STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-045
October 2020

STATE BOARD OF ADMINISTRATION

Information Technology General Controls and Florida PRIME System Application-Level General Controls

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and Executive Director of the State Board of Administration

Article IV, Section 4(e) of the State Constitution (1968), as amended, establishes the State Board of Administration (SBA). The SBA Board of Trustees is composed of the Governor, as Chair, the Chief Financial Officer, and the Attorney General. The Trustees delegate administrative and investment authority to an appointed Executive Director. Mr. Ashbel Williams served as Executive Director and Chief Investment Officer during the audit period.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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

FLAuditor.gov

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

STATE BOARD OF ADMINISTRATION

Information Technology General Controls and Florida PRIME System Application-Level General Controls

SUMMARY

This operational audit of the State Board of Administration (SBA) focused on evaluating selected SBA information technology (IT) general controls and selected application-level general controls for the Florida PRIME System. The audit also included a follow-up on the findings included in our report No. 2017-199 that were applicable to the scope of this audit. Our audit disclosed the following:

Finding 1: SBA change management controls for the Florida PRIME System continue to need improvement to ensure that program code changes are appropriately authorized, tested, approved, and implemented into the production environment consistent with the established change management process.

Finding 2: Certain security controls related to logical access, user authentication, logging and monitoring, configuration management, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of SBA data and IT resources.

BACKGROUND

The State Constitution[1] establishes the State Board of Administration (SBA) governed by a three-member Board of Trustees composed of the Governor, as Chair, the Chief Financial Officer, and the Attorney General. The SBA provides a variety of investment services to State and local governmental entities and, pursuant to State law,[2] the SBA is to ensure that moneys invested are handled in the best interests of the State.

State law[3] establishes the Local Government Surplus Funds Trust Fund (Fund)[4] as an investment vehicle for local governmental units to invest surplus funds. The Florida PRIME System is a Web-based system developed internally by the SBA to administer the Fund. Local governments (participants) execute an Authorizing Resolution to establish an account in the local government’s name for the purpose of transmitting funds for investment in the Fund and to establish an authorized representative to transmit and withdraw funds, to issue letters of instruction, and to take all other actions deemed necessary or appropriate for the investment of funds. The authorized representative executes a Participant Account Maintenance Form (PAMF) that includes contact and banking information and a list of participant designees authorized to initiate transactions. Designated SBA employees use the PAMF to set up a Fund account in the Florida PRIME System. Participants (external users) and certain SBA employees (internal users) use the Florida PRIME System to record and view investment transaction information.

[1] Article IV, Section 4(e) of the State Constitution.

[2] Section 215.44(2)(a), Florida Statutes.

[3] Section 218.405, Florida Statutes.

[4] Since August 2009, the SBA has used the name “Florida PRIME” to refer to the Fund.

The SBA conducts withdrawals from and deposits to participant Fund accounts through the SBA's qualified public depository.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation into the production environment. Effective change management controls also ensure that the established change management process is followed when program code changes are implemented into the production environment and only approved changes are implemented into the production environment. The SBA's *Information Technology Change Control* procedure required changes to application program code or configuration follow the change control process established and managed by the SBA's change management module (ticketing system) within the service desk software.

To evaluate the appropriateness of SBA change management controls for program code changes implemented into the Florida PRIME System production environment, we requested a system-generated list of all program code changes implemented during the period July 1, 2018, through November 20, 2019. However, the SBA was unable to provide a system-generated list of all program code changes implemented. Instead, the SBA provided a list from the ticketing system of the closed service tickets for the Florida PRIME System for the period July 1, 2018, through November 20, 2019, which represented the requests in the ticketing system that required program code changes to the Florida PRIME System. According to SBA management, to ensure that all program code changes implemented into the Florida PRIME System production environment were requested and approved in the ticketing system, each month management reconciled program code files with a Windows Explorer modified date from the prior month to ticketing system approval records for the same period. Our review of the SBA's monthly reconciliation process found, however, that it did not ensure that all program code changes were requested in and managed by the ticketing system because only the most recent modified date as recorded by Windows Explorer was used and program code files with more than one modification in a month were not evaluated by the SBA. Additionally, the reconciliation only verified that approval for implementation was recorded on a closed ticket for the same date as the identified program code change file but did not determine whether the changes made on that date related to the closed service ticket, therefore limiting the assurance that the changes made were approved.

Notwithstanding the limitation of the ticketing system list, we examined SBA records for the eight service tickets completed and implemented with respect to the Florida PRIME System during the period July 1, 2018, through November 20, 2019. For each service ticket on the list, we requested documentation to evidence that the service ticket was authorized, the program code changes to address the service ticket were tested, the program code changes were approved to be moved into the production environment by the user and the Application and Development Manager, and the changed program code was implemented into the production environment by someone other than the programmer. Our examination found that SBA records did not demonstrate that:

- Seven of the service tickets were authorized by the user.
- The program code changes to address four of the service tickets were tested by the user.

According to SBA management, Florida PRIME System users sometimes verbally or informally communicated service ticket authorizations and user testing approvals and did not retain evidence of the testing.

Without an effective reconciliation process that compares all program code changes implemented into the Florida PRIME System production environment as recorded in version control software to the closed service ticket requests in the ticketing system, the SBA's assurance that all program code changes are appropriately authorized, tested, approved, and implemented and do not bypass the SBA's change management process is limited. Similar findings were noted in prior audits of the SBA, most recently in our report No. 2017-199 (Finding 5).

Recommendation: We recommend that SBA management enhance reconciliation controls to ensure that all implemented Florida PRIME System program code changes are managed by, and do not bypass, the SBA's change management process. We also recommend that SBA management ensure that documentation is retained to demonstrate that Florida PRIME System program code changes are appropriately authorized, tested, approved, and implemented into the production environment.

Finding 2: Security Controls – Logical Access, User Authentication, Logging and Monitoring, Configuration Management, and Vulnerability Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and information technology (IT) resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, logging and monitoring, configuration management, and vulnerability management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising SBA data and IT resources. However, we have notified appropriate SBA management of the specific issues.

Appropriate security controls related to logical access, user authentication, logging and monitoring, configuration management, and vulnerability management would help ensure the confidentiality, integrity, and availability of SBA data and IT resources. Similar findings were communicated to SBA management in connection with prior audits of the SBA, most recently with our report No. 2017-199 (Finding 9).

Recommendation: We recommend that SBA management improve certain security controls related to logical access, user authentication, logging and monitoring, configuration management, and vulnerability management to ensure the confidentiality, integrity, and availability of SBA data and IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the SBA had taken corrective actions for the applicable findings included in our report No. 2017-199.

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 September 2019 through February 2020 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 significant IT general controls and Florida PRIME System application-level general controls applicable to State Board of Administration (SBA) operations during the period July 2019 through February 2020 and selected actions prior and subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's 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 determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2017-199 that were applicable to the scope of this audit (Finding 3, and Findings 1, 5, 6, 7, 8, and 9 as they relate to the Florida PRIME System).
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[5] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

[5] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the SBA Board of Trustees and SBA Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that the internal control components significant to our audit objectives included control environment, control activities, information and communication, and monitoring. The associated underlying principles significant to our objectives included:

- SBA Board of Trustees and management commitment to integrity and ethical values.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the SBA's goals and objectives.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management design of control activities to achieve the SBA's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the SBA's objectives.
- Management communication of information internally necessary to achieve the SBA's objectives.
- Management communication of information externally necessary to achieve the SBA's objectives.
- Management activities to monitor the SBA's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; 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 systems 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 and evaluating the IT systems and related significant 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:

- Reviewed applicable laws, rules, SBA policies and procedures, and other guidelines and interviewed SBA personnel to obtain an understanding of selected SBA IT general controls and application-level general controls for the Florida PRIME System.
- Obtained an understanding of the user account management processes for the Florida PRIME System, including: the processes for authorizing, creating, modifying, and revoking user accounts; periodic access reviews; granting and revoking access to the Florida PRIME System database; logging and monitoring of system and security events; and business process flows for the Florida PRIME System interfaces to the qualified public depository.
- Obtained an understanding of the process for requesting, authorizing, testing, approving, implementing, and reconciling changes to the Florida PRIME application code and data.
- Obtained an understanding of the SBA's process for granting, discontinuing, logging, and periodic review of physical access to the data center and other secured areas, and an understanding of other physical security measures in place.
- Obtained an understanding of the SBA's network infrastructure design and configuration; vulnerability management controls, including the use of authenticated scans and the time frames and processes for analysis and remediation; and the process for reviewing, analyzing, and implementing software updates for network devices.
- Evaluated logical access controls for the Florida PRIME System, including user access authorization procedures and processes. Specifically, we evaluated:

  - SBA procedures and examined SBA records to determine whether semi-annual periodic access reviews were performed to assess the appropriateness of user access privileges for the Florida PRIME System.
  - The appropriateness of access privileges as of December 10, 2019, for the nine Florida PRIME System internal application user accounts, including whether the user accounts were assigned to current employees.
- Evaluated logical access controls including policies, procedures, and processes for assigning administrative access for the SBA's network, high-risk network devices, the Florida PRIME System database and instance, and the application and database servers. Specifically, we evaluated:
  - The 15 active database administration accounts as of November 12, 2019, with membership in the *sysadmin* fixed server role allowing access to the Florida PRIME System database and the database instance.
  - The eight active Florida PRIME System database user accounts as of November 12, 2019.
  - For the three Florida PRIME servers (database and external application as of November 26, 2019, and internal application as of January 6, 2020), the 25 accounts and one group that were assigned either local administrator privileges on the respective server or had full control permissions to the Florida PRIME System directory on their respective server.
  - The 20 active administrative accounts with access to the network (user and service accounts) as of November 6, 2019, with membership in the *Enterprise Admins*, *Schema Admins*, *Domain Admins*, and *Administrators* security groups.
  - The accounts with administrative access as of November 6, 2019, and November 20, 2019, for three high-risk network devices.
- Evaluated the adequacy of authentication controls for the network domain, high-risk network devices, and the Florida PRIME System internal and external end-users, database, and internal and external application and database servers.
- Evaluated the effectiveness of interface controls for the Florida PRIME System, including interface listings, processing procedures, and reconciliations between the Florida PRIME System and the qualified public depository.
- Evaluated the effectiveness of selected SBA logging and monitoring controls.
- Evaluated the adequacy of SBA policies and procedures for application and data changes to the Florida PRIME System, including evaluating the eight service tickets for program code changes applied to the application during the period July 1, 2018, through November 20, 2019, to determine whether SBA appropriately requested, tested, approved, and implemented the changes.
- Evaluated the adequacy of SBA policies and procedures for authorizing, removing, periodically reviewing, and logging physical access to the data center and other secured areas, including evaluating the appropriateness of the 20 active users as of November 13, 2019, with access to the computer room and telecommunication rooms.
- Evaluated the adequacy of SBA configuration management policies, procedures, and processes for ensuring patches for high-risk network devices were timely analyzed and applied as necessary, including evaluating three high-risk network devices as of November 6, 2019, to determine whether the network device operating system was supported and up to date.
- Evaluated vulnerability management controls including the sufficiency of policies and procedures, timely performance of authenticated scans, and timely communication, analysis, and remediation of identified vulnerabilities.

- 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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

STATE BOARD OF ADMINISTRATION
OF FLORIDA

1801 HERMITAGE BOULEVARD, SUITE 100
TALLAHASSEE, FLORIDA 32308
(850) 488-4406

POST OFFICE BOX 13300
32317-3300

RON DESANTIS
GOVERNOR
CHAIR

JIMMY PATRONIS
CHIEF FINANCIAL OFFICER

ASHLEY MOODY
ATTORNEY GENERAL

ASHBEL C. WILLIAMS
EXECUTIVE DIRECTOR &
CHIEF INVESTMENT OFFICER

October 16, 2020

Ms. Sherrill Norman
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Our responses to the preliminary and tentative findings and recommendations which may be included in your report on the Operational Audit of the State Board of Administration are discussed below:

Finding Number 1:

Recommendation: We recommend that SBA management enhance reconciliation controls to ensure that all implemented FLORIDA PRIME System program code changes are managed by, and do not bypass, the SBA's change management process. We also recommend that SBA management ensure that documentation is retained to demonstrate that Florida PRIME System program code changes are appropriately authorized, tested, approved, and implemented into the production environment.

Response: Management agrees and will implement enhanced reconciliation controls and will ensure documentation is retained to demonstrate changes are appropriately authorized, approved and implemented into the production environment.

Finding Number 2:

Recommendation: We recommend that SBA management improve certain security controls related to logical access, user authentication, logging and monitoring, configuration management and vulnerability management to ensure the confidentiality, integrity, and availability of SBA data and IT resources.

Response: Management has received the Auditor General's specific recommendations with respect to this finding and will continue to improve certain security controls related to the items mentioned therein.

Please do not hesitate to contact us if you have questions or need additional information.

Sincerely,

Ashbel C. Williams
Executive Director/CIO