An Audit Report on

Information Technology Services at the Health Professions Council

June 2018

Report No. 18-034

State Auditor's Office reports are available on the Internet at http://www.sao.texas.gov/.

An Audit Report on

Information Technology Services at the Health Professions Council

SAO Report No. 18-034
June 2018

Overall Conclusion

The Health Professions Council (Council) had a significant weakness in its data security controls that allowed at least one participating agency to view another agency's confidential data. The Council also had weaknesses in its user access and authentication processes.

The Council had change management processes in place and implemented some processes to ensure that it administers information technology support services (ITSS) in accordance with applicable requirements. However, the Council should strengthen its processes regarding the help desk support system and contract monitoring, and it should provide guidance to agencies regarding the identification and classification of sensitive information.

User Account Management and Authentication. While the Council implemented some policies and processes for account management, the Council had control weaknesses in user access management and authentication at the virtual, network, server, database, and application levels. For example, the Council did not have key controls to ensure that only current employees with a business need had access to resources.

Contract Monitoring. The statement of work for the Versa Regulation Database (Versa) and hosted services contract did not include methods to monitor vendor performance. Subsequently, the Council is not performing monitoring activities related to key deliverables in the contract,

Background

The State of Texas created the Health Professions Council (Council) in 1993 to achieve the benefits of consolidation and create efficiencies among the different health licensing and regulatory agencies. Texas Occupations Code, Chapter 101, mandated an initial membership of 14 agencies, with one member appointed from each participating agency. As of May 2018, 16 agencies representing more than 45 professional licensing boards or programs for certification, documentation, permitting, or registration were members of the Council. As of May 2018, the Council had seven full-time equivalents with appropriations of $1,083,230. The Council is funded entirely by transfers of funds from member agencies depending on the services provided. The Council provides a range of services, including administering a shared regulatory database (Versa Regulation), a shared document imaging application (Laserfiche), and information technology support services.

Versa Regulation Database. Micropact, a Council vendor, administers this shared regulatory database that allows participating agencies to manage their licensees and track any system or agency issues through its help desk ticketing capabilities. The vendor is responsible for making all code changes, implementing upgrades, and managing the related infrastructure through a hosted, cloud-based service.

Information Technology Support Services (ITSS). The Council provides ongoing technical support to participating agencies. It ensures that printers are operational and network connectivity is established. It also makes purchasing recommendations, provides application enhancements, administers Web sites, supports servers and computers, and performs information resource management duties when requested. Additionally, the Council is responsible for network authentication and managing user access.

See Appendix 3 for participating agencies utilizing Versa and ITSS services.

Source: The Council.

This audit was conducted in accordance with Texas Government Code, Section 321.0132.

For more information regarding this report, please contact Becky Beachy, Audit Manager, or Lisa Collier, First Assistant State Auditor, at (512) 936-9500.

such as tracking the resolution times for help desk tickets and the availability rate of hosted services.

ITSS. The Council administered ITSS in accordance with the memorandum of understanding. However, the Council did not provide guidance to participating agencies on identifying and classifying sensitive data or determining user access levels for related applications. In addition, the Spiceworks application used for help desk support did not contain reliable information. Auditors noted inaccurate information in several key fields.

Table 1 presents a summary of the findings in this report and the related issue ratings. (See Appendix 2 for more information about the issue rating classifications and descriptions.)

Table 1

Summary of Chapters/Subchapters and Related Issue Ratings		
Chapter/ Subchapter	Title	Issue Rating [a]
1-A	The Council Had a Significant Weakness in Data Security Controls That Allowed at Least One Participating Agency to Observe Another Agency's Confidential Information	High
1-B	While the Council Had Some Policies and Processes for Account Management and Authentication, It Should Strengthen Controls to Protect Data from Unauthorized Access	Medium
1-C	The Council Had Controls in Place to Ensure That Changes Made to Versa Were Appropriate	Low
2	The Council Performed Some Monitoring Related to the Contract; However, It Should Strengthen Its Processes to Include Reviewing Key Deliverables	Medium
3	The Council Provided Support Services in Accordance with Applicable Requirements; However, It Should Strengthen Its Process for Documenting and Monitoring Help Desk Tickets and Provide Guidance to Participating Agencies on User Access and Data Classification	Medium

[a] A subchapter is rated Priority if the issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern and reduce risks to the audited entity.

A subchapter is rated High if the issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern and reduce risks to the audited entity.

A subchapter is rated Medium if the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

A subchapter is rated Low if the audit identified strengths that support the audited entity's ability to administer the program(s)/functions(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Auditors communicated other, less significant issues separately in writing to Council management.

Summary of Management's Response

At the end of certain chapters in this report, auditors made recommendations to address the issues identified during this audit. The Council generally agreed with the recommendations in this report.

Audit Objective and Scope

The objective of this audit was to determine whether the Health Professions Council has processes and related controls to help ensure that it administers information technology services in accordance with applicable requirements and protects participating agency data.

The scope of this audit covered selected general controls over the Council's information technology systems and related processes; selected aspects of contract management for the Council's contract for database services with a vendor; selected ITSS functions; physical security over the Council's server room; help desk support tickets; and other supporting documentation from September 1, 2016, through January 31, 2018.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

The Council Had a Significant Weakness in Its Data Security Controls; However, It Had Some Processes to Help Protect Data and Manage Changes to the System

The Health Professions Council (Council) had a significant weakness in its data security controls allowing at least one participating agency to view another agency's confidential information (see Appendix 3 for more information about the participating agencies). In addition, while the Council had some policies and processes for account management and authentication, those controls were not always operating effectively. Auditors identified non-current employees with access to network resources and employees with access that was not appropriate for their job responsibilities.

With the exception of the weakness noted above, the Council had controls in place to ensure that changes made to the Versa Regulation Database (Versa), which participating agencies use to manage their licensees and register and track complaints, were appropriate. In addition, the Council had adequate physical controls and all 17 changes to Versa that auditors tested were properly authorized, approved, tested, and moved to the production environment.

Chapter 1-A

The Council Had a Significant Weakness in Data Security Controls That Allowed at Least One Participating Agency to Observe Another A**gency's** Confidential Information

Chapter 1-A Rating:

High [1]

The Council did not ensure that information in Versa was properly segregated for participating agencies. Auditors observed at least one agency that could access the confidential information of another participating agency. The Council worked on a plan with the vendor in fiscal year 2015 to upgrade Versa. The Council asserted that the upgrade included customization to the original code in Versa to segregate data for the different agencies. However, the vendor did not implement those data segregation controls properly.

[1] Chapter 1-A is rated as High because the issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern and reduce risks to the audited entity.

The Council asserted that it, along with participating agencies, performed user acceptance testing for some functionality related to the Versa upgrade prior to its implementation. However, the Council asserted that testing did not include the data segregation controls. The Department of Information Resources' *Security Controls Standards Catalog*[2] states that state agencies should analyze system changes to determine how the changes may affect security prior to implementation of those changes.

After auditors brought the data security weakness to its attention, the Council worked with the vendor to address it. On May 9, 2018, the vendor implemented a fix, which the Council reviewed. Auditors observed that the fix corrected the data segregation issue.

Recommendation

The Council should continue to test vendor software updates and customizations prior to implementation to ensure that data remains properly segregated.

Management's Response

The Council agrees with the recommendations. As the report indicates, a fix for this issue has already been implemented. However, the Council will also implement regular reviews by the agencies to ensure that future fixes do adhere to segregation requirements.

Issue Rating: High

Implementation date: Implemented effective immediately.

Responsible Party: Administrative Officer

[2] Title 1, Texas Administrative Code, Chapter 202, requires state agencies to comply with the security standards defined in the Department of Information Resources' *Security Control Standards Catalog*. This catalog provides state agencies specific guidance for implementing security controls and specifies the minimum requirements that agencies must meet to provide appropriate levels of information security.

Chapter 1-B

While the Council Had Some Policies and Processes for Account Management and Authentication, It Should Strengthen Controls to Protect Data from Unauthorized Access

Chapter 1-B Rating:

Medium [3]

The Council lacked controls to ensure that user access, user access review, and authentication were appropriate (see text box for information about the access and authentication areas reviewed). Also, the Council did not perform user access reviews for most system components; however, physical access controls were adequate to protect against unauthorized access. Auditors determined there were inconsistencies in authentication controls and inappropriate user access across participating agencies.

User Access

The Council should strengthen user access controls over certain information system resources. Auditors identified (1) accounts that belonged to former employees and (2) user access that did not align with business needs.

Access and Authentication Reviewed

Auditors reviewed the following areas of logical access and authentication that the Council administrated:

- Network access and password settings for Council employees and employees of the eight participating agencies.
- User access to Laserfiche, Spiceworks, and Versa applications by Council and participating agencies.
- Application password settings for Laserfiche and Versa.
- Database access to Versa and password settings.
- Access and password settings to virtual servers.

Source: The Council.

Title 1, Texas Administrative Code, Chapter 202, requires agencies to adopt an overall set of security policies that are in accordance with the Department of Information Resources' *Security Control Standards Catalog.* For user account management, the *Security Control Standards Catalog* states that an organization must monitor the use of information system accounts and notify account managers when accounts are no longer required or when users are transferred or no longer employed with the organization. The catalog also states that access should employ the principle of least privilege, which would result in a user receiving only the necessary level of access. However, the Council did not have policies and procedures governing user account setup and management. If system access is not determined by business needs and administrative privileges are not appropriately restricted, unauthorized data changes could occur.

[3] Chapter 1-B is rated as Medium because the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

User Access Review

While the Council performed user access reviews of Versa Regulation application users, it did not perform user access reviews on some system resources.

Information owners must approve access to information resources and periodically review access lists based on documented risk management decisions, as required by Title 1, Texas Administrative Code, Chapter 202. The Council had a user access review policy for Versa; however, that policy did not cover the other system layers. Without a periodic review, employees could have access that is not appropriate to their job functions, and that could lead to a compromise of data integrity.

Physical Access

The Council had adequate controls, including policies and procedures, an on-site evacuation map, and appropriate theft-prevention measures, for physical access to the on-site server room. Auditors also accounted for all keys issued to Council staff.

Authentication

The Council had password controls appropriately configured at the Versa application and Linux server levels. However, the Council did not establish appropriate password settings for some systems.

The *Security Control Standards Catalog* states that passwords should have sufficient strength for their intended use; establish minimum and maximum lifetime restrictions; and be changed in a defined time frame. While the Council had a policy and procedure for passwords in relation to Versa, the Council lacked comprehensive password policies covering all system levels. Without strong and consistent passwords, the Council may put agencies at risk for possible unauthorized data access.

In addition, the Council is responsible for setting up password controls for each participating agency; however, the Council did not appropriately configure agencies' network password controls. Because the Council did not have a policy for network passwords, auditors used the policy settings established for Versa. Issues varied across the agencies receiving information technology support services (ITSS).

Uniform settings for each agency would not only ensure compliance with established rules, it would create efficiencies in managing settings for the Council and the eight agencies receiving ITSS.

Recommendations

The Council should:

- Develop and implement comprehensive information technology policies and procedures covering areas such as account management, authentication, and user access reviews.
- Grant and maintain user access, which includes administrative access, based on valid business needs and ensure proper restrictions on administrative authority.
- Remove access in a timely manner when users either change job responsibilities or leave employment.
- Perform periodic reviews of access for virtual, network, Versa, Spiceworks, and Laserfiche environments and take appropriate action to address any access issues identified during those reviews.
- Set up appropriate password restrictions for system resources.

Management's Response

The Council agrees with the recommendations and remediation for the recommendations have already begun. The Council is currently codifying policies for each agency that will include direction for account management authentication and user access reviews. The Council will ensure that the agencies follow directions in the Security Control Standards Catalog when implementing passwords. One remedy will be a checklist stored in our help-desk tickets that ensures user access is reviewed and maintained as per the Council's forthcoming Policy Manual. Further, regular annual reviews of access will be provided to the agencies to update any changes going forward. Following the new onboarding and off boarding checklists will ensure that previous employees will not have access. New logs will provide records of physical visits to the Council's server room.

Issue Rating: Medium

Implementation date: September 1, 2018

Responsible Party: Administrative Officer

Chapter 1-C

The Council Had Controls in Place to Ensure That Changes Made to Versa Were Appropriate

Chapter 1-C Rating: Low [4]

The Council implemented controls and processes governing the management of program code changes to Versa, and it ensured those processes were consistently followed (see text box for a definition of change management).

The Council had a documented process for change management utilizing Spiceworks, a help desk software. That process begins with participating agencies notifying the Council of any Versa errors they encounter or any customizations they require. The Council then works with the vendor to develop, test, and implement system changes. However, as discussed in Chapter 1-A, auditors identified an instance in which a portion of the upgrade was not fully tested. That instance was not included in the sample of the changes discussed in this chapter.

With the assistance of the Council, auditors identified a population of code changes to Versa that occurred from September 1, 2016, through January 31, 2018. From that population, auditors selected a sample of 17 changes that consisted of 1 enhancement (adding new functionality) and 16 break/fix (problem) items. All changes tested were properly authorized, approved, tested, and migrated. Auditors were unable to determine a complete population of code changes due to limitations in the data (see Chapter 3 for more information about those limitations).

Change Management

ISACA, an independent association that certifies professionals in information technology governance, defines change management as:

"All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed, and authorized prior to implementation and reviewed against planned outcomes following the implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment."

Source: ISACA's *Control Objectives for Information and Related Technology* (COBIT), version 4.1.

Management's Response

The Council agrees with the recommendations and have already created additional classifications for tickets in our Help desk system to better track code changes.

Issue Rating: Low

Implementation date: Implemented fix effective immediately.

Responsible Party: Administrative Officer

[4] Chapter 1-C is rated as Low because the audit identified strengths that support the audited entity's ability to administer the program(s)/functions(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Chapter 2

The Council Performed Some Monitoring Related to the Contract; However, It Should Strengthen Its Processes to Include Reviewing Key Deliverables

Chapter 2 Rating:

Medium [5]

The Council did not have formal processes in place to ensure compliance with significant contractual requirements. In addition, while the Council's statement of work contained most of the required elements in the *State of Texas Contract Management Guide*, it did not contain elements for monitoring the vendor for compliance with key provisions, such as provisions related to hosted services and the help desk.

Contracted Services

The Council contracts with a vendor for database services. Those services are comprised of two components, Versa Regulation and Versa Online. Because the Council is responsible only for administering Versa Regulation for its particpating agencies, auditors reviewed only that component.

Participating agencies use Versa Online to control public access for licensees, update license information, and accept payment. Versa Regulation manages day-to-day operations for regulatory functions.

The contract also stipulates that the vendor will provide the Council with database hosting through a third party. Those database hosting services were reviewed as part of this audit.

Source: The Council.

Contract Monitoring

The Council did not have processes in place to ensure compliance with significant requirements in the contract for database services (see text box). However, the Council asserted it had biweekly phone meetings with the vendor. The purpose of those meetings was to discuss the status of any issues requiring a help desk ticket, ideas for resolution, and any estimated costs. While the Council was able to provide emails sent to the vendor referencing those biweekly meetings, it did not have a formal set of meeting minutes or a communication log. The *State of Texas Contract Management Guide* states that keeping a master contract administration file containing items such as records/minutes of all internal and external meetings provides a basis for settling claims and disputes should they arise.

In addition, the Council did not monitor the following significant contract requirements:

- Ticket Resolution Times. The Council did not track the vendor's ticket resolution times. The statement of work differentiates ticketed issues based on severity and has corresponding specific times required for response and resolution.
- Availability of Hosted Services. The Council did not track the availability of hosted services. The statement of work specifies that hosted services will be available 99.5 percent of the time, but the Council did not have reports or other documentation that showed it monitored or determined compliance with this provision.

[5] Chapter 2 is rated as Medium because the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

- Statement on Standards for Attestation Engagement (SSAE). While an SSAE 16 was available from the contracted third party providing hosting services, the Council asserted that it did not review that report. Additionally, the Council stated that it did not verify the adequacy of that vendor's internal controls. (See the text box for more information about SSAE reports.)

Statement on Standards for Attestation Engagements (SSAE)

An SSAE 16 report (as of May 2017, referred to as SSAE 18) is the report of an attestation by an independent reviewer based on a set of standards. As noted by the American Institute of Certified Public Accountants (AICPA):

"The attestation standards establish requirements for performing and reporting on examination, review, and agreed-upon procedures engagements that enable practitioners to report on subject matter ordinarily other than financial statements, for example, an entity's compliance with laws or regulations, the effectiveness of an entity's controls over the security of a system."

Source: AICPA.

The statement of work did not contain provisions for contract monitoring (see the Statement of Work section below for additional information). According to the *State of Texas Contract Management Guide,* monitoring vendor performance is a key function of proper contract administration. By not performing monitoring activities for significant deliverables and criteria in the contract, the Council cannot ensure that all contracted services are being performed. In addition, the Council lacks information on the effectiveness and quality of services provided.

Statement of Work

The Council included in its statement of work most of the elements that the *State of Texas Contract Management Guide* requires. Those elements included (1) quantity; (2) quality; (3) criteria for determining satisfactory contract completion; and (4) corrective action for noncompliance with contract terms and deliverables. However, the statement of work lacked other *State of Texas Contract Management Guide* requirements. Specifically, it did not provide the Council with sufficient methods to monitor vendor performance. No reports were required to show (1) availability of hosted services or (2) help desk metrics.

As of September 1, 2015, Texas Government Code, Section 2157.0685,[6] requires agencies to submit statements of work to the Department of Information Resources prior to awarding a contract. This new process could potentially mitigate the Council's lack of monitoring elements in the future.

The Council asserted there has been no observed issues with system downtime and the vendor has been quick to resolve issues. However, the Council is limiting itself both on reports that may be required and monitoring

[6] Texas Government Code, Section 2157.0685, became effective September 1, 2015, as enacted by the 84th Legislature (Senate Bill 20).

that can be performed to ensure that the vendor delivered services as described in the contractual agreement.

Recommendations

The Council should:

- Develop and implement procedures to monitor compliance with requirements for significant contract deliverables, including hosted services and status for help desk services.
- Include vendor reporting requirements in contracts to ensure compliance with key deliverables. These should include reports on (1) the availability of hosted services and (2) help desk ticket metrics.
- Obtain and review either an SSAE 16 or similar reports/attestations on the effectiveness of internal controls from all contracted vendors.

Management's Response

The Council agrees with this recommendation and will ask the vendor for additional reporting to fulfill the guidelines set forth in the recommendations. Reports will be generated weekly to ensure vendor meets their up time percentages. In the future the Council will request that the vendor provide regular reporting related to Ticket Resolution Times to ensure that the vendor is fulfilling the contract parameters. The Council will include these deliverables in the next review of the Support Contract.

Issue Rating: Medium

Implementation date: September 1, 2018.

Responsible Party: Administrative Officer

Chapter 3

The Council Provided Support Services in Accordance with Applicable Requirements; However, It Should Strengthen Its Process for Documenting and Monitoring Help Desk Tickets and Provide Guidance to Participating Agencies on User Access and Data Classification

Chapter 3 Rating:

Medium [7]

The Council provided information technology support services (ITSS) in accordance with its memorandum of understanding with participating agencies. However, the Council did not have policies and procedures providing guidance to participating agencies on (1) user access levels for the network and supported applications and (2) identifying and classifying sensitive data. In addition, auditors determined that the data from the Spiceworks help desk application was not reliable.

Memorandum of Understanding. The Council provided ITSS in accordance with its memorandum of understanding with the participating agencies receiving ITSS (see Appendix 3 for a list of participating agencies). Every biennium, the agencies sign a memorandum of understanding with the Council that describes the services provided. Those services included, but were not limited to, email and network administration, desktop support, Web page development, imaging system administration, and when requested, serving as the information resource manager. In addition, the Council performed regularly scheduled server backups and patched services based on the latest updates.

Guidance to Participating Agencies. The Council did not have documented policies and procedures providing guidance to participating agencies on (1) user access levels for the network and supported applications and (2) identifying and classifying sensitive data. Only one of the eight agencies receiving ITSS stated it could recall having a conversation with the Council regarding classifying sensitive information. In addition, there was uncertainty between the participating agencies and the Council regarding the responsibility of identifying and classifying sensitive data. By not providing guidance and discussing data classification with participating agencies, the Council increases the risk that sensitive information will not be properly identified or adequately protected.

In addition, auditors identified issues with participating agencies regarding users with access that did not correspond with job responsibilities. By not providing documented guidance on access levels, the Council is putting

[7] Chapter 3 is rated as Medium because the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

agencies at risk for unauthorized access to data, which may result in compromised data integrity.

Spiceworks Data Reliability. Auditors determined that the Council's help desk ticket data in its Spiceworks application was not reliable (see text box for more information about the Spiceworks application). There were 167 (7.6 percent) duplicate tickets from a population of 2,210 closed tickets from September 1, 2016, through January 31, 2018. In addition, the data contained inaccurate information in the following key system fields:

Spiceworks Help Desk Application

The Council uses the Spiceworks application to document help desk tickets. Participating agencies or the Council can open a ticket when an issue is identified. The system contains information such as a description of the issue, a ticket open date, a ticket close date, who worked the ticket, and the status of the ticket.

Source: The Council.

- The Worked By field was blank for 320 (14.5 percent) tickets, signifying that a ticket was not assigned.
- Despite being part of a population of closed tickets, the Disposition field stated New, In Progress, or Waiting on User for 962 (43.5 percent) tickets, implying that the tickets may not have been closed properly.
- The Close Date field was not always the true date of when work was completed. While testing the Council's change management process, auditors identified several tickets for which the Council had completed the work months prior to the entered close date.

In addition, the Spiceworks data did not contain an indicator for identifying true code changes, such as break fixes or enhancements, in Versa. This would allow the Council to determine whether an issue is a systematic problem that requires additional support from the vendor or an isolated incident. Also, based on the information in the Days Open field, the Council had some help desk tickets open for more than 1,000 days. The Council asserted this is because participating agencies do not respond to the Council to close the tickets.

The Council asserted that it did not identify and correct the errors discussed above because it does not have a process to review the information entered into Spiceworks for completeness and accuracy. Without reliable information, the Council cannot accurately track key metrics, such as average ticket times, proper dispositions, and whether an issue might be a systematic problem requiring a custom solution.

Recommendations

The Council should:

- Develop and implement documented policies that outline the responsibilities of the Council and participating agencies regarding (1) user access levels and (2) the identification and classification of sensitive or confidential data.

- Develop and implement a process to verify that the information entered into the Spiceworks application is complete and accurate.

Management's Response

While the Council generally agrees with this set of recommendations it should be noted that in certain cases tickets are repeated in reports but not necessarily in the system. Nevertheless, the Council will include user access level reviews and how to identify and classify sensitive data in each agency's annual review.

Currently the only quality assurance for Spiceworks comes from ticket submitters. The Council will continue to monitor the submission of tickets to ensure the accuracy of the submissions.

Issue Rating: Medium

Implementation date: September 1, 2018.

Responsible Party: IT Staff

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Health Professions Council (Council) has processes and related controls to help ensure that it administers information technology services in accordance with applicable requirements and protects participating agency data.

Scope

The scope of this audit covered selected general controls over the Council's information technology systems and related processes; selected aspects of contract management for the Council's contract for database services with a vendor; selected information technology support services (ITSS) functions; physical security over the Council's server room; help desk support tickets, and other supporting documentation from September 1, 2016, through January 31, 2018.

Methodology

The audit methodology included gaining an understanding of the Council's change management process, contract management process, logical access controls, physical security controls, and ITSS responsibilities. The audit methodology also consisted of collecting and reviewing policies and procedures related to the Council's information technology systems. Auditors also reviewed documentation related to logical access lists, contract terms and monitoring, and change management. In addition, auditors performed a walkthrough of the server room and reviewed the Council's ITSS data and the ITSS memorandum of understanding, which outlines expectations between the Council and participating agencies.

Data Reliability and Completeness

Auditors used Spiceworks help desk data extracts as part of the audit testing procedures. As discussed in Chapter 3, the help desk data contained errors and inconsistencies, including duplicate help desk ticket numbers, tickets for which no code changes were made, and selected key fields that did not always contain accurate data. Additionally, user access was not appropriate for some users tested.

Auditors also used the data from Spiceworks to test change management. Because of the issues discussed in this section and in Chapter 3, auditors

determined that the change management data was not reliable for purposes of this audit. However, auditors did use that data for testing because it was the most complete population available to auditors during the course of this audit.

Sampling Methodology

To assess the Council's change management processes, auditors selected a random sample of 16 system changes that appeared to involve a modification to the application code of the Versa Regulation Database (Versa). In addition, auditors used a risk-based sample to select one additional code change for testing. The sample items were not representative of the population; therefore, it would not be appropriate to project the test results to the population.

Information collected and reviewed included the following:

- The Council's policies and procedures.
- Logical access lists for the systems reviewed.
- The Council's change management documentation for system changes made to Versa.
- Password settings for the Council's network and key applications and systems.
- The Council's organizational charts and current employment attestations for the Office's contracted employees.
- Documentation related to the physical security of the Council's server room.
- The contract for Versa between the Council and the vendor, effective August 2015.
- The memorandum of understanding detailing the Council's ITSS.

Procedures and tests conducted included the following:

- Interviewed the Council's employees to identify operational processes, information technology controls, and the systems used to support participating agencies.
- Reviewed and tested the Versa contract and monitoring documentation to determine whether the contract contains adequate provisions to safeguard state data and whether the Council was monitoring key service requirements and reports in the contract.

- Tested technical support documentation to determine whether the Council was providing the required services to participating agencies as required by the memorandum of understanding.
- Tested change management documentation to determine whether changes were documented, authorized, approved, developed, tested, and migrated.
- Tested logical access lists to determine whether they were appropriate and managed according to the Council's policies.
- Tested system password settings to determine compliance with the Council's policies.
- Tested key physical security controls for the server room to determine compliance with the Council's policies.

Criteria used included the following:

- Title 1, Texas Administrative Code, Chapter 202.
- Texas Government Code, Chapter 2157.
- Texas Occupations Code, Chapter 101.
- Department of Information Resources' *Security Control Standards Catalog*, version 1.3.
- The Council's policies and procedures.
- *State of Texas Contract Management Guide* (Version 1.13, September 2014).

Project Information

Audit fieldwork was conducted from December 2017 through May 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 based on our audit objectives.

The following members of the State Auditor's staff performed the audit:

- Isaac A. Barajas (Project Manager)
- Yue Zhang, CISA (Assistant Project Manager)

- Anna Howe, CFE
- Dana Musgrave, MBA (Quality Control Reviewer)
- Becky Beachy, CIA, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgement and rated the audit findings identified in this report. Those issue ratings are summarized in the report chapters/sub-chapters. The issue ratings were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Table 2 provides a description of the issue ratings presented in this report.

Table 2

Summary of Issue Ratings	
Issue Rating	**Description of Rating**
Low	The audit identified strengths that support the audited entity's ability to administer the program(s)/functions(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.
Medium	Issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.
High	Issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.
Priority	Issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

Appendix 3

Health Professions Council's Information Technology Services

Table 3 shows the services in which Health Professions Council agencies participated during the 2018-2019 biennium.

Table 3

Services in Which Health Professions Council Members Participated During the 2018-2019 Biennium			
Participating Agency	Versa Regulation Database	Information Technology Support Services (ITSS)	Document Imaging (Laserfiche)
Board of Chiropractic Examiners		X	X
Board of Examiners of Psychologists	X	X	X
Board of Pharmacy	X		X
Board of Plumbing Examiners	X		
Board of Professional Geoscientists		X	
Board of Professional Land Surveying	X		
Board of Veterinary Medical Examiners		X	
Executive Council of Physical Therapy and Occupational Therapy Examiners		X	X
Funeral Service Commission	X	X	X
Office of Public Insurance Counsel		X	
Optometry Board	X	X	X
Texas Board of Nursing			X
Texas State Board of Dental Examiners	X		X

Source: Legislative Budget Board Staff Reports, January 2017.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair
The Honorable Joe Straus III, Speaker of the House, Joint Chair
The Honorable Jane Nelson, Senate Finance Committee
The Honorable Robert Nichols, Member, Texas Senate
The Honorable John Zerwas, House Appropriations Committee
The Honorable Dennis Bonnen, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Health Professions Council

Members of the Health Professions Council
- Mr. Chris Kloeris, J.D., Chairman
- Ms. Allison Benz, R.Ph.
- Mr. John Helenberg
- Mr. John Maline
- Ms. Janice McCoy
- Mr. Darrel Spinks, J.D.
- Ms. Katherine Thomas, M.N., R.N.
- Mr. Brint Carlton
- Mr. W. Boyd Bush
- Mr. Patrick Fortner
- Mr. Tony Estrada
- Ms. Lisa Hill
- Mr. Charles Horton

Mr. John Monk, Administrative Officer