STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-198
June 2016

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Versa: Regulation

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Business and Professional Regulation

Section 20.165, Florida Statutes, creates the Department of Business and Professional Regulation. The head of the Department is the Secretary of Business and Professional Regulation who is appointed by the Governor, subject to confirmation by the Senate. Ken Lawson served as Secretary during the period of our audit.

The team leader was Arthur Wahl, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Versa: Regulation

SUMMARY

This operational audit of the Department of Business and Professional Regulation (Department) focused on evaluating selected information technology (IT) controls applicable to Versa: Regulation. Our audit disclosed the following:

Finding 1: Change management controls related to Versa: Regulation program changes need improvement to ensure that only authorized, tested, and approved program changes are implemented into the production environment.

Finding 2: The access privileges for some Department employees did not promote an appropriate separation of duties and did not restrict users to only those functions appropriate and necessary for their assigned job duties.

Finding 3: The Department did not timely deactivate the Versa: Regulation accounts for one former and one transferred employee.

Finding 4: Contrary to the retention requirements set forth in the State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies*, the Department did not retain relevant Versa: Regulation access control records related to the deactivation of employee access privileges.

Finding 5: Certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources need improvement to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

BACKGROUND

The Department of Business and Professional Regulation (Department) was established by State law[1], and authorized to establish uniform application forms and certificates of licensure for use by the divisions within the Department. In 2013, the Department implemented new licensing software, Versa: Regulation, to provide a comprehensive view of all data related to a license, allowing Department staff to navigate licenses, transactions, complaints, or other information related to licensee accounts. The primary information technology (IT) infrastructure for Versa: Regulation is located in Tallahassee, Florida.

[1] Sections 20.165 and 20.165(8), Florida Statutes.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls over program changes ensure that only authorized, tested, and approved program changes are implemented into the production environment. Further, the effectiveness of change management controls is enhanced through controls that ensure that the change management control process is followed when program changes are implemented into the production environment.

Our audit procedures disclosed that, although the Department used a change management system for tracking the authorization, testing, approval, and implementation of program changes, the Department had not established controls, such as the use of a reconciliation process, to ensure that all program changes implemented into the production environment followed the Department's change management process.

Absent effective change management controls to ensure that all program changes are authorized, tested, and approved, the risk is increased that erroneous or unauthorized program changes may be implemented into the production environment and not be timely detected.

Recommendation: We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to Versa: Regulation are implemented into the production environment.

Finding 2: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are appropriate and necessary for the user's assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. Our audit procedures disclosed that access controls related to Versa: Regulation security roles and the production database need improvement.

Versa: Regulation security roles (security roles) were used to group and control access privileges to Versa: Regulation. Our examination of assigned security roles disclosed that some users were assigned security roles that included access privileges that were inappropriate and unnecessary for the users' assigned job duties. Specifically, we found that:

- Nine programmers were granted access privileges assigned to the System Administrator role, allowing the programmers to update Versa: Regulation as end users and to perform security administration changes. In response to our audit inquiry, Department management stated that the System Administrator role had originally been established with permissions for configuration, security administration, and end-user-level functions and that to perform one or more of these functions, the System Administrator role must be granted.
- Three Versa: Regulation security administrators were granted access privileges assigned to the System Administrator role, allowing them the ability to update Versa: Regulation as end users and make configuration changes to Versa: Regulation through the Administration Module.

- Two Department end users were granted access privileges assigned to the Modify License Add/Change/View role at the Departmentwide level rather than only to the level necessary for their assigned job duties.
- Three Department end users were granted access privileges assigned to the Modify License Add/Change/View role that were not needed to perform their assigned job duties.

In addition, we noted that ten programmers and four nonprogrammers were granted update access privileges to the Versa: Regulation production database that should have been limited to database support staff. In response to our audit inquiry, Department management stated that all business-level troubleshooting and configuration maintenance functions were assigned to these programmers who had knowledge of the business process.

Notwithstanding the Department's responses, the existence of inappropriate and unnecessary access privileges increases the risk that unauthorized modification, loss, or disclosure of Versa: Regulation data and related IT resources may occur.

Recommendation: We recommend that Department management limit user access privileges to Versa: Regulation and the production database to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

Finding 3: Employee Access Deactivation

Agency for Enterprise Information Technology (AEIT) rules[2] provide that access authorization shall be promptly removed when the user's employment is terminated or access to information resources is no longer required. Prompt action is necessary to ensure that former or transferred employees or others do not misuse the former or transferred employees' access privileges.

Our audit procedures disclosed that one former employee had active Versa: Regulation access privileges although, as of December 14, 2015, 4,081 days (approximately 11 years) had elapsed since the employee separated from Department employment. This former employee's active access privileges had been brought forward from the previous licensing software in 2013 when Versa: Regulation was implemented. Additionally, one employee transferred within the Department and was given a new Versa: Regulation account; however, Department staff did not deactivate the employee's prior account until 59 days after the new account was granted. Although these two accounts were not timely deactivated, Department management indicated that the accounts were not used subsequent to the dates of the employees' employment separation and transfer.

Without timely deactivation of former or transferred employee Versa: Regulation accounts, the risk is increased that the accounts may be misused by the former or transferred employee or others.

Recommendation: We recommend that Department management ensure that the Versa: Regulation accounts of former and transferred employees are timely deactivated.

[2] AEIT Rule 71A-1.007(6), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records, property, administrative authority, and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed.

Finding 4: Retention of Access Control Records

The State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies* (*General Records Schedule*) provides that access control records must be retained for 1 anniversary year after superseded or after the employee separates from employment. However, we noted that the nightly scripts run by the Department removed the security permissions that were tied to the user accounts that were deactivated each day. Therefore, the Department did not retain relevant Versa: Regulation access control records related to the deactivation of employee access privileges although required by the *General Records Schedule*.

Without adequate retention of relevant Versa: Regulation access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur.

Recommendation: We recommend that Department management ensure that relevant Versa: Regulation access control records are retained as required by the *General Records Schedule*.

Finding 5: Security Controls – User Authentication, Logging, and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Versa: Regulation data and related IT resources. However, we have notified appropriate Department management of the specific issues. Without appropriate security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources, the risk is increased that the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources may be compromised.

Recommendation: We recommend that Department management improve certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from November 2015 through January 2016 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to Versa: Regulation during the period November 2015 through January 2016 and selected actions prior and subsequent thereto. The audit included selected business process application controls over transaction data input, processing, and output and selected application-level general controls over logical access to programs and data, configuration management, and contingency planning. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel.
- Obtained an understanding of Versa: Regulation data and business process flows, including key sources of data input and interfaces, key application transactions and processes, and key types of data output related to the application.
- Evaluated the effectiveness of selected Versa: Regulation business process application controls related to data input, processing, and output.
- Evaluated selected Versa: Regulation transaction data interface and reconciliation controls.

- Evaluated selected contingency planning controls related to Versa: Regulation.
- Obtained an understanding of the Versa: Regulation computing platform including the applicable hardware, operating system, database management system, and security software.
- Obtained an understanding of Department procedures for its account management processes for authorizing, creating, modifying, and revoking Versa: Regulation access privileges.
- Determined whether the Department had procedures for periodically reviewing Versa: Regulation access appropriateness.
- Evaluated the effectiveness of selected access controls related to access privileges for appropriateness related to Versa: Regulation and supporting IT resources. Specifically, we reviewed:
  - Access privileges granted for 20 of 48 Versa: Regulation users as of December 14, 2015, to determine the appropriateness of the access granted.
  - Access privileges granted to the Versa: Regulation database for all 17 users as of January 4, 2016, to determine the appropriateness of the access granted.
- Evaluated selected user authentication controls for Versa: Regulation.
- Evaluated the effectiveness of selected logging and monitoring controls for Versa: Regulation and related IT resources, including records retention.
- Obtained an understanding of the Department's change management processes applicable to Versa: Regulation, including identification of policies and procedures for change control.
- Evaluated the effectiveness of selected Versa: Regulation change management controls. Specifically, we evaluated 18 of 181 program changes that were implemented into the production environment during the period July 1, 2015, through December 15, 2015, to determine whether the selected Versa: Regulation changes were appropriately authorized, tested, and approved.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

Florida Department of Business & Professional Regulation

Office of the Secretary
Ken Lawson, Secretary
1940 North Monroe Street
Tallahassee, Florida 32399-1000
Phone: 850.413.0755 • Fax: 850.921.4094

Ken Lawson, Secretary

Rick Scott, Governor

June 8, 2016

Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

In accordance with Section 11.45(4)(d), Florida Statutes, I have enclosed our response to the preliminary and tentative audit findings and recommendations included in your information technology audit of Versa: Regulation.

We appreciate the time and energy put forth by your staff, as well as your continuing efforts to improve the operations of state government.

If you have any questions concerning this response, please contact Lynne T. Winston, Inspector General, at (850) 414-6700.

Sincerely,

Ken Lawson

cc: Matilde Miller, Chief of Staff
Joseph Martin, Chief Information Officer
Lynne T. Winston, Inspector General

KL:sll

Enclosure

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Response to Preliminary and Tentative Audit Findings and Recommendations
Information Technology Audit of
Department of Business and Professional Regulation Versa: Regulation

Finding No. 1: Change Management Controls

Change management controls related to Versa: Regulation program changes need improvement to ensure that only authorized, tested, and approved program changes are implemented into the production environment.

Recommendation

We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to Versa: Regulation are implemented into the production environment.

Agency Response

The department's existing change management policies and procedures are designed to ensure that only authorized, tested, and approved program changes are implemented into the Versa: Regulation production environment. The department agrees, however, that additional monitoring would provide additional assurance. To this end, we will evaluate our existing change management procedures to identify opportunities for improvement. We will also evaluate the feasibility of modifying the application's functionalities in this regard.

Finding No. 2: Appropriateness of Access Privileges

The access privileges for some Department employees did not promote an appropriate separation of duties and did not restrict users to only those functions appropriate and necessary for their assigned job duties.

Recommendation

We recommend that Department management limit user access privileges to Versa: Regulation and the production database to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

Agency Response

The department concurs with these recommendations. The department's Information Systems Security Policy (DBPR Policy 2.3) requires supervisors to identify least privilege security roles and permissions for each employee granted access to department IT resources, including Versa: Regulation. The policy further requires supervisors to regularly review the access privileges of staff and ensure such access is appropriate for their job duties. During the course of the Auditor General's review, Division of Technology management reviewed the Versa: Regulation permissions of those technology staff identified by the auditors and modified any unnecessary privileges, accordingly. The Division of Technology relies on supervisors in each departmental business unit to identify appropriate access for their employees. To facilitate

proper oversight of user privileges, the Division of Technology conducts periodic Versa: Regulation entitlement reviews, at which time supervisors must certify that the employee's access remains appropriate for the responsibilities of the position or notify the division of any required changes.

Finding No. 3: Employee Access Deactivation

The Department did not timely deactivate the Versa: Regulation accounts for one former and one transferred employee.

Recommendation

We recommend that Department management ensure that the Versa: Regulation accounts of former and transferred employees are timely deactivated.

Agency Response

The department concurs with this recommendation. The department's existing Information Systems Security Policy (DBPR Policy 2.3) requires supervisors to notify the Division of Technology immediately upon a user's separation from or movement within the department. To help ensure adherence to this policy, the Division of Technology will communicate these requirements through periodic email notifications to supervisory staff and in the regularly scheduled meetings of senior and executive staff.

Finding No. 4: Retention of Access Control Records

Contrary to the retention requirements set forth in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies, the Department did not retain relevant Versa: Regulation access control records related to the deactivation of employee access privileges.

Recommendation

We recommend that Department management ensure that relevant Versa: Regulation access control records are retained as required by the General Records Schedule.

Agency Response

In accordance with the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies, the department's Division of Technology retains requests to add, modify, or remove user permissions for all business systems, including Versa: Regulation, by use of access request forms and the Remedyforce tracking system. The department acknowledges that access control records are not retained within the Versa: Regulation application itself. The Division of Technology will therefore explore the feasibility of enhancing existing records retention procedures by modifying the Versa: Regulation system to capture permission changes.

Finding No. 5: Security Controls – User Authentication, Logging, and Monitoring

Certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources need improvement to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

Recommendation

We recommend that Department management improve certain security controls related to user authentication, logging, and monitoring for Versa: Regulation and related IT resources to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related IT resources.

Agency Response

The department has implemented improved security controls in certain areas and is actively working to develop and implement additional improvements to ensure the confidentiality, integrity, and availability of Versa: Regulation data and related information technology resources.