The University of Texas System Administration
Compliance with Texas Administrative Code, Chapter 202
Security Control Standards: Program Management
FY 2017

November 2017

THE UNIVERSITY OF TEXAS SYSTEM AUDIT OFFICE
210 WEST SEVENTH STREET
AUSTIN, TX 78701
(512) 499-4390

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Audit Office
210 West 7th Street
Austin, Texas 78701
512-499-4390 | Fax: 512-499-4426
WWW.UTSYSTEM.EDU

November 3, 2017

Phil Dendy
Chief Compliance and Risk Officer
The University of Texas System
210 W 7th Street
Austin, Texas 78701

Dear Mr. Dendy:

We have completed our audit of TAC 202: Program Management at System Administration. The detailed report is attached for your review. We conducted our engagement in accordance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal*.

We will follow-up on recommendations made in this report to determine their implementation status. If recommendations are found not to be implemented by the implementation dates reported, clients will be required to request approval from the System Administration Internal Audit Committee (IAC) to extend implementation dates with an explanation of the delay. The first extension request must be made in writing, and subsequent requests are required to be made in person at an IAC meeting. Requests for extension, either in writing or in person, must be made by the appropriate party at the Director level or above. This process will help to enhance accountability and ensure that audit recommendations are implemented in a timely manner.

We appreciate the assistance provided by information security management and staff at system administration. We hope the recommendations presented in our report are helpful.

Sincerely,

J. Michael Peppers, CPA, CIA, QIAL, CRMA

cc: Ms. Helen Mohrmann, Chief Information Security Officer
Ms. Lori McElroy, Information Security Officer, UT System Administration, Common Use Infrastructure

The University of Texas System Audit Office
UT System Administration TAC 202 Audit: Program Management
Fiscal Year 2017

Audit Report

November 2017

EXECUTIVE SUMMARY

Texas Administrative Code 202 (TAC 202), originally enacted in 2002, outlines mandatory information security controls to be implemented by all State agencies and institutions of higher education. Rule §202.76 further requires that a review for compliance with specified control standards "be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program." This audit is intended to meet that requirement for University of Texas (UT) System Administration.

A Priority Finding is defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*" Non-Priority findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated. This audit resulted in four high level and one medium level finding, but no priority findings.

CONCLUSION

Based on our audit, The UT System Administration information security program generally complies with program management information security standards required by TAC Title 1, Part 10, Chapter 202, with minor exceptions in the areas of Risk Management Strategy; Information System Inventory; Plan of Action and Milestones; and Testing, Training, and Monitoring.

Chief Audit Executive
J. Michael Peppers, CPA, CIA, QIAL, CRMA

Engagement Manager
Wesley T. Maxwell, CISSP, CISA, GSNA, GCED

BACKGROUND

Texas Administrative Code 202 (TAC 202), originally enacted in 2002, outlines mandatory information security controls to be implemented by all State agencies and institutions of higher education. Rule §202.76 further requires that a review for compliance with specified control standards "be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program." This audit is intended to meet that requirement for UT System Administration.

The Texas Department of Information Resources (DIR) made significant revisions to TAC 202 in March 2015 to align control requirements with federal information security standards. This resulted in development of a *Security Control Standards Catalog* (Catalog)[1] that defines minimum security requirements and implementation guidance for 26 control groups such as access control, training, contingency planning, risk assessment, and system acquisition. Although a biennial compliance review has always been a requirement of TAC 202, it now pertains specifically to a review for compliance with the minimum security standards documented in the Catalog.

AUDIT OBJECTIVE

The objective of this audit was to determine compliance with relevant control standards promulgated by DIR in the Catalog, as required by TAC 202 rule §202.76(c).

SCOPE & METHODOLOGY

The scope of the audit included current information security controls in place at UT System Administration. A risk assessment was conducted based on Catalog control groups to identify those areas of highest risk. Based on this work, the Program Management group was selected for the Fiscal Year (FY) 2017 audit. Required security control standards as of March 2017 are listed in Appendix A.

Procedures to determine compliance with relevant information security control standards included the following:

- Interview of responsible Office of Information Security employees;
- Review of available policy and procedure documentation; and
- Limited testing where appropriate.

The audit was conducted in accordance with guidelines set forth in *The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing*.

ENGAGEMENT RESULTS

The TAC 202 program management section relates to information security requirements that are independent of any specific information system, technology, or methodology. These controls can be considered the foundational basis for effective management of an information security program. Additionally, an organization's ability to implement appropriate controls depends on the strength and maturity of its security program management.

We reviewed 16 internal controls associated with UT System Administration's Information Security Office's (ISO) security program management. The controls in place for 12 of the 16 areas comply with the minimum standards found within DIR's Security Catalog. To further strengthen the information security program, we made five recommendations for the following control areas:

[1] http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf

- Risk Management Strategy
- Information System Inventory
- Plan of Action and Milestones Process
- Testing, Training, and Monitoring

Risk Management Strategy

DIR Security Control Standard PM-9 requires that organizations develop a comprehensive strategy to manage risk to operations and assets, individuals, or other organizations associated use of information systems. Currently, risk management activities performed by the Information Security Office (ISO) are predominately related only to IT disaster recovery. Without a comprehensive plan that effectively manages information security risks, it may lead to the ISO's inability to prevent or respond timely to unanticipated, emerging, or zero-day incidents that may impact confidentiality, integrity, and availability of critical information assets.

The observation described above is considered a **high-level** finding due to the possibility of a data breach occurring to a mission critical system if a strategy does not clearly identify and manage information security at risk. The finding level is in accordance with UT System's Internal Audit finding classification system.

> ***Recommendation 1:*** The ISO should implement and maintain a risk management strategy across the organization to manage security risk to UT System Administration information technology (IT) operations and assets.
>
> ***Management Response:*** The ISO has recently become aware of an effort to develop a strategic enterprise-level risk management program. This program may also include a security risk management strategy that satisfies this finding. The Audit, Compliance, and Risk Management Committee of the Board of Regents is meeting on November 8th and November 9th, 2017 to discuss enterprise risk management. The ISO will publish an update with a plan to develop this strategy by February 28th, 2018.
>
> ***Implementation Date:*** February 28th, 2018

Information System Inventory

DIR Security Control Standard PM-5 requires organizations to develop and maintain an inventory of their information systems. In addition, Section 3.2.2 of the University of Texas Systemwide Policy 165 (UTS165) requires IT inventories to include mission critical applications and systems containing confidential data. Although an inventory of information systems exists, it does not address specialized devices such as teleconference equipment or printers, software applications and programming interfaces, and does not includes the classification of data processed or stored. When IT inventory does not identify critical systems that store or process confidential data, it may be difficult for management to determine the level of internal controls needed for those systems to mitigate risks to university individuals, operations, or assets.

The observation described above is considered a **high-level** finding due to the risk of data breach or system failure if the system is not identified or classified at a level appropriate to the criticality of the system or type of data within the system so that it may be protected appropriately. The finding level is in accordance with UT System's Internal Audit finding classification system.

> ***Recommendation 2:*** The ISO should update and maintain an IT inventory to include the classification of data stored or processed on all UT System Administration hardware and software assets.

Management Response:

1) The Information Security Office will use available tools to perform scans and improve our existing inventory of UT System Administration-owned or managed computing devices deployed throughout the institution.
2) The inventory will designate mission critical applications, systems that contain Confidential data, and the Information Resource Owner.
3) The inventory will be classified through a collaborative effort between the Information Security Office, the Information Security Administrator for the department, and the data owner.
4) The inventory will be updated at least annually or after a significant change has occurred that may lead to reclassification of the information system resource(s).

Implementation Date: July 31st, 2018

Plan of Action and Milestones Process

DIR Security Control Standard PM-4 requires the ISO to implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed, maintained, and reported. The ISO has processes in place to track and monitor remediation activities relating to security activities and incidents; however, milestones associated with the plans of action and remediation actions do not exist. Without milestones, it may be difficult to prioritize risk response actions and ensure consistency with the security goals and objectives of the organization.

The observation described above is considered a **high-level** finding due to the risk that remediation activities, if not carefully planned and tracked, are not completed timely or do not effectively address information security exposures. The finding level is in accordance with UT System's Internal Audit finding classification system.

Recommendation 3: The ISO should create a process for ensuring milestones exist for plans of action and security remediation activities.

Management Response:

1) The Information Security Office will use industry-accepted methodologies and processes to establish and track milestones for security remediation activities. These milestones are intended to correct deficiencies noted during ongoing assessments of the security controls in order to reduce risk to an acceptable level and align with current policy and standards.
2) Plan of Action and Milestones (POA&M) will include: 1) high level objectives that are inclusive of remediation tasks; 2) scheduled dates for reaching these milestones; 3) criticality rating; and 4) responsible parties.
3) The Information Security Office will approach this in two phases:
    a. Phase 1: We will have two projects with POA&M included and publish them by May 15th 2018.
    b. Phase II: We will have the POA&M process included in all Information Security projects published after December 31st, 2018.
4) The ISO will report the status of POA&M in the FY19 annual security report.

Implementation Dates: Phase 1: May 15th, 2018; Phase 2: December 31st, 2018

Testing, Training, and Monitoring

UT System Staff Information Security Awareness Training
DIR Security Control Standard PM-14 requires a process for conducting security training related to information systems. In addition, section 18.1.2 of UTS165 requires recurring training at least biennially for employees and workers with access to institutional information resources. The ISO follows UT System policy in requiring compliance training to address security information and data protection biennially.

According to Verizon's 2017[2] breach report, 30% of all information security breaches in the education space were attributed to internal sources mostly caused by human error as opposed to malicious intent.

New and innovative attacks are being directed at end-users to gain access to confidential data. At the same time, many of the information security safeguards used to protect critical systems and data rely on end-users to successfully recognize and prevent these attacks. With a two-year gap between required end-user security training, there is an increased risk of attackers leveraging deficient end-user security practices allowing for the unauthorized disclosure, modification, or loss to confidential data.

The observation described above is considered a **high-level** finding due to the risk that a data breach will occur because of the lack of timely and effective end-user training. The finding level is in accordance with UT System's Internal Audit finding classification system.

> ***Recommendation 4:*** The ISO should provide additional training more frequently than the two-year requirement to ensure end users are aware of and able to assist in guarding against high risk, pervasive cybersecurity threats.
>
> ***Management Response:***
> 1) The ISO will design a general security awareness program for all System Administration users which will include at least annual security awareness training that will be implemented through a variety of avenues.
> 2) The ISO will collaborate with other technology and privacy teams to review the general security awareness program annually and update as necessary based on industry-recognized emerging security threats.
>
> ***Implementation Date:*** April 30th, 2018

ISO Staff Certification
DIR Security Control Standard PM-13 requires the establishment of an information security workforce development and improvement program. In addition, the updated section 2054.545(a) of the Texas Government Code, Section 12 of Texas House Bill 8, was enacted by the 85th Legislature and became effective on September 1, 2017. It states that the organization shall create an analysis of the percentage of personnel in cybersecurity who currently hold appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity (NICE) Education; and a strategy for mitigating any workforce-related discrepancy in cybersecurity or other cyber-related positions with the appropriate training and certifications. Currently, four of six ISO staff hold industry security certifications recognized by NICE. Without relevant cyber security training and related certifications, security threats may not be remediated timely or adequately, leading to unauthorized access to resources or disclosure of confidential data.

[2] Verizon Breach Report - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

The observation described above is considered a **medium-level** finding due to the possibility of a data breach occurring because information security staff may not be sufficiently knowledgeable in mitigation strategies for rapidly changing cybersecurity threats. The finding level is in accordance with UT System's Internal Audit finding classification system.

Recommendation 5: The ISO should perform a training analysis and create a strategic plan for cyber-security related positions.

Management Response:

1) The Information Security Officer has already begun to organize an initiative to conduct a needs-assessment and training analysis for ISO staff based off the roles and knowledge, skills, and abilities as defined in the NICE Cybersecurity Workforce Framework. A parallel initiative to develop a needs assessment for Information Security Administrators (ISAs) has also begun and expected to be complete by the implementation date.
2) The Information Security Officer and each ISO staff member will develop a customized training and/or certification plan.
3) The ISO will publish staff cybersecurity-related certifications on a UT System Administration internal security website.

Implementation Date: March 15th, 2018

Appendix A
Security Control Standards: Program Management

The Department of Information Resources (DIR) *Security Control Standards Catalog* includes 16 program management controls. All are required.

Control	Risk Statement
PM-1 Information Security Program Plan Information resources security program consistent with these standards, and the state organization's head is responsible for the protection of information resources	Lack of a comprehensive security program may result in the compromise of sensitive information due to loss of integrity or confidentiality.
PM-2 Senior Information Security Officer A senior information security officer is appointed, with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Responsibility for the security program has not been defined.
PM-3 Information Security Resources The Information Security Office has long-term and short-term budgeting and capital planning initiatives in place.	Management does not provide guidance for security within the organization through clear direction, demonstrated financial commitment, explicit assignment, and acknowledgement of information security responsibilities.
PM-4 Plan of Action and Milestones Process The Information Security Office develops and updates, a plan of action and milestone process for the information system that documents the organization's planned, implemented, and evaluated remedial actions.	Performance monitoring, assessment and reporting are not performed appropriately whereby remedial actions are not identified or initiated.
PM-5 Information System Inventory An inventory of information systems is maintained.	Important information assets requiring protection have not been clearly identified and inventoried.
PM-6 Information Security Measures of Performance The Information Security Office maintains periodic reporting and performance measurement mechanisms in place.	Management has not aligned the technology architecture with corporate strategy or external threats.
PM-7 Enterprise Architecture Enterprise technology architecture is developed with consideration for information security and the resulting risk to operations and information assets.	Management does not review new technology infrastructure or modifications to existing technology infrastructure to ensure that implementations are in line with strategic goals.
PM-8 Critical Infrastructure Plan Information security issues are addressed in the development, documentation, and updating of a critical infrastructure and resource protection plan.	Management does not have a documented critical infrastructure plan.

Control	Risk Statement
PM-9 Risk Management Strategy The Information Security Office develops a comprehensive strategy to manage risk to organizational operations and assets, individuals.	Basic risk management activities have not been incorporated into IT-related activities (e.g., setting risk appetite, identification of risks, risk assessment, reporting criteria, etc.) and may lead to unanticipated losses or the inability to respond appropriately to risks.
PM-10 Security Authorization Process The Information Security Office has defined designated information security roles and responsibilities relating to the authorization process.	The lack of security authorization process for information systems may result in new information systems causing security and compatibility issues.
PM-11 Mission/Business Process Definition The Information Security Office has written security mission that is accepted by executive management	The IT strategy is not aligned with the business strategy or fully understood by the board and executives, limiting the achievement of value objectives for the organization.
PM-12 Insider Threat Program An active insider threat program is established.	Lack of consistent process to manage insider threats may result in an inability to respond to (detect and prevent) malicious insider activity.
PM-13 Information Security Workforce Information security training opportunities are available to personnel on a continuous basis.	Lack of establishing focused security workforce development and improvement programs, may result in unclear expectations on safeguarding organizational operations and assets.
PM-14 Testing, Training, and Monitoring Information security training program specific to organizational systems is established.	Inadequate mechanisms to test, monitor and remediate information security capabilities may result in suspicious or anomalous activities going undetected.
PM-15 Contacts with Security Groups and Associations Employee personnel are members of external information security organizations.	Inadequate contacts and communication protocols with relevant authorities and special interest groups may result in the lack of knowledge of latest security threats and industry trends, information security incidents going unreported or unsupported by legal authorities.
PM-16 Threat Awareness Program A threat awareness program is in place.	Failure to conduct a suitable and relevant threat awareness program and failure to publish notifications to enhance awareness of organizational policies and procedures may result in a security breach of the operational environment.