following:

- Inadequate oversight and monitoring, including financial reviews and reconciliations
- Lack of written policies and procedures
- Challenges in obtaining information to make informed decisions
- Employee turnover in key functions, and
- Inappropriate segregation of duties

When control activities are not adequate, or do not exist, the department's operations may be adversely impacted, along with the department's goals and objectives.

Recommendation:

Management should continue its efforts to enhance the internal control system as corrective actions are taken to resolve the following observations.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: November 30, 2019

Management is in the process of strengthening the internal controls throughout the department by developing and implementing standard operating procedures and properly segregating incompatible duties. We have also recently hired a financial analyst to provide financial reviews and reconciliations on a preset frequency for all activities within the department. In addition, as indicated in the responses to the subsequent observations, management is taking the actions necessary to minimize the risks identified.

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.

Service Center

The Small Animal Imaging Facility (SAIF) is a core MDA research resource that is both fee-for-service as well as partially funded by the Cancer Center Support Grant (CCSG). The facility provides researchers with access to imaging technologies and expertise for all stages of research. The facility offers imaging equipment optimized for small animal research, as well as provides support for animals before, during, and after experiments. Users of the SAIF Lab schedule services through the iLab website, and then either an internal transfer or external invoice is generated for services rendered.

Observation 2:

Establish Consistent Billing and Collection Practices

RANKING: HIGH

While the SAIF Lab has established billing rates, they are not consistently billing for all services provided. We identified waived service charges without valid documented support, as well as external services that were not billed. Furthermore, services that were invoiced were not consistently collected. In addition, management was unable to provide approval for the established rates.

Recommendation:

Management should develop controls to ensure consistent billing and collection for all services provided. Additionally, management should maintain supporting documentation when services are not billed due to equipment maintenance, errors or other unforeseen circumstances. Finally, management should obtain formal documented approval from Research Finance for established billing rates in accordance with institutional policy. Management should coordinate with Institutional Compliance as they implement these corrective actions.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Charles Kingsley

Due Date: November 30, 2019

Management has taken or will take the following corrective actions, in coordination with Institutional Compliance:

- *The SAIF Administrative team in collaboration with the CCSG Office and iLabs support implemented waived charge justifications within the SAIF's iLabs site. This ensures that all waived charges are appropriately documented when charges are waived moving forward. The waived charge justification implementation date was 3/21/19.*
- *Management has started to implement controls to ensure consistent internal and external billing and collections. For example:*

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.

- *The IP Administrative team has enacted a plan to address external billing deficiencies. This plan consists of having the SAIF Operations Manager continue to oversee operations and service. The IP Grants Team will generate all internal and external billing to customers, and IP's Financial Analyst will assist with backend collections and reconciliations.*
- *In addition, the CCSG Executive Committee is discussing ways to streamline external billing across all CCSG cores going forward. We have already begun the process of identifying which external payments are missing so that we can follow up using the action plan described previously.*
- *Management will obtain formal written approval from Research Finance for established billing rates in accordance with institutional policy.*

Observation 3:**Implement Controls over SAIF Lab Activities****RANKING: HIGH**

Most SAIF Lab activities are managed through iLab, an application utilized by all MD Anderson core grant facilities. iLab is a core facility management software that is used for activities such as managing service requests and reservations, billing and invoicing, and reporting. Controls within the SAIF Lab, including those related to iLab, are not adequate to ensure consistent billing and collections, as indicated in Observation #2. Specifically,

- Lack of segregation of duties – One employee currently performs schedule and/or rate changes, invoice and collection management, monthly reconciliations, and record maintenance. No oversight or monitoring is being performed related to these activities. As a result, there is limited assurance that these activities are being performed as management intended.
- Excessive access to the iLab application - all 17 SAIF employees have Administrative Level access to iLab, which allows them to access all administrative settings, edit functions, and billing and reporting. As a result, inappropriate changes or deletions could be made to service records or billing transactions without proper authorization.
- Inadequate revenue reconciliation process - reconciliations are inconsistently performed, as demonstrated by the fact that all revenues are not being collected (see Observation #2). Also, there was no evidence of supervisory review. The risks are therefore increased that errors or irregularities in revenues will occur and go undetected.

Institutional policies mandate that appropriate internal controls should be established over financial activities.

Recommendation:

Management should implement controls over SAIF Lab activities to ensure that duties are adequately segregated, access to the iLab application is appropriately restricted, and comprehensive revenue reconciliations are consistently performed and reviewed. Controls should include regular oversight and monitoring of key SAIF Lab activities.

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.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: November 30, 2019

With regard to segregation of duties, the SAIF management will develop and implement standard operating procedures to ensure proper segregation of duties.

With regard to iLabs, the SAIF management team worked with iLab support to create tiered access to this application. All SAIF technicians' access will be changed to a member permission level. The member level only allows for managing user reservations on the calendars and doesn't allow for any admin level changes to charges or calendar functions. Members with administrative privileges with access to updating the tool and its configuration will include the SAIF Director, Deputy Director, Manager, Grant Manager, and Department Administrator. Additional designation/privileges changes can be made based on recommendations by the Audit or CCSG Executive Committees.

With regard to revenue reconciliations, the IP Administrative team has enacted a plan to use IP's Grants team along with IP's Financial Analyst to conduct reconciliations for SAIF. As described in Observation 2 above.

Asset Management

Asset management involves all processes associated with the asset life cycle – acquisition, inventory, and disposal. Property Officers are responsible for the accounting of all capital and controlled assets entrusted to the department.

Computers, mobile devices, and other information technology (IT) assets are used across the institution to store and transmit sensitive, confidential data. Tracking and monitoring of these devices through the institutional acquisition and inventory process is critical to protect this data.

Observation 4:**Strengthen Controls over Assets****RANKING: MEDIUM**

The Department had 302 assets during the period. During our review, we noted the following areas where asset controls should be enhanced, including designation of a departmental property officer:

- Missing property report forms were not submitted to Materials Management as required for 16 missing assets, including 4 that were not adequately protected – see Observation #5.
- Eleven IT assets (computers and tablets) were not reported missing to University of Texas Police Department (UTPD) or Information Security (IS).
- Offsite authorization and data security agreement forms were not completed for 12 IT assets located in remote locations.

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.

- A server purchased using a procurement card could not be positively verified due to the lack of identifying information.
- The Certification of Annual Inventory for FY 2018 was not completed until requested during the audit.

The Information Resources Security Operations Manual (IRSOM) and the Asset Control Manual (ACM) provide requirements for oversight and protection of Institutional assets. Requirements include completion and reconciliation of annual physical inventory, reporting of missing assets, maintenance of offsite asset authorizations, and property tagging. Without adequate controls over assets, there is an increased risk that theft or losses may occur and not be detected in a timely manner.

Recommendation:

Management should strengthen controls related to assets to ensure that all required reporting occurs, offsite authorizations are completed, purchased assets are tagged and verifiable, and the annual certifications are completed timely.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: August 31, 2019

Department management has taken or plans the following actions:

- *Management has designated a property officer as well as a backup. Both will be trained on the institutional policies related to assets.*
- *Management has established a process for tracking all purchased equipment and assets. These assets will be logged in an equipment database.*
- *The Office Supervisor is assigned the duty to ensure the reconciliation of available assets with items logged into the database and certifies their findings on a timely annual basis.*
- *Going forward, management will identify all remote assets on an annual basis and ensure offsite authorization forms are completed.*
- *Management will contact the vendor to obtain necessary information to validate the server purchased.*

Observation 5:

**Ensure Computers and Mobile Devices
Are Protected**

RANKING: MEDIUM

The Information Resources Security Operations Manual requires the protection of desktops, laptops, and mobile computing devices that view or store confidential information. We identified nine computers and numerous mobile devices that did not contain sufficient protective measures. Without these device management protections, sensitive information could be accessible to unauthorized individuals.

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.

Recommendation:

Management should coordinate with the Information Technology department to ensure all computers and mobile devices are protected.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: August 31, 2019

The Office Supervisor and Manager of the Scientific Computer Research for Imaging Physics are the gatekeepers for all new computers and mobile devices. They will coordinate with the Information Technology department to ensure all computers and mobile devices are protected.

Personnel Management

Kronos is the official institutional time and attendance management system. Effective personnel management includes, but is not limited to, the weekly review and approval of timecards and the accurate and timely recording of extramural (EXT) and employee leave.

Observation 6:

Approve Timecards as Required

RANKING: MEDIUM

Institutional Policy requires department managers to review all time and leave captured in Kronos for accuracy and complete approval process in the system by 11:59 p.m. each Tuesday. A timecard review of 6 weeks, selected between January 2018 and August 2018, revealed that 136 out of 517 (26%) timecards were not approved in Kronos by department management, increasing the risk that errors may not be detected or corrected. Although management built a query to identify all employees for timecard approval, the query was incorrect so that some employees were missed. Management indicated that the Kronos query has since been refined to include all required employees.

Recommendation:

Management should enhance processes to ensure that all employee timecards are included in review and approved by management each week in accordance with institutional policy.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: June 30, 2019

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.

Management coordinated with HR to update the hyperlink list in Kronos so that only employees for Imaging Physics are included in the report. Previously the list included employees from the Division, who had the same time code as those in IP, but were not IP employees. Management has also created operating procedures to address this key issue. Classified staff are required to submit leave requests in a timely manner and obtain direct supervisor approval in order to minimize Kronos corrections.

Observation 7:

Establish Process over Extramural Leave

RANKING: MEDIUM

Imaging Physics does not have a process in place to ensure the accuracy of extramural leave. A review of 41 trips during fiscal year 2018 indicated that EXT/PTO days were not accurately recorded in Kronos for 17 (41%) trips. When extramural leave is not managed properly, Kronos leave balances may be incorrect and the 30-day extramural leave limit may also be exceeded.

Extramural leave is granted annually to eligible faculty members to pursue outside professional activities or interests with or without personal financial gain. Per policy, extramural leave must be recorded in Kronos and may not exceed 30 working days in any fiscal year without prior approval.

Recommendation:

Management should establish a process to ensure that all extramural leave complies with institutional policies and is recorded in Kronos. Management should also conduct a full review of faculty EXT/PTO leave and coordinate with Human Resources to determine the course of action for any undocumented leave.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: June 30, 2019

Management will establish a process to ensure that extramural leave and paid time off is recorded accurately in Kronos by reviewing leave requests in conjunction with travel documentation. The department has hired additional support staff (within the last year, Office Supervisor and 2 Administrative Assistants) to ensure that all extramural leave complies with institutional policies and is recorded in Kronos. Management will work with the timekeepers and Human Resources to ensure PTO balances are corrected for FY2018.

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.

Grants Management

Grants management relates to the administrative tasks required to comply with the financial, reporting, and program requirements of federal, state, and private sponsors, as well as institutional policies. It includes, but is not limited to, effort reporting, grant closeouts, material transfer agreements, grant reporting, and shared cost allocations.

Observation 8:

Ensure Timely, Accurate Effort Reporting

RANKING: MEDIUM

Effort is not certified accurately or timely. According to management, effort is certified based on payroll distribution instead of actual time spent on a project. Additionally, in fiscal year 2018, the department had a total of 54 employees who had effort allocated to sponsored projects and required certification. Of these, 23 (43%) effort cards were not certified by the November 15, 2018 deadline; however, 21 of them were subsequently certified by month end.

According to both federal guidelines and the Institution's Effort Certification policy, employees must certify the accuracy of effort that is committed to sponsored projects. While payroll distribution describes the sources of an employee's salary, effort certification describes the employee's actual effort on a project. This effort must be certified annually within 45 days of notification that the effort reports are ready for review.

Non-compliance with federal regulations relating to effort reporting may result in penalties and fines and possible loss of future funding for the Institution.

Recommendation:

Management should enhance controls to ensure that effort reflects actual time spent on projects and is reported timely. Management should coordinate with Institutional Compliance to determine if any corrective action is warranted for fiscal year 2018 effort cards that have been certified.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: November 30, 2019

Management has developed standard operating procedures for effort reporting to address this key issue and has hired a grants team (within the last year, clinical protocol manager, grants program manager and grants program coordinator) to ensure timely closeouts. Quarterly meetings are being conducted with faculty to review projects (including effort for all personnel on the project, and projected financial balances). Moving forward, payroll is not being used as the source of effort certification. We will work with Institutional Compliance to determine and address any corrective action necessary for FY18. The Protocol Manager will monitor certifications to ensure they are timely.

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.

Observation 9:**Complete Grant Closeouts Timely****RANKING: MEDIUM**

Imaging Physics is not consistently providing information to Grants and Contracts to initiate timely closeout of projects. According to management, there are currently 41 completed projects that have not yet been submitted to Grants & Contracts for closeout, with some dating as far back as 2006. The new grants manager provided evidence that the department is now making a good faith effort to reconcile and closeout completed sponsored projects.

According to institutional policy and in order to satisfy sponsor requirements for the timely closing of sponsored projects, principal investigators and departments must submit all expenditures related to projects for processing. Non-compliance with grant requirements may impact future funding for the Institution.

Recommendation:

Management should continue efforts to closeout all completed sponsored projects in a timely manner.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: November 30, 2019

Management has hired a grants team (within the last year, clinical protocol manager, grants program manager and grants program coordinator) to ensure timely closeouts. A post-award process including tracking has been implemented. Management is also planning to formally document the internal process.

Due to changes in management, and previous administration's record keeping, there was no outline for the closeout process. Management has been proactive in moving projects into closeout with Grants and Contracts and have meetings scheduled with the Huron consultants to review Imaging Physics specifically to expedite closeout.

Financial Management

Departments are responsible for establishing appropriate controls over the Institution's financial resources. Key controls should include but are not limited to properly segregated duties, timely reconciliations for significant financial activities, adequate supporting documentation for transactions, and monitoring to ensure that transactions are authorized, appropriate, accurate and complete.

Observation 10:

Resolve Deficit Account Balances

RANKING: MEDIUM

During the review, we identified 16 departmental funds with significant deficit balances totaling \$1,288,683 as of November 2018. This included \$926,427 for grant accounts and \$362,256 for non-grant accounts. As a result, Institutional funds may be required to cover unbudgeted expenses. Management has a fiscal responsibility to review and monitor funds in order to prevent deficit balances as well as detect possible errors.

Recommendation:

Management should continue efforts to resolve all deficit account balances.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: November 30, 2019

Management is working with the Division to help clear deficits for non-grant accounts from previous years. The Grants Team is reconciling and requesting closeouts for grant accounts. Management has also implemented quarterly financial review meetings with each faculty to go over grant and non-grant accounts to prevent deficits. The Clinical Protocol Manager (grants) and Office Supervisor (non-grants) serves as delegate approver to ensure appropriate expenditures and funding is in the account.

Observation 11:

Implement Controls in Training Course Revenue Management

RANKING: MEDIUM

Imaging Physics does not have adequate controls in place over its training courses to ensure proper segregation of duties, accounting, reconciliation, and oversight. The department offered two training courses during fiscal year 2018 with recorded revenue of \$41,000. All net revenues derived from the courses are to be designated for course facilitators to use for future student training opportunities.

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.

During the review, we noted the following observations surrounding the department's management of short courses:

- One employee is responsible for registration, collection, receipt, deposit, and recordkeeping. When one person is involved in all aspects of a transaction, there is an increased risk that errors or irregularities may occur and go undetected.
- The 2018 Practice Oral Exam registration fee collection included \$9,000, but we were unable to determine if revenue collection was complete due to lack of a signed roster.
- Registration checks were received in February/March 2018, but not deposited until April 2018, increasing the risk of theft or loss.
- Copies of checks were maintained on the shared drive without bank account information redacted, increasing the risk of inappropriate use of personal information.
- There was no evidence of secondary review or reconciliation of course revenues or expenses to ensure all transactions were captured and appropriate.
- Revenues and expenses for all courses are comingled in one account. As a result, there is no way to ensure that every course is profitable.
- Earned revenues designated for facilitators were not previously tracked, resulting in some overspending. Although the financial analyst maintained a spreadsheet, 3 out of 16 facilitators overspent the revenue designated for their use.

The need for financial controls is necessary to ensure funds are complete, properly safeguarded, allocated, and accounted for in accordance with institutional policy.

Recommendation:

Management should implement processes and procedures to enhance controls related to all training courses, including:

- Proper segregation of duties in collection and deposit of course fees
- Maintenance of signed course rosters
- Timely deposit of registration fees
- Redaction of banking information for all electronically maintained checks
- Management review and reconciliation of short course revenues/expenses
- Purchase review and approval process for facilitator spending requests

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: August 31, 2019

The Education Team is now comprised of a Program Manager, Program Coordinator and Administrative Assistant. This new process will include both the Program Manager and Program Coordinator as well as oversight provided by the Financial Analyst.

Once a short course is developed, the following procedures will be required to develop accurate records and provides a system of checks and balances.

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.

- *The Program Coordinator will develop a roster of attendees as course registration occurs. The roster will include course participant, payment amount collected, date received and form of payment.*
- *The roster will be used as a sign in for course participants each day the short course is held.*
- *Checks received will be recorded daily on the roster by the Program Coordinator.*
- *Checks will be stored in a lock box and secured in a locked drawer.*
- *The Program Manager will review the weekly registration and payments collected. Deposits will be made in accordance with institutional policy.*
- *The Financial Analyst will then reconcile deposits to general ledger entries.*
- *On a monthly basis, the Financial Analyst will meet with the Program Manager to review the monthly report of short course financial transactions.*
- *For record keeping purposes, bank information must be redacted on scanned copies of checks.*

Please note that the Mock Oral Exam Short Course is not being offered this year due to lack of interest on the part of the faculty in Imaging Physics. It is undetermined if and when it will be offered again. The GEANT4 Short Course was offered for the first time in 2018. It is undetermined if and when it might be offered again.

Observation 12:

Improve Documentation of Monthly Expense Review

RANKING: LOW

The Institution's policy on department fund transaction reviews requires reconcilers and primary signers to access the STAT tool monthly, perform a review for the statistical samples, and certify the accuracy of transactions. In order for the monthly certification to provide management with the necessary information for the Annual Attestation process, the appropriateness of transactions must be determined by an individual who has first-hand knowledge of the business purpose. While there was support for the expenses reviewed, there was no evidence that grant-related transactions were reviewed by an individual who has first-hand knowledge to ensure they were reasonable and necessary.

Recommendation:

Management should ensure that the review of grant-related transactions is documented.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: June 30, 2019

Management has created standard operating procedures to ensure all purchases from grant funds are allowable and reasonable. The Financial Analyst and Grants Team are working together to reconcile statistical sampling monthly and provide supporting documentation which includes approvals from the PI and Grants team.

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.

Observation 13:**Ensure Appropriateness of Procurement Card Purchases and Timely Reconciliations****RANKING: LOW**

While procurement card purchases for fiscal year 2018 only totaled \$44,200, the department does not have controls in place to ensure purchases comply with institutional policy and are reconciled and reviewed timely. We reviewed a sample of the department's procurement card purchases and identified 4 of 13 (31%) transactions that were inappropriate including a server, hard drives, memory cards, and door keypads. Although we located a server within the department, there was not sufficient information (i.e. property tag or serial number) to validate whether it was the actual server purchased. When controlled assets are not purchased through the approved process and tagged accordingly, this creates a gap in the control mechanism to properly facilitate tracking of the asset within the institution.

While monthly procurement card transaction logs were signed by the supervisor, they were not always dated. As a result, we were unable to determine whether the reconciliations were timely. When guidelines are not followed, it may result in unallowable or inappropriate procurement card purchases. Institutional guidelines mandate types of items which may or may not be purchased with a departmental procurement card. These guidelines also require timely reconciliations of monthly purchases.

Recommendation:

Management should implement appropriate controls over procurement card purchases to ensure that they are in accordance with the Procurement Card Program User's Guide and that they are reconciled and reviewed timely. Additionally, management should contact the vendor to obtain adequate identifying information to locate the server purchased. Finally, management should coordinate with Materials Management Services to properly tag the asset for inventory tracking.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: June 30, 2019

Management has created standard operating procedures to ensure compliance with procurement card guidelines, including timely reconciliations. As indicated in the response to Observation #4, management will contact the vendor in order to obtain the information necessary to validate the server. Once validated the server will be properly tagged.

Observation 14:**Ensure Chairman's Fund Expenditures are Approved and Supported****RANKING: LOW**

We reviewed a sample of 11 chairman's funds expenditures totaling approximately \$10,700 to ensure compliance with the Institution's fund guidelines. Of those reviewed, three of the eleven (27%) expenditures had exceptions as noted below:

- A business entertainment expense totaling \$5,500 did not receive prior approval from the President's office as required. All business entertainment events over \$2,000 require this prior approval.
- Expenditures totaling \$1,875 did not have supporting documentation to determine reasonableness, business purpose and proper approval, as required by institutional policy.

When expenditures are not approved or supported, there is limited assurance that they are reasonable and in compliance with institutional guidelines.

Recommendation:

Management should enhance current processes to ensure all chairman's fund expenditures are appropriately documented and obtain all approvals required by institutional policies.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: June 30, 2019

Management will develop and implement standard operating procedures to ensure that chairman's fund expenditures are adequate documented and properly approved.

System Access

The Department's Scientific Computing Research (SCR) team created the CT Protocol Management System. This is an electronic clinical tracking system used for faculty effort tracking, equipment testing, image analysis, and quality assurance. Management is responsible for coordinating with Information Security to complete a risk assessment, maintaining documented criteria for granting access and appropriately modifying access upon termination or position change.

Observation 15:

Complete System Risk Assessment

RANKING: MEDIUM

According to the Informational Resources Security Operations Manual, information systems owners are responsible for performing risk assessments and remediating system vulnerabilities and/or compliance deficiencies. All identified risks are to be documented, tracked, and managed during the system's life cycle.

At the time of the review, the department had not yet completed an Information Security risk assessment for the CT Protocol Management System, creating potential for unidentified risks and vulnerabilities that may adversely impact the institution.

Recommendation:

The Department should coordinate with Information Security (IS) to conduct a risk assessment and then implement a plan to ensure that all identified risks are addressed.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: Implemented

The risk assessment for the CT protocol management System has been successfully completed and the next assessment is scheduled for 3/26/2021.

Observation 16:

Strengthen System Access Processes

RANKING: MEDIUM

The CT Protocol Management System utilizes the Institution's Active Directory for the initial login. While the Scientific Computing Research (SCR) team issues and manages user permissions within the various system applications, we noted several opportunities for improvement:

- There was no formal criteria for granting access and determination of user permissions.
- Account permissions were not disabled when employees were terminated or transferred positions.

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.

- The system had a generic guest account which did not require a password yet had access to restricted information due to a permission set up error.

If appropriate criteria is not utilized for granting and modifying user access, individuals may be able to inappropriately access information within the system.

Recommendation:

Management should implement formal criteria for granting access and appropriately modifying access upon termination or position change. The department should also consult with Information Security regarding continued usage of the generic guest account to access functionalities within the system.

Management's Action Plan:

Responsible Executive: Dr. John Hazle

Owner: Rose Delphin

Due Date: Implemented

Management has implemented the following:

- *The Scientific Computing Resources (SCR) group is notified by Imaging Physics Operations that a user no longer works with the department. SCR will then suspend the user's account and the user will no longer have access to the application.*
- *If the user returns to MD Anderson, the user's account (even though now a valid MD Anderson username) will remain suspended in the application unless SCR is asked by upper management to re-enable the account.*
- *The permissions for the generic guest account have been corrected.*

Appendix A

Objective, Scope and Methodology:

The objective of this review was to provide a general assessment of the financial, administrative, and compliance controls within the Department. Testing periods varied based upon the area or process reviewed; however, all selected transactions occurred between September 2017 and November 2018, unless otherwise noted below.

Our methodology included the following procedures:

- Interviewed key personnel and reviewed relevant organizational policies to understand financial and administrative processes within the Department.
- Reviewed grant administration processes related to effort reporting and certification; allowable expenditures; cost allocation; subrecipient monitoring; timely progress reports; and use of material transfer agreements.
- Reviewed the results of the Department's 2018 physical inventory and assessed processes and controls over assets.
- Reviewed IT assets reported as non-encrypted and validated current status.
- Tested procurement card transactions and reconciliations for compliance with institutional guidelines.
- Reviewed documentation to ensure required monthly certification of selected expenditures, payroll expense reviews, and reconciliation of grant accounts.
- Reviewed grant and non-grant account activity to determine whether deficit balances were properly resolved.
- Examined timekeeping and leave records to determine if institutional leave management guidelines were followed.
- Tested short course revenues/expenses for supporting documentation, segregation of duties, and timely deposit.
- Tested expenditures of Chairman's funds for allowability and appropriateness.
- Reviewed CT Protocol Management system access to ensure it was managed in accordance with institutional security guidelines.
- Reviewed and evaluated SAIF Lab controls and processes. Scope included fiscal years 2016-2018.

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

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."