CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS

IA # 02-15 – INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS

REPORT DATE: AUGUST 14, 2015

ISSUED: SEPTEMBER 14, 2015

TABLE OF CONTENTS

The Oversight Committee
Cancer Prevention & Research Institute of Texas
1701 North Congress Avenue, Suite 6-127
Austin, Texas 78701

This report presents the results of the internal audit follow up procedures performed for the Cancer Prevention and Research Institute of Texas (CPRIT or the Institute) during the period July 27, 2015 through August 14, 2015 related to the findings from the 2014 Internal Audit Reports over CPRIT Governance and Information Technology, dated June 19, 2014 and July 25, 2014, respectively.

The objective of these follow up procedures was to validate that adequate corrective action has been taken in order to remediate the issues identified in the prior year Internal Audit Reports over CPRIT Governance and Information Technology.

To accomplish this objective, we conducted interviews with key personnel responsible for CPRIT Governance and Information Technology. We also reviewed documentation and performed specific testing procedures to validate actions taken. Procedures were performed at the Cancer Prevention & Research Institute of Texas office and were completed on August 14, 2015.

The following report summarizes the findings identified, risks to the organization, recommendations for improvement and management's responses.

Weaver and Tidwell, L.L.P.

WEAVER AND TIDWELL, L.L.P.
Austin, Texas
September 14, 2015

CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS
IA# 02-15 INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS
AUGUST 14, 2015
ISSUED: SEPTEMBER 14, 2015

BACKGROUND

In 2014, internal audits over the Institute's governance processes and information technology processes were completed and reported to the Oversight Committee. The internal audit report over the CPRIT's governance structure and activities identified four areas for improvement related to policies, procedures and overall training and awareness of the Oversight Committee.

The internal audit report over information technology (IT) processes identified five areas for improvement related to policies, procedures, the annual risk assessment, security administration and the updating of the disaster recovery and business continuity plan.

The 2015 Internal Audit Plan included performing procedures to validate that CPRIT management has taken steps to address the internal audit findings.

FOLLOW-UP OBJECTIVE AND SCOPE

The follow up procedures focused on the remediation efforts taken by CPRIT management to address the findings included in the 2014 CPRIT Governance and Information Technology Internal Audit Reports, and to validate that appropriate corrective action had been taken. We reviewed each report and identified the following findings:

CPRIT Governance

1. The Oversight Committee was in the process of gaining an understanding of the Institute's strategic plan and improving CPRIT's strategic direction through the program priority setting process.
2. The Institute's Policies and Procedures Guide had not been updated since 2009 and did not incorporate the changes made to the Texas Administrative Code.
3. The Oversight Committee was not consistently provided with meeting materials with sufficient time to review prior to their meetings. Additionally, the Oversight Committee was not fully aware of Grantee activity.
4. The Oversight Committee was not fully aware of requirements and constraints regarding appropriate communication in accordance with the Texas Administrative Code and Open Meetings Act. Additionally, the Oversight Committee was still forming subcommittees and establishing a regular meeting schedule.

Information Technology

1. The IT policies and procedures had been updated as required by the Texas Administrative Code (TAC 202); however, 14 of the 27 policy documents were awaiting Management review and communication to employees.
2. The IT risk assessment had not been completed. Additionally, remediation of IT vulnerabilities identified in third-party penetration tests had been performed; however, no reports had been prepared evidencing the mitigation of the risks identified by the scans.
3. There had been no reviews of systems and networks user accounts and the individual rights for each.
4. The Disaster Recovery Plan and Business Continuity Plan were not up to date.
5. Backup tapes had not been rotated to a secure off-site facility.

CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS
IA# 02-15 INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS
AUGUST 14, 2015
ISSUED: SEPTEMBER 14, 2015

Our procedures included interviewing key personnel within the Legal, Operations and IT groups in order to gain an understanding of the corrective actions taken to address the findings in the respective report, reviewing policies and procedures, obtaining related documentation and/or performing observations and testing to ensure that policies and procedures are appropriately implemented.

EXECUTIVE SUMMARY

Through our interviews, review of documentation, observations and testing we identified 2 findings. The list of findings includes those items that have been identified and are considered to be non-compliance issues with CPRIT policies and procedures, rules and regulations required by law, or where there is a lack of procedures or internal controls in place to cover significant risks to CPRIT. These issues could have significant financial or operational implications.

A summary of our results, by area, is provided in the table below. *See the Appendix for an overview of the Assessment and Risk Ratings*.

OVERALL ASSESSMENT	SATISFACTORY

SCOPE AREA	RESULT	RATING
Governance: Validate that appropriate corrective action has been taken in order to adequately remediate the findings identified in the Internal Audit Report dated June 19, 2014	We identified that the four findings identified in the 2014 CPRIT Governance Internal Audit Report have been remediated by CPRIT management.	**STRONG**
Information Technology: Validate that appropriate corrective action has been taken in order to adequately remediate the findings identified in the Internal Audit Report dated July 25, 2014	We identified that remediation efforts have been made for all five findings from the 2014 Information Technology Internal Audit Report. However, two of the findings were only partially remediated. The two findings that were partially remediated relate to: • Completing an IT risk assessment to meet all the requirements in TAC 202 • Including systems administered and hosted by third parties in the annual user access review	**SATISFACTORY**

CONCLUSION

Based on our evaluation, CPRIT management has made efforts to remediate the findings from the 2014 internal audit reports. However, continued efforts need to be made to fully remediate findings from the Information Technology Internal Audit.

In order to completely remediate the Information Technology Internal Audit, CPRIT should continue to refine the IT risk assessment process to include all relevant systems and applications, including applications and systems hosted and administered by third parties. The risk assessment process should also include documentation of CPRIT's inherent risk profile and a detailed risk response plan.

Additionally, CPRIT should include all applications and systems hosted and administered by third parties in the annual application access review in order to evaluate access rights to all CPRIT data.

We recommend that CPRIT continue to remediate the IT finding and strengthen the existing processes. Internal Audit will conduct follow-up procedures to validate remediation efforts in Fiscal Year 2016.

DETAILED PROCEDURES PERFORMED, FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS
IA# 02-15 INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS
AUGUST 14, 2015
ISSUED: SEPTEMBER 14, 2015

DETAILED PROCEDURES PERFORMED, FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

CPRIT Governance

Our procedures included interviewing key personnel within the Legal and Operations groups to gain an understanding of the corrective actions taken in order to address the findings identified in the 2014 CPRIT Governance Internal Audit Report as well as examining existing documentation and communications and performing testing in order to validate those corrective actions. We evaluated the existing policies, procedures and processes in their current state.

FY 14 Finding 1: Strategic Direction and Oversight - The Oversight Committee was in the process of gaining an understanding of the Institute's strategic plan and improving CPRIT's strategic direction through the program priority setting process.

Procedures Performed: We interviewed personnel in the Legal and Operations groups and learned that the Program Priority Project was presented to the Oversight Committee and approved during the November 19, 2014, Oversight Committee meeting. We reviewed the Program Priority Project documentation and determined that the Oversight Committee had established priorities for the three grant programs: Research Program, Prevention Program and Product Development Program.

Results: Finding remediated.

FY 14 Finding 2: Policies and Procedures Guide - The Institute's Policies and Procedures Guide had not been updated since 2009 and did not incorporate the changes made to the Texas Administrative Code.

Procedures Performed: We obtained and reviewed a draft of the updated GPRIT Grant Policies and Procedures Guide. This draft of the updated policies and procedures is currently in the process of being reviewed and approved by CPRIT management. We obtained the draft and verified that it meets the Texas Administrative Act Section 2001.004 requiring state agencies to "Adopt rules of practice and index rules, orders and decisions." Furthermore, we verified that the Guide includes an updated policy stating that it is to be reviewed and updated at least annually.

Results: Finding remediated.

FY 14 Finding 3: Oversight Committee Materials - The Oversight Committee was not consistently provided with meeting materials with sufficient time to review prior to their meetings. Additionally, the Oversight Committee was not fully aware of Grantee activity.

Procedures Performed: We selected a sample of two of the five Oversight Committee meetings and six of 24 Subcommittee meetings from November 1, 2014 through June 30, 2015. We identified that Oversight Committee materials were made available to the members of the Oversight Committee at least one week in advance of the meeting, and Subcommittee meeting materials were made available to the respective subcommittee between three and seven days in advance of their meeting. The Meeting materials were provided either as attachments to the meeting notification emails or were posted to the Sharepoint Data room, which is available to all members. Additionally, we identified that Officer's Reports were included in the meeting materials provided to the Oversight Committee. These reports discuss items such as grant award recommendations and budget adjustments of grantees.

Results: Finding remediated.

FY 14 Finding 4: Oversight Committee Training - The Oversight Committee was not fully aware of requirements and constraints regarding appropriate communication in accordance with the Texas Administrative Code and Open Meetings Act. Additionally, the Oversight Committee was still forming subcommittees and establishing a regular meeting schedule.

Procedures Performed: We interviewed personnel from the Legal group and obtained a memo prepared by the General Counsel providing training and guidance to the Oversight Committee on the Open Meetings Act. We determined that the guidance was sufficient to inform the Oversight Committee of the requirements per the Open Meetings Act. Additionally, we identified that Subcommittees were formed and regular meeting schedules were established.

Results: Finding remediated.

Information Technology

Our procedures included interviewing key personnel within the Information Technology and Operations groups to gain an understanding of the corrective actions taken in order to address the findings identified in the 2014 Information Technology Internal Audit Report as well as examining existing documentation and communications in order to validate those corrective actions. We evaluated the existing policies, procedures and processes in their current state.

FY 14 Finding 1: Review and Approval of IT Policies - The IT policies and procedures had been updated as required by the Texas Administrative Code (TAC 202); however, 14 of the 27 policy documents were awaiting Management review and communication to employees.

Procedures Performed: We obtained all IT policies and verified that the policies have been approved by CPRIT Management. Additionally, we verified that all current employees have completed IT Security Awareness and Policy Training and have acknowledged receipt of all the policies included on the Institute's SharePoint site.

Results: Finding remediated.

FY 14 Finding 2: IT Risk Assessment - The IT risk assessment compliant with TAC 202 had not been completed. Additionally, remediation of IT vulnerabilities identified in third-party penetration tests had been performed; however, no reports had been prepared evidencing the mitigation of the risks identified by the scans.

Procedures Performed: We obtained the risk assessment performed by CPRIT using Texas' Department of Information Resources' (DIR) Governance, Risk and Compliance tool, Archer. We reviewed the completed IT Self-Assessment Questionnaires for networks, applications and organizational security. Additionally, we obtained the Remediation Report in response to the penetration testing and verified that management addressed the issues identified in the report.

Results: Finding partially remediated. We identified that CPRIT used DIR's IT risk assessment tool to complete IT Self-Assessment questionnaires for the applications and systems administered by CPRIT personnel. However, the risk assessment did not include completed questionnaires for the CARS/CGMS application, which is administered by SRA International. The IT risk assessment also did not include documentation of the determination of which NIST risk questionnaire type to complete (High, Medium, or Low risk), or a risk response plan. We identified that CPRIT's Information Technology Manager prepared the Information Technology Remediation Report that responded to the findings from the penetration test conducted by DIR.

Finding 01 – MODERATE – The IT risk assessment was started with the completion of the DIR administered IT Self-Assessment Questionnaires. However, the IT risk assessment did not include:

1) Identification and assessment of all individually significant IT systems (including hosted applications such as CARS/CGMS)
2) Documentation of the determination of inherent risk
3) Risk response plan detailing the acceptance, transference or mitigation of risks

Recommendation: CPRIT should include all significant applications, including applications hosted by a third party, in the annual IT Risk Assessment. Additionally, the IT Risk Assessment should include documentation on how CPRIT determines and defines the inherent risk of the agency and the risk response plan detailing the acceptance, transference or mitigation of risk for each application and system included in the risk assessment.

CPRIT Management Response: CPRIT management agrees that it should include all significant third-party applications in the annual IT Risk Assessment, documenting the determination of the inherent risk rating and the risk response plan. During this audit cycle, the agency underwent significant changes to its information technology infrastructure, including a major migration to cloud-based provider systems and services for many core functions. In this same period, the Department of Information Resources revised Texas Administrative Code, Sec. 202.24, requiring state agencies to incorporate third-party hosted systems in the IT risk assessment in the same manner as internal agency resources. The agency will work with its vendors to develop a delivery schedule for standard attestation and security certifications (e.g., SOC 1, SSAE16, SAS 70, etc.) so that complete risk assessments can be performed on all systems utilized by the agency. Due to the complexity of some systems, CPRIT may engage a third-party vendor to assist with the evaluation of the risks of those systems and development of the risk response plan.

Responsible Party: Chief Operating Officer, Information Technology Manager
Implementation Date: July 31, 2016

FY 14 Finding 3: User Access Reviews – There had been no formal reviews of systems and network user accounts and the individual rights for each user, and no resulting reports were produced.

Procedures Performed: We obtained evidence of CPRIT's access review performed by the Information Technology Manager and Systems Administrator. We reviewed the access review documentation to ensure that all systems and applications that are utilized by and contain CPRIT data were included in the access review.

Results: Finding partially remediated. The access review included a review of physical access to on-site IT hardware and logical access to CPRIT's network resources, administrative access to servers and applications, and administrator access to third-party applications and systems administered by CPRIT. However, the access review did not include access permissions to applications and systems that are not administered by CPRIT, such as CARS/CGMS.

Finding 02 – LOW – CARS/CGMS was not included in the annual access review. The Operations Manager sends all access requests for each CPRIT employee, as needed, to SRA International who sets up the user account within CARS/CGMS. However, there is no periodic review of access to CARS/CGMS to ensure that access rights are valid.

Recommendation: CPRIT should include CARS/CGMS as part of their annual review of access to their applications and systems, verify appropriate access, and take the necessary corrective action to address any inappropriate access identified.

CPRIT Management Response: CPRIT management agrees that CARS/CGMS should be included in the agency's annual review of access to applications and systems. CPRIT will change its internal process to require that all requests for access including additions, removals, and role changes to the CARS/CGMS application hosted by SRA International are submitted through the existing IT ticketing system so that CPRIT access requests will be formally documented and can be verified against access records from CARS/CGMS. CPRIT's Information Technology Manager will work with SRA International to perform security reviews of the CARS/CGMS application, documenting the results and any necessary remediation efforts if there are findings.

Responsible Party: Chief Operating Officer, Information Technology Manager, Operations Manager

Implementation Date: December 1, 2015

FY 14 Finding 4: Business Continuity Plan - The Disaster Recovery Plan and Business Continuity Plan were not up to date.

Procedures Performed: We interviewed key personnel in the IT group and obtained the updated Business Continuity Plan draft, which includes emergency management and information technology. We reviewed the draft Business Continuity plan to ensure that it was up to date based on our understanding of the current IT environment.

Results: Finding remediated.

FY 14 Finding 5: Relocation of Backup Tapes - Backup tapes were not rotated offsite to a secure facility.

Procedures Performed: We interviewed key personnel in the IT group and identified that CPRIT has migrated to a cloud-based backup system. We also identified that all existing backup tapes have been relocated to the Texas State Library. We also examined records from the Texas State Library documenting the receipt of CPRIT backup tapes to validate that the tapes were moved to a secure offsite facility.

Results: Finding remediated.

APPENDIX

CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS
IA# 02-15 INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS
AUGUST 14, 2015
ISSUED: SEPTEMBER 14, 2015

The appendix defines the approach and classifications utilized by Internal Audit to assess the residual risk of the area under review, the priority of the findings identified, and the overall assessment of the procedures performed.

REPORT RATINGS

The report rating encompasses the entire scope of the engagement and expresses the aggregate impact of the exceptions identified during our test work on one or more of the following objectives:

- Operating or program objectives and goals conform with those of the agency
- Agency objectives and goals are being met
- The activity under review is functioning in a manner which ensures:
    - Reliability and integrity of financial and operational information
    - Effectiveness and efficiency of operations and programs
    - Safeguarding of assets
    - Compliance with laws, regulations, policies, procedures and contracts

The following ratings are used to articulate the overall magnitude of the impact on the established criteria:

Strong	The area under review meets the expected level. No high risk rated findings and only a few moderate or low findings were identified.
Satisfactory	The area under review does not consistently meet the expected level. Several findings were identified and require routine efforts to correct, but do not significantly impair the control environment.
Unsatisfactory	The area under review is weak and frequently falls below expected levels. Numerous findings were identified that require substantial effort to correct.

CANCER PREVENTION & RESEARCH INSTITUTE OF TEXAS
IA# 02-15 INTERNAL AUDIT FOLLOW UP PROCEDURES REPORT OVER PRIOR YEAR GOVERNANCE AND INFORMATION TECHNOLOGY FINDINGS
AUGUST 14, 2015
ISSUED: SEPTEMBER 14, 2015

RISK RATINGS

Residual risk is the risk derived from the environment after considering the mitigating effect of internal controls. The area under audit has been assessed from a residual risk level utilizing the following risk management classification system.

High

High risk findings have qualitative factors that include, but are not limited to:

- Events that threaten the agency's achievement of strategic objectives or continued existence
- Impact of the finding could be felt outside of the agency or beyond a single function or department
- Potential material impact to operations or the agency's finances
- Remediation requires significant involvement from senior agency management

.

Moderate

Moderate risk findings have qualitative factors that include, but are not limited to:

- Events that could threaten financial or operational objectives of the agency
- Impact could be felt outside of the Institute or across more than one function of the agency
- Noticeable and possibly material impact to the operations or finances of the agency
- Remediation efforts that will require the direct involvement of functional leader(s)
- May require senior agency management to be updated

Low

Low risk findings have qualitative factors that include, but are not limited to:

- Events that do not directly threaten the agency's strategic priorities
- Impact is limited to a single function within the agency
- Minimal financial or operational impact to the organization
- Require functional leader(s) to be kept updated, or have other controls that help to mitigate the related risk