P&N

Postlethwaite & Netterville

Board of Regents – Internal Audit of Louisiana Office of Student Financial Assistance (LOSFA) – TOPS Initial Eligibility and Renewals Processes

December 20, 2018

assurance - consulting - tax - technology - pncpa.com

Postlethwaite & Netterville, A Professional Accounting Corporation

Table of Contents

Objective & Scope

An internal audit was conducted to assess the Louisiana Office of Student Financial Assistance (LOSFA) processes and applicable internal controls related to the Taylor Opportunity Program for Students (TOPS) initial eligibility and renewals/continuing eligibility.

Overview

- Obtained documented policies and procedures
- Interviewed LOSFA personnel to gain an understanding of the applicable processes and underlying systems
- Performed walkthroughs of the TOPS processes and Award System
- Assessed appropriateness of Award System access for certain user roles and system change management process
- Assessed the audit process for TOPS

The scope period included in the audit was July 1, 2017 – October 31, 2018

Observations Summary

- Based on the results of our preliminary risk assessment performed and walkthrough of the automation controls in the Awards System, the objective of our audit was primarily related to evaluation of the design of controls related to 1) the Awards System, such as access and change management; and 2) manual TOPS processes and controls, such as the risk based audits performed by LOSFA personnel and TOPS exceptions processes.

- During our walkthrough, we identified certain internal controls designed to mitigate risks associated with processes for determining TOPS initial eligibility and renewals, as follows*:

  - Processes related to determining initial and continuing eligibility for TOPS were automated in the Awards System. In addition, inputs used for determining TOPS eligibility were independently entered into the system and system edit controls were in place on certain high risk data fields that prevented LOSFA users from making changes in the system. These controls were designed to increase data integrity in the system and reduce the risk of human error or intentional manipulation of data.

  - After TOPS eligibility was determined by the system, a manual review was performed by LOSFA personnel, on a representative sample basis, prior to issuance of award notifications. This detective control was designed to help identify and reduce the risk of errors in TOPS award determinations.

  - Risk-based audits were performed annually, on a sample basis, related to high schools, colleges and/or proprietary schools. As part of these audits, the inputs used for determining TOPS eligibility and award level were verified for accuracy, with a goal of identifying any errors in TOPS awards and any associated overpayments to be paid back by the institutions. This process served as a detective and corrective control and was designed to reduce the risk of overall overpayments by the program.

- Based on our procedures, no high risk observations were identified. All five observations identified were assessed to be **moderate to low** risk to the organization and relate to the following two areas:

  - Award System Access

    - Identified instances where user access was not limited in the system based on job responsibilities.

  - Award System Change Management

    - Change management procedures were not formalized in a written policy and user acceptance testing was not performed independently in the test environment.

  Please refer to the Results section of this report for additional details.

Tests of operating effectiveness were not performed for each of the controls described.

Results: Award System Access

Observation	Risk	Root Cause	Recommendation	Responsible Party	Management Response
Risk Rating: Moderate					
It was explained that access to the Award System is role-based, and users with access to the "LOSFA-IT", "LOSFA-Ops" and "LOSFA - Admin" roles *(See Note) have access to maintain user accounts (i.e. add new users and modify current users' access permissions). Additionally, the "LOSFA - IT" role has access to implement source code/system changes that could impact system functionality and TOPS eligibility determinations. The following observations were identified related to user access for these roles: 1. User provisioning access within the system appears to be excessive. At the time of testing, nine unique users had access to add, modify and delete user access in the system, as follows: - 1 user with access to the "LOSFA-Admin" role - 1 user with access to both the "LOSFA-Admin" and "LOSFA-IT" roles - 5 users with access to the "LOSFA-IT" role - 2 users with access to the "LOSFA-Ops" role 2. Per analysis of the user access listing for the "LOSFA-IT", "LOSFA-Ops" and/or "LOSFA - Admin" roles and discussion with management, access for the following users was not limited based on their job responsibilities: a. Five users did not need access to maintain user accounts based on their job responsibilities, as follows: - 1 user with access to the "LOSFA-Admin" role - 1 user with access to both the "LOSFA-Admin" and "LOSFA-IT" roles - 3 users with access to the "LOSFA-IT" role b. Per discussion with management, one of the six users with access to the "LOSFA-IT" role did not need access to implement source code system changes based on his/her job responsibilities. *NOTE: Prior to the issuance of the report, management removed the "LOSFA- Admin" role from the system.	- New users may be inappropriately added -Access by unauthorized or inappropriate parties -Potential for users to make unauthorized or inappropriate changes in the system	- Defined system roles were not in alignment with job responsibilities - Lack of formal process for performing a periodic review of defined system roles to ensure that access permissions granted are commensurate with individual's job responsibilities.	- Management should consider limiting system access related to user provisioning and implementing source code/system changes based on job responsibilities. If deemed appropriate, management should consider creating additional system roles to limit these user permissions. Additionally, management should consider the following: - Review the current access privileges granted for all other roles/users in the system to ensure that access is limited based on job responsibilities. - Perform a periodic review of all roles and user access for appropriateness.	IT Management	When the Award System was first launched in August 2010, all IT application programmers and project leaders were provided user access to assist with many portions of the system. Going forward, LOSFA Programs will have three distinct user profiles: LOSFA_IT, LOSFA_Ops, and LOSFA_ITUser. The LOSFA_IT role will be assigned to the ITTops developers. We will modify this role to remove the ability to modify user permissions/accounts and the ability to set an approval status on TOPS exceptions. The LOSFA_Ops role will be limited to user permissions/accounts. The LOSFA_ITUser roles will provide limited access; this role will not have access to development system changes or user profiles. IT Management will also review user access and user role reports on a quarterly basis to determine if any revisions are required. Anticipated Date of Implementation: January 4, 2019

Results: Award System Access (continued)

Observation	Risk	Root Cause	Recommendation	Responsible Party	Management Response
Risk Rating: Moderate					
While there was a process for granting and modifying access to the Award System, it appears the established process was not consistently followed. Of the 15 individual users with access to the "LOSFA - Admin", "LOSFA - IT", "LOSFA-Ops" and/or "LOSFA - Legal" roles, P&N noted the following: - 1 user who transferred to another department, but his/her access was not updated to limit his/her system capabilities based on the current role at LOSFA -3 users who were terminated but their access was not removed from the Award System. It was explained that access is obtained through LOSFA-issued equipment only (i.e. LOSFA users cannot logon from personal devices). As a result, terminated users would not be able to logon to the Award System once they no longer have access to LOSFA equipment.	- Access by unauthorized or inappropriate parties -Potential for users to make unauthorized or inappropriate changes in the system	- The LAN request form, used to facilitate the process for granting and modifying access, was not completed fully and/or the requested changes were not implemented as requested on the form. - There was no periodic review/monitoring process to ensure that the established process related to user provisioning was followed. - Lack of training on the established user provisioning process.	- Management should ensure the established process for granting and modifying access is followed and appropriate monitoring controls are implemented. For example, management should consider performing periodic reviews of current users for appropriateness. -Additionally, management should ensure that all employees involved in user provisioning are trained on the established process.	IT Management/HR	LOSFA's existing procedures cover the removal of terminated employees and modification to access of existing employees from our network and our mid-range systems; it does not specifically include the applications. IT Management will update the procedures to require LOSFA_Ops to update the user permissions in the Award System via the LAN Request submitted through our Track It system. LOSFA will also perform a clean-up to terminate all employees that are no longer with LOSFA or employees who no longer require access to the Award System. IT Management will also review user access and user role reports on a quarterly basis to determine if any revisions are required. Anticipated Date of Implementation: January 4, 2019

Results: Award System Access (continued)

Observation	Risk	Root Cause	Recommendation	Responsible Party	Management Response
Risk Rating: Moderate					
At the time of testing, the TOPS exception process involved both system and manual components. It was explained that the Legal department was responsible for handling TOPS exceptions, and all documentation was manually obtained and processed. Once all applicable documentation was obtained, TOPS exceptions were presented to committee(s) for approval. After committee(s) approval, the Audit department was responsible for changing the status of the exception within the system to an approved status, which would then make the student eligible for TOPS. While the manual components of the process allow for segregation of duties, the system did not, as described below: - It was explained that any user with access to the "LOSFA-Legal" role could change the status of TOPS exceptions to eligible within the system, and all employees in the Legal department were granted access to this role. - In addition, the IT group also had access to the "LOSFA - Legal" role, and as such, had the ability to change the status of TOPS exceptions to eligible. Furthermore, it appears there was no periodic review of activity logs in the system to detect any unauthorized status changes.	-TOPS exceptions may be inappropriately and/or inaccurately made eligible in the system	- Roles within the system were not designed and granted to allow for proper segregation of duties in the TOPS exception approval process.	- To allow for the appropriate segregation of duties in the system, management should consider updating LOSFA- Legal role to remove access to change the status of TOPS exceptions to eligible. - Management should consider limiting the IT group's access to this functionality in the system. In the event that removing access for either LOSFA - Legal or IT Group is not feasible, management should consider performing an independent periodic review of the system user activity log(s) to ensure that only authorized individuals have moved TOPS exceptions to eligible in the system.	IT Management /Legal	LOSFA Programs will update the LOSFA_Legal user role to remove the ability to set the status of TOPS exceptions to approved. By removing this function from the LOSFA_Legal role, the LOSFA_IT staff will no longer have access. A new role will be created for LOSFA_Audit to retain access to set the status of TOPS exceptions to approved. Anticipated Date of Implementation: January 18, 2019

Results: Award System Change Management

Observation	Risk	Root Cause	Recommendation	Responsible Party	Management Response
Risk Rating: Low					
It was explained that updates to the Award System were submitted via change requests through a ticketing system (Track-It), which captured details of the change to be made, the requestor, dates submitted and completed, and any other relevant notes. However, it appears that a formal change management policy had not been documented. Additionally, while approvals of changes were kept in email archives, approvals were not documented in the ticketing system.	- Unapproved system changes may be implemented -Potential for inaccurate changes to rules engines/tables that may impact eligibility determinations in the system	- Lack of a documented process for change management	-Management should consider developing and documenting a formal change management policy. Additionally, management should consider evaluating the system's workflow capabilities that would require appropriate approvals in the system prior to implementing change in the production environment. In the event management determines that system approvals are not feasible, management should consider implementing monitoring controls, such as performing a periodic review of all changes implemented to ensure the change(s) were supported and implemented as requested. At a minimum, changes having a significant impact on the system should receive additional levels of review/approval.	IT Management	Our existing policy requires that all program changes are submitted by the users via the Track It system. IT will develop and document a more formal change management policy for the Award System. The policy will include the submission of a document specifying the detailed description of the specifications requiring modifications or enhancements and an approval by the next level supervisor (and attorney where applicable). This document will be included in the Track It. Currently as an internal control, IT Management gets an email regarding all development updates to the production version of the Award System. Additionally, IT Management receives an email of all changes that are made to the Award System. This email is reviewed daily for all changes that are made with appropriate comments by the developers. IT Management will continue this practice. Anticipated implementation date: February 1, 2019

P&N
Postlethwaite & Netterville

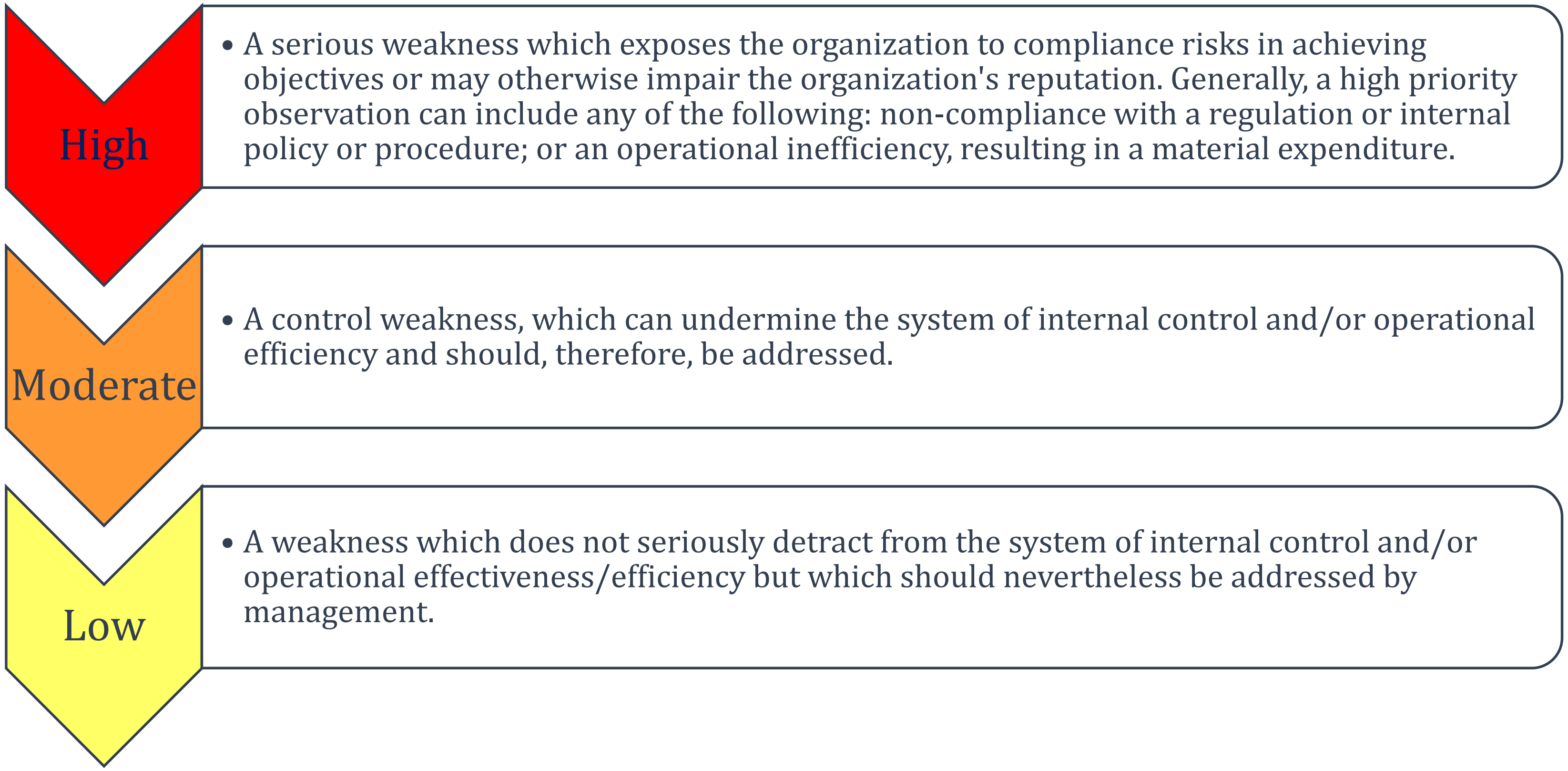
Results: Award System Change Management (continued)

Observation	Risk	Root Cause	Recommendation	Responsible Party	Management Response
Risk Rating: Low					
User acceptance testing of any source coding/changes to the Award System was not performed in the test environment. Instead, results generated by the system were exported by IT from the test environment, manually formatted and provided to the Scholarship & Grants (S&G) division for review. After the user acceptance testing was completed, approval was provided by S&G for changes to be implemented into production by IT. In addition to the user acceptance testing as described above, management explained that S&G division also performs a review on a sample of records in the production environment prior to the issuance of award notifications.	-Potential for inappropriate or unintended changes to be undetected and implemented through the Award System	- Lack of change management process requiring testing of changes made to be performed independently by the user in the test environment	- Management should consider requiring the review of implemented changes to be performed independently by the user directly in the test environment. In the event management determines this is not feasible, management should consider implementing additional procedures to verify that the exported results have not been altered from the results in the test environment (i.e. IT should explore if the system can generate a pre-formatted, read only report that can then be directly retrieved by S&G from the test environment, or at a minimum, S&G may physically observe IT retrieve, format and send the results to S&G for user acceptance testing).	S&G and/or IT Department(s)	IT has reviewed the existing process of generation of test data in spreadsheets for efficient review and acknowledgement of testing results. We have found that the tool can be updated to set the directory of the spreadsheets to one that is accessible by SG. The process will include IT submitting the job to create the test results and the process will automatically save the generated file into this new directory. IT will no longer manipulate the spreadsheet (e.g., change column headers, remove blank columns, adjust column/row size, etc.) unless in the presence of the SG employee. This process will also be documented in our formal change management policy. Anticipated implementation date: December 28, 2018

P&N
Postlethwaite & Netterville

Appendix A: Risk Rating Definitions

Risk ratings were assigned as follows:



High

- A serious weakness which exposes the organization to compliance risks in achieving objectives or may otherwise impair the organization's reputation. Generally, a high priority observation can include any of the following: non-compliance with a regulation or internal policy or procedure; or an operational inefficiency, resulting in a material expenditure.

Moderate

- A control weakness, which can undermine the system of internal control and/or operational efficiency and should, therefore, be addressed.

Low

- A weakness which does not seriously detract from the system of internal control and/or operational effectiveness/efficiency but which should nevertheless be addressed by management.

Appendix B:
Assumptions and Limiting Conditions

Our procedures were not designed to detect fraud, to constitute a financial statement audit, review, compilation, or to provide assurance on the internal controls or information provided. Accordingly, we will not express an opinion or conclusion, nor provide any other form of assurance on the completeness and accuracy of the information. Additionally, the projection of any conclusions, based on our findings, to past or future periods is subject to the risk that changes may have occurred during the passage of time that may alter the validity of such conclusions. Furthermore, the projection of any conclusions, based on our findings, to the whole population is subject to the risk that the samples selected may not accurately reflect the population as a whole.

This engagement was conducted in accordance with the *American Institute of Certified Public Accountants' Statement on Standards for Consulting Services (SSCS) and the International Standards for the Professional Practice of Internal Auditing (Standards).*

P&N
Postlethwaite & Netterville

Appendix C: Transmittal Letter

December 20, 2018

Regent Jay Seale
Audit Committee Chair
Louisiana Board of Regents
1201 N. Third Street, Suite 6-200
Baton Rouge, LA 70802

Dear Regent Seale:

As presented in this enclosed report, Postlethwaite & Netterville, APAC (P&N) has completed our internal audit of LOSFA's TOPS eligibility and renewals processes. On the pages above, this report provides: 1) the procedures performed, 2) a summary of the observations noted during our engagement, 3) recommended actions to consider related to the TOPS processes.

These recommendations are only for your consideration, and are not intended to be implemented without management's thorough understanding and acceptance.

P&N appreciates the cooperation and assistance provided by LOSFA's personnel during this engagement. We sincerely appreciate this opportunity to be of service to you. Please do not hesitate to contact us if you have any questions related to this report or any other matters.

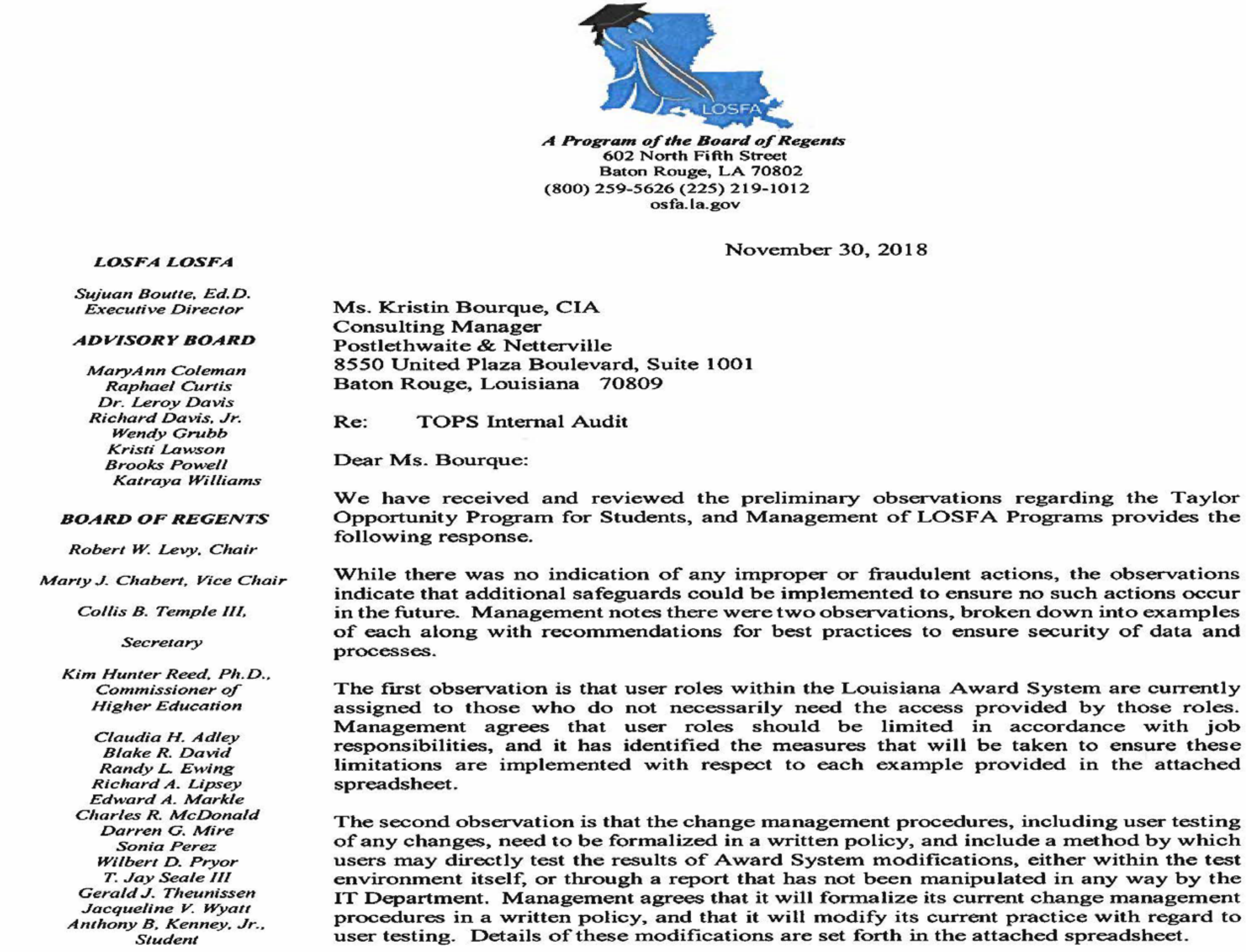
Sincerely,

Postlethwaite & Netterville, APAC

POSTLETHWAITE & NETTERVILLE, APAC

Appendix D: Management Response Letter

**Letter accompanied management responses noted in the tables on pages 5-9 of this report.*



LOSFA

A Program of the Board of Regents
602 North Fifth Street
Baton Rouge, LA 70802
(800) 259-5626 (225) 219-1012
osfa.la.gov

November 30, 2018

Ms. Kristin Bourque, CIA
Consulting Manager
Postlethwaite & Netterville
8550 United Plaza Boulevard, Suite 1001
Baton Rouge, Louisiana 70809

Re: TOPS Internal Audit

Dear Ms. Bourque:

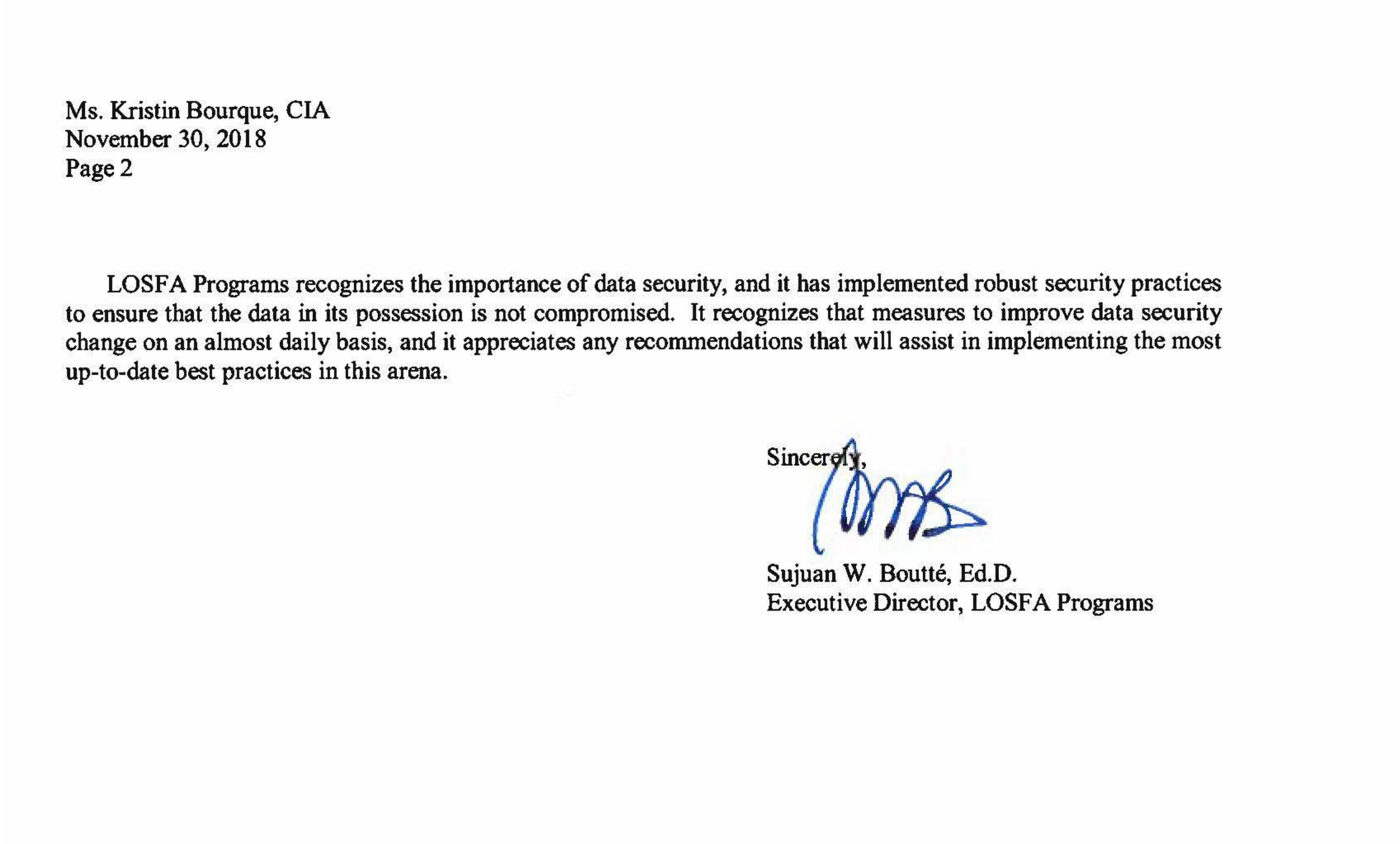
We have received and reviewed the preliminary observations regarding the Taylor Opportunity Program for Students, and Management of LOSFA Programs provides the following response.

While there was no indication of any improper or fraudulent actions, the observations indicate that additional safeguards could be implemented to ensure no such actions occur in the future. Management notes there were two observations, broken down into examples of each along with recommendations for best practices to ensure security of data and processes.

The first observation is that user roles within the Louisiana Award System are currently assigned to those who do not necessarily need the access provided by those roles. Management agrees that user roles should be limited in accordance with job responsibilities, and it has identified the measures that will be taken to ensure these limitations are implemented with respect to each example provided in the attached spreadsheet.

The second observation is that the change management procedures, including user testing of any changes, need to be formalized in a written policy, and include a method by which users may directly test the results of Award System modifications, either within the test environment itself, or through a report that has not been manipulated in any way by the IT Department. Management agrees that it will formalize its current change management procedures in a written policy, and that it will modify its current practice with regard to user testing. Details of these modifications are set forth in the attached spreadsheet.

Appendix C: Management Response Letter (Continued)



Ms. Kristin Bourque, CIA
November 30, 2018
Page 2

LOSFA Programs recognizes the importance of data security, and it has implemented robust security practices to ensure that the data in its possession is not compromised. It recognizes that measures to improve data security change on an almost daily basis, and it appreciates any recommendations that will assist in implementing the most up-to-date best practices in this arena.

Sincerely,

Sujuan W. Boutté, Ed.D.
Executive Director, LOSFA Programs

P&N Contact Information:

Laura Soileau, Director

lsoileau@pncpa.com

Ana Krivic, Associate Director

akrivic@pncpa.com

Kristin Bourque, Manager

kbourque@pncpa.com

Mary Minor Butler, Senior

mbutler@pncpa.com

P&N
Postlethwaite & Netterville

P&N

Postlethwaite & Netterville

A Professional Accounting Corporation