Information Technology Internal Audit Report

Report #2014-05

July 25, 2014

CANCER PREVENTION AND RESEARCH INSTITUTE OF TEXAS

Table of Contents

Executive Summary

In support of the FY2014 Internal Audit Plan, a review of the information technology (IT) process was conducted in June 2014. The IT department is responsible for setting up and supporting IT operations at the Agency. The CPRIT primary offices are located in Austin, TX; and the Chief Scientific Officer has an office in 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.

An internal audit of the IT processes was performed previously in August 2013, 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 still has some opportunity to improve and establish a strong IT governance structure.

CPRIT continues to work towards establishing leading practices within the IT operations. However, during the FY 2014 IT internal audit, the following improvement opportunities were noted, in descending priority:

- **IT Policies and Procedures not approved or communicated** – In efforts to remediate the findings in the FY 2012 and 2013 IT internal audit reports, the CPRIT IT department has created and updated 100% of the IT policies required by Texas Administrative Code. However, 14 of the 27 policies have not yet been reviewed and approved by management, and 26 of the policies have not been formally communicated to CPRIT employees.

- **Incomplete IT Risk Assessment –** As recommended as part of the FY 2012 and 2013 IT internal audit remediation plans, a detailed risk assessment of the IT environment has not been performed. It was also noted that remediation testing has not been performed for the vulnerabilities identified during penetration testing conducted during the audit period.

- **Security Access Reviews not performed** – Management has not conducted an annual review of user accounts and access permissions.

- **Insufficient Disaster Recovery Plan and Business Continuity Plan** – As recommended in the FY 2012 and 2013 IT internal audit remediation plan, the current disaster recovery plan and business continuity plan should be updated, implemented, and tested to reflect the current IT environment

- **Backup tapes not rotated offsite** – During the period audited, CPRIT was also under review of the Attorney General. As part of this review, the backup logs were maintained on site for inspection and were not rotated to an offsite location.

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 544 grants totaling $1,020,947,235.[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
- IT management and governance:
    - Assess the overall IT function to determine whether sufficient resources and skill sets have been appropriated to support the technology requirements
    - Validate that required policies and procedures are updated and approved by Management
- Information access, security, privacy and safeguarding:
    - Determine whether the security management structure is appropriate for support of business objectives
    - Evaluate whether appropriate access has been granted to the network and selected applications

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

- Assess completion of non-disclosure agreements
- Evaluate the performance of risk assessment of information resources

- IT system availability and recoverability:
  - Validate whether databases are sufficiently backed-up and whether systems are correctly configured to reflect the backup policy
- IT system adequacy:
  - Evaluate sufficiency of the systems to support CPRIT's business objectives

Scope and Testing Approach

The audit performed was designed to evaluate and test compliance with established policies and procedures as of June 2014. Internal Audit interviewed staff and completed field work in June 2014. Our procedures included discussions with the following CPRIT personnel:

Name	Title
Alfonso Royal	Finance Manager
Lisa Nelson	Operations Manager
Therry Simien	Information Technology Officer

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
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.

IT Policies and Procedures

Texas Administrative Code (TAC) §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 June 2014, all policies and procedures have been updated. However, 14 out of 27 policy documents are awaiting Management review and communication to employees. See Appendix B for details around testing of IT recommended policies.

Recommendation: As recommended by TAC §202.25 and to ensure CPRIT has established proper IT governance and protocols, all IT policy documents should be reviewed periodically, approved by the state agency head or another designated representative, and communicated formally to all CPRIT employees.

Management's Response 2014:

All policies required by Texas Administrative Code (TAC) §202.25 have been created or updated to reflect the current IT operating environment. Additionally, an agency Intranet deployment is in progress so that policies can be reviewed at, maintained in and disseminated to staff from a central location. During this audit cycle, Management has reviewed drafts of over half of the updated policies and their recommended changes were incorporated and approved. Completion of management review, final updates, formal adoption, and dissemination to staff of all remaining policies will be completed by the end of November 2014.

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

Management's Response 2013:

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 2013: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation 2013: May 31, 2014

IT Risk Assessment

TAC §202.22 states that a "risk assessment of information resources shall be performed and documented" which ranks the associated 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 June 2014, a formal IT risk assessment has not yet been performed.

We also noted that per Management's response in 2013, initial penetration testing was performed by a third party provider, the Department of Information Resources (DIR), during the audit period. While no exploits were found, a significant number of vulnerabilities were identified during the testing period. Although we understand from discussion with IT that remediation work has begun on these vulnerabilities, no remediation reports were prepared which evidence elimination or mitigation of these risks and acceptance of same by agency head or representative.

Recommendation: Based on the guidelines set forth in TAC §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 TAC §202.22.

However, in the interim, Management should ensure that vulnerabilities identified during penetration testing are remediated, documented and reviewed by management.

Management's Response 2014:

Our agency's initial penetration test occurred at that beginning of the current audit period in September 2013 and was performed by the Department of Information Resources (DIR). Relocation planning for the agency began during this audit cycle as well. With its long-term lease expiring at the end of August 2014 and new state office space not being ready for occupancy until February 2015, it was determined that the agency would have to perform two physical moves, one at the end of August 2014 into temporary leased space and the second in February 2015.

With the requirement of two physical moves, IT began relocating public facing services and websites offsite onto a mixture of cloud platforms and government class datacenters. Where possible, consolidation of virtual machine hosts was also performed. As it has moved sites to external providers, CPRIT must secure permission from those providers to allow DIR's testing to occur. Obtaining these permissions is still in process. The creation of formal remediation documentation was impacted by this state of change.

Now that the agency's initial physical relocation has been completed and the majority of critical systems and services have been migrated offsite, IT can work with the agency's new Chief Compliance Officer to implement formal assessment guidelines that meet or exceed state, federal and industry regulations and standards and to create and maintain formal remediation documentation for any future penetration testing.

Person Responsible 2014: Heidi McConnell / Therry Simien / Lisa Nelson / David Reisman
Revised Target Date for Implementation 2014: May 31, 2015

Management's Response 2013:
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 2013: Heidi McConnell / Therry Simien / Lisa Nelson / Chief Compliance Officer
Revised Target Date for Implementation 2013: May 31, 2014

Security Access Reviews

TAC §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 June 2014, a quarterly review has not been performed.

During the IT audit, Internal Audit also requested system access rights for new hires during the period; however, this information was not provided.

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 should also ensure that all new user access documentation for employees is maintained.

Management's Response 2014:
Informal security audits are performed when staffing changes occur at the agency. The IT ticketing system also tracks the requests for additions of new and modifications to existing user accounts, security group and email accounts. In conjunction with the Comptroller of Public Accounts, CPRIT performs security access checks of USAS every six months.

With the agency's recent physical move and migration from on-site systems to an almost completely hosted infrastructure, new and existing access control systems and methods must be coordinated and centrally consolidated for documentation and monitoring purposes. Where possible, automated checks for access right modifications will be implemented and regular reporting scheduled. Formal assessments of all agency access control systems will be performed semi-annually, documented and reported to agency management.

Person Responsible 2014: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation 2014: May 31, 2015

Management's Response 2013:
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 2013: Therry Simien / Lisa Nelson
Target Date for Implementation 2013: March 31, 2014

Disaster Recovery Plan & Business Continuity Plan

TAC §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."

Based on the results of the FY 2012 audit, the agency was scheduled to update the Disaster Recovery Plan as well as the Business Continuity Plan to include an electronic records retention schedule by December 2013. However, the agency determined in the fall of 2013 that it was not feasible based on either cost or resource considerations to establish and maintain an electronic records systems at the standards required to implement such a system. While the two plans have not been completely updated, the combination of the existing paper document retention schedule, email policy and backup process for electronic files mitigate risks associated with business continuity.

In addition to the work on the electronic records retention schedule, the agency and its third-party grants management support vendor, SRA International, Inc. (SRA), defined a 24-hour recovery time objective for the primary grant application and award system which SRA manages and hosts for CPRIT.

We note that the agency is preparing to move to a cloud-based information technology infrastructure which will occur in conjunction with the agency's physical relocation by the end of August 2014.

Recommendation: Since IT systems are critical to CPRIT's operations, Management should implement an up to date 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 2014:
Substantial progress was made during this audit period in preparing updated disaster recovery and business continuity plans for the agency. Internally, a formal committee of stakeholders was formed to review agency electronic record storage options, usage of existing storage systems and the agency's paper retention schedule and physical filing systems. Additionally, as part of the agency's relocation planning, an assessment was also performed on all internal agency IT infrastructure systems and where possible, planning began to relocate these resources, such as email, offsite. Finally, the agency has been working with SRA International, Inc. to establish a new level of recoverability for the agency's grants management system and lower the recovery time objective for CARS-CGMS from 24 hours to 12 hours.

After the agency's second physical move is completed in February 2015, a second round of assessments can be performed and the configuration for a cloud and on-premises hybrid can be fully defined and documented so the agency's consolidated disaster recovery and business continuity plans can be finalized.

Person Responsible 2014: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation 2014: May 31, 2015

Management's Response 2013:
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

Back Up Tapes

During our IT audit, we noted that backup tapes were not rotated offsite during the period. We understand that these were part of the investigations of the Attorney General and Travis Country District Attorney. However, the rotation of backup tapes to an offsite location is essential to mitigate the risk of loss of data. It was also noted that email notification for backups are only run for non-windows applications. For Windows applications, a manual process is conducted to ensure the backup was performed. However, evidence of this check is not maintained.

Recommendation: Management should ensure that backup tapes are rotated off site and an action plan is implemented to reduce the risk of data loss while backup tapes are under investigation. Management should also implement email notifications of backups performed for windows applications to ensure that backups are performed successfully and to maintain an audit trail of same.

Management's Response:
All agency historical backup tapes have been catalogued and will be relocated offsite to the Texas State Library. As a product of our recent agency move, essential agency data including email and shared storage systems is also maintained in the data centers the agency's new cloud providers.

New backup procedures must be established to incorporate both the agency's cloud infrastructure components and remaining on-premises systems to include auditable backup processes, which will produce email notifications. The backup mechanisms of the new cloud providers' data centers must be reviewed, and the agency's existing backup policy will be updated as necessary to ensure applicability to the agency's changed environment.

Person Responsible: Heidi McConnell / Therry Simien / Lisa Nelson
Revised Target Date for Implementation: June 30, 2015

Appendix A –
Texas Administrative Code, §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.

(c) Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the state agency head or his or her designated representative(s). The state agency head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The state agency head or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under §2054.077(c), Government Code.

Appendix B –
Texas Administrative Code §202.25 – IT Policies

TAC §202.25 Recommended IT Policy Area	Policy covers requirements of TAC?	Policy Created / Updated?	Policy Approved by Management?	Policy Communicated to Employees?
Acceptable Use	✓	✓	✓	X
Account Management	✓	✓	X	X
Administrator / Special Access	✓	✓	✓	X
Application Security	✓	✓	X	X
Backup / Recovery	✓	✓	X	X
Change or Configuration Management	✓	✓	✓	X
Electronic Communication	✓	✓	X	✓
Encryption	✓	✓	✓	X
Firewall	✓	✓	✓	X
Incident Management	✓	✓	X	X
Identification / Authentication	✓	✓	✓	X
Internet / Intranet Use	✓	✓	X	X
Intrusion Detection	✓	✓	X	X
Network Access	✓	✓	X	X
Network Configuration	✓	✓	X	X
Physical Access	✓	✓	✓	X
Portable Computing	✓	✓	X	X
Privacy	✓	✓	✓	X
Security Monitoring	✓	✓	X	X
Security Awareness and Training	✓	✓	✓	X
Platform Management	✓	✓	X	X
Authorized Software	✓	✓	✓	X
System Development and Acquisition	✓	✓	X	X
Third Party Access	✓	✓	✓	X
Malicious Code	✓	✓	X	X
Wireless Access	✓	✓	✓	X
Vulnerability Assessment	✓	✓	X	X
Total	**27 / 27**	**27 / 27**	**12 / 27**	**1 / 27**