STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-146
March 2021

FLORIDA STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

Sherrill F. Norman, CPA
Auditor General

Policy Board Members and Executive Director of the Northwest Regional Data Center

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

Tim Brown served as Executive Director of the NWRDC and the following individuals served as Board members during the period of our audit:

Board Member	Customer Entity Represented
Dr. Mehran Basiratmand, Chair	Small User Representative
Henry Martin, Vice Chair	K-12 Representative
Jesus Arias, Nonvoting Member	Institutional Affiliate
Michael Dieckmann, Nonvoting Member to 11-8-19	University of West Florida
Ronald Henry, Nonvoting Member	Florida A&M University
Gene Kovacs	Board of Governors
Damu Kuttikrishnan	Florida Department of Revenue
Jane Livingston	Florida State University
Dr. Andre Smith	Florida Department of Education
Sandra Stevens	City, County, and Local Government Representative

The team leader was Benjamin Ho, CISA, 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

FLORIDA STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

SUMMARY

This operational audit of the Northwest Regional Data Center (NWRDC) focused on evaluating selected significant information technology (IT) controls applicable to data center operations and included a follow-up on the findings noted in our report No. 2020-054. Our audit disclosed the following:

Finding 1: IT asset management procedures and processes need improvement to ensure that IT assets are accounted for and inventory records are accurate and complete.

Finding 2: NWRDC controls for periodic access reviews need improvement.

Finding 3: Certain NWRDC security controls related to vulnerability management, physical access, and user authentication need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.

BACKGROUND

The Northwest Regional Data Center (NWRDC) is an auxiliary operation of Florida State University (University) and is headed by a Policy Board (Board) consisting of representatives from its customer entities. The Board appoints an Executive Director who is responsible for the daily operations 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.

The NWRDC provides a variety of information technology (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 NWRDC's customer entities consist of State agencies, universities, colleges, school districts, municipal and county governments, a consortium, and nonprofit entities 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 its operating costs and allocates the billings based on the respective services provided to each customer. A list of the NWRDC customer entities is included in this report as ***EXHIBIT A***.

FINDINGS AND RECOMMENDATIONS

Finding 1: IT Asset Management

Effective IT asset management controls include the maintenance of a complete, accurate, and up-to-date inventory of IT resources (e.g., physical and virtual servers, network devices, databases) to ensure that management is knowledgeable of all IT resources for which they are responsible. Further, a complete, accurate, and up-to-date inventory is necessary for the effective monitoring, testing, and evaluation of

IT resources and the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors.

As part of our audit, we conducted inquiries of NWRDC management and staff and reviewed NWRDC policies, procedures, and records for managing IT assets. To facilitate the tracking of NWRDC-managed IT assets, the NWRDC maintained various manually prepared inventory spreadsheets of physical and virtual IT assets and also utilized a network discovery tool to detect networked IT assets. While the NWRDC *Policy and Procedure Manual* (*Manual*)[1] broadly addressed the tracking, reassignment, and movement of hardware and electronic media and specified that each quarter the inventory spreadsheets were to be reconciled to the IT assets detected by the network discovery tool, the *Manual* did not identify the responsible staff or specify the processes followed or documentation to be retained. Similar findings were noted in prior audits of the NWRDC, most recently in our report No. 2020-054 (Finding 1).

Pursuant to the *Manual*, each quarter NWRDC staff reconciled inventory by comparing the IT assets listed on the inventory spreadsheets to the IT assets identified by the network discovery tool. As part of the reconciliation, NWRDC staff researched when IT assets listed on the inventory spreadsheets were missing from the scan results and updated the inventory spreadsheets accordingly. While reconciling from the inventory spreadsheets to the scan results identified IT assets on the spreadsheets that were not detected by the network discovery tool, the reconciliation did not identify IT assets that were connected to the network and detected by the network discovery tool but omitted from the inventory spreadsheets. The omission of IT assets from the inventory spreadsheets may lead to inadequate management of those resources.

To evaluate the accuracy and completeness of the inventory spreadsheets, we compared selected IT assets from the May 15, 2020, scan to the inventory spreadsheets to determine whether the spreadsheets were up to date as of May 18, 2020. Specifically, our comparison of 15 of the 191 Linux IT assets identified in the networked IT assets scan results to the inventory spreadsheets found that 7 of the 15 Linux IT assets were not recorded on the inventory spreadsheets. In response to our audit inquiry, NWRDC management was unable to provide an explanation for the discrepancies; however, NWRDC management indicated that they thought reconciling the inventory spreadsheets to the scan results was sufficient to ensure accountability over IT assets.

To evaluate the accuracy and completeness of the IT assets identified by the network discovery tool, we compared 60 of the 355 IT assets listed on the May 18, 2020, inventory spreadsheets in five device categories to the IT assets from the scan results of networked IT devices. Our comparison found that 9 IT assets listed on the inventory spreadsheets were not in the scan results. According to NWRDC management, while 1 IT asset had been decommissioned on January 27, 2020, it was not removed from the inventory spreadsheet due to an oversight. NWRDC management indicated that the other 8 IT assets were valid as recorded on the inventory spreadsheets; however, configuration of the network discovery tool was ongoing to ensure that all IT assets are discovered when a scan is conducted.

Comprehensive IT inventory procedures that include reconciliations of all IT assets on the network facilitate complete, accurate, and up-to-date IT inventory records necessary to ensure that management

[1] NWRDC *Policy and Procedure Manual*, *Section 7.80*, *Tracking Reassignment/Movement of Inventories*, effective November 4, 2019.

is knowledgeable of all IT assets for which they are responsible, IT systems are configured as intended by management, and relevant security patches and other critical updates are timely implemented.

Recommendation: We again recommend that NWRDC management establish comprehensive IT inventory reconciliation procedures that identify the responsible staff and specify the processes followed and documentation to be retained. Additionally, we recommend that NWRDC management enhance the IT inventory reconciliation procedures by reconciling both the IT assets listed on the inventory spreadsheets to the scan results and the scan results to the IT assets listed on the inventory spreadsheets. Any differences noted during the reconciliation process should be promptly resolved.

Finding 2: Periodic Review of Access Privileges

Periodic reviews of access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic review consists of identifying the current logical access privileges of all users and evaluating the assigned access privileges to ensure that they align with users' job responsibilities.

To facilitate the periodic review of employee accounts and the assigned access privileges, the *Manual*[2] required employee accounts and privileges (logical access for IT devices, systems, and applications) be reviewed annually in accordance with documented procedures and for validity and appropriateness based on an employee's role and the principles of least privilege and need to know. However, our review of the NWRDC *Logical Access Review Procedures* (*Procedures*) found that, although the *Manual* had been updated in January 2019 to require annual access reviews, the *Procedures* had been under revision since June 2018, were incomplete, and did not align to the *Manual* or the current annual review process. According to NWRDC management, the annual review process included all employee accounts and logical access privileges in accordance with the *Manual*. NWRDC management also indicated that the *Procedures* remained under revision and that most elements of the *Procedures* were still valid.

Without up-to-date procedures for periodic reviews of logical access, the reviews may not be conducted consistent with the *Manual* and, as a result, management's assurance that access privileges were properly granted and remain appropriate is limited.

Recommendation: We recommend that NWRDC management finalize the *Procedures* for periodic reviews of access privileges and ensure that the *Procedures* and the *Manual* align to established periodic logical access privilege review processes.

Finding 3: Security Controls- Vulnerability Management, Physical Access, and User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to vulnerability management, physical access, and user authentication need improvement to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources. We are not disclosing specific

[2] NWRDC *Policy and Procedure Manual*, *Section 7.90*, *Workforce and Authorization Management*, effective January 10, 2019.

details of the issues in this report to avoid the possibility of compromising customer entity data and related IT resources. However, we have notified appropriate NWRDC management of the specific issues.

Without appropriate security controls related to vulnerability management, physical access, and user authentication, the risk is increased that the confidentiality, integrity, and availability of customer entity data and related IT resources may be compromised. A similar finding related to physical access was communicated to NWRDC management in connection with our report No. 2020-054.

Recommendation: We recommend that NWRDC management improve certain security controls related to vulnerability management, physical access, and user authentication to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the NWRDC had taken corrective actions for the findings included in our report No. 2020-054.

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 March 2020 through September 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 controls applicable to Northwest Regional Data Center (NWRDC) operations during the period July 2019 through June 2020 and selected actions 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 at the NWRDC.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2020-054.
- 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)[3] 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.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the NWRDC Policy Board and NWRDC 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 all components of internal control were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- NWRDC Policy Board and management commitment to integrity and ethical values.
- NWRDC Policy Board exercise of oversight responsibility.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve NWRDC goals and objectives.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management establishment of clear objectives to enable the identification of risks and define risk tolerances.
- Management identification and analysis of and response to risks.
- Management consideration of the potential for fraud.

[3] 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.

- Management design of control activities to achieve NWRDC 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 NWRDC objectives.
- Management communication of information internally necessary to achieve NWRDC objectives.
- Management communication of information externally necessary to achieve NWRDC objectives.
- Management activities to monitor the NWRDC 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, NWRDC policies and procedures, and other guidelines, and interviewed NWRDC personnel to obtain an understanding of selected NWRDC operations.
- Interviewed NWRDC personnel and examined NWRDC records to obtain an understanding of NWRDC processes for IT asset management; vulnerability management, including vulnerability testing, analysis, and remediation; and restricting physical access to NWRDC facilities and sensitive IT resources, including the granting, discontinuing, logging, and periodic review of physical access to NWRDC facilities and sensitive IT resources.

- Interviewed NWRDC personnel and examined NWRDC records to obtain an understanding of the NWRDC's network infrastructure and related hardware, software, and authentication methods, data center services provided, and customers served.
- Evaluated the effectiveness of NWRDC IT asset (inventory) tracking controls by comparing:
    - 60 of the 355 IT assets included on the manually prepared inventory spreadsheets as of May 18, 2020, for five IT asset device categories to the IT assets identified in the scan results of networked IT devices to determine whether the IT assets included on the inventory spreadsheets were identified in the scan results.
    - 15 of the 191 Linux IT assets identified in the May 15, 2020, scan results of networked IT devices to the IT assets on the manually prepared inventory spreadsheets to determine whether the IT assets identified in the scan results were included on the inventory spreadsheets.
- Evaluated the appropriateness of mainframe access privileges as of April 30, 2020, for 15 of the 75 administrative accounts with selected elevated access privileges.
- Evaluated the adequacy of policies, procedures, and processes for periodic NWRDC systems and network access reviews.
- Evaluated the adequacy of NWRDC policies and procedures for authorizing, removing, periodically reviewing, and logging physical access to sensitive IT areas, including evaluating the appropriateness of access to sensitive IT areas for 52 active key cards assigned to employees as of May 7, 2020.
- Evaluated the adequacy of selected NWRDC IT infrastructure authentication controls.
- Evaluated NWRDC vulnerability management controls, including the adequacy of NWRDC policies and procedures and the effectiveness of vulnerability management processes (the timely performance of authenticated scans and the timely communication, analysis, and remediation of identified vulnerabilities for the NWRDC network, mainframe, Windows, and open systems environments).
- 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, CPA
Auditor General

EXHIBIT A

NWRDC CUSTOMER ENTITIES

AS OF JUNE 30, 2020

Higher Education Entities

Broward College	Florida Polytechnic University	State College of Florida
Chipola College	Florida State University	University of Central Florida
Florida A&M University	Florida Virtual Campus	University of Florida
Florida Atlantic University	Gulf Coast State College	University of North Florida
Florida Center for Interactive Media at Florida State University	New College of Florida	University of South Florida
Florida Gulf Coast University	Palm Beach State College	University of West Florida
Florida International University		

State Agencies and Other Government Entities

Board of Governors	Department of Highway Safety and Motor Vehicles	Early Learning Coalition of the Emerald Coast
Department of Business and Professional Regulation	Department of the Lottery	Florida Commission on Human Relations
Department of Education	Department of Revenue	Florida Prepaid College Board
Department of Financial Services	Department of State	Statewide Guardian Ad Litem
Department of Health	Division of State Technology,[a] Department of Management Services	

K-12 School Districts

Bay County District School Board	Miami-Dade County District School Board	Panhandle Area Educational Consortium:
Columbia County District School Board	Monroe County District School Board	Calhoun County District School Board
Florida Atlantic University Schools	Nassau County District School Board	Florida A&M University Developmental Research School
Florida School for the Deaf and the Blind	Palm Beach County District School Board	Franklin County District School Board
Florida State University Schools	Pinellas County District School Board	Gadsden County District School Board
Florida Virtual School	Santa Rosa County District School Board	Gulf County District School Board
Hillsborough County District School Board	St. Johns County District School Board	Holmes County District School Board
Manatee County District School Board	Suwannee 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 Entities

Alachua County Government	City of Jacksonville	Orange County Clerk of Courts
Big Bend Hospice	City of West Palm Beach	Orange County Comptroller
City of Boca Raton	Florida State University Foundation	Palm Beach County Board of County Commissioners
City of Boynton Beach	Health Care District of Palm Beach County	Palm Beach County Clerk and Comptroller
City of Coral Springs	Miami-Dade County Government	Tallahassee Memorial HealthCare, Inc.
City of Delray Beach	Orange County Board of County Commissioners	The Ringling Museum of Art, Florida State University

[a] Effective July 1, 2020, the Division of State Technology was abolished and the Florida Digital Service was established in its place.

Source: Dianna Norwood, Associate Director, Administrative Services, NWRDC.

MANAGEMENT'S RESPONSE

NWRDC™
Northwest Regional Data Center

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

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

March 8, 2021,

Dear Ms. Norman,

Please accept Florida State University's response to your February 4th letter with preliminary and tentative audit findings in the recent audit of 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
Assistant Vice President for NWRDC & FLVC
Florida State University

cc:
Sam McCall, Chief Audit Officer, Florida State University
Mehran Basiratmand, CTO, Florida Atlantic University; Chair, NWRDC Policy Board
Jane Livingston, Assoc. VP & CIO, Florida State University

Finding 1: IT asset management procedures and processes need improvement to ensure that IT assets are accounted for and inventory records are accurate and complete.

Recommendation: We again recommend that NWRDC management establish comprehensive IT inventory reconciliation procedures that identify the responsible staff and specify the processes followed and documentation to be retained. Additionally, we recommend that NWRDC management enhance the IT inventory reconciliation procedures by reconciling both the IT assets listed on the inventory spreadsheets to the scan results and the scan results to the IT assets listed on the inventory spreadsheets. Any differences noted during the reconciliation process should be promptly resolved.

NWRDC Response: Agreed. NWRDC is in the process of implementing a configuration management database (CMDB) to replace the previously existing manual spreadsheet processes for inventory management of IT devices and systems. NWRDC will reconcile the CMDB records against reports from a network discovery tool and promptly resolve any discrepancies.

Finding 2: NWRDC controls for periodic access reviews need improvement.

Recommendation: We recommend that NWRDC management finalize the *Procedures* for periodic reviews of access privileges and ensure that the *Procedures* and the *Manual* align to established periodic logical access privilege review processes.

NWRDC Response: Agreed. NWRDC will finalize the logical access review procedures and ensure that the procedures align with the policy statement in NWRDC's Policy Manual.

Finding 3: Certain NWRDC security controls related to vulnerability management, physical access, and user authentication need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.

Recommendation: We recommend that NWRDC management improve certain security controls related to vulnerability management, physical access, and user authentication to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources.

NWRDC Response: Agreed. NWRDC will improve security controls in these areas as noted.