REPORT NO. 2015-101
FEBRUARY 2015

FLORIDA STATE UNIVERSITY

NORTHWEST REGIONAL DATA CENTER

DATA CENTER OPERATIONS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE NORTHWEST REGIONAL DATA CENTER

The Florida State University (University) is the administrative host institution and fiscal agent for the Northwest Regional Data Center (NWRDC). The NWRDC Charter establishes a Policy Board (Board) as the governing body for NWRDC. The Board's primary function is to establish and promulgate policies for the NWRDC. The Executive Director, who is selected by the Board, is responsible for the overall administration of the NWRDC.

Board members and the customer entities represented and the Executive Director who served during the period of our audit are listed below:

Board Member	Customer Entity Represented
Mehran Basiratmand, Chair	Florida Atlantic University
Michael Barrett, Vice Chair	Florida State University
Michael Dieckmann, Non-Voting Member	University of West Florida
Ted Duncan	Department of Education
Levis Hughes, Management Committee Member	Department of Education
Michael A. James, Non-Voting Member	Florida A&M University
Gene Kovacs	State University System of Florida Board of Governors
Damu Kuttikrishnan	Department of Revenue
Henry Martin, K-12 Representative, Management Committee Member	Walton County School District
Donald J. Muccino	Florida Virtual Campus
Peter M. Taylor, Board Member Emeritus, Non-Voting Member	

Tim Brown, Executive Director

The audit team leader was T. Wayne Revell, CISA, and the audit was supervised by Chris Gohlke, 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

FLORIDA STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

SUMMARY

Section 1004.649, Florida Statutes, outlines the provisions for the Northwest Regional Data Center (NWRDC) at the Florida State University (University) to provide data center services to its State agency customers. Our operational audit focused on evaluating the effectiveness of selected information technology (IT) controls relevant to the NWRDC data center operations. We also determined the status of corrective actions regarding prior audit findings included in our report No. 2013-012 that were applicable to the scope of this audit.

Our audit disclosed areas in which improvements in IT controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: The NWRDC had not established written procedures regarding aspects of the hardware and systems software change process, selected password parameters, certain physical security controls, and performance monitoring.

Finding No. 2: The NWRDC did not have a mechanism in place to ensure that all hardware and systems software changes were properly authorized, tested, approved, and implemented. Also, the NWRDC did not maintain documentation of the testing and implementation of hardware and systems software changes.

Finding No. 3: Certain NWRDC security controls related to user authentication and the disclosure of sensitive security information needed improvement.

Finding No. 4: Some NWRDC employees had unnecessary physical access privileges to the off-site backup storage vault.

BACKGROUND

The NWRDC is an auxiliary operation of the University and is headed by a Policy Board (Board), consisting of representatives from customer entities. The Board selects an Executive Director to be responsible for the daily operation of the data center. In its capacity as the administrative host institution and fiscal agent, the University is the contracting authority for the NWRDC and provides legal support and executive oversight. All NWRDC positions are filled with employees of the University and follow University policies for payroll, leave, and other personnel actions.

The NWRDC provides a variety of IT services to its customer entities, including facilities and infrastructure services, storage and recovery services, network and mainframe services, and security and other managed services. The customer entities consist of State agencies, universities, colleges, school districts, city and county governments, and various consortia and non-profit groups that contract with the NWRDC for the aforementioned IT services. The NWRDC operates on a cost-recovery basis whereby the NWRDC bills the customer entities for a portion of its operating costs associated with the specific services provided to each customer entity. Lists of the NWRDC customer entities and services offered by the NWRDC are included in this report as EXHIBITS A and B, respectively.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Procedures

Effective management includes the establishment of procedures that describe management's expectation for controlling data center operations. Written procedures and other related documentation help ensure that management directives are clearly communicated, understood, accepted, and followed by staff. Our audit disclosed that the NWRDC had not established written procedures relating to hardware and software changes, selected password parameters, certain physical security controls, and performance monitoring as described below:

- The NWRDC did not have written procedures addressing the detailed requirements for documenting and tracking the testing and implementation of hardware and systems software changes. Additionally, the NWRDC lacked procedures for a periodic review process to prevent or detect unauthorized changes. See related issues in Finding No. 2. A similar finding was noted in our report No. 2013-012.
- The NWRDC did not have written security control procedures defining password parameters for the NWRDC network and open systems.
- The NWRDC did not have detailed written procedures regarding the granting and discontinuing of physical access privileges to data center resources. See a related issue in Finding No. 4.
- Although the NWRDC monitored performance, the NWRDC did not have written procedures for mainframe or open systems performance monitoring. A similar finding was noted in our report No. 2013-012.

Without written procedures, the risk is increased that hardware and systems software changes, password parameter security controls, physical security controls, and mainframe or open systems performance monitoring may not be done or followed consistently and in a manner pursuant to management's expectations and that performance problems, should they occur, may not be timely detected and corrected.

Recommendation: The NWRDC should establish written procedures to address aspects of the hardware and software change process, selected password parameters, certain physical security controls, and performance monitoring.

Finding No. 2: Change Controls

Effective change controls help ensure that all changes are tracked, documented, and approved. Comprehensive documentation includes documentation that changes were successfully tested and functioned as intended prior to being implemented.

The NWRDC provided us with a listing of hardware and systems software changes that had been manually entered by staff into the *RemedyForce* system used for tracking the authorization, testing, approval, and implementation of hardware and systems software changes. While the NWRDC was able to provide logs of all hardware and system software changes, the NWRDC did not have a mechanism in place to ensure that all changes to hardware and systems software were entered and tracked in the *RemedyForce* system. Additionally, through our inquiry and other audit procedures, we determined that the NWRDC did not maintain documentation supporting the testing and implementation of hardware and systems software changes. A similar finding was noted in our report No. 2013-012.

Without a mechanism to ensure that all changes to hardware and systems software changes are properly authorized, tested, approved, and implemented and documentation related to the testing and implementation of hardware and systems software changes is maintained, the risk is increased that erroneous or unauthorized changes could be moved into the production environment without timely detection.

Recommendation: The NWRDC should establish a mechanism to provide reasonable assurance that all hardware and systems software changes are properly authorized, tested, approved, and implemented. In addition, the NWRDC should ensure that the testing and implementation of hardware and systems software changes is properly documented.

Finding No. 3: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain NWRDC security controls related to user authentication and the disclosure of sensitive security information that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising NWRDC customer-entity data and IT resources. However, we have notified appropriate NWRDC management of the specific issues. Similar findings were noted in our report No. 2013-012. Without adequate security controls related to user authentication and the disclosure of sensitive information, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: The NWRDC should improve security controls related to user authentication and the disclosure of sensitive information to ensure the continued confidentiality, integrity, and availability of customer-entity data and IT resources.

Finding No. 4: Physical Security

Effective security controls ensure that access to facilities is limited to individuals having a legitimate need for the access to perform their job duties. The effectiveness of physical security controls depends on the effectiveness of the entity's policies and practices pertaining to the overall facility and to areas housing sensitive information technology components.

We reviewed the physical access privileges of 22 NWRDC employees who had been granted physical access privileges to the off-site backup storage vault (off-site vault) as of November 13, 2014, to determine that physical access privileges to the off-site vault were appropriate. For 3 of 22 employees' physical access privileges we reviewed, we determined that physical access privileges to the off-site vault were not necessary. In response to our inquiry, NWRDC management indicated that the physical access privileges would be removed for the 3 employees. When physical access privileges to the off-site vault are not appropriately restricted, there is an increased risk that individuals may gain access to confidential or exempt information.

Recommendation: The NWRDC should provide for periodic review to ensure that physical access privileges to the off-site vault are appropriately restricted.

PRIOR AUDIT FOLLOW-UP

The NWRDC had taken corrective actions for five of the eight findings included in our report No. 2013-012 that were applicable to the scope of this audit. Corrective actions were not taken for one of the eight prior audit findings

as described in the findings above. In addition, two prior audit findings were only partially corrected. One prior audit finding included in our report No. 2013-012 was not in the scope of this audit.

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 October 2014 through January 2015 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational 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. An additional objective was to determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2013-012 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to the NWRDC operations during the period October 2014 through December 2014. The audit included selected general IT controls related to security controls and operational controls.

This audit was designed to identify, for the IT 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 IT operational policies, procedures, or practices. The focus of this IT operational 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 controls included within the scope of the audit, the 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 our audit; obtaining an understanding of the IT 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 our audit, we:

- Interviewed NWRDC personnel.
- Obtained an understanding of the statutory requirements, contractual obligations, and service-level agreements performance level requirements of the NWRDC's operations.
- Obtained an understanding of the directives, policies, procedures, and processes governing the NWRDC's operations.
- Obtained an understanding of the impact of data center consolidation on the NWRDC's operations.
- Obtained an understanding of the executive management organizational structure of the NWRDC, including the Policy Board structure.
- Obtained an understanding of the organizational structure for management and administration of IT resources including a description of the separation of responsibilities between the NWRDC and customer staff.
- Obtained an understanding of the services provided or offered by the NWRDC.
- Obtained an understanding of performance and capacity monitoring performed by the NWRDC.
- Obtained an understanding of environmental safeguards protecting IT resources.
- Obtained an understanding of the disaster recovery process, including backup procedures.
- Obtained an understanding of systems software and network infrastructure component change controls, including patch management.
- Obtained an understanding of the IT infrastructure and architecture of the NWRDC, including applicable network and component diagrams.
- Obtained an understanding of the logical access control mechanisms employed by the NWRDC for the protection of customer IT resources.
- Obtained an understanding of the physical access controls at the NWRDC for the protection of customer-entity IT resources.
- Obtained an understanding of background screening requirements and processes followed.
- Observed and evaluated the effectiveness of statutory and contractual requirements related to the NWRDC and the Policy Board.
- Observed and evaluated the effectiveness of controls in place to track and report service-level agreement metrics.
- Observed and evaluated the effectiveness of monitoring controls in place to ensure that equipment capacity is not exceeded and performance levels are maintained appropriately.
- Observed and evaluated the effectiveness of environmental safeguards in place to protect IT resources, including fire, water, power, and air conditioning.
- Observed and evaluated the effectiveness of disaster recovery planning and testing and controls in place for continuity of NWRDC operations, including proper tape backup and rotation and provisions for an off-site backup facility. Specifically, we tested 10 of 57 backup tapes stored off-site on October 27, 2014, and November 3, 2014, to determine whether the NWRDC maintained an accurate inventory of on-site and off-site physical backup tapes.

- Observed and evaluated the effectiveness of systems software and network infrastructure component change controls to ensure that only authorized changes are made and that upgrades and patches are timely installed to ensure that IT resources are properly protected. We reviewed two changes to determine that the processes noted were in place.
- Observed and evaluated the effectiveness of logical access controls in place for networking components and systems software administered by the NWRDC to restrict access to authorized personnel. Specifically, we examined 35 User IDs to determine if users' administrative access to the NWRDC systems software was appropriate.
- Observed and evaluated the effectiveness of security controls in place to protect customer-entity IT resources.
- Observed and evaluated the effectiveness of physical access controls to the NWRDC to ensure access had been appropriately limited.
- Observed and evaluated the effectiveness of background screenings for the NWRDC staff who are able to access customer-entity IT resources. Specifically, we tested documentation for 12 of 60 NWRDC staff, including employees and contractors, to determine whether individuals holding positions of special trust had undergone appropriate background checks and fingerprinting.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing 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 those matters requiring corrective action.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated February 13, 2015, the NWRDC Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT C**.

EXHIBIT A
LIST OF NWRDC CUSTOMER ENTITIES AS OF DECEMBER 13, 2014

Higher Education	
Chipola College	New College of Florida
Florida A&M University	Pensacola State College
Florida Atlantic University	Polk State College
Florida Gulf Coast University	St. Thomas University
Florida International University	University of Central Florida
Florida State College at Jacksonville	University of Florida
Florida State University	University of North Florida
Florida State University Foundation	University of South Florida
Florida Virtual Campus	University of West Florida
State Government	
Department of Agriculture	Florida Prepaid College Board
Department of Business and Professional Regulation	Florida Board of Governors
Department of Education	Florida Surplus Lines Service Office
Department of Financial Services	Office of the Auditor General
Department of Highway Safety and Motor Vehicles	Statewide Guardian Ad Litem
Department of Revenue	
K-12 School Districts	
Alexander D. Henderson University School	Santa Rosa County District School Board
Bay County District School Board	St. Johns County District School Board
Escambia County District School Board	Suwannee County District School Board
Florida A&M University Developmental Research School	
Hillsborough County District School Board	
Lee County District School Board	
Leon County District School Board	
Miami-Dade County District School Board	
Nassau County District School Board	
Palm Beach County District School Board	
Panhandle Area Educational Consortium: Calhoun County District School Board Florida State University Schools, Inc. Franklin County District School Board Gadsden County District School Board Gulf County District School Board Holmes County District School Board Jackson County District School Board Jefferson County District School Board Liberty County District School Board Madison County District School Board Taylor County District School Board Wakulla County District School Board Walton County District School Board Washington County District School Board	
Local Government, Health Care, and Other	
City of Tallahassee	Palm Beach County Clerk & Comptroller
City of Jacksonville	Palm Beach County Government
LearnSomething, Inc.	Tallahassee Memorial Healthcare
Orange County Clerk	The Ringling Museum of Art, Florida State University
Orange County Government	

EXHIBIT B
LIST OF SERVICES OFFERED BY THE NWRDC AS OF DECEMBER 13, 2014

Service Category	Service Description
Facilities Services	Raised Floor Space
	Rack Space
	Electrical Circuits
	Collocation Support and Monitoring
	Off-site Collocation
Infrastructure Services	Closed Infrastructure
	Standard Physical Server
	Custom Physical Server Configurations
Storage and Recovery Services	Backup
	Tier 1 Storage
	Tier 2 Storage
	Tier 3 Storage
	Modular Storage
	Remote Replication
	Internal Replication
	Fiber Channel Ports
	IOPS on Demand
Network Services	Network 10 GB Fiber Port
	Network 1 GB Port
	Commodity Internet Access
	Network VPN Tunnel
	VPN Client
	Tallahassee Fiber Loop Right to Use
	Tallahassee Fiber Loop Maintenance
Managed Services	System Administrator (Server)
	System Administrator (Virtual Host)
	Backup System Administrator
	Storage Administrator
	Network Administrator
	Operator
	Personnel
Security Services	Penetration Test
Mainframe Services	Mainframe Processing

EXHIBIT C
MANAGEMENT'S RESPONSE

NWRDC™
Northwest Regional Data Center

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.245.3500 Phone
850.245.3570 Fax

David W. Martin
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

February 13, 2015

Dear Mr. Martin,

Please accept Florida State University's response to your January 22nd letter regarding the recent audit of the Northwest Regional Data Center. As always, please let us know if there are any questions or if we can be of any assistance. Thank you.

Sincerely,

Tim Brown
Executive Director, Northwest Regional Data Center
Florida State University

Cc:
Sam McCall, Chief Audit Officer, Florida State University
Michael Barrett, Assoc. VP and CIO, Florida State University; Vice-Chair of NWRDC Policy Board
Mehran Basiratmand, CTO, Florida Atlantic University; Chair of NWRDC Policy Board

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 1: The NWRDC had not established written procedures regarding aspects of the hardware and systems software change process, selected password parameters, certain physical security controls, and performance monitoring.

Recommendation: The NWRDC should establish written procedures to address aspects of the hardware and software change process, selected password parameters, certain physical security controls, and performance monitoring

FSU\NWRDC Response: NWRDC agrees with this recommendation to update our procedures. In some of the cases mentioned, our practices exceeded our documentation. Even though our practices may have been correct, we agree with the need to have those practices properly documented.

Finding No. 2: The NWRDC did not have a mechanism in place to ensure that all hardware and systems software changes were properly authorized, tested, approved, and implemented. Also, the NWRDC did not maintain documentation of the testing and implementation of hardware and systems software changes.

Recommendation: The NWRDC should establish a mechanism to provide reasonable assurance that all hardware and systems software changes are properly authorized, tested, approved, and implemented. In addition, the NWRDC should ensure that the testing and implementation of hardware and systems software changes is properly documented.

FSU\NWRDC Response: NWRDC agrees with this recommendation. While we do have policies and procedures in place regarding change management, we do not currently have a process in place to reconcile approved changes against the actual systems. NWRDC will investigate options to resolve this issue. As this may impact NWRDC budget and service rates, plans will be included in the FY 15-16 budget with implementation to be completed by June 30th of 2016.

Finding No. 3: Certain NWRDC security controls related to user authentication and the disclosure of sensitive security information needed improvement.

Recommendation: The NWRDC should improve security controls related to user authentication and the disclosure of sensitive information to ensure the continued confidentiality, integrity, and availability of customer-entity data and IT resources.

FSU\NWRDC Response: NWRDC agrees with this recommendation. There are certain technical restrictions that may hamper a direct resolution to the concern regarding security controls. As discussed with the audit team, NWRDC will work to better document the controls that are in place to compensate for this issue.

The security information that is mentioned as being disclosed is an instruction document for customers that discusses the steps needed to connect to an NWRDC service. While we agreed to move the document to a more secure location, we believe this information to be common knowledge and posed no additional security threat. At no point was personal sensitive or identifiable information disclosed.

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 4: Some NWRDC employees had unnecessary physical access privileges to the off-site backup storage vault.

Recommendation: The NWRDC should provide for periodic review to ensure that physical access privileges to the off-site vault are appropriately restricted.

FSU\NWRDC Response: As stated in the report, NWRDC agrees with this recommendation and has decreased the number of staff approved for access to the off-site vault.