Information Technology Internal Audit Report

Report #2013-03

August 9, 2013

CANCER PREVENTION AND RESEARCH INSTITUTE OF TEXAS

Table of Contents

Executive Summary

In support of the FY2013 Internal Audit Plan, a review of the information technology (IT) process was conducted in August 2013. The IT department is responsible for setting up and supporting IT operations at the Agency. The CPRIT offices are located in Austin, TX; however, the Chief Scientific Officer has an office in downtown Houston, which is also serviced and maintained by the CPRIT IT department. The department is also responsible for the Agency's various websites, cloud services operations, video conference system, data closet, and typical back-office IT operations.

This was the third annual IT audit for the Agency. An internal audit of the IT processes was performed previously in June 2012 and May 2011. As a result of those audits, Internal Audit provided CPRIT findings and recommendations to improve overall efficiency and effectiveness within their IT operations. Although some steps have been made to remediate these findings, CPRIT needs to place importance on establishing a strong IT governance structure.

CPRIT continues to work towards establishing leading practices within the IT operations. However, during the FY 2013 IT internal audit, the following improvement opportunities were noted, in descending priority:

- **Outdated IT Policies and Procedures** – In efforts to remediate the findings in the FY 2012 IT internal audit, the CPRIT IT department recently began reviewing and creating IT policies required by Texas Administrative Code, Chapter 202, Subchapter B – Security Standards for State Agencies. However, many of the developed policies have not yet been reviewed and approved by management.

- **Incomplete IT Risk Assessment –** As recommended as part of the FY 2012 IT internal audit remediation plan, a detailed risk assessment of the IT environment has not been performed.

- **Insufficient Disaster Recovery Plan and Business Continuity Plan** – As recommended as part of the FY 2012 IT internal audit remediation plan, a disaster recovery plan and business continuity plan has not been developed, implemented, or tested.

- **Inadequate Review or Evidence of Third-Party Control Environment –** the third party grants management provider, SRA, has not provided adequate evidence of their internal control environment to provide assurance that CPRIT's information is secure and recorded accurately within the application.

Background Information

Background

Texas voters approved a constitutional amendment in 2007 establishing the Cancer Prevention and Research Institute of Texas (CPRIT) and authorized the state to issue $3 billion in bonds to fund groundbreaking cancer research and prevention programs and services in Texas. To date, CPRIT has funded almost 500 grants totaling $835,820,450.[1]

CPRIT's goals are to:

- Create and expedite innovation in the area of cancer research, thereby enhancing the potential for a medical or scientific breakthrough in the prevention of cancer and cures for cancer;
- Attract, create, or expand research capabilities of public or private institutions of higher education and other public or private entities that will promote a substantial increase in cancer research and in the creation of high-quality new jobs in this State; and
- Continue to develop and implement the Texas Cancer Plan by promoting the development and coordination of effective and efficient statewide public and private policies, programs, and services related to cancer and by encouraging cooperative, comprehensive, and complementary planning among the public, private, and volunteer sectors involved in cancer prevention, detection, treatment, and research.

Audit Objectives

The main objective of the audit was to verify that the IT infrastructure is appropriately safeguarded and that data reliability and accuracy are maintained within the environment.

The specific audit objectives were:

- Verify that prior year audit findings had been addressed and corrected
- Validate that the Agency's IT environment is compliant with the requirements identified in the Texas Administrative Code, Chapter 202, Subchapter B – Security Standards for State Agencies
- Assess the overall IT function to determine whether sufficient resources and skill sets have been appropriated to support the technology requirements
- Evaluate whether appropriate access has been granted to the network and selected applications
- Validate whether databases are sufficiently backed-up and whether back-ups are restorable
- Confirm that the Agency follows IT general computer controls

[1] Figures provided by the CPRIT website. http://www.cprit.state.tx.us/

In order to assess the IT department, Internal Audit reviewed the following:

- Compliance with Texas Administrative Code requirements
- Internal policies and procedures

Scope

Although current legislation may potentially change procedural and reporting requirements for CPRIT, the audit performed was designed to evaluate and test compliance with established policies and procedures as of July 2013. Internal Audit interviewed staff and completed field work in August 2013.

Our procedures included discussions with the following CPRIT personnel:

Name	Title
Heidi McConnell	Chief Operating Officer
Alfonso Royal	Finance Manager
Lisa Nelson	Operations Manager
Therry Simien	Information Technology Officer

Testing Approach

During the IT audit, Internal Audit performed procedures that included: inquiry, observation, inspection and re-performance. See the matrix below for a description listing of each type of test performed.

Type	Description
Inquiry	Inquired of appropriate personnel. Inquiries seeking relevant information or representation from CPRIT personnel were performed to obtain among other things: • Knowledge and additional information regarding the policy or procedure • Corroborating evidence of the policy or procedure In conducting this internal audit, we interviewed: • Therry Simien, Information Technology Officer • Alfonso Royal, Finance Manager • Lisa Nelson, Operations Manager
Observation	Observed the application or existence of specific controls as represented.
Inspection	Inspected documents and records indicating performance of the controls, including: • Examination of documents or records for evidence of performance, such as existence of required documentation and approvals. • Inspection of CPRIT systems documentation, such as policies and procedures, network diagrams, flowcharts and job descriptions.
Re-performance	Re-performed the control activity performed by CPRIT to gain additional evidence regarding the effective operation of the control activity.

Statement of Auditing Standards

This internal audit was conducted in accordance with generally accepted government auditing standards (GAGAS). The internal audit also follows the guidelines set forth by the Institute of Internal Auditors (IIA) and conforms to the Standards for the Professional Practice of Internal Auditing, the code of ethics contained in the Professional Practices Framework as promulgated by the IIA.

Although due professional care in the performance of this audit was exercised, this should not be construed to imply that unreported irregularities do not exist. The deterrence of fraud is the responsibility of management. Audit procedures alone, even when executed with professional care, do not guarantee that fraud will be detected. Specific areas for improvement are addressed later in this report.

Findings, Observations, and Recommendations

Summary of Findings and Related Recommendations

The section below provides details regarding the audit findings and corresponding reference to the Texas Administrative Code rule.

Statement on FY 2012 Information Technology Audit Remediation

Following the fiscal year 2012 internal audit, the remediation of IT findings was significantly delayed. IT staff priorities were shifted to support the agency's 2012 annual conference logistics, electronic conference registration system and electronic scientific abstract collection system; to assist legal counsel with high-priority data requests related to investigations; to relocate the remote office IT infrastructure from Dallas to Houston; and to support communication projects. As a result, longer-term, non-user related projects (e.g., documentation updates) were effectively placed on hold. Management has made completion of all outstanding IT infrastructure and operational compliance projects a high priority during the current year within staffing constraints.

IT Policies and Procedures

Rule §202.25 lists suggested policies that should be created and implemented by the information security officer. Per the results of the FY 2012 IT audit, policies and procedures were scheduled to be completed and/or up-to-date by March 2013. As of July 2013, all policies and procedures have not been finalized. CPRIT has 11 out of 26 recommended IT policies documented. While some policies have been developed, none of them have been approved by management. Please see Appendix B for details around testing of IT recommended policies.

Recommendation: To ensure CPRIT has established proper IT governance and protocols, CPRIT needs to finalize its IT security policies and procedures as recommended by Texas Administrative Code §202.25. The agency should update all existing policies to reflect the actual processes taking place. The policies should also be approved by the state agency head or another designated representative.

Management's Response:

During this audit cycle, significant progress has been made in the review, updating and creation of IT policies. As shown in Appendix B of the report, nearly half of the recommended policies have been submitted to agency senior management for final approval. IT staff is now in the process of revising those policies to incorporate management's recommendations with the expectation to have this process completed within the next 30 days. The remaining policies and procedures will continue to be updated and/or created over the next several months.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation: May 31, 2014

Prior Year (FY 2012) Audit Management's Response:
CPRIT's policies and procedures are still being updated to reflect the many changes to agency infrastructure, systems and additional deployed services that have occurred since the new base IT infrastructure was deployed. Over the next several months, CPRIT will continue to document currently deployed critical agency infrastructure systems and services as well as systems and services that will be deployed over this same time span. CPRIT will also develop or update any relevant agency policy or procedure.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation: March 31, 2012

IT Risk Assessment

Rule §202.22 states that a "risk assessment of information resources shall be performed and documented" that ranks the risks as high, medium, or low. Per the results of the FY 2012 audit, an IT risk assessment was scheduled to be performed by December 2012. As of July 2013, a formal IT risk assessment has not yet been performed.

Recommendation: Based on the guidelines set forth in Rule §202.22, it was determined that CPRIT appears to be classified as "low-risk" and therefore should consider completing a biennial assessment. By completing a risk assessment periodically, CPRIT will be able to reassess changes that affect the IT environment. Please see Appendix A, for more detail around the risk classification levels in Texas Administrative Code, Subchapter B, Rule §202.22.

Management's Response:
The tool CPRIT previously used to perform its initial risk assessment (Information Security Awareness, Assessment, and Compliance) ISAAC program was discontinued on August 1, 2013. After a new Chief Compliance Officer is on staff, that person will help define and implement new formal assessment guidelines. Once these guidelines have been established, CPRIT IT will work to implement them as quickly as possible.

CPRIT has contracted with the Department of Information Resources (DIR) to provide quarterly controlled penetration testing of infrastructure systems and services. After each testing cycle, a report will be created detailing vulnerabilities found and remediation recommendations. Once DIR has received confirmation that remediation processes have been established, a new cycle will be implemented to test again. An initial penetration test occurred at the end of September 2013. No exploits were found in the IT systems but some system vulnerabilities were noted. IT staff is addressing those items. The remediation of those items will be tested during the next penetration test DIR conducts.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson / Chief Compliance Officer
Revised Target Date for Implementation: May 31, 2014

Prior Year (FY 2012) Management's Response:
While the initial risk assessment was not completed by the time the internal audit field work was being conducted as originally anticipated due to resource needs for other IT projects, it was performed in June 2012 utilizing the ISAAC (Information, Security Awareness, Assessment, and Compliance) tool created and maintained by Texas A&M University (TAMU) and licensed by DIR for state agencies. Based on the results of the initial assessment, a timeline of required actions to address deficient areas has been incorporated into the current IT plan. Assessment results combined with existing agency policies and TAC §202 is planned to be used to develop a controls matrix for the necessary testing of procedural processes and scheduling of identified compliance activities.

CPRIT will ensure newly implemented technical controls comply with existing agency policies and amend agency policies to comply with TAC §202. Once compliance in key areas has been addressed, a follow-up assessment will be performed in six months and reviewed. Risk assessments will be scheduled to occur annually.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation: December 31, 2012

Disaster Recovery Plan & Business Continuity Plan

Rule §202.24 states "agencies shall maintain written Business Continuity Plans that address information resources so that the effects of a disaster will be minimized, and the state agency will be able either to maintain or quickly resume mission-critical functions. The state agency head or his or her designated representative(s) shall approve the plan."

Per the results of the FY 2012 audit, a Disaster Recovery Plan and Business Continuity Plan were scheduled to be updated by December 2013. Additionally, an electronic records retention schedule was scheduled to be written and implemented by December 2013. As of July 2013, neither of these documents had been finalized.

In response to the FY 2012 internal audit, the DuPont FM 200 fire suppression system in its server room is now fully active. The system will alert specified personnel as well as the authorities in the instance of smoke, fire, or drastic change in room temperature. These alerts include a phone call and text and email alerts.

In an effort to decrease the risk of system unavailability and data recovery, the CPRIT IT group is looking into cloud services to store all public facing data and limiting data stored on servers to confidential data. This transition will protect data in the instance of a disaster as well as increase the available capacity on CPRIT servers.

Recommendation: Since IT systems are critical to CPRIT's operations, Management should update their disaster recovery plan to ensure the continued operation of the IT systems, or rapid recovery of the systems in case of a natural disaster.

Likewise, CPRIT should also ensure that a business continuity plan is kept updated to guarantee that all aspects of a business remain functioning in the midst of a disruptive event. These plans should include a business impact analysis, a risk assessment, and evidence of implementation, testing, and maintenance.

Management's Response:
CPRIT has worked to reduce overall business impact on agency operations of the most common disasters by implementing a server room environmental monitoring and alert system and performing the relocation of several agency public facing resources to cloud provider systems that are geographically separated from the agency. This work continues and will focus on internal services that can be relocated off-site for redundancy or efficiency purposes.

CPRIT will update the agency's existing business continuity plan to reflect these infrastructure changes and will design and implement an effective routine testing schedule.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation: December 31, 2014

Prior Year (FY2012) Management's Response:
Assessments have been completed for all key agency public facing resources, such as CPRIT's primary website, to determine if they could be co-located or relocated to off-site service providers. The implementation of relocating and co-locating these resources off-site is currently underway.

CPRIT is continuing to develop an electronic records retention schedule to be used for planning and testing to ensure that access to critical electronic information can be maintained in the event of a primary site disaster.

CPRIT will update the agency's existing business continuity plan, establishing current controls-based testing protocols for that plan and the scheduling of routine testing.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson / Laurie Baker
Revised Target Date for Implementation: December 31, 2013

Security Access Reviews

Rule §202.21 states that the agency should "review access lists based on documented risk management decisions." Per the results of the FY 2012 audit, CPRIT was scheduled to perform quarterly reviews of systems and network access lists, badge access lists, 3rd party agency sponsored system access (e.g. USAS, GMS), and user accounts. As of July 2013, a quarterly review has not been performed.

Recommendation: To prevent unauthorized use of proprietary information or programmatic information that could result in undesirable financial, reputational, regulatory, or operational impacts, CPRIT should consider conducting a semi-annual review of all network users, all badge access holders, and all users with access to USAS. Any exceptions should be noted and remediated immediately.

Management's Response:

While informal security audits have been performed when staffing changes occurred, security access reviews have not been performed regularly. CPRIT will complete a second, formal review of user accounts, third-party agency sponsored accounts and physical access system lists. Final assessment report guidelines will be defined and documented, and quarterly reviews will be scheduled.

Person Responsible: Therry Simien / Lisa Nelson
Target Date for Implementation: March 31, 2014

Prior Year (FY2012) Management's Response:

CPRIT completed a review of systems and network access lists in June 2012 after the internal audit fieldwork was completed. CPRIT audited system user accounts, including third-party agency sponsored accounts (e.g. USAS, GMS), network access, facility system access keys, and badge access lists. A formal assessment report will be created and quarterly reviews will be implemented.

Person Responsible: Therry Simien / Lisa Nelson
Target Date for Implementation: June 30, 2012

Self-Assessment Review

The State Auditor's Office website provides a self-assessment document to help state agencies determine their compliance with TAC §202. Per the results of the FY 2012 audit, a TAC 202 self-assessment was scheduled to be completed by June 2013. As of July 2013, CPRIT has not yet performed a TAC 202 self-assessment.

Recommendation: CPRIT management should complete the self-assessment for state agencies annually. By performing the self-assessment, the IT department can help ensure compliance with TAC 202.

Management's Response:
CPRIT is continuing to address areas of noncompliance with requirements in TAC §202 and working to establish an annual self-assessment review schedule.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Target Date for Implementation: December 31, 2013

Prior Year (FY2012) Management's Response:
Management agrees that a regular self-assessment be performed. While the self-assessment was not completed as originally anticipated due to resource needs for other IT, CPRIT performed an initial self-assessment in June 2012 to determine compliance with TAC §202. CPRIT is addressing areas of noncompliance specified in TAC §202 and will establish an annual assessment schedule.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Target Date for Implementation: June 30, 2013

Additional Recommendations

The following was noted in 2011 and 2012 to improve IT operations and to align with leading practices.

Grants Management System Third Party Provider Review

The grants management application is hosted by a third party service provider, SRA International, Inc. CPRIT does not currently require SRA to provide any evidence of review of SRA processes or control environment.

Recommendation: Because safeguarding the information contained within the grants management application is crucial to CPRIT's reputation, CPRIT should ensure that the information contained in the SRA application is appropriately safeguarded from unauthorized external users. If SRA has had a third-party perform an independent controls attestation report for the current period, CPRIT should obtain a copy the report and review the report to ensure that SRA's controls are operating effectively. One of the common reports obtained by service providers is the SOC 2 (Service Organization Controls) Report.

A SOC 2 Report is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy. This type of report is applicable when an entity outsources a business task or function to another entity (usually one that specializes in that task or function). One way a user auditor may obtain evidence about the quality and accuracy of the data provided to a user entity by a service organization is to obtain a service auditor's report on controls at the service organization that affect data provided to the user entities. The rationale for this approach is that controls are designed to prevent, or detect and correct, errors or misstatements. If controls at a service organization are operating effectively, errors in data provided to the user entities will be prevented, or detected and corrected, and misstatements in the user entities' financial statements will be avoided.

Management's Response:
SRA has been providing the annual and quarterly SSAE 16 reports, also called Service Organization Controls (SOC) 1 Reports for assurance of the suitability of design and operating effectiveness of controls. CPRIT will work with SRA to obtain a SOC 2 Report to provide the assurances of security, availability, processing integrity, confidentiality and privacy at the service organization.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Target Date for Implementation: June 30, 2014

Prior Year (FY2012) Management's Response:
Management agrees with the recommendation that CPRIT complete a formal written assessment of the SSAE 16 annual and quarterly reports to verify that CPRIT understands the management controls over logical controls, physical controls, and change management in place at Savvis, where SRA-managed systems for CPRIT are housed. CPRIT will use these assessments to have SRA rectify any findings identified in these reports. The SSAE 16 annual report is available in December of each year, so the written assessment will be completed by the end of January and assessments of quarterly reports will be completed within 30 days after they are received by CPRIT.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Target Date for Implementation: January 31, 2013

Appendix A – Texas Administrative Code, Subchapter B, Rule §202.22

(a) A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Medium," or "Low," based primarily on the following criteria:

(1) High Risk-annual assessment--Information resources that:
- (A) Involve large dollar amounts or significantly important transactions, such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately, or
- (B) Contain confidential or other data such that unauthorized disclosure would cause real damage to the parties involved, or
- (C) Impact a large number of people or interconnected systems.

(2) Medium Risk-biennial assessment--Information resources that:
- (A) Transact or control a moderate or low dollar value, or
- (B) Data items that could potentially embarrass or create problems for the parties involved if released, or
- (C) Impact a moderate proportion of the customer base.

(3) Low Risk-biennial assessment--Information resources that:
- (A) Publish generally available public information, or
- (B) Result in a relatively small impact on the population.

(b) A system change could cause the overall classification to move to another risk level.

Appendix B – Texas Administrative Code, Subchapter B, Rule §202.25 – IT Policies

The following IT policies have been created and/or updated at the Agency:

Rule §202.25 Recommended IT Policy Area	Policy Created?
Acceptable Use	✓
Account Management	
Administrator/Special Access	✓
Application Security	
Backup/Recovery	
Change or Configuration Management	✓
Encryption	✓
Firewall	✓
Incident Management	
Identification/Authentication	
Internet/Intranet Use	
Intrusion Detection	
Network Access	
Network Configuration	
Physical Access	✓
Portable Computing	
Privacy	✓
Security Monitoring	
Security Awareness and Training	✓
Platform Management	
Authorized Software	✓
System Development and Acquisition	
Third Party Access	✓
Malicious Code	
Wireless Access	✓
Vulnerability Assessment	
Total	**11 / 26**