Agenda Item: 7.7
Prepared by: Mark Majek, Kathy Thomas, Deborah Bell and Jaye Stepp
Meeting Date: April 2016

Summary of Request:

The Board approved an internal audit plan for 2016 which included an audit of agency information technology security standards.

Historical Perspective:

The security standards for information technology was selected on the annual risk assessment update for fiscal year 2016. This audit was conducted in compliance with Texas Administrative Code 202 which establishes a baseline of security standards for Texas state agencies and institutions of higher education.

Pros: The Board of Nursing will be in compliance with the Texas Internal Audit Act, the internal audit plan approved by the Board for fiscal year 2016 and will provide the Texas Board of Nursing affirmation of meeting baseline information technology security standards for the State of Texas.

Cons: None.

Staff Recommendation:

Board Action: Move to accept Internal Audit Report #2016-1, Texas Administrative Code 202 Information Systems Security Audit as prepared by E. Jaye Stepp, CPA for fiscal year 2016.

Texas Board of Nursing

Internal Audit Report #2016-1

TAC-202 Information Systems Security Audit

Prepared by:
E. Jaye Stepp, CPA, CIA, CGAP, CRMA
Austin, Texas

Table of Contents

Acronyms and Abbreviations

ASP	Agency Security Plan
CPA	Comptroller of Public Accounts, Texas
DIR	Department of Information Resources, Texas
DRP	Disaster Recovery Plan
ED	Executive Director
FISMA	Federal Information Security Management Act
GRC	Governance, Risk, and Compliance
IA	Internal Audit
IIA	Institute of Internal Auditors
IPPF	International Professional Practices Framework, IIA's
ISO	Information Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
SDLC	Systems Development Life Cycle
TAC	Texas Administrative Code
TGC	Texas Government Code

E. J. STEPP, CPA

305 CARGILL DRIVE, SPICEWOOD, TEXAS 78669-2450

Internal Audit Report

March 31, 2016

Texas Board of Nursing

The following report provides the results of the internal audit of the Board of Nursing's compliance with revised Texas Administrative Code 202 Information Security Standards.

We conducted this audit in accordance with *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Overall, based on the results of our review and testing, controls in place at BON provide reasonable assurance of compliance with the revised TAC-202 information security standards. Opportunities for improvement exist in the development of additional procedures, as detailed in the attached report.

Jaye Stepp

CPA, CIA, CGAP, CRMA

E. J. Stepp, CPA
Internal Auditor for BON
Austin, Texas

Executive Summary

Audit Purpose

Texas Administrative Code 202 establishes a baseline of security standards for Texas state agencies and institutions of higher education. Setting security standards at the federal level is the Federal Information Security Management Act (FISMA), which requires federal agencies and their contractors to safeguard their information systems and assets. The National Institute of Standards and Technology, known as NIST, helps develop standards and guidelines for FISMA. FISMA was updated in 2013 and the committee of state Information Security Officers (ISO) and others have revised TAC 202 to move it closer to FISMA and NIST. The revised TAC 202 covers agency responsibilities and includes a Control Standards Catalog developed by the Texas Department of Information Resources (DIR).

DIR plays a leadership role in affecting Texas IT policy. Texas Government Code Chapter 2054, the Information Resources Management Act, describes information technology—or resources—as strategic assets that must be properly managed because of their value.

The Control Standards Catalog was initiated by DIR to help state agencies implement security controls. It specifies the minimum information security requirements that state organizations must employ to provide an appropriate level of security relevant to levels of risk. DIR’s Control Crosswalk maps the revised TAC 202 in industry standards, regulatory requirements, and compliance mandates. It is meant to relate the controls specified in revised TAC 202 to other requirements that agencies may have for protecting information and information systems. DIR’s goal is that when the Control Crosswalk is integrated into the GRC portal, agencies will be able to input all steps taken and generate reports showing how state, federal, and industry-specific requirements have been met. The GRC portal provides incident management and analysis as well as risk assessment analysis to state agencies.

DIR also created a template for Agency Security Plans (ASP) that will provide a uniform understanding of agency security program maturity. Agencies are asked to provide the controls they have in place for each security objective. In the template agencies are also asked to detail how they measure effectiveness and efficiency of the security controls and to indicate challenges and their roadmap for the next 12 months.

Objectives of this audit are to ensure BON’s compliance with revised TAC 202. The Control Standards Catalog prioritized implementation to ensure that more fundamental controls are implemented first. Controls that existed in the previous version of TAC 202 were required first; other controls that were not previously required under TAC 202 were prioritized for implementation over the next two years.

Overall Conclusion

The BON has over thirty IS Security Policies currently in place or in process of implementation, providing general compliance with DIR's control standards and implementation schedule for the revised TAC 202. The BON has limited IT staff to work on the control standards compliance and ASP documentation in addition to their daily responsibilities at the agency. Agency efforts to document security policies and procedures and implement the revised TAC 202 requirements are commendable and efforts are ongoing. The DIR Control Standards Catalog and Agency Security Plan will guide the agency through the process.

There is one recommendation resulting from this audit, relating to the requirement for an annual report to the agency head on information security. Details are provided in the body of this report.

Acknowledgements

The BON staff was cooperative in providing requested audit information, documents, and responses to inquiries and surveys in a timely manner.   We appreciate the input and assistance provided in the audit process. IT staff additionally indicated that the Hobby building is in need of better bandwidth and multiple lines in and out of the facility to allow BON to have quicker response and failover times.

Objectives, Scope, and Methodology

Audit Objectives: The following audit objectives were developed and agreed-upon by the auditor and the client:

Audit Objective A –Compliance: Review the information provided by client as well as the identified rules, laws, regulations, and information from other sources to determine BON's responsibilities for maintaining IS Security per DIR's directives. Perform procedures to determine if Security policies and procedures align with identified criteria, including the DIR Security Control Standards Catalog developed for state agencies, and with deadlines for implementation from 2015 to 2017.

Audit Objective B – Controls, Operations: Evaluate the agency's controls over activities related to IS standards and safeguards identified under the previous objective.

Audit Objective C – Communications and Reporting: Review and evaluate the processes for communications to staff on matters related to changes in IS security standards through training or direct communications. Evaluate reporting processes for required reports to outside agencies, as applicable.

Scope:

The scope of the audit was limited to FY-2015 and FY-16 year-to-date reports and information security processes and controls currently in place.

Methodology:

Meetings were held with the Information Resource Manager and the Systems Analyst, who also serves as the agency's Information Security Officer (ISO). Meetings discussed the processes and controls around the BON information security procedures and plans. The DIR minimum standards were compared to the current state to assess the agency's compliance with DIR's control standards implementation schedule. We requested and reviewed documents including written policies, procedures, tracking and reporting documents.

Sources of Information & Criteria:

Texas Administrative Code 202, Revised 2013
DIR's Security Control Standards Catalog
DIR's Agency Security Plan Instructions and Template
DIR's Control Crosswalk
BON's Information Services Security Policies

Audit Results and Recommendations

The results and recommendations presented in this section represent the conclusions of the internal audit program which was developed based on audit objectives established and agreed upon with the BON management.

Audit Objective A – Compliance:

The agency is in compliance with TAC-202, as revised, in the staggered implementation of controls defined by the Department of Information Resources (DIR) in conjunction with the TAC revision. All procedures required to be in place for 2015 and 2016 are either in place, in process, not applicable, or another entity's responsibility (DIR, TFC).

Areas that need strengthening include:

§202.20 Responsibilities of the Agency Head – the senior agency officials are to support the agency ISO in developing at least annually, a report on agency information security program, as specified in

- §202.21(b)(11) on reporting to the state agency head the status and effectiveness of security controls; and
- §202.23(a) Agency Reporting, that each ISO shall report, at least annually, to the agency head on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirement of this chapter and:
    - (1) effectiveness of current information security program and status of key initiatives;
    - (2) residual risks identified by the agency risk management process; and
    - (3) agency information security requirements and requests.

As a small agency, the BON has open communications and does not present an annual report. The reports that currently are provided to agency management are statistical reports with data provided for calculating performance measures. We recommend that the BON develop a separate annual report that includes the information defined above for informational purposes and to ensure compliance.

§202.21 Responsibilities of the Information Security Officer – all responsibilities of the ISO are being met, except for the annual report to management on the status of security controls, as discussed above. A formal, annual report to the agency head and management would strengthen compliance and provide historical data for future analysis.

§202.23 Security Reporting again refers to the agency ISO reporting, at least annually, to the agency head on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirement of this chapter.

§202.24 Agency Information Security Program related to the program developed, documented, and implemented on an agency-wide information security program that includes protections based on risks for all agency information and information resources. There is a provision (6) for “a process to justify, grant and document any exceptions to specific program requirements in accordance with requirements and processes defined in this chapter.”

§202.25 Managing Security Risks related to risk assessments of the agency’s information and information resources to be performed and documented. The BON addresses this section with their Disaster Recovery Plan (DRP) and practices related to the new system discussions on security prior to installation at the agency. For full compliance the BON should for document the frequency of future risk assessments as stated in §202.25(2).

Recommendation #2016-1-01

An annual report from the ISO to the agency head that addresses all of the criteria cited in TAC 202 above would provide added information to management while providing compliance with TAC 202 requirements.

Management Response #2016-1-01

The BON staff agree with this recommendation and will start preparing an official report from the ISO on the status of information security measures and procedures at the Board of Nursing.

Responsible party: Information Security Officer

Implementation date: 8/31/16

Audit Objective B – Controls, Operations:
Evaluate the agency’s controls over activities related to IS security and safeguards identified under the previous objective.

We used the criteria identified in the DIR Security Control Standards Catalog for testing the BON’s implementation of control steps. Tests were based on required implementation dates, so that we are only considering compliance for the requirements due to be implemented in 2015 and 2016. Additional requirements due in 2017 and others that have no required implementation date were considered for determining over all compliance status for the agency.

There were 282 separate control steps recommended in the DIR Control Standards Guide. Of those 41 (15%) were to be implemented in 2015; 64 (23%) scheduled for implementation in 2016 and 17 (8%) items scheduled for implementation in 2017. Additionally, there were 154 other recommendations that do not have an implementation date assigned to them.

Our audit tested compliance primarily for those steps slated for implementation in 2015 and 2016. All control steps scheduled for implementation in those time frames are in place at BON, as well as most of the control steps recommended for 2017. Some of the recommended control steps are not under the BON's control, specifically those in the area of Physical and Environmental Protection that relate to building security and physical access that are the responsibility of the Texas Facilities Commission (TFC). As such, these specific controls were considered as not applicable to the BON and were not considered for BON's compliance assessment.

The Information Services Security Policies that are in place are expanding as work is on-going to ensure compliance with regulators and law. A table with the summary of the DIR Controls by category is provided with the BON compliance rates, by percentage and by number of control processes, as an exhibit at the end of this report.

Recommendations: None for this section

Audit Objective C – Communications and Reporting

TAC 202 requirements for reporting to DIR:
§202.21(12) – Monthly reports on non-compliance, as applicable
§202.23(A)(3) – Monthly report on information systems requirements and requests
§202.23(b)(11) – Incident reports – monthly and/or urgent incident reporting

Monthly Incident reports to DIR are filed as required, without exception. There have been minimal incidents to report. Daily vulnerability scan reports are shared with DIR in addition to the constant updates from the BON's firewall. Urgent incident reports are filed immediately with DIR through Archer. Most incidents are low to medium at BON, and reported in the end-of-month incident report to DIR.

The Agency Security Plan (ASP) reporting will provide a uniform understanding of agency security program maturities to DIR. Agencies are asked to provide the controls they have in place for each security objective. Agencies are asked measure their maturity level, to detail how they measure effectiveness and efficiency of the security controls, and to indicate challenges and their roadmap for the next 12 months. The BON's ASP was completed in October of 2014. The BON should continue to review and update this plan to further identify and document the progress to optimized maturity levels.

Internal reporting on from the ISO includes quarterly reports provided to the Director of Operations, Executive Director, and agency management of quarterly statistics by various agency functions. This data is used for calculating performance measures. Management is responsible for reviewing the data for accuracy. The IRM has written a program to use the data for calculating the actual amounts reported.

The report to the agency head discussed under the first audit objective and audit recommendation is centered around reporting to the agency head and management on the state of information security measures and procedures at the agency. The recommendation 2016-1-01 also applies here.

Recommendations: None for this section

EXHIBIT I – Summary of Compliance with DIR Control Standards

#	CONTROL CATEGORIES	Due 2015	Due 2016	Due 2017	No date
1	Access Controls (25)	100% (6/6)	100% (3/3)	100% (3/3)	69% (9/13)
2	Authority and Purpose (2)	None	None	None	0% (0/2)
3	Accountability, Audit and Risk Management (8)	None	None	None	0% (0/8)
4	Awareness and Training (5)	100% (2/2)	100% (1/1)	0% (0/1)	0% (0/1)
5	Audit and Accountability (16)	100% (1/1)	100% (8/8)	100% (1/1)	33% (2/6)
6	Security Assessment and Authorization (9)	100% (1/1)	100% (2/2)	100% (4/4)	100% (2/2)
7	Configuration Management (11)	100% (3/3)	100% (4/4)	100% (1/1)	67% (2/3)
8	Contingency Planning (13)	100% (3/3)	100% (3/3)	100% (1/1)	100% (6/6)
9	Data Quality and Integrity (2)	None	None	None	100% (2/2)
10	Data Minimization and Retention (3)	None	None	None	0% (0/3)
11	Identification and Authentication (11)	100% (3/3)	100% (4/4)	None	75% (3/4)
12	Individual Participation and Redress (4)	None	None	None	100% (4/4)
13	Incident Response (10)	100% (2/2)	100% (3/3)	100% (2/2)	100% (3/3)
14	Maintenance (6)	None	100% (1/1)	100% (3/3)	100% (2/2)
15	Media Protection (8)	n/a	n/a	n/a	n/a
16	Physical and Environmental Protection (20)	100% (3/3)	100% (5/5)	100% (2/2)	90% (9/10)
17	Planning (9)	100% (1/1)	100% (1/1)	100% (1/1)	100% (6/6)
18	Program Management (16)	100% (3/3)	100% (5/5)	None	100% (8/8)
19	Personnel Security (8)	100% (1/1)	100% (4/4)	100% (3/3)	None
20	Risk Assessment (6)	100% (2/2)	100% (2/2)	None	50% (1/2)
21	System and Service Acquisition (22)	100% (3/3)	100% (3/3)	100% (1/1)	20% (3/15)
22	System and Communication Protection (44)	100% (3/3)	100% (7/7)	None	48% (16/33)
23	Security (2)	None	None	None	100% (2/2)
24	System and Information Integrity (17)	100% (2/2)	100% (3/3)	0% (0/1)	0% (0/11)
25	Transparency (3)	None	None	None	0% (0/3)
26	Use Limitation (2)	None	None	None	0% (0/2)

The BON has control policies, procedures, and processes in effect to comply with DIR Control Standards implementation requirements for years 2015, 2016, and most of 2017. Other control steps without required implementation dates are also substantially complete.

****

Report Distribution Page

Texas Board of Nursing

Kathy Shipp, MSN, RN, FNP, Board President
Deborah Bell, CLU, ChFC, Board Liaison for Internal Audit

Katherine Thomas, MN, RN, FAAN, Executive Director
Mr. Mark Majek, Director of Operations
Mr. Jeremy Bruker, Information Resources Manager
Mr. Bill Ray, Information Security Officer

Oversight Agencies

Governor's Office of Budget and Planning, and Policy
Ms. Kate McGrath

Legislative Budget Board
Mr. Ed Osner

Sunset Advisory Commission
Mr. Joey Longley

State Auditor's Office
Internal Audit Coordinator