REPORT NO. 2010-173
MARCH 2010

SOUTHWOOD SHARED RESOURCE CENTER

DATA CENTER OPERATIONS

Information Technology Operational Audit

For the Period
July 2009 Through November 2009
and Selected Actions Through January 8, 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE SOUTHWOOD SHARED RESOURCE CENTER

Pursuant to Section 282.205(1), Florida Statutes, the Southwood Shared Resource Center (SSRC) is established within the Department of Management Services (DMS) for administrative purposes only and is a separate budget entity that is not subject to control, supervision, or direction by DMS in any manner. Pursuant to Section 282.203(2), Florida Statutes, the head of the SSRC is the Board of Trustees, consisting of representatives from customer entities. The Executive Director is employed by the Board of Trustees and serves at the pleasure of the Board.

Board members and the customer entities represented and the Executive Director who served during July 2009 through November 2009 are listed below:

Board Member	Customer Entity Represented
Nelson Hill, Chair	Department of Transportation
David Faulkenberry, Vice Chair	Department of Management Services
Blanca Bayo	Department of Revenue
Ron Lauver	Department of Education
Nelson Munn	Department of Highway Safety and Motor Vehicles
Kevin Patten	Fish and Wildlife Conservation Commission
David Stokes	Department of Health
Kevin Thompson	Agency for Workforce Innovation

John Wade, Executive Director

The audit team leader was Daniel Pearce, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

SOUTHWOOD SHARED RESOURCE CENTER

Data Center Operations

SUMMARY

Pursuant to Sections 282.203 and 282.205, Florida Statutes, the Southwood Shared Resource Center (SSRC) was established as a primary data center to serve as an information system utility for customer entities. Our audit focused on evaluating selected information technology (IT) controls relevant to SSRC data center operations during the period July 2009 through November 2009 and selected actions through January 8, 2010.

The results of our audit are summarized below:

Finding No. 1: Contrary to State law, service-level agreements (SLAs) had not been established with some SSRC customer entities.

Finding No. 2: In one instance noted, a service-level agreement performance level had not been met by the SSRC.

Finding No. 3: A data backup tape was not properly accounted for in the SSRC tape management system and contained the commingled data of more than one customer entity, contrary to customer expectations.

Finding No. 4: The SSRC did not remove the access privileges of a reassigned employee in a timely manner.

Finding No. 5: The SSRC lacked comprehensive procedures for periodic reviews of access privileges and standardized change control testing.

Finding No. 6: Certain SSRC security controls needed improvement in the areas of monitoring security events and authenticating system users.

BACKGROUND

Section 282.201(1), Florida Statutes, provides that agency data centers and computing facilities are to be consolidated into primary data centers to the maximum extent possible by 2019. The SSRC was established as one of the primary data centers to which State agencies are to migrate their computing resources.

Pursuant to Chapter 2008-116, Section 17, Laws of Florida, all data center functions performed, managed, operated, or supported by State agencies with resources and equipment currently located in the SSRC, excluding application development, shall be transferred to the SSRC, and the agencies shall become a full service customer entity by July 1, 2010. During the audit period, agencies were in the process of transferring data center functions to the SSRC. In addition, as of July 6, 2009, the mainframe operations of the Agency for Workforce Innovation (AWI), the Department of Management Services (DMS), the Department of Transportation (DOT), and the Department of Highway Safety and Motor Vehicles (DHSMV) had already been consolidated into the SSRC, pursuant to Chapter 2008-116, Section 18.

The SSRC is headed by a Board of Trustees, consisting of representatives from customer entities. The Board appointed an Executive Director to be responsible for the daily operation of the data center. The SSRC provides a variety of IT services to its customer entities, including equipment hosting and server management services. The customer entities consist of State agencies and other governmental entities that contract with the SSRC for the aforementioned IT services. The SSRC operates on a cost-recovery basis whereby the SSRC bills the customer entities for a portion of its operating costs associated with the specific services provided to each customer entity.

Lists of SSRC customers and services offered by the SSRC are included in this report as EXHIBITS A and B, respectively.

Pursuant to Section 282.201(2)(a), Florida Statutes, the Agency for Enterprise Information Technology (AEIT) is responsible for collecting and maintaining information necessary for developing policies relating to the data center system. In addition, pursuant to Section 282.201(2)(f), Florida Statutes, AEIT shall develop and establish rules relating to the operation of the State data center system which comply with applicable Federal regulations. AEIT is also responsible, pursuant to Section 282.201(2)(e), Florida Statutes, for developing and submitting to the Legislature by December 31, 2010, an overall consolidation plan for State data centers.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Service-Level Agreements

A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. SLAs are necessary to define IT services provided by the SSRC to the State agencies and other governmental entities and to ensure that services provided by the SSRC support the business objectives of the customer entities. SLAs define the roles and responsibilities of each party, including security management practices, service renewal provisions, and termination requirements. SLAs also set forth the billing methodology and the costs of the services to be paid by the customer entities.

As previously discussed, Section 282.201(2)(f), Florida Statutes, provides that AEIT shall develop and establish rules related to the operation of the State data center system. Section 282.201(2)(f)2., Florida Statutes, provides that the rules may address the requirement for service-level agreements to be established between a data center and its customer entities for services provided. Section 282.203(1)(g), Florida Statutes, requires each primary data center to enter into an SLA with each customer entity to provide services as defined and approved by the Board in compliance with rules of AEIT. As of the end of the audit period, AEIT had not yet developed rules related to the operation of the State data center system.

As of November 30, 2009, the SSRC was providing various services, such as managed servers and mainframe services, to a customer base of 36 entities (see EXHIBITS A and B). As of November 13, 2009, signed SLAs existed with 15 entities for all of the services provided to those entities. In addition, signed SLAs existed with another 10 of the entities for some of the services provided.[1] There were no signed SLAs between the SSRC and the remaining 11 entities.

Chapter 2008-116, Section 18, Laws of Florida, required the SSRC and mainframe agencies (DOT and DHSMV) to establish SLAs by April 30, 2009. DOT signed an SLA with the SSRC for mainframe services. However, as of January 8, 2010, the SSRC and DHSMV had not been able to successfully negotiate service-level terms and had not entered into an SLA for mainframe services.

Without a service-level agreement that establishes in writing the requirements of both the SSRC and a customer entity, the risk is increased that customer IT service requirements and SSRC expectations of the customer will not be sufficiently met. Under such conditions, the effective, efficient, and secure operation of State IT systems could be jeopardized.

[1] Some of these SLAs were entered into with the SSRC's predecessor, the DMS Shared Resource Center.

Recommendation: The SSRC and customer entities should establish mutually agreed-upon service-level agreements as provided in State law. In connection with developing rules relating to the operation of the State data center system pursuant to Section 282.201(2), Florida Statutes, AEIT should consider establishing guidance to promote the timely execution of SLAs between primary data centers and customer entities.

Finding No. 2: SLA Performance

The SLAs that were in effect between the SSRC and the customer entities contained, in part, provisions and requirements for how the SSRC would provide IT services and meet service-level requirements. As a part of our audit, we reviewed the performance of the SSRC in meeting the requirements set forth in the signed SLAs.

Our review disclosed that the SSRC's IBM Mainframe Managed Services SLA with DOT required that unplanned outages and major problems be detected by the SSRC within one hour of occurrence. However, a major system problem went undetected for over six hours until DOT notified the SSRC of the problem. SSRC then remedied the problem within the recovery of services time frame required by the SLA. In response to audit inquiry, SSRC staff indicated that they consider this type of incident to be an interruption of service and such interruptions will be addressed according to the requirements of the SLA. Without timely detection of unplanned outages or major problems, the risk is increased that critical IT-dependent services will not be available.

Recommendation: The SSRC should continue to review controls to ensure that unplanned outages or major problems, should they occur, are timely detected and reported to applicable customers.

Finding No. 3: Tape Management

There are a number of steps that an entity can take to minimize the risk of data loss that may occur from unexpected events. One example is routinely backing up data files and programs and securely storing the backups at an off-site location. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate. Another example is maintaining the security requirements of the backup data in transit and storage.

As a part of our audit, we reviewed the backup tape handling procedures at the SSRC. We noted that 1 of the 53 backup tapes included in our test was not properly accounted for in the SSRC tape management system. Although at the time of our testing the tape was not properly accounted for, the tape was still in the possession of the SSRC and was subsequently returned to the off-site storage facility where it belonged. Additionally, the tape in question contained entity data that the SSRC agreed to keep separated from the data of other entities; however, other entities' data was comingled on the tape.

If backup tapes cannot be located in the event of a loss of production data, the risk is increased that the SSRC's and entities' abilities to timely and completely restore the lost information could be hindered. If data is not appropriately separated as intended, the risk is increased that the security of sensitive or confidential data could be compromised.

Recommendation: The SSRC should improve the accuracy of its tape management system and, where applicable, ensure that data on backup tapes is appropriately separated pursuant to customer entity expectations.

Finding No. 4: Timely Removal of Reassigned Employee Access

Effective management of system access privileges includes provisions to timely remove unnecessary employee access privileges when employee reassignments occur. Prompt action is necessary to ensure that the access privileges are not misused by the reassigned employee or others.

As a part of our audit, we reviewed the SSRC employees' systems software access privileges for systems housed at the SSRC. Our review of access privileges for mainframe systems disclosed that the access privileges of one employee were not removed for a period of 853 days following his reassignment to a position that did not require the access privileges.

In response to audit inquiry, the SSRC subsequently removed the reassigned employee's access privileges. Without timely removal of reassigned employee's access privileges, the risk is increased that the access privileges could be misused by the reassigned employee or others.

Recommendation: The SSRC should enhance its procedures to ensure that the access privileges of reassigned employees are removed in a timely manner.

Finding No. 5: IT Procedures

Sound IT management includes the establishment of written procedures that describe management's expectations for controlling an entity's IT operations. Written procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff. Our audit disclosed that the SSRC had not established written procedures for some IT functions. Specifically:

- The SSRC did not have procedures in place for periodically reviewing the appropriateness of access privileges assigned to users of certain systems or reviewing changes to access privileges.
- The SSRC had implemented change control procedures that allowed the data center to plan, schedule, and track changes to the production and test environments; however, the procedures did not address the detailed processes to be used for testing changes to certain types of systems software.

Without written procedures, the risk is increased that IT controls may not be followed consistently and in a manner pursuant to management's expectations.

Recommendation: The SSRC should establish comprehensive written procedures for the review of access privileges and the testing of systems software changes.

Finding No. 6: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain SSRC security controls needed improvement in the areas of monitoring security events and authenticating system users. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising State agency data and IT resources. However, we have notified appropriate SSRC management of the specific issues. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that customer entity data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The SSRC should implement the appropriate security controls in the areas of monitoring security events and authenticating system users to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

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 in accordance with applicable 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 audit were to determine the effectiveness of selected IT controls related to SSRC data center operations 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; the safeguarding of IT resources; the effectiveness and efficiency of IT operations.

The scope of our audit focused on evaluating selected IT controls relevant to SSRC data center operations during the period July 2009 through November 2009 and selected actions through January 8, 2010, including selected general IT controls over operations and security, governance of the SSRC, and the data center consolidation migration process.

In conducting our audit, we:

- Interviewed SSRC personnel.
- Obtained an understanding of the IT infrastructure and architecture of the SSRC.
- Obtained an understanding of logical access paths and tested whether logical access controls ensured that access to systems software was restricted to authorized users.
- Obtained an understanding of physical access controls and tested whether physical access controls ensured that access to the data center floor was restricted to authorized individuals.
- Obtained an understanding and tested the effectiveness of background screenings of SSRC staff with access to customer entity IT resources.
- Obtained an understanding and tested the effectiveness of selected controls over the modification of systems software.
- Evaluated the adequacy of environmental safeguards in place to protect IT resources.
- Obtained an understanding and evaluated the adequacy of selected disaster recovery and continuity of operations planning controls.
- Obtained an understanding and tested the effectiveness of tape handling procedures.
- Obtained an understanding and tested the effectiveness of inventory and equipment tracking procedures.
- Obtained an understanding and tested for the fulfillment of signed service-level agreement requirements.
- Obtained an understanding of the statutory requirements of SSRC data center operations and evaluated the SSRC's compliance with selected requirements.
- Obtained an understanding of the data center consolidation process.

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

MANAGEMENTS' RESPONSES

In letters dated March 18, 2010, and March 25, 2010, the Executive Directors of the Southwood Shared Resource Center and the Agency for Enterprise Information Technology, respectively, provided responses to our preliminary and tentative findings. These letters are included at the end of this report as EXHIBIT C.

EXHIBIT A
LIST OF SSRC CUSTOMERS

Agency for Health Care Administration	Department of Revenue
Agency for Persons with Disabilities	Department of State
Agency for Workforce Innovation	Department of Transportation
Children's Home Society	Department of Veterans' Affairs
Community-Based Care of Seminole	Fish and Wildlife Conservation Commission
Department of Business and Professional Regulation	Greater Orlando Aviation Authority
Department of Children and Family Services	Justice Administrative Commission
Department of Citrus	Legislature
Department of Community Affairs	Miami-Dade Expressway Authority
Department of Corrections	Northwest Florida Water Management District
Department of Education	Office of the Governor
Department of Elder Affairs	Parole Commission
Department of Financial Services	Public Service Commission
Department of Health	Santa Rosa County
Department of Highway Safety and Motor Vehicles	State Attorney - 14th Circuit
Department of Juvenile Justice	State Board of Administration
Department of Lottery	State Courts
Department of Management Services	Suwannee River Water Management District

EXHIBIT B
LIST OF SERVICES OFFERED BY THE SSRC

Data Center Management	SRC Floor Tiles
	SRC Rack Mounts
	SRC Tape Vault
	Off-Site Tape Storage
	Print Impressions
	SRC Office Space
Mainframe Services	IBM Batch CPU Time
	IBM CICS CPU Time
	IBM DB2 CPU Time
	IBM TSO CPU Time
	IBM Middleware CPU Time
	IBM Tape Cartridges
	IBM Print Management
	Unmirrored Disk Storage
	Unisys Managed Service
Open Systems Platform	Oracle Premium Managed Server
	Open Systems Net Based Services
	UNIX Managed Services
	Electronic Data Interchange (EDI) Translation
Windows Platform	Hosted Messaging (E-mail)
	Windows Managed Server
	Unmanaged Windows Server
Storage Management	Backup Service
	Unmirrored Disk Storage
	Mirrored Disk Storage
Graphics	Graphics

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT C
MANAGEMENTS' RESPONSES

State of Florida
Southwood Shared Resource Center
2585 Shumard Oak Boulevard
Tallahassee, Florida 32399-0950

Phone: 850-413-9300
Fax: 850-921-8343
http://SSRC.myflorida.com

Governor Charlie Crist

John M. Wade, Executive Director

March 18, 2010

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your preliminary and tentative audit findings of the *Southwood Shared Resource Center, Data Center Operations, Information* Technology *Operational Audit*. Our response corresponds with the order of your findings and recommendations contained in the document provided to the Southwood Shared Resource Center on March 8, 2010.

Finding No. 1: Service-Level Agreements

Contrary to State law, service-level agreements (SLA's) had not been established with some SSRC customers entities.

Recommendation

The SSRC and customer entities should establish mutually agreed-upon service-level agreements as provided in State law. In connection with developing rules relating to the operation of the State data center system pursuant to Section 282.201(2), Florida Statutes, AEIT should consider establishing guidance to promote the timely execution of SLAs between primary data centers and customer entities.

Response

The SSRC agrees with the recommendation, and supports the proposed proviso language mandating agencies to execute an SLA for services from the SSRC no later than September 1, 2010.

Finding No. 2: SLA Performance

In one instance noted, a service-level agreement performance level had not been met by the SSRC.

Recommendation

The SSRC should continue to review controls to ensure that unplanned outages or major problems, should they occur, are timely detected and reported to applicable customers.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Response

The SSRC agrees with this recommendation. On September 22, 2009, the SSRC corrected the problem by generating automated emails that alert the IBM technical support team to contact vendors regarding acquisition of new license keys prior to expiration of existing keys. This process is identified in a new operating procedure OP352 – Vendor Software License Key Renewal.

Finding No. 3: Tape Management

A data backup tape was not properly accounted for in the SSRC tape management system and contained the commingled data of more than one customer entity, contrary to customer expectations.

Recommendation

The SSRC should improve the accuracy of its tape management system and, where applicable, ensure that data on backup tapes is appropriately separated pursuant to customer entity expectations.

Response

The SSRC agrees with this recommendation. On March 10, 2010, the SSRC added additional controls to its tape management system procedure OP906 – Iron Mountain Offsite Procedures. These controls include: acquiring a list of tapes monthly from the various library owners that vault at Iron Mountain to ensure proper location of tapes and automatic 7 day return of any tapes requested from offsite before their expiration date, unless library owners request in writing that tapes are not to be returned. In addition, the SSRC is in the process of establishing a procedure to review and assess stored data in accordance with customer expectations identified in SLA.

Finding No. 4: Timely Removal of Reassigned Employee Access

The SSRC did not remove the access privileges of a reassigned employee in a timely manner.

Recommendation

The SSRC should enhance its procedures to ensure that the access privileges of reassigned employees are removed in a timely manner.

Response

The SSRC agrees with this recommendation. The SSRC is currently in the process of establishing an employee transfer process similar to our employee termination process that will allow the manager to review access security privileges for new duties and responsibilities. The anticipated completion date is April 16, 2010.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Finding No. 5: IT Procedures

The SSRC lacked comprehensive procedures for periodic reviews of access privileges and standardized change control testing.

Recommendation

The SSRC should establish comprehensive written procedures for the review of access privileges and the testing of systems software changes.

Response

The SSRC agrees with this recommendation. The SSRC will develop written procedures for reviewing access privileges and the testing of system software changes by April 16, 2010.

Finding No. 6: Other Security Controls (Confidential)

Certain SSRC security controls needed improvement in the areas of monitoring security events and authenticating system users.

Recommendation

The SSRC should implement the appropriate security controls in the areas of monitoring security events and authenticating system users to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Response

The SSRC agrees with the recommendation. The SSRC has budgeted for FY10-11 software tools to enhance security controls in the areas of monitoring security events and authenticating users.

If further information is needed concerning our response, please contact Cathy Kreiensieck, Chief of Enterprise Planning & Management, Southwood Shared Resource Center at 413-9309.

Sincerely,

John M. Wade
Executive Director, Southwood Shared Resource Center

CC: George Zimmerman
Nelson Hill

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Governor Charlie Crist
Attorney General Bill McCollum
Chief Financial Officer Alex Sink
Commissioner Charles H. Bronson

Agency for Enterprise Information Technology
David W. Taylor
Executive Director
State Chief Information Officer

March 25, 2010

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

Dear Mr. Martin:

I have reviewed the preliminary and tentative audit findings and recommendations on your Information Technology Operational Audit of the Southwood Shared Resource Center (SSRC) Data Center Operations for the period July 2009 through November 2009 and selected actions through January 8, 2010.

In response to Finding No. 1: The Agency for Enterprise Information Technology (AEIT) agrees with the recommendation. AEIT will include this issue in the Data Center System rulemaking process that will be completed by October 31, 2010.

If you have any questions, please contact me as below.

Sincerely,

David W. Taylor
Executive Director and State CIO
Agency for Enterprise Information Technology
4030 Esplanade Way, Suite 135
Tallahassee, FL 32399-0950
Phone: 850-922-7502

cc: Mike Russo, Chief Information Security Officer
Agency for Enterprise Information Technology
John Wade, Executive Director
Southwood Shared Resource Center

DWT/dc

Agency for Enterprise Information Technology
4030 Esplanade Way, Ste 135
Tallahassee, Florida 32399-0950
850.922.7502: TEL, 850.487.9937: FAX