THE UNIVERSITY OF TEXAS
MD Anderson ~~Cancer~~ Center

Department of Internal Audit

13-401 Texas Administrative Code 202

Strategic Area: Information Technology
Risk Type: Financial, Operational and Reputational
Audit Manager: Shawn Magee

Overview:

The Texas Administrative Code (TAC) was created by the Texas Legislature in 1977 and is a compilation of all state agency rules in Texas. Title 1 Part 10, Chapter 202, Subchapter C addresses Information Security Standards for Higher Education organizations.
TAC 202 provides the following guidance:

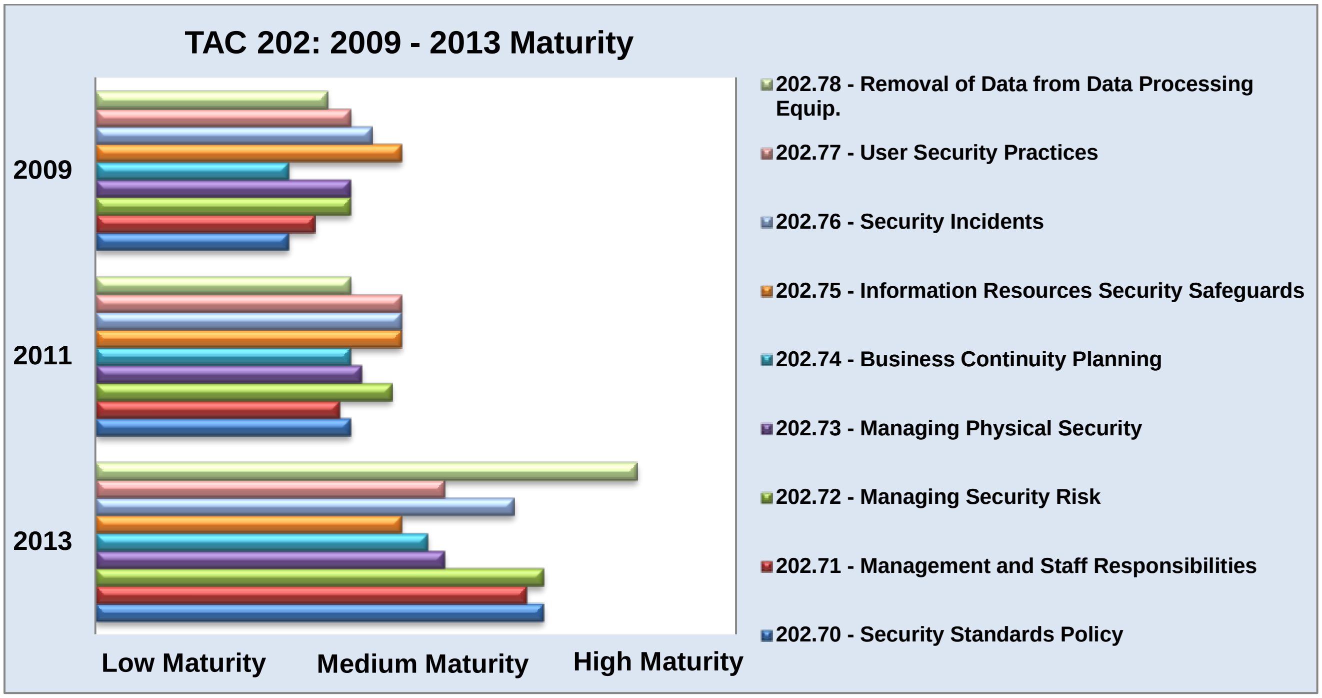
- Information resources must be available and protected commensurate with the value of the assets;
- Information resources security program is required consistent with these standards;
- All individuals are accountable for their actions relating to information resources;
- Risks to information resources must be managed. The expense of security safeguards must be commensurate with the value of the assets being protected;
- The integrity of data, its source, its destination, and processes applied to it must be assured. Changes to data must be made only in an authorized manner; and
- Information resources must be available when needed. Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.

Audit Results Summary:

As part of our assessment of TAC 202 for 2013, we considered the results of prior assessments in 2009 and 2011 and identified improvements in policy and procedure design, maturity, and effectiveness, which demonstrated the progression of the institution along the maturity continuum. The table below illustrates the institutions progression along the maturity continuum from low maturity to high maturity over the last 4 years. In our evaluation the maturity level of the institution, we considered the existence and formality of processes as well as the effectiveness of those processes. In the maturity continuum, Low Maturity correlates to a lack of policies or procedures and moves along the continuum to include informal policies and procedures or poorly designed and ineffective policies and procedures. Medium Maturity correlates to defined policies and procedures which do not operate effectively or achieve their objectives and moves along the continuum to policies and procedures which are effective overall across the institution with only minor variances or exceptions. High Maturity correlates to defined policies and procedures which continue to achieve their objectives and are determined to operate effectively throughout the institution. We evaluated the institution's level of maturity for each of the corresponding TAC 202 subsections. The intent of our evaluation of maturity is to provide an assessment of the directional improvements over the years rather than an exact measurement of effectiveness.

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.

Refer to Appendix A for additional details on each subsection.



We noted improvements for subsection 202.78 ' Removal of Data from Data Processing Equipment" where management has implemented new tools and refined the process for destroying and degaussing decommissioned servers and drives over the last few years. We also noted improvements for subsections 202.70 ' Security Standards Policy' and 202.71 "Management and Staff Responsibilities' where management continued to refine existing policies and processes, supplementing them with tools and more effective implementation resulting in a more comprehensive enterprise wide risk assessment and more robust procedures for ensuring access to systems remains appropriate. Although we noted improvements across most subsections in the maturity of formalized processes, we also noted areas for continued improvement.

Management Summary Response:

Management has identified action plans for each of the observations in the report.

Number of recommendations to be monitored by UT System: None

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.

Objective, Scope and Methodology:

The primary objectives of this assessment were to evaluate the controls and processes in place in support of MD Anderson's compliance with Texas Administrative Code Chapter 202 Subchapter C (TAC 202) and to assess the associated policy statements and processes. Our procedures included interviewing key personnel regarding processes in place to address TAC 202 requirements and analyzing supporting policies, procedures, and documentation that management referenced in support of their efforts. We performed procedures to evaluate policy statements and processes in the following areas identified in TAC 202:

- Security Standards Policy (Rule 202.70);
- Management and Staff Responsibilities (Rule 202.71);
- Managing Security Risks (Rule 202.72);
- Managing Physical Security (Rule 202.73);
- Business Continuity Planning (Rule 202.74)
- Information Resources Security Safeguards (Rule 202.75);
- Security Incidents (Rule 202.76);
- User Security Practices (Rule 202.77); and
- Removal of Data from Data Processing Equipment (Rule 202.78).

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

The courtesy and cooperation extended during the engagement was sincerely appreciated.

Sherri Magnus

Sherri Magnus, CPA, CIA, CFE, CRMA
Vice President and Chief Audit Officer
December 5, 2013

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.

Background:

Texas Administrative Code Chapter 202 Subchapter C (TAC 202) rules address the following high level topics within the stated requirements for institutions of higher education:

- Policies and Procedures/Communication;
- Institution Wide Risk Assessment;
- Reporting of the Current State of Information Security;
- Security Incidents;
- Business Continuity Planning;
- Change Management;
- Program Development;
- Application Access;
- Passwords;
- Encryption;
- Audit Logging;
- Vulnerability Scanning;
- Physical Security; and
- Disposal of data and storage devices.

The Information Security Officer has been appointed as the delegate by the President to address the requirements of TAC 202. Policies of the State of Texas, which apply to all state institutions of higher education, require that each institution apply the Security Standards Policy based on documented risk management decisions. MD Anderson documents its risk management decisions annually through the President's Report. In accordance with TAC 202 Rule 202.70, the following state policies must be considered and addressed:

(1) Information resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. These assets shall be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to state information resources shall be appropriately managed.

(2) All institutions of higher education are required to have an information resources security program consistent with these standards, and the institution of higher education head is responsible for the protection of information resources.

(3) All individuals are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by the institution of higher education and consistent with applicable laws.

(4) Risks to information resources shall be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.

(5) The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner.

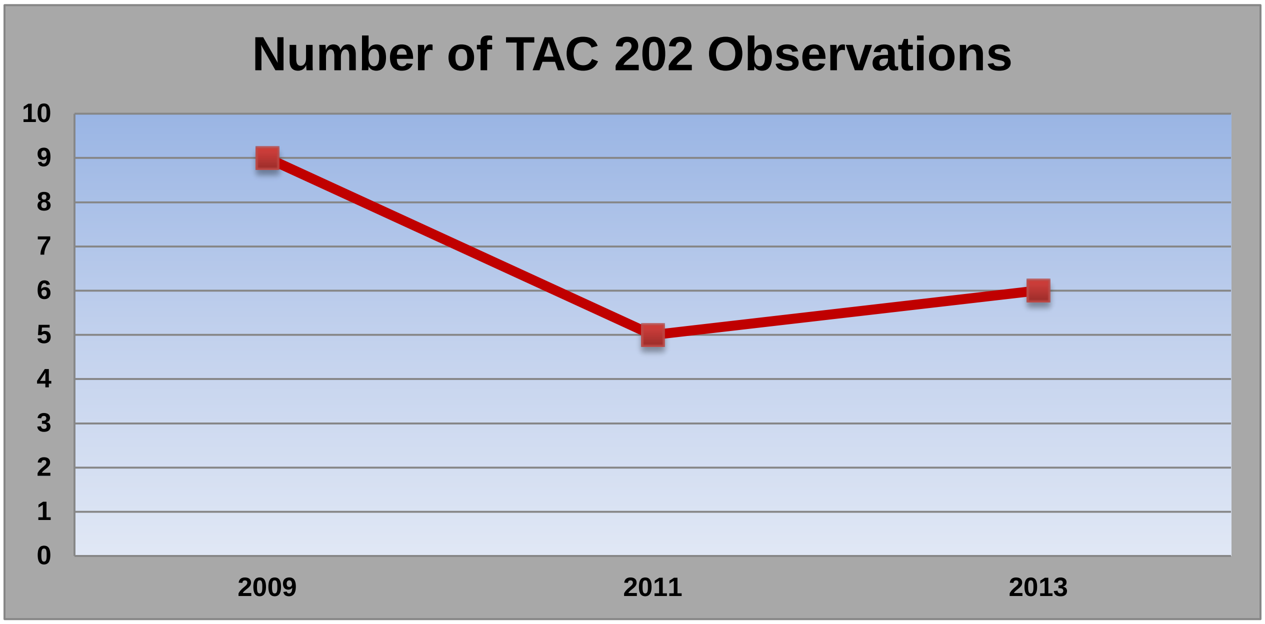
(6) Information resources shall be available when needed. Continuity of information resources supporting critical governmental services shall be ensured in the event of a disaster or business disruption.

(7) Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

(8) Institutions of higher education shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

TAC 202 Observation Trending

Internal Audit performed an analysis of the number of observations resulting from TAC 202 assessments from 2009 - 2013. The scope of procedures performed from 2009 - 2013 varied considering additional procedures performed as part of the annual internal audit plan which provided coverage over certain subsections of TAC 202. As noted in the chart below, there has been a decrease in the number of observations since 2009. Although we noted improvements in the institution's processes and procedures as noted in the Maturity Model, six observations were noted during the 2013 assessment. In the 2009 and 2011 assessments, observations were noted at a broader level in response to absent or less mature processes. Prior assessments focused on the robustness of the institution’s policies and procedures and the effectiveness of those practices.



Because more mature processes have been put in place, the 2013 assessment focused on the effectiveness of those more mature processes. Internal Audit noted there were instances where the maturity level of an area increased from a design prospective; however, an observation may have been identified when evaluating operating effectiveness. Observations resulting from the

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.

2013 assessment in most cases resulted from a small subset of the population assessed and were more specific rather than broad in nature as in prior year observations.

Summary of Current and Prior Year Observations

202.70 - Security Standards Policy

- 2009 - No documented Risk Assessment to drive a risk based approach towards information security across the Institution.

202.71 - Management and Staff Responsibilities

- 2009 - No guidelines around assigning monetary values for assets.
- 2011 - Policies did not indicate that the Information Security Officer is responsible for annually reporting the status and effectiveness of information resources security controls.
- 2011 - Policies did not contain documentation of the roles and responsibilities of the Information Security Officer.
- 2013 - Report used to perform the weekly review of Active Directory users to Identity Vault is not complete and accurate.

202.72 - Managing Security Risks

- 2009 - Information Security Officer did not report on an annual basis on the status and effectiveness of information resources security controls.
- 2011- Internal Audit noted the President's report was not presented in a timely fashion.
- 2013 - The institution does not have a process in place to evaluate risk at the enterprise wide level.

202.73- Managing Physical Security

- 2013- Employees maintained access to sensitive areas of the institution after they were transferred or separated from the institution.

202.74– Business Continuity Planning

- 2013- Timeline of the business continuity planning validations should be further along and the planed timeline for completion should be shortened.

202.75 - Information Resources Security Safeguards

- 2009 - A failure was identified during the testing of terminated users for the following applications (CARE, MedAptus, and My MD Anderson).
- 2009 – An exception was noted during the evaluation of the user access reviews.
- 2011 – User access review of the in-scope applications was not performed by the security administrator.

202.76 - Security Incidents

- 2009 – No requirements for communication and documentation of security incidents on a consistent basis between departments.
- 2013 - Reporting security incidents to the Texas Department of Information Resources (DIR) could not be validated for January 2013.

202.77 - User Security Practices

- 2009 – User Acknowledgement forms were not signed prior to the users being granted access to information resources.

- 2009 – There was no requirement to have contractors comply with the Employee Education Event (EEE) training.
- 2013 - The Information Security User Acknowledgement form was not signed by the users at satellite locations prior to the users being granted access to information resources.

202.78 – Removal of Data from Data Processing Equipment

- 2009 – No process in place to track that all hard drives that are required to be degaussed are in fact degaussed.
- 2011 - Internal Audit noted that Management does not maintain documentation of the servers/racks that have been decommissioned and removed for storage.

Observation 1:

Weekly review of Identity Vault and Active Directory Accounts

Texas Administrative Code 202.71 - Management and Staff Responsibilities describes the roles and responsibilities of users of information resources of the institution. Account Services utilizes a different authentication hub (i.e. Identity Vault) in addition to Active Directory for users to access applications. Weekly reviews of user accounts within Identity Vault and Active Directory are performed to identify any discrepancies. According to management, all active users should have Active Directory and Identity Vault accounts.

Internal Audit identified a list of 30 users that did not have an associated employee ID number. While there were valid reasons for the discrepancy, management had not identified this during their weekly reviews.

Recommendation:

Account Services should reevaluate the report parameters utilized to perform the weekly review of Identity Vault and Active Directory accounts to ensure the listing is complete and accurate.

Management's Action Plan:

Responsible EVP: Leon Leach
Owner: Less Stoltenberg
Contributor:
Due Date: 11/30/13

Account Services will work with the Identity Management Steering team enhance the current reconciliation process to better ensure that there are stronger controls between the Identity Vault and Active Directory.

Observation 2:

Enterprise Wide Risk Assessment

Texas Administrative Code 202.72 (a) – Managing Security Risk states "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". The institution has established a

Governance Risk and Compliance (GRC) component which resides within Information Security. The GRC tool is utilized to assess an application's risk and to determine if the application is within compliance of institutional standards. The frequency of a risk assessment is determined by the tier ranking of the application. Tier 1 applications are required to have a risk assessment performed annually. Tier 2 and 3 applications are required to have a risk assessment performed bi-annually. Application owners or designees are required to complete the risk assessment by answering questionnaires and undergoing system analysis. Once the risk assessment has been completed, it is routed to the Information Security group to evaluate the answers documented by the application owner / designee.

While the institution has a detailed risk assessment process in place to evaluate risk at the application level, there is no process in place to evaluate risk at the enterprise wide level.

Recommendation:

The institution should implement a process which evaluates the risk of the institution at an enterprise wide level.

Management's Action Plan:

Responsible EVP: Leon Leach
Owner: Less Stoltenberg
Contributor:
Due Date: 2/28/14

Information Security will develop and complete an enterprise risk assessment based on the National Institute of Standard and Technology (NIST) special publication 800-30 Revision 1. This high-level risk assessment will be used to evaluate enterprise risks and assign Information Security Risk resources to higher risk projects and initiatives. The intention of this risk assessment is to satisfy the TAC 202 requirement of an annual assessment of high-risk applications. This will also result in the current "risk assessment" process being altered including, but not limited to, ceasing annual risk assessments of tier 1 applications.

Observation 3:

Managing Physical Security

Texas Administrative Code 202.73 – Managing Physical Security states "the institution of higher education head or his or her designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction".

Our review revealed that 32 employees still had access to the main door of the In-Patient Pharmacy, when they had transferred to a different division and no longer required access. We also noted that two employees inappropriately had access to the Substance Vault, where controlled substances are maintained. Both employees were former pharmacy staff that have separated from the institution. It should be noted recent improvements to the pharmacy inventory management system have introduced additional layers of security in the vault area requiring both Pyxis C-II Safe access and biometric authorization/authentication in order to access the vault.

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:
The institution should implement appropriate audit and control processes to monitor and ensure compliance with institutional policy regarding the granting of appropriate badge access and timely removal of access upon termination or employee transfers to other departments and divisions. UTPD, Information Security, and Human Resources should collaborate to streamline and automate these processes where technically possible and ensure adequate resources are allocated. In addition, management should periodically confirm that employees with access to critical areas are active employees authorized to have such access.

Management's Action Plan 3.1:
Responsible EVP: Leon Leach
Owner: Less Stoltenberg
Contributor:
Due Date: 8/31/14

Information Security will collaborate with UTPD to enhance the badge processes and determine methods to automated provisioning and deprovisioning and recertification of badge access where technically feasible. Information Security will partner with UTPD to implement a process for the periodic review and removal of badge access related to employee transfers and terminations.

Management's Action Plan 3.2:
Responsible EVP: Leon Leach
Owner: Raymond Gerwitz
Contributor:
Due Date: 8/31/14

UTPD will partner with Information Security to implement a process for the audit (automated where technically feasible) of required removal of restricted badge access permissions related to employee transfers and terminations. This review will measure compliance with UTMDACC Institutional Policy #ADM0282 Identification Badge Policy Section 3.4 and allow the immediate remediation of any identified exceptions.

Observation 4:

Maturity of the Business Continuity Planning Process

Texas Administrative Code 202.74 - Business Continuity Planning (BCP) addresses the institution's plan of action in a state of emergency to maintain or quickly resume mission-critical functions. While management has a plan in place, Internal Audit noted the timeline of Business Continuity's validation process will not be complete until the summer of 2015. Internal Audit noted the validation process should be further along and should complete sooner than currently planned due to the criticality of the areas identified.

Recommendation:
The institution should consider providing additional resources to the Environmental Health and Safety department in order to shorten the timeline for completing the Business Continuity Plan validations for the 23 critical areas.

Management's Action Plan:

Responsible EVP: Leon Lech
Owner: Matthew Berkheiser
Contributor: Devina Patel
Due Date: 8/31/14

In May 2012 the Business Continuity responsibilities were moved to the Environmental Health & Safety (EH&S) department. In addition, an Executive Business Impact Analysis (BIA) was completed in May 2012. EH&S is currently editing the Business Continuity Policy to reflect the findings of the BIA which focused on 25 key areas/departments. The policy will reflect which departments need only an emergency plan and which departments need to maintain additional Business Continuity plans. Meetings have been held with the following several to review their plans based on the BIA and meetings are scheduled for the remaining critical departments through April 2014.

EH&S department is working with the vendor from Virtual Corporation to merge the templates for Departmental Emergency and Business Continuity Plans. Expected completion date of this project is September 30th, 2013. Once the merge is completed, there will be one Emergency and Business Continuity Plan template for departments wanting to complete their plans. Areas / departments listed as critical according to the BIA will be required to complete this plan. EH&S will assign 3 Safety Specialists that will work closely with these areas to complete their plans. Expected completion of all plans is August 2014.

Observation 5:

Security Incident Reporting of Texas Department of Information Resources

Texas Administrative Code 202.76 – Security Incidents states "institution of higher education shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident".
Information Security prepares a monthly summary of security incidents for submission to the Texas Department of Information Resources (DIR). Although the 2012 reports were submitted, the hyperlink to the 2013 DIR reports did not yield any reports when selected. Per inquiry with the process owner, the DIR does not provide notification when the monthly incident report is received. While it appears the reports were prepared, we could find no evidence to confirm the incident reports for 2013 were uploaded to DIR.

Recommendation:

Information Security should enhance the reporting communication process to inform Information Security Management when the incident report has been uploaded to the Texas Department of Information Resources (DIR). In addition, Information Security should consult with the vendor that supports DIR to determine if a communication workflow can be created to provide a notification when a report has been uploaded.

Management's Action Plan:
Responsible EVP: Leon Leach
Owner: Less Stoltenberg
Contributor:
Due Date: 11/30/13

Information Security will alter the current communication process to notify both Institutional Compliance and the Executive Director and Chief Information Security Officer of the monthly report. Additionally, Information Security will request the Department of Information Resources (DIR) provide notifications of submitted reports.

Observation 6:

Information Security Acknowledgement form approval

Texas Administrative Code 202.77 (a) – User Security Practices states "all authorized users (including, but not limited to, institution of higher education personnel, temporary employees, and employees of independent contractors) of the institution of higher education's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the institution of higher education or they shall not be granted access to information resources. The institution of higher education head or his or her designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to institution of higher education information resources."
The institution has a process in place where each user is required to acknowledge their agreement with the "Information Security User Acknowledge" form. Upon acknowledgment, the signed form is scanned and stored in the user's profile. Acknowledgment forms for institutional employees are managed through Human Resources; however, employees at the institution's satellite locations and educational centers are managed by different groups such as Trainee & Alumni Affairs, Faculty & Academic Affairs, and Health Professions.
Our review revealed that 1 of 45 employees selected for testing did not sign or agree to the acknowledgement form prior to or on their hire date. The employee was a summer program student employee of a satellite locations managed through Faculty & Academic Affairs and Health Professions.

Recommendation 6.1:
Human Resources should implement procedures to ensure that all required documents are obtained before a user is granted access to information resources.

Management's Action Plan 6.1:
Responsible EVP: Dr. Dmitrovsky
Owner: Dr. Shirley Richmond
Contributor: Chineme Amadi
Due Date: 8/31/13

Manual processes were previously in place in 2012 to obtain and file signed acknowledgement forms during the on-boarding process, which were vulnerable to human error. In April 2013, the School of Health Professions began using the Discovery System, which automated the online

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.

form completion process prior to student acceptance into the program. Since implementation of the Discovery System, acknowledgment forms have been obtained prior to acceptance and start date. The forms are stored online and easily accessible.

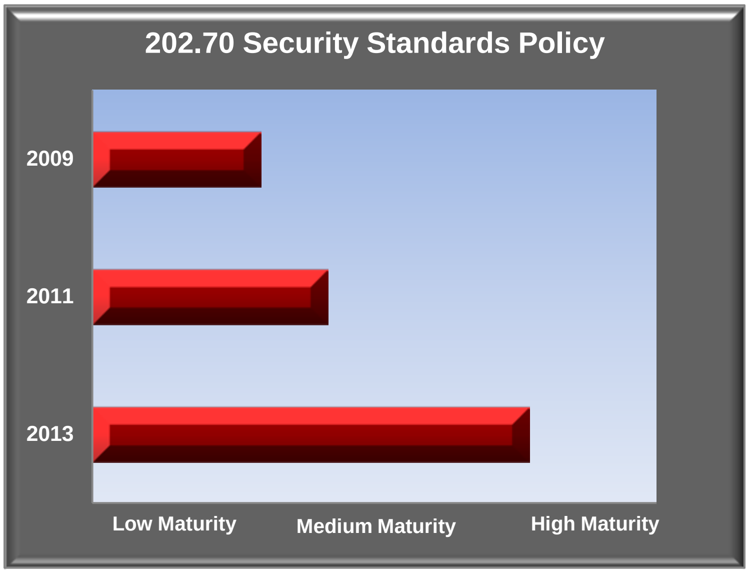
Recommendation 6.2:
Human Resources should implement procedures to ensure that all required documents are obtained before a user is granted access to information resources.

Management's Action Plan 6.2:
Responsible EVP: Dr. Dmitrovsky
Owner: Sherri De Jesus
Contributor: Sunita Hamilton
Due Date: 8/31/13

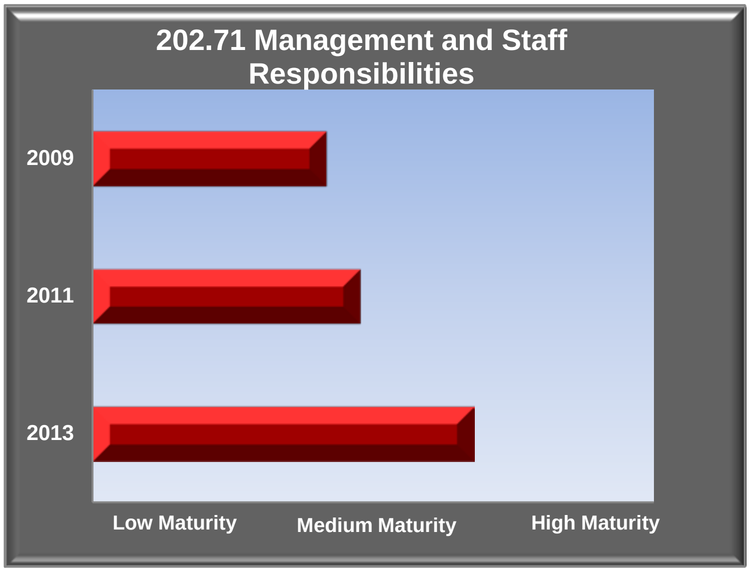
Manual processes were previously in place in 2012 to obtain and file signed acknowledgement forms during the on-boarding process, which were vulnerable to human error. In April 2013, the School of Health Professions began using the Discovery System, which automated the online form completion process prior to student acceptance into the program. Since implementation of the Discovery System, acknowledgment forms have been obtained prior to acceptance and start date. The forms are stored online and easily accessible.

Appendix A

202.70 - Security Standards Policy: From 2009 – 2011, Internal Audit noted exceptions regarding the institution not having a process in place to assess the risk of applications that are utilized by the institution. As a result, the institution implemented an online Governance Risk & Compliance (GRC) tool to evaluate the risk of applications utilized by the institution. Although the institution evaluated key applications, the risk assessment was noted as deep for specific applications rather than broad including all applications and institutional risks. In 2013, Internal Audit noted the institution is implementing a new GRC solution which will provide a broader view of all applications and enterprise wide institutional risk. Although as noted in 202.72, the institution has not completed a full enterprise wide risk assessment at this point, Internal Audit noted the institution's maturity level to this process has increased from 2009 – 2013.

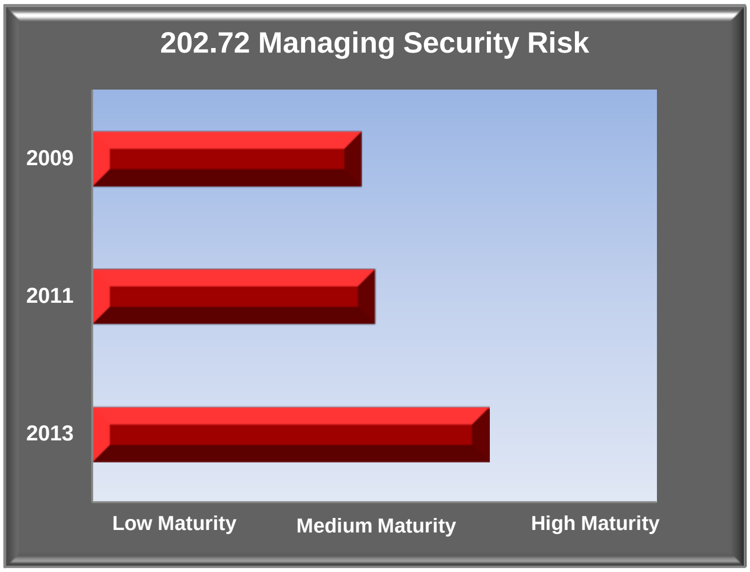


202.71 – Management and Staff Responsibilities: From 2009 – 2011, Internal Audit noted exceptions regarding the documentation of assets, the lack of documentation related to the roles and responsibilities of the Information Security Officer, and the reporting responsibility of the Information Security Officer. The institution has since implemented policies and procedures which enable the tracking and valuation of assets and has clarified roles and responsibilities within the Operations Manual. During the 2013 assessment, Internal Audit noted the institution has documented the roles and responsibilities of users of information resources which include but are not limited to end users, data owners, application owners, CISO, etc. As mentioned above in 202.70 Management and Staff Responsibilities, the CISO is responsible for reporting on the state of the Information Security Department to the president of the institution. As such, Internal Audit noted the process operated effectively during the 2013 TAC 202 assessment. The institution has also implemented a recertification process for user access to sensitive applications as well as a detailed review process for users with Active Directory (AD) and Identity Vault (IV) accounts. Although an observation was noted related to the review of AD and IV, Internal Audit noted the institution's maturity level increased from 2009 – 2013 due to the identification and ownership of assets, documentation of roles and responsibilities, enhancements to the recertification process, and the development of new monitoring and access review controls.

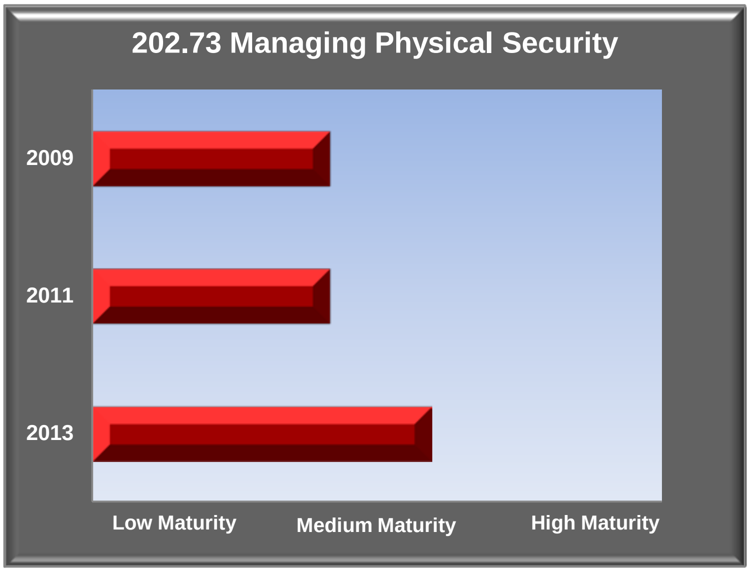


Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.

202.72 - Managing Security Risk:
From 2009 – 2011, Internal Audit noted observations during the 2009 and 2011 evaluations of the institution's compliance with reporting the current state of Information Security to Executive Management of the Institution. In 2009, the CISO did not report the status and effectiveness of information resources security controls. In 2011, the information was reported but was communicated to the President in an untimely manner in the President's Report. The 2013 assessment noted the process has matured, as the President's Report addresses the state of Information Security within the institution and the report was finalized and communicated to the appropriate parties in a timely manner. Management implemented a timeline for reporting the state of Information Security as a result of the 2011 assessment. An observation was noted related to the completion of an enterprise wide IT security assessment. The new GRC process and tools cited in 202.70 will enable the needed assessment. Internal Audit noted the institution's maturity level to this process increased from 2009 – 2013.

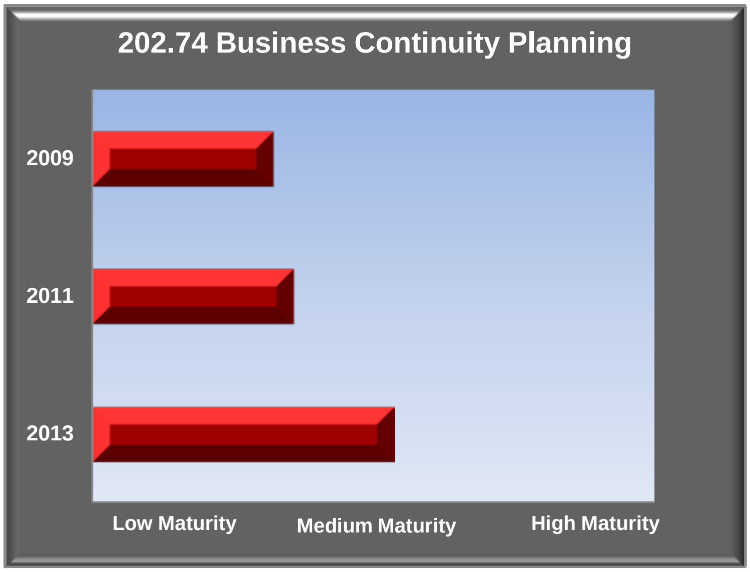


202.73 - Managing Physical Security:
From 2009 – 2011, Internal Audit performed limited procedures around physical security as a result of procedures performed by the external auditors and 2009 Internal Audits of Campus Security and Physical Access to Facilities. During the 2013 assessment, Internal Audit performed additional procedures to gain an understanding of the physical security process and assessed the appropriateness of users with access to critical areas within in the institution. Through the validation of prior internal audit findings and the procedures performed, Internal Audit noted the level of maturity process of physical access had increased from 2009 - 2013. Although some areas for improvement were noted, the overall maturity levels of procedures in place were improved.

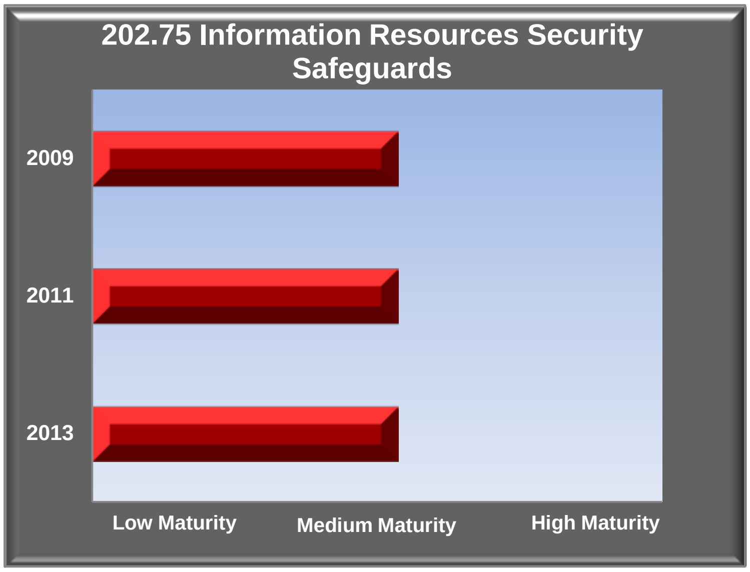


Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.

202.74 - Business Continuity Planning: From 2009 – 2011, Internal Audit performed limited procedures due to an Internal Audit of Business Continuity Planning in 2008 and the results of subsequent validations of identified observations as well as an independent review of BCP performed by the external auditors in 2012. During the 2013 assessment, Internal Audit noted that funding was provided to address outstanding observations related to an Enterprise Business Impact Analysis provided by Virtual Corporation in 2012. Additionally, the BCP group was reorganized under Environmental Health & Safety to provide a more robust and effective organization. Through the procedures performed, Internal Audit noted the institution moved along the maturity continuum by completing an assessment and developing a roadmap; however, due to the expected timeline for completing the BCP program, the current state of maturity is not as far along as expected.

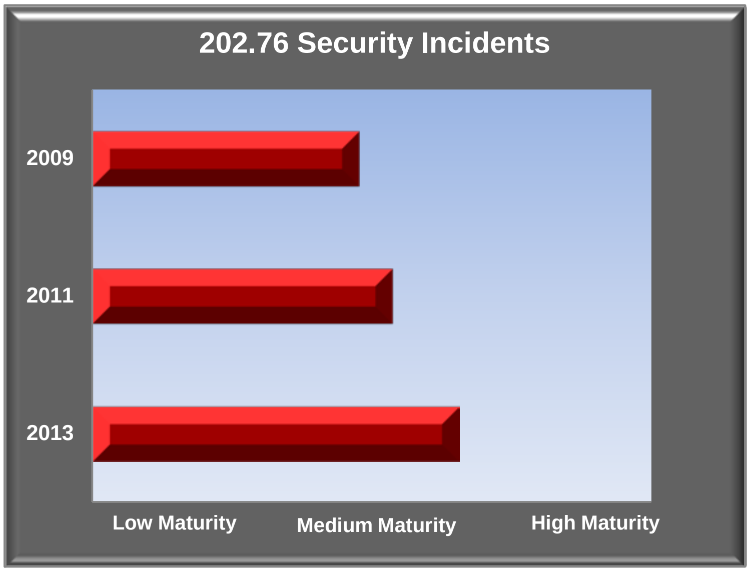


202.75- Information Resources Security Safeguards: From 2009 – 2011, Internal Audit noted the institution has documented policies and procedures to address section 202.75. However, exceptions have been noted during the operating effectiveness of planned applications assessments in the areas that are directly related to TAC 202.75 (i.e. terminated user access, modified user access, user access review, etc.). Internal Audit assessed the operating effectiveness of such procedures during the 2012 and 2013 application assessments of Cirius Prebill, MedAptus, Eclipse and Clinic Station. The institution has a documented process in place to address section 202.75; however, Internal Audit had noted observations during the noted application assessments. Internal Audit noted the operating effectiveness of this area remains the same.

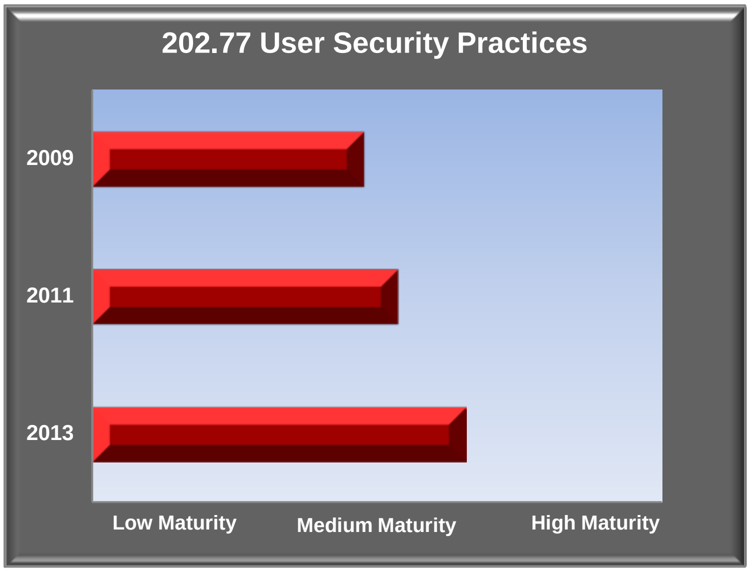


Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.

202.76 - Security Incidents: From 2009 – 2011, Internal Audit noted exceptions as a result of poor communication of security incidents between departments. In 2009, incidents were not reported regularly to the Texas Department of Information Resources (DIR). In 2011, all incidents were not communicated within the institution and to Texas Department of Information Resources (DIR) timely. As a result of the 2011 assessment, a security incident meeting and other forms of shared communication were established to ensure timely communication within the institution to enable timely reporting to the state. During the 2013 assessment, Internal Audit noted an increase in the maturity of this process as Information Security now posts security incidents on a secured SharePoint site for department review prior to submitting to DIR. Internal Audit observed evidence of timely internal review and noted timely submission of reports to DIR for 2012. Internal Audit noted timely internal review, but was unable to confirm the timely submittal to DIR for 2013. Although we noted observations regarding the submittal to DIR, Internal Audit noted that processes were in place to ensure appropriate parties (UTPD, Information Security, and Institutional Compliance) were apprised of security incidents timely.

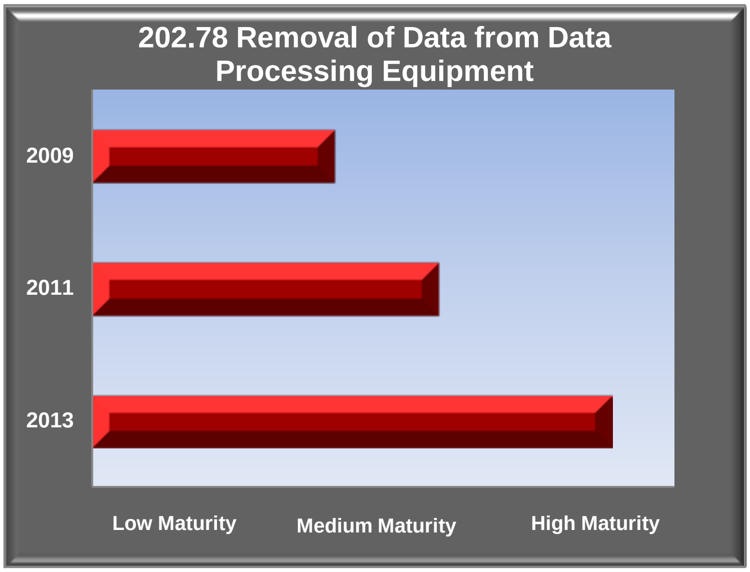


202.77 - User Security Practices: From 2009 – 2011, Internal Audit noted observations related to end user's approval of the "Information Security User Acknowledgement" form and user compliance of the EEE training. Internal Audit also noted through other assessments that end user security awareness initiatives were lacking. During the 2013 assessment, Internal Audit noted several areas of improvement, including improved end user information security communications distributed by Institutional Compliance and Information Security and improved user's compliance with the EEE training process. The Employee Development department is responsible for the communication and distribution of mandatory trainings throughout the institution through the online communication tool "Employee Notes". The Employee Development department has also implemented a non-compliant escalation process to monitor and track all users that are not compliant with the EEE or other mandatory trainings. Internal Audit noted observations related to the "Information Security User Acknowledgement" form approval the for satellite locations. However, Internal Audit noted the collection of the "Information Security User Acknowledgment" forms and provisioning of access to information resources through centralized Human Resources has improved through a mature process that operated effectively during the 2013 assessment. Internal Audit noted increased maturity progression of this section.



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.

202.78 - Removal of Data from Data Processing Equipment: From 2009 – 2011, Internal Audit noted exceptions related to the tracking of degaussed hard drives and servers during the decommissioning process. As a result of the 2011 assessment, DCOTS implemented new processes and systems to follow devices from removal through degaussing. During the 2013 assessment, Internal Audit noted the institution implemented more robust tracking and inventorying of devices through the utilization of the following applications: Computer Equipment Management System CEMS, Resource One (PeopleSoft), and Master Track. Internal Audit also noted the institution has a tracking process in place with a third party vendor to identify which assets have been destroyed once they are received by the vendor. Internal Audit noted the institution's maturity level for this area increased from 2009 – 2013.



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.