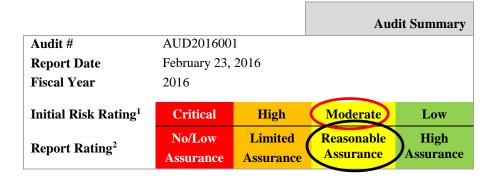
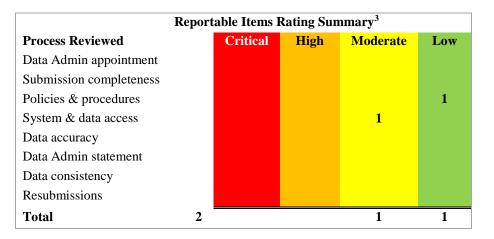
PERFORMANCE FUNDING AUDIT

For the Year Ending 2016





		Distribution
Various	Finance & Audit Con	nmittee
John Delaney	President	
Tom Serwatka	Chief of Staff	
Shari Shuman	VP – Administration	and Finance
Scott Bennett	AVP – Administratio	on and Finance
Earle Traynham	Provost	
Jay Coleman	Associate Provost	
Mauricio Gonzalez	Vice President – Stud	lent Affairs
Tim Giles	Director – Continuin	g Education
Bob Wood	Dean – Continuing E	ducation
<u>Jim Stultz</u>	State Auditor Genera	l - Audit Manager
Randy Arend	State Auditor Genera	l - Audit Supervisor

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

¹The Initial Risk Rating measures the <u>inherent</u> risk and is determined during the annual risk assessment process.

²The Report Rating is the residual risk based on auditing management's controls and

processes. Report Ratings are defined in Attachment 2 on page 12

³Reportable Items rating scale is defined in Attachment 1 on page 11

Office of Internal Auditing

-Page Intentionally Blank-

Table of Contents

Detailed Observations & Recommendations	б
Moderate Risk Items	7
Low Risk Items	9
Attachments	10
Attachment #1 – Issue Classifications/Ratings	11
Attachment #2 – Report Classifications/Ratings	



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 <u>reasonable</u> 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 <u>Attachment #1 – Issue Classifications</u> 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	Open Date 2/19/2016	Responsible
Issue Number 1 Rating Moderate	Due Date TBD	Party Information Technology
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

	Issue		Open Date	2/19/2016	Responsible	
Issue Number 1	Rating	Moderate	Due Date	TBD	Party	Information Technology
Issue			Recommendation		Management Actio	
					to gain access. The s used in this manner.	solitary SID by itself simply cannot be
					abuse that would alle Microsoft has a large including built-in ad SIDs that are well-kn these, then there wou restrictions anywher not the case. Even of	tanding use of SIDs with no known ow someone to gain system access. e number of standardized SIDs, ministrator accounts, with defined nown. If there were a way to abuse uld effectively be no security e within a Windows OS. This is clearly n a brand new computer, there are S-1-1-0, the Everyone group), some of l'.
					although not directly issue, is that the Uni a comprehensive rev Human Resources an that there may be so that may help in this Naturally, as with an to monitor any devel	hything this sensitive, we will continue lopments in this area. Should the e stand ready to engage in an

Detailed Observations, Recommendations & Management Responses.

Detailed Observations, Recommendations & Management Responses.

	Low	Risk Items		
	Open Date	2/19/2016	Responsible	
ssue Number 6 Issue Rating Low	Due Date	TBD	Party	Institutional Research
2010	Recommendation		Management Action P	lon
Any of the processes/procedures for extracting and abmitting Performance Based Funding data to the oard of Governors are not formally documented. his process is fairly complex. Historically, one erson performed the data extraction, validation and abmission. Two people inherited the process without detailed procedures. Fortunately, these staff members are competent and have been able to meet eadline and expectations. Additionally, these ndividuals have made improvements to the process. A process this critical should be fully documented so nat staff, current and future, can easily identify the bjectives and produce accurate deliverables.	Recommendation Management should ensu Based Funding processes disseminated to appropria	are documented and	Management Action P Procedures are currently b	

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 <u>most</u> risks will be mitigated. The collective issues in this report are considered minor.

End Report