University of North Florida

Office of Internal Auditing

PERFORMANCE FUNDING AUDIT

For the Year Ending 2016

Audit Summary

Audit #	AUD2016001
Report Date	February 23, 2016
Fiscal Year	2016

Initial Risk Rating[1]	**Critical**	**High**	**Moderate**	**Low**
Report Rating[2]	**No/Low Assurance**	**Limited Assurance**	**Reasonable Assurance**	**High Assurance**

Reportable Items Rating Summary[3]

Process Reviewed	**Critical**	**High**	**Moderate**	**Low**
Data Admin appointment				
Submission completeness				
Policies & procedures				1
System & data access			1	
Data accuracy				
Data Admin statement				
Data consistency				
Resubmissions				
Total	**2**		**1**	**1**

Distribution

Various	Finance & Audit Committee
John Delaney	President
Tom Serwatka	Chief of Staff
Shari Shuman	VP – Administration and Finance
Scott Bennett	AVP – Administration and Finance
Earle Traynham	Provost
Jay Coleman	Associate Provost
Mauricio Gonzalez	Vice President – Student Affairs
Tim Giles	Director – Continuing Education
Bob Wood	Dean – Continuing Education
Jim Stultz	State Auditor General - Audit Manager
Randy Arend	State Auditor General - Audit Supervisor

Contact(s)

Audit Director:	Robert Berry, CPA, CIA, CISA, CCEP
Auditor:	Jenny Johnson
IT Auditor	Khareem Gordon

[1]The Initial Risk Rating measures the inherent risk and is determined during the annual risk assessment process.
[2]The Report Rating is the residual risk based on auditing management's controls and processes. Report Ratings are defined in Attachment 2 on page 12
[3]Reportable Items rating scale is defined in Attachment 1 on page 11

-Page Intentionally Blank-

Table of Contents

Executive Summary.

Background

The Florida Board of Governors (BOG) is authorized to "operate, regulate, control, and be fully responsible for the management of the whole University system". The BOG monitors Florida State University System (SUS) schools activity, and awards funding, using the results of 10 performance measurements. The measurements derive partially from data prepared the universities and others obtained from and prepared by the BOG. The BOG requests that each University perform an audit of the processes to ensure the completeness, accuracy, and timeliness of data submissions. This report summarizes audit results.

Conclusion

The University has adequate processes to provide reasonable assurance that data is complete, accurate and timely.

Objectives & Scope

The purpose of the audit was to assess the effectiveness of processes designed to ensure the completeness, accuracy, and timeliness of data submissions to the BOG that support the University's Performance-Based Funding (PBF) Metrics. The BOG extracts data from files the University provides and performs additional calculations. The University is not involved in these extractions and additional calculations. Therefore, these items are not included in the audit scope.

The BOG did not provide a uniform audit program, however, the BOG requested that, at a minimum, the audit includes reviewing the following:

1. The appointment of the Data Administrator by the University president and his/her duties as outlined in the position description.

2. The processes used to ensure the completeness, accuracy and timely submission of data to the BOG.

3. Any available documentation including policies, procedures, desk manuals to assess their adequacy for data submissions.

4. System access controls and user privileges to determine if data is adequately secured from unauthorized access.

5. The accuracy of data.

6. The veracity of the University Data Administrator's data submission statements that indicate, "I certify that this file/data represents the position of this University for the term being reported."

7. The consistency of data submissions with the data definitions and guidance provided by the Board of Governors through the Data Committee and communications from data workshops.

8. The University Data Administrator's data resubmissions to the Board of Governors with a view toward ensuring these resubmissions are both necessary and authorized. This review should also evaluate how to minimize the need for data resubmissions.

Issue Summary

The following is a summary of the issues resulting from this audit engagement. These items are discussed in detail in the "Detailed Observations, Recommendations & Management Responses" section of the report.

See *Attachment #1 – Issue Classifications* for issue ratings.

Critical Issues

None

High Risk Issues

None

Executive Summary.

Moderate Risk Issues

1. There were two terminated employees with access to the virtual folder containing performance funding data.

Low Risk Issues

1. Policies and procedures need updating.

Follow Up

Please note there is a structured open items follow-up process. Follow-up occurs based on the target completion dates established by management. As always, the Office of Internal Auditing is available to partner with staff to discuss feasible risk mitigating control processes. Please feel free to contact us should you wish to discuss any aspect of the audit report.

Management's Responsibilities for Internal Controls

Management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls. This and any internal audit enhances and complements, but does not substitute management's continuing emphasis on control activities.

Inherent Limitations in Internal Controls Systems

There are inherent limitations in all internal control systems. As a result, errors or irregularities may occur and not be detected. Specific limitation examples include but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and cost/benefit constraints.

Acknowledgement

We would like to express our gratitude to your management and staff for their assistance and cooperation during the audit. We will request that your department complete a Customer Survey. You will receive the survey shortly after the distribution of the final report.

Performance Funding Audit

Detailed Observations & Recommendations

Detailed Observations, Recommendations & Management Responses.

Moderate Risk Items

Issue Number	1	**Issue Rating**	**Moderate**	**Open Date**	2/19/2016	**Responsible Party**	Information Technology
				Due Date	TBD		

Issue	Recommendation	Management Action Plan
The organization does not sufficiently revoke user access to folders upon employee termination. There are several terminated employee user ids with access to the folder containing performance based funding data. Additionally, there are several unassociated SIDs[1] with access to this data. The SID is a unique name (alphanumeric character string) that is used to identify an object, such as a user or a group of users. The SID works in conjunction with the username/password to control access to resources. Windows grants or denies access and privileges to resources based on ACLs[2], which use SIDs to uniquely identify users and their group memberships. When a user requests access to a resource, the user's SID is checked by the ACL to determine what the user allowed to view, create or alter. Unassociated SIDs are those that are not associated with a username/password. The terminated network access reduces the risk of unauthorized access, however, remaining underlying access permissions (i.e. SIDs) may still leave network resources vulnerable. [1]SID – Security Identifier> A security identifier (SID) is a unique value used to identify a trustee. Each account has a unique SID that is stored in a security database. [2]Short for access control list, a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file.	There is no quick fix for this risk. It is a massive multiyear undertaking in which management would need to (1) clean up access issues for each folder/file on the network (2) develop and implement a process to remove permissions going forward and (3) develop a process where resource owners can be aware of and have accountability for who has access to their information.	Security Identifiers (commonly abbreviated as SIDs) are a unique identifier used by Microsoft's Windows operating systems to tie security attributes to a user, group or other security principal. The SID is immutable, meaning that it is unique for the lifetime of the principal. Windows grants access to resources based on access control lists, which use SIDs to uniquely identify users and their group memberships. In order to log in and receive an access token, users must first authenticate using their user ID and password. This is then parsed by the authentication system and the SID is used to match the security rights to the user. Orphaned SIDs occur when a security principal's account object is deleted, but they have been granted explicit security rights to an object in the system, e.g. a file or directory. These orphaned SIDs persist unless specifically targeted and cleaned up. We respectfully disagree with the finding that orphaned SIDs represent a discernible security risk. This assertion is backed up by two pieces of information. One is that the SID itself cannot be used to gain access to resources. It would still require a user object with an associated password in order to gain access. If a malicious user or process has access to a user account and valid password, which would be required to leverage a SID, then the question of orphaned SIDs becomes moot. An attacker with a valid account and password would of course be able

Detailed Observations, Recommendations & Management Responses.

Issue Number	1	**Issue Rating**	**Moderate**	**Open Date**	2/19/2016	**Responsible Party**	Information Technology
				Due Date	TBD		

Issue	Recommendation	Management Action Plan
		to gain access. The solitary SID by itself simply cannot be used in this manner. Second is the long standing use of SIDs with no known abuse that would allow someone to gain system access. Microsoft has a large number of standardized SIDs, including built-in administrator accounts, with defined SIDs that are well-known. If there were a way to abuse these, then there would effectively be no security restrictions anywhere within a Windows OS. This is clearly not the case. Even on a brand new computer, there are dozens of SIDs (e.g. S-1-1-0, the Everyone group), some of which are 'orphaned'. One item that may be seen as a mitigating component, although not directly intended as a response to this specific issue, is that the University is in the process of conducting a comprehensive review of the account lifecycle with Human Resources and other stakeholders. It is expected that there may be some changes as a result of any findings that may help in this specific instance. Naturally, as with anything this sensitive, we will continue to monitor any developments in this area. Should the situation change, we stand ready to engage in an appropriate response.

Detailed Observations, Recommendations & Management Responses.

Low Risk Items

Issue Number	6	**Issue Rating**	Low	**Open Date**	2/19/2016	**Responsible Party**	Institutional Research
				Due Date	TBD		

Issue	Recommendation	Management Action Plan
Many of the processes/procedures for extracting and submitting Performance Based Funding data to the Board of Governors are not formally documented. This process is fairly complex. Historically, one person performed the data extraction, validation and submission. Two people inherited the process without detailed procedures. Fortunately, these staff members are competent and have been able to meet deadline and expectations. Additionally, these individuals have made improvements to the process. A process this critical should be fully documented so that staff, current and future, can easily identify the objectives and produce accurate deliverables.	Management should ensure that Performance Based Funding processes are documented and disseminated to appropriate personnel.	Procedures are currently being developed.

Attachments

Attachment #1 – Issue Classifications.

Attachment #1 – Issue Classifications/Ratings

The following categories are used to rate each of the issues presented in this report.
These ratings represent the risk each issue poses to the overall effectiveness and efficiency of the specific function audited.

Rating	Description
Critical	This item should be addressed with a sense of urgency. Processes and controls are either nonexistent or fail to effectively manage risks. For example, the current processes do not sufficiently prevent or detect asset misappropriation, noncompliance with regulations, transactional errors, etc. Finally, the underlying assets affected (finances, reputation, property, stakeholders, etc) are considered significant (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc).
High	This item should be addressed with high priority. Formal processes and controls may exist, however, they fail to effectively manage risks. For example, the current processes do not sufficiently prevent or detect asset misappropriation, noncompliance with regulations, transactional errors, etc. Finally, the underlying assets affected (finances, reputation, property, stakeholders, etc) are considered significant (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc) but is not substantial enough to be considered critical.
Moderate	Formal or informal processes and controls may exist, however, they are only partially effective at managing risks. For example, prevention or detection of unwanted outcomes may occur, but, the prevention does sufficiently cover the population at risk or the detection is not timely. Finally, the underlying assets affected (finances, reputation, property, stakeholders, etc) are moderately significant (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc).
Low	Formal process and controls exist and are partially effective at managing risks. However, the underlying assets affected (finances, reputation, property, stakeholders, etc) are minimal (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc).

Attachment #1 – Issue Classifications.

Attachment #2 – Report Classifications/Ratings

The following categories represent the final, comprehensive rating for the area reviewed.
The issues presented in this report are considered collectively in developing a final rating.

Rating	Description
No/Low Assurance	Several significant deficiencies exist in the system of processes designed to direct activities. Current collective processes do not provide reasonable assurance that assets are complete, accurate, secure, in compliance with regulations or uphold the organization's brand. Underlying assets are of significant value (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc). A corrective action plan should be undertaken immediately and given the highest priority.
Limited Assurance	At least one significant deficiency exists in the system of processes designed to direct activities. Collective processes do not provide reasonable assurance that assets are complete, accurate, secure, in compliance with regulations or uphold the organization's brand. Underlying assets are of significant value (i.e. dollar amount, number of stakeholders impacted, potential fines, extent of media exposure etc).
Reasonable Assurance	Processes are operating in a manner that provides reasonable assurance that most **major** risks will be mitigated. There may be some activities that do not provide reasonable assurance that assets are complete, accurate, secure, in compliance with regulations or uphold the organization's brand. However, these are not major to the process as a whole.
High Assurance	Processes are operating in a manner that provides reasonable assurance that most risks will be mitigated. The collective issues in this report are considered minor.

End Report

STATE UNIVERSITY SYSTEM of FLORIDA
Board of Governors

Performance Based Funding

Data Integrity Certification

Name of University: University of North Florida

Period Ending: March 1, 2016

INSTRUCTIONS: Please respond "Yes," "No" or "N/A" in the blocks below for each representation. Explain any "No" or "N/A" responses to ensure clarity of the representation and include copies of supporting documentation as attachment(s).

Performance Based Funding Data Integrity Certification Representations				
Representations	**Yes**	**No**	**N/A**	**Comment / Reference**
1. I am responsible for establishing and maintaining, and have established and maintained, effective internal controls and monitoring over my university's collection and reporting of data submitted to the Board of Governors Office which will be used by the Board of Governors in Performance Based Funding decision-making.	☒	☐	☐	
2. These internal controls and monitoring activities include, but are not limited to, reliable processes, controls, and procedures designed to ensure that data required in reports filed with my Board of Trustees and the Board of Governors are recorded, processed, summarized and reported in a manner which ensures its accuracy and completeness.	☒	☐	☐	
3. In accordance with Board of Governors Regulation 1.001(3), my Board of Trustees has required that I maintain an effective information system to provide accurate, timely, and cost-effective information about the university, and shall require that all data and reporting requirements of the Board of Governors are met.	☒	☐	☐	
4. In accordance with Board of Governors Regulation 3.007, my university shall provide accurate data to the Board of Governors Office.	☒	☐	☐	
5. In accordance with Board of Governors Regulation 3.007, I have	☒	☐	☐	

Performance Based Funding
Data Integrity Certification

Performance Based Funding Data Integrity Certification Representations				
Representations	**Yes**	**No**	**N/A**	**Comment / Reference**
appointed a Data Administrator to certify and manage the submission of data to the Board of Governors Office.				
6. In accordance with Board of Governors Regulation 3.007, I have tasked my Data Administrator to ensure the data file (prior to submission) is consistent with the criteria established by the Board of Governors Data Committee. The due diligence includes performing tests on the file using applications/processes provided by the Board of Governors Information Resource Management (IRM) office.	☒	☐	☐	
7. When critical errors have been identified, through the processes identified in item #6, a written explanation of the critical errors was included with the file submission.	☒	☐	☐	
8. In accordance with Board of Governors Regulation 3.007, my Data Administrator has submitted data files to the Board of Governors Office in accordance with the specified schedule.	☒	☐	☐	
9. In accordance with Board of Governors Regulation 3.007, my Data Administrator electronically certifies data submissions in the State University Data System by acknowledging the following statement, "Ready to submit: Pressing **Submit for Approval** represents electronic certification of this data per Board of Governors Regulation 3.007."	☒	☐	☐	
10. I am responsible for taking timely and appropriate preventive / corrective actions for deficiencies noted through reviews, audits, and investigations.	☒	☐	☐	
11. I recognize that the Board's Performance Based Funding initiative will drive university policy on a wide range of university operations - from admissions through graduation. I certify that university policy changes and decisions impacting this initiative have been made to bring the university's operations and practices in line with State University System Strategic Plan goals and have not been made for the	☒	☐	☐	

Performance Based Funding
Data Integrity Certification

Performance Based Funding Data Integrity Certification Representations				
Representations	**Yes**	**No**	**N/A**	**Comment / Reference**
purposes of artificially inflating performance metrics.				

I certify that all information provided as part of the Board of Governors Performance Based Funding Data Integrity Certification is true and correct to the best of my knowledge; and I understand that any unsubstantiated, false, misleading or withheld information relating to these statements render this certification void. My signature below acknowledges that I have read and understand these statements. I certify that this information will be reported to the board of trustees and the Board of Governors.

Certification: _____ Date 02/25/16
President

I certify that this Board of Governors Performance Based Funding Data Integrity Certification has been approved by the university board of trustees and is true and correct to the best of my knowledge.

Certification: _____ Date 02/25/16
Board of Trustees Chair