STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-004
July 2016

COMPREHENSIVE RISK ASSESSMENTS AT SELECTED STATE AGENCIES

Sherrill F. Norman, CPA
Auditor General

State Agency Heads

The Florida Statutes establish the various State agencies and provide the title and selection process for the head of each State agency. The table below shows the six State agencies included in the scope of this information technology operational audit and the respective agency heads who served during the period of our audit.

State Agency	Established by Florida Statutes	State Agency Head
Agency for Health Care Administration	Section 20.42	Elizabeth Dudek, Secretary
Agency for State Technology	Section 20.61	Jason M. Allison, Executive Director and Chief Information Officer
Department of Children and Families	Section 20.19	Mike Carroll, Secretary
Department of Economic Opportunity	Section 20.60	Jessie Panuccio, Executive Director through January 8, 2016 Theresa "Cissy" Proctor, Executive Director from January 9, 2016
Department of Education	Section 20.15 and Article IX, Section 2 of the State Constitution	Pam Stewart, Executive Director and Commissioner of Education
Department of Transportation	Section 20.23	Jim Boxold, Secretary

The team leader was Debbie Clark, CPA, and the audit was supervised by Brenda Shiner, 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 are available at:

www.myflorida.com/audgen

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

COMPREHENSIVE RISK ASSESSMENTS AT SELECTED STATE AGENCIES

SUMMARY

This operational audit focused on evaluating selected information technology (IT) controls applicable to the comprehensive risk assessment process at the following State agencies: Agency for Health Care Administration (AHCA), Agency for State Technology (AST), Department of Children and Families (DCF), Department of Economic Opportunity (DEO), Department of Education (DOE), and Department of Transportation (DOT). Our audit disclosed the following:

Finding 1: The risk assessment guidance provided by the AST to the State agencies did not sufficiently promote compliance with the National Institute of Standards and Technology risk assessment requirements.

Finding 2: The AST's oversight of the State agencies' risk assessments needs improvement to better assist State agencies with the timely submittal of properly completed risk assessments.

Finding 3: The risk assessment process for AHCA, DCF, DEO, DOE, and DOT did not include the classification of data and categorization of IT systems. Additionally, AHCA, DOE, and DOT did not develop risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

Finding 4: Selected IT security controls for AHCA, DCF, DEO, DOE, and DOT need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

BACKGROUND

Pursuant to the Federal Information Security Management Act of 2002 (FISMA), the National Institute of Standards and Technology (NIST) developed information security standards and guidelines, including minimum requirements, for all Federal agency operations and assets. Federal Information Processing Standards (FIPS) issued by NIST are compulsory for Federal agencies. Special publications are also developed and issued by NIST as recommendations and guidance documents.

Agency for Enterprise Information Technology (AEIT) rules[1] provide that the State will follow FIPS and NIST standards and guidance. The AEIT rules[2] require each State agency to categorize its information technology (IT) resources according to FIPS Publication 199 as either low impact, moderate impact, or high impact. The impact categorization for an IT system is defined as the estimated magnitude of harm that could result from an unauthorized access, modification, destruction, or loss of availability of an IT

[1] AEIT Rule 71A-1.001(9), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records, property, administrative authority, and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed.

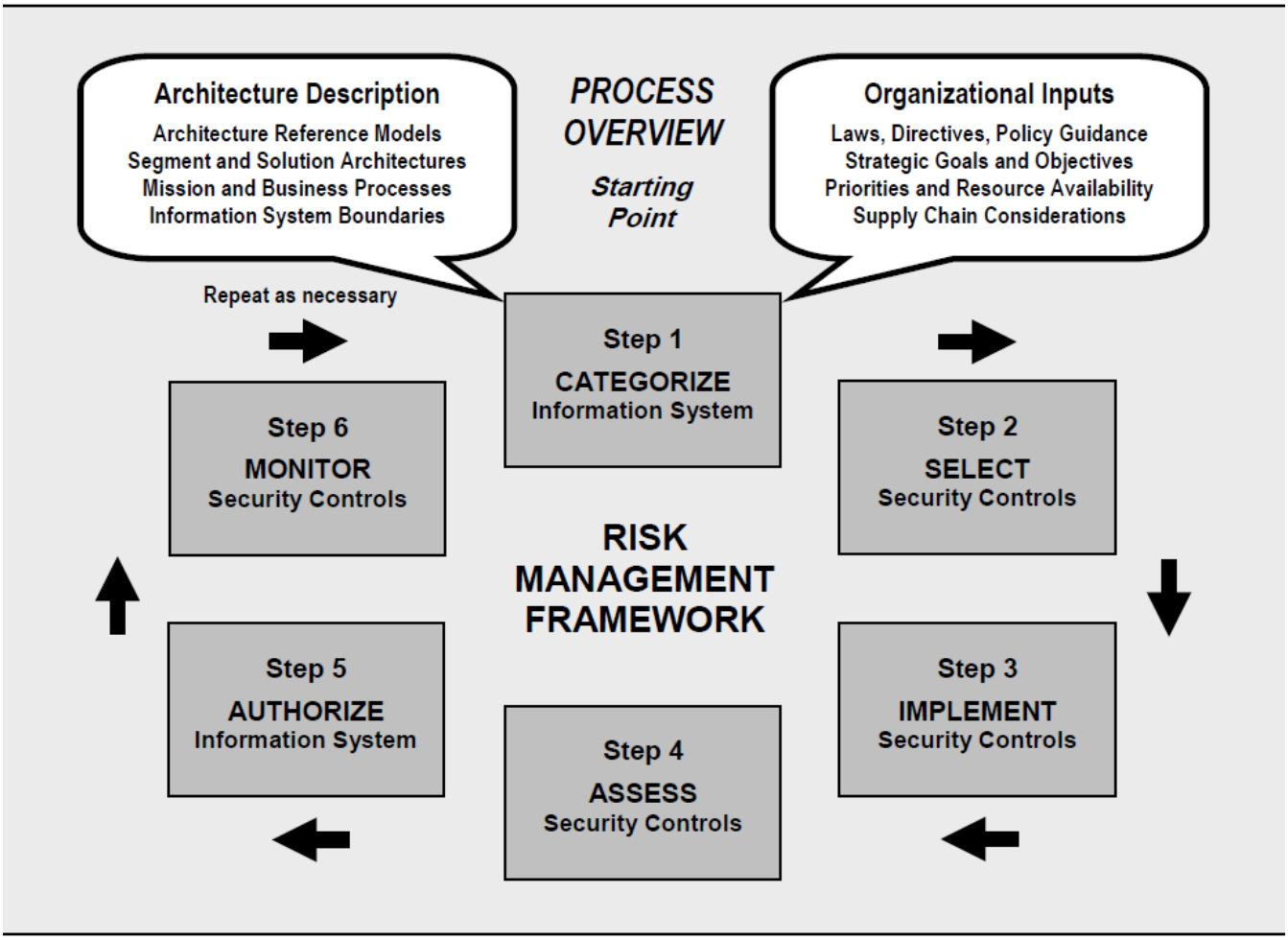
[2] AEIT Rule 71A-1.020(1), Florida Administrative Code.

system or resource. The AEIT rules[3] also require State agencies to implement a documented risk management program, including risk analysis for high impact systems.

State agencies, as defined in State law,[4] must conduct and update every 3 years a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the agency. State law[5] requires the risk assessment to comply with the methodology developed by the Agency for State Technology (AST). For the risk assessment due March 31, 2015, a total of 31 State agencies were required to complete the risk assessment process.

Guidelines developed by NIST include a risk management framework,[6] as shown in Chart 1, that provides direction on the steps to be undertaken to identify and assess risk in an organization.

Chart 1
NIST Risk Management Framework



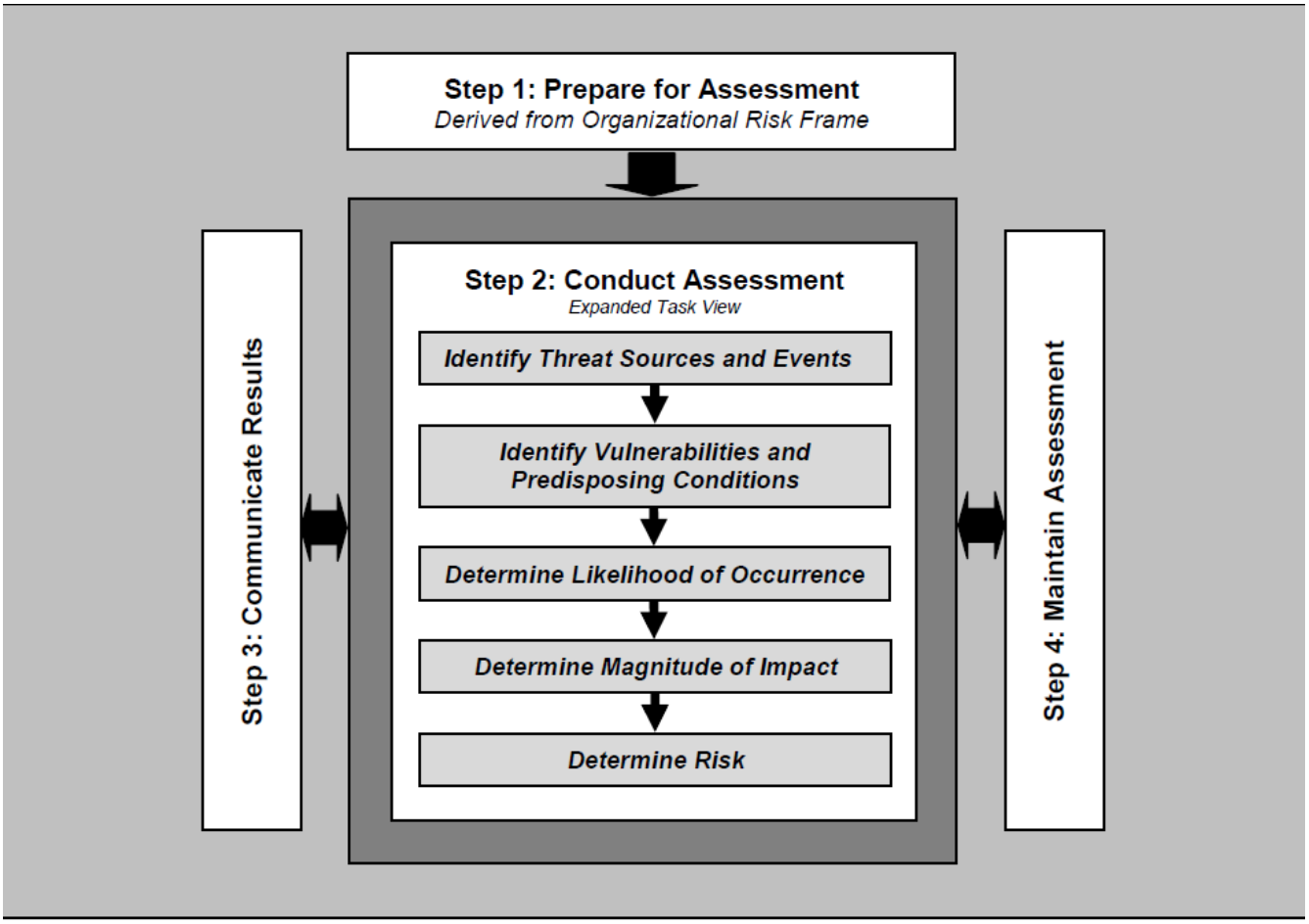
Source: NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

[3] AEIT Rule 71A-1.020(2), Florida Administrative Code.
[4] Section 282.318(2), Florida Statutes.
[5] Section 282.318(4)(c), Florida Statutes.
[6] NIST Special Publication 800-37.

As shown in Chart 1, the process of assessing IT security controls (i.e., performing a risk assessment) occurs in Step 4 of the framework and, prior to assessing the controls, an organization must categorize their information systems (Step 1), which includes the classification of data.

According to NIST,[7] the purpose of a comprehensive risk assessment is to inform decision makers and support risk responses by identifying relevant threats; identifying vulnerabilities; determining the likelihood of occurrence given the potential for threats exploiting vulnerabilities; determining the magnitude of harm (impact); and determining risk. The NIST risk assessment process is illustrated in Chart 2.

Chart 2
NIST Risk Assessment Process



Source: NIST Special Publication 800-30, *Guide for Conducting Risk Assessments.*

[7] NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*.

FINDINGS AND RECOMMENDATIONS

Finding 1: Comprehensive Risk Assessment Methodology – AST

Pursuant to State law,[8] the AST is to develop and publish for use by State agencies an IT security framework that includes guidelines and processes for using a standard risk assessment methodology. The methodology must include the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions. Additionally, State law[9] requires each State agency head to conduct, and update every 3 years, a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the agency. The risk assessment conducted must comply with the risk assessment methodology developed by the AST.

For the 2014 risk assessment due March 31, 2015, the AST required State agencies to utilize the self-assessment survey process that was used to perform assessments in 2008 and 2011. The self-assessment survey process was developed by the AEIT and consisted of a survey tool that compared State agency IT security controls to AEIT Rules[10] and identified IT security gaps. However, the survey tool did not provide the guidance necessary for State agencies to conduct a comprehensive risk assessment consistent with NIST standards and guidelines.[11] Specifically, the survey tool did not include instructions to guide State agencies in identifying and assessing the significance, likelihood, and impact of potential threats to, and vulnerabilities of, the State agencies' significant IT systems. Additionally, the survey tool did not provide guidance to State agencies relative to the analysis of existing controls that could mitigate or eliminate identified IT system threats. In response to our audit inquiry, AST management stated that they intended to update the recommended risk assessment guidance documentation before the next 3-year risk assessment due in March 2018.

Absent sufficiently comprehensive guidance, State agencies may lack the information necessary to conduct a comprehensive risk assessment, increasing the risk that security threats and vulnerabilities will not be identified and addressed, and that State agency data and IT resources may be susceptible to loss, compromise, and misuse.

Recommendation: We recommend that the AST incorporate the applicable NIST guidance in the methodology for future State agency risk assessments.

Finding 2: Comprehensive Risk Assessment Oversight – AST

Pursuant to State law,[12] State agencies must submit their completed comprehensive risk assessments to the AST and the AST is responsible for assisting State agencies with compliance with the Information Technology Security Act. The AST created a tracking sheet to record the receipt of each State agency's

[8] Section 282.318(3)(b)2., Florida Statutes.

[9] Section 282.318(4)(c), Florida Statutes.

[10] AEIT Rule 71A-1, Florida Administrative Code.

[11] NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*.

[12] Section 282.318(3)(b)3. and (c), Florida Statutes.

risk assessment and updated the sheet with the date each State agency uploaded its risk assessment to the secure portal used for collecting the risk assessments.

As part of our audit, we reviewed the AST's tracking sheet to determine whether the risk assessments due March 31, 2015, were completed and submitted timely to the AST and noted that the AST's oversight of the State agencies' risk assessments needs improvement. Specifically, we found that:

- Risk assessments were not submitted by 5 of the 31 State agencies and, as of March 1, 2016, the AST had not followed up with the State agencies.
- Risk assessments were not timely submitted by 4 of the 26 State agencies that submitted a risk assessment. The late risk assessments were submitted from 14 to 169 days late.
- Four of the 26 risk assessments submitted were incomplete and 6 were not signed by the appropriate State agency personnel.

Additionally, while AST management stated that they intended to review five State agency risk assessments for completeness, as of March 1, 2016, the AST could not provide documentation of such reviews.

Absent a sufficient risk assessment oversight process, the AST is not able to provide all the assistance necessary to promote State agency compliance with the Information Technology Security Act and the risk is increased that State agencies will not timely identify security threats to the data, information, and IT resources of the agencies.

Recommendation: The AST should develop an effective process for ensuring that State agency risk assessments are timely submitted and that the risk assessments submitted were properly completed and signed by appropriate State agency personnel.

Finding 3: Data Classification, Categorization of IT Systems, and Risk Mitigation

A comprehensive risk assessment includes data classification and categorization of IT systems based on the security objectives of confidentiality, integrity, and availability of information to effectively identify and prioritize IT security controls and IT security control deficiencies. For IT security control deficiencies identified during the risk assessment process, mitigation plans should be developed to resolve or reduce the risks.

For the 3-year risk assessment due March 31, 2015, AHCA, DCF, DEO, DOE, and DOT conducted a risk assessment that included identification of IT security controls and security control deficiencies. However, our examination of the agencies' risk assessment documentation disclosed that the agencies' did not complete the data classification and categorization of IT systems, thereby limiting the effectiveness of an ongoing risk management program and the development of security plans. Specifically, we found that the agencies':

- Specialized security awareness training was limited without the classification of data, including identification of confidential and exempt data that required specialized training.
- Audit logging and monitoring was limited without the identification of confidential and exempt data that requires logging and monitoring of access and transactions involving such data.
- Analysis of configuration management IT security controls for IT systems was ineffective without the classification of data and categorization of IT systems.

- Disaster recovery planning was less effective without the categorization of IT systems.
- IT security controls over backup resources were less effective without the identification of confidential and exempt data.
- Data loss prevention and incident response was limited without the identification of confidential and exempt data that should be monitored for loss or unauthorized access.

Additionally, AHCA, DOE, and DOT did not developed risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

The lack of data classification and categorization of IT systems and risk mitigation plans may reduce the agencies' assurance that risks and all likely threats and vulnerabilities have been identified and evaluated, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to mitigate through appropriate IT security controls, and which residual risks to formally accept.

Recommendation: To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Finding 4: IT Security Controls

IT security controls are safeguards and countermeasures prescribed for information systems or organizations that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems or organizations and satisfy a set of defined security requirements. According to the NIST framework, IT security controls include critical IT functions and activities. Such IT functions and activities include security awareness training, logging and monitoring, configuration management, standards for identification and authentication, disaster recovery planning, data loss prevention and incident response planning, and ongoing risk management.

Our review of selected IT security controls at AHCA, DCF, DEO, DOE, and DOT disclosed that some IT security controls need improvement. Specifically, we found that:

AHCA

- AHCA's policy on initial security awareness training needs improvement to ensure that the training is timely completed and acceptable use forms are signed by new employees prior to accessing IT resources, including confidential and exempt data.
- AHCA lacked a policy for configuration management addressing agency-managed hardware and software with the exception of mobile devices. Additionally, AHCA lacked a complete list of IT resource configurations.
- Certain IT security controls related to audit logging and monitoring and the use of administrative and service accounts need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising AHCA data and IT resources. However, we have notified appropriate AHCA management of the specific issues.

DCF

- The DCF lacked comprehensive policies, procedures, and guidelines for configuration management for the DCF-managed servers and all systems deployed in the DCF environment with the exception of mobile devices.
- The DCF lacked a comprehensive disaster recovery plan for one critical application.
- Certain IT security controls related to audit logging and monitoring and the use of administrative and service accounts need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising DCF data and IT resources. However, we have notified appropriate DCF management of the specific issues.

DEO

- The DEO lacked comprehensive policies, procedures, and guidelines for configuration management for DEO-managed hardware and software deployed in the DEO environment with the exception of mobile devices. Additionally, the DEO lacked network diagrams and a complete list of IT resource configurations and their associated owners or custodians for all DEO systems.
- The DEO lacked comprehensive policies, procedures, and guidelines for the backup and recovery of DEO-managed IT systems. Additionally, although the DEO conducted annual disaster recovery testing, DEO management could not provide documentation to support the testing or an evaluation of the test results.
- Certain IT security controls related to audit logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising DEO data and IT resources. However, we have notified appropriate DEO management of the specific issue.

DOE

- While the DOE had a draft security awareness policy[13] that required initial and annual security awareness training, the policy has been in draft form since 2010. Additionally, the policy lacked a requirement that annual training be documented, and DOE management stated that annual records of security awareness training were not maintained.
- The DOE lacked comprehensive policies, procedures, and guidelines for configuration management for application software deployed in the DOE environment. Additionally, while the DOE had created templates for IT development that analyzed systems and ensured IT security controls were effective and appropriate, the DOE lacked policies and procedures to ensure the use of the development templates.
- While the DOE relied on the Northwest Regional Data Center (NWRDC) for disaster recovery (DR) services, the NWRDC DR plan stated that NWRDC staff were only responsible for the recovery of the NWRDC mainframe and the loading of customer data. The NWRDC DR plan further stated that the customer was responsible for performing recovery steps as required once the customer systems were operational; however, the DOE did not have a documented and tested DR plan. Additionally, the DOE had not completed the identification of the IT systems to be designated as critical for priority DR services.
- The DOE had not identified application owners, defined security-related business requirements, or developed system security plans.
- Certain IT security controls related to audit logging and monitoring, the use of administrative and service accounts, and data loss prevention and incidence response need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising

[13] DOE, *Information Security Awareness Policy*, InfoSec 2.5.

DOE data and IT resources. However, we have notified appropriate DOE management of the specific issues.

DOT

- While the DOT had implemented Office of Information Systems (OIS) Method and Practice documents for baseline hardening, written policies and procedures that enforced the use of the OIS Method and Practice documents were not in place. Additionally, while the DOT had a documented change control process that required configuration changes for systems and applications to be approved, the process did not require verification of the systems and applications configurations to the baseline prior to implementation.
- While the DOT had a DR plan for critical IT resources and annually tested the DR plan for the mainframe, annual testing of the DR plan was not always performed for other critical IT resources.
- The DOT had not developed system security plans for all DOT systems.
- Certain IT security controls related to audit logging and monitoring need improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising DOT data and IT resources. However, we have notified appropriate DOT management of the specific issue.

The lack of appropriate IT security controls increases the risk that the confidentiality, integrity, and availability of agency data and IT resources may be compromised.

Recommendation: To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

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 2015 through January 2016 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 IT controls applicable to selected State agency comprehensive risk assessments due March 31, 2015, and selected actions taken subsequent thereto. The overall objectives of the 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 as related to the risk assessment process.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and 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 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 and controls 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 the IT systems and 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:

- Interviewed personnel at six selected State agencies: Agency for Health Care Administration (AHCA), Agency for State Technology (AST), Department of Children and Families (DCF), Department of Economic Opportunity (DEO), Department of Education (DOE), and Department of Transportation (DOT).
- Obtained an understanding of the key processes used for completing the comprehensive risk assessment process at the selected State agencies.
- Obtained an understanding of the key process used for the guidance and oversight process at the AST.
- Observed and evaluated the AST controls related to the guidance and oversight of the State agencies' comprehensive risk assessments and determined whether the comprehensive risk assessments due March 31, 2015, had been timely and properly submitted to the AST.
- Observed and evaluated the risk assessment processes, including assessing the IT security controls related to data classification and categorization of IT systems; security awareness training; logging and monitoring; configuration management; standards for identification and authentication; disaster recovery planning; data loss prevention and incident response planning; and ongoing risk management at the selected State agencies.
- 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. Managements' response is included in this report under the heading ***MANAGEMENTS' 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

MANAGEMENTS' RESPONSE

RICK SCOTT
GOVERNOR

ELIZABETH DUDEK
SECRETARY

July 22, 2016

Ms. Sherrill F. Norman
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Thank you for the opportunity to respond to the preliminary and tentative findings and recommendations from your information technology operational audit of the Comprehensive Risk Assessments at Selected Agencies: Agency for Health Care Administration. In accordance with your request, we have emailed you the preliminary and tentative audit findings document with our response for findings 3 and 4 incorporated therein.

If you have any questions regarding our response, please contact Mary Beth Sheffield, Audit Director, at 412-3978.

Sincerely,

Elizabeth Dudek
Secretary

ED/szg
Enclosure

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308
AHCA.MyFlorida.com

Facebook.com/AHCAFlorida
Youtube.com/AHCAFlorida
Twitter.com/AHCA_FL
SlideShare.net/AHCAFlorida

Agency for Health Care Administration
Auditor General Information Technology Operational Audit
of the Comprehensive Risk Assessments at Selected State Agencies
Response to Auditor General's P&T Audit Findings and Recommendations

Finding 3:
Data Classification, Categorization of IT Systems, and Risk Mitigation. The risk assessment process for AHCA, DCF, DEO, DOE, and DOT did not include the classification of data and categorization of IT systems. Specifically, we found that the agencies':

- Specialized security awareness training was limited without the classification of data, including identification of confidential and exempt data that required specialized training.
- Audit logging and monitoring was limited without the identification of confidential and exempt data that requires logging and monitoring of access and transactions involving such data.
- Analysis of configuration management IT security controls for IT systems was ineffective without the classification of data and categorization of IT systems.
- Disaster recovery planning was less effective without the categorization of IT systems.
- IT security controls over backup resources were less effective without the identification of confidential and exempt data.
- Data loss prevention and incident response was limited without the identification of confidential and exempt data that should be monitored for loss or unauthorized access.
- Additionally, AHCA, DOE, and DOT did not developed risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

Recommendation:
To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Agency Response:
AHCA will conduct an internal project within the agency to classify data. AHCA will also contract with a vendor to assist our agency in developing IT risk mitigation plans.

Agency Contact:
Karen Calhoun
(850) 412-4849

Finding 4:
IT Security Controls. Selected IT security controls for AHCA, DCF, DEO, DOE, and DOT need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

Specifically, we found that:

- AHCA's policy on initial security awareness training needs improvement to ensure that the training is timely completed and acceptable use forms are signed by new employees prior to accessing IT resources, including confidential and exempt data.
- AHCA lacked a policy for configuration management addressing agency-managed hardware and software with the exception of mobile devices. Additionally, AHCA lacked a complete list of IT resource configurations.
- Certain IT security controls related to audit logging and monitoring and the use of administrative and service accounts need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising AHCA data and IT resources. However, we have notified appropriate AHCA management of the specific issues.

Recommendation:
To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

Agency Response:
AHCA is in the process of developing new security policies and procedures based on Rule 74-2, F.A.C., which became effective March 10, 2016. AHCA is also proposing a FY 2017-2018 Legislative Budget Request to address monitoring and audit logging solutions.

Agency Contact:
Karen Calhoun
(850) 412-4849

State of Florida
Agency for State Technology

4050 Esplanade Way, Suite 115
Tallahassee, FL 32399-0950
Tel: 850-412-6050

Rick Scott, Governor

Jason M. Allison
State CIO/Executive Director

July 15, 2016

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

Dear Ms. Norman:

Pursuant to section 11.45(4)(d), Florida Statutes, enclosed is the Agency for State Technology's (AST) response to the preliminary and tentative audit finding and recommendations for the information technology operational audit of the *Comprehensive Risk Assessments at Selected State Agencies.*

AST appreciates the time and energy put forth by your staff to improve the operations of state government. If you have any questions concerning AST's response, please contact Tabitha McNulty, Inspector General, at 850-412-6022.

Sincerely,

Jason M. Allison
State CIO/Executive Director

JA:tam

Enclosure

cc: Curtis Unruh, Deputy Executive Director
Danielle Alvarez, Chief Information Security Officer
Tabitha McNulty, Inspector General

Agency for State Technology
Corrective Action Plan
Auditor General's Comprehensive Risk Assessment at Selected State Agencies

Finding #	**1**
Finding Title	**Comprehensive Risk Assessment Methodology - AST**
Finding Statement	The risk assessment guidance provided by the AST to the State agencies did not sufficiently promote compliance with the National Institute of Standards and Technology [NIST] risk assessment requirements.
Recommendation	We recommend that the AST incorporate the applicable NIST guidance in the methodology for future State agency risk assessments.
Program Response	The Agency for State Technology (AST) concurs and on March 16, 2016, AST promulgated Rule 74-2, Florida Administrative Code. This Rule incorporated the applicable NIST guidance.
Status Date	July 2016
Contact Person	Danielle Alvarez
Program/Unit	Chief Information Security Officer
Phone Number	850-412-6050

Finding #	**2**
Finding Title	**Comprehensive Risk Assessment Oversight - AST**
Finding Statement	The AST's oversight of the State agencies' risk assessments needs improvement to better assist State agencies with the timely submittal of properly completed risk assessments.
Recommendation	The AST should develop an effective process for ensuring that State agency risk assessments are timely submitted and that the risk assessments submitted were properly completed and signed by appropriate State agency personnel.
Program Response	AST concurs. AST has drafted a process to track timely submission and completion of agency risk assessments. The final process document will be completed by July 31, 2016, and therefore, will be in place before the next 3-year risk assessment due date.
Status Date	July 2016
Contact Person	Danielle Alvarez
Program/Unit	Chief Information Security Officer
Phone Number	850-412-6050

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

July 19, 2016

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

Dear Ms. Norman:

Thank you for the opportunity to respond to your June 24 list of preliminary and tentative audit findings and recommendations on the audit titled *Comprehensive Risk Assessment at Selected State Agencies: Agency for Health Care Administration (AHCA), Agency for State Technology (AST), Department of Children and Families (DCF), Department of Economic Opportunity (DEO), Department of Education (DOE), and Department of Transportation (DOT).*

Enclosed is the Department of Children and Families' response. Should you have any questions, please contact Joseph Vastola, Chief Information Officer, at (850) 320-9132.

Sincerely,

Mike Carroll
Secretary

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Work in Partnership with Local Communities to Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS
FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES
Comprehensive Risk Assessments at Selected State Agencies:
Agency for Health Care Administration (AHCA),
Agency for State Technology (AST), Department of Children and Families (DCF),
Department of Economic Opportunity, (DEO), Department of Education (DOE),
and Department of Transportation (DOT).

Finding No. 3: The risk assessment process for AHCA, DCF, DEO, DOE, and DOT did not include the classification of data and categorization of IT systems. Additionally, AHCA, DOE, and DOT did not develop risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

Recommendation: To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Response: The Department has completed a provisional data classification and categorization of IT systems. The Department will continue to update and implement this recommendation through its risk assessment processes.

Finding No. 4: Selected IT security controls for AHCA, DCF, DEO, DOE, and DOT need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

Recommendation: To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

Response: Currently, the Department is updating the policies, procedures, and guidelines for configuration management for the Department's managed servers and systems in the Department's environment.

The Department is working with the newly contracted vendor to create a comprehensive disaster recovery plan.

Currently, the Department is updating the policies and procedures related to audit logging and monitoring along with the use of administrative and service accounts.

Rick Scott
GOVERNOR

FLORIDA DEPARTMENT of ECONOMIC OPPORTUNITY

Cissy Proctor
EXECUTIVE DIRECTOR

July 15, 2016

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

Dear Ms. Norman:

Enclosed is the Department's response to the preliminary and tentative findings resulting from your information technology operation audit. We thank you and your staff for recommendations designed to enhance the efficiency of services to the citizens of our State.

If you have additional questions or needs, please contact Jim Landsberg, Inspector General, at (850) 245-7141.

Sincerely,

Cissy Proctor

CP/tc

Enclosure

Florida Department of Economic Opportunity | Caldwell Building | 107 E. Madison Street | Tallahassee, FL 32399
866.FLA.2345 | 850.245.7105 | 850.921.3223 Fax
www.floridajobs.org | www.twitter.com/FLDEO | www.facebook.com/FLDEO

Finding 3: Data Classification, Categorization of IT Systems, and Risk Mitigation.

Auditor Recommendation: To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, **DEO**, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Department of Economic Opportunity (DEO) Response:

DEO will include classification of data and categorization of IT systems for future risk assessment processes.

Finding 4: IT Security Controls

Auditor Recommendation: To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, **DEO**, DOE, and DOT management improve their agencies' IT security controls.

Department of Economic Opportunity (DEO) Response:

DEO is acutely aware of a need for security control improvement, and current security resources are fully utilized toward this effort.

- Policies related to configuration management and Backups are in the process of being updated and are expected to be published no later than Jan 1, 2017.

- A holistic IT procedure and guideline refresh project has been requested within DEO's IT Governance process. The project has not yet been scheduled, but is expected to begin Q2 2016-17 based on available resources. This should address issues with procedures and guidelines related to configuration management, backups, and audit logging and monitoring.

FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

July 22, 2016

Sherrill F. Norman, CPA
Auditor General
Office of Auditor General
111 West Madison Street, Suite G74
Tallahassee, FL 32399-1450

Dear Ms. Norman:

The following responses are offered with respect to the information technology operational audit of the Comprehensive Risk Assessments at Selected State Agencies.

Data Classification, Categorization of IT Systems, and Risk Mitigation

Finding 3: The risk assessment process for DOE did not include the classification of data and categorization of IT systems. Additionally, DOE did not develop risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

Recommendation: To ensure effective, comprehensive risk assessments, we recommend that DOE management include the classification of data and categorization of IT systems in their risk assessment processes and that management develop risk mitigation plans for all identified IT security control deficiencies.

Response: The Department through an engagement with Deloitte has already developed a comprehensive plan for Enterprise Data Governance that addresses classification of data and IT systems. In such, the plan outlines the resources needed for classifying and categorizing of all DOE information systems including data. Therefore, the Department is currently implementing Enterprise Data Governance based on the plan.

IT Security Controls

Finding 4: Selected IT security controls for DOE need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

Recommendation: To better ensure the confidentiality, integrity, and availability of agency data

and IT resources, we recommend that DOE management improve their agency's IT security controls.

Response: The Department agrees that additional policies/plans are needed to address security awareness, disaster recovery, and configuration management. These policies will be drafted within the next 90 days. The remaining confidential control issues are being addressed.

If you need additional information, please feel free to contact Martha K. Asbury, Assistant Deputy Commissioner, Finance and Operations, at (850) 245-0420 or via email at Martha.Asbury@fldoe.org.

Sincerely,

Pam Stewart

Pam Stewart
Commissioner

PS/tln

cc: Mike Blackburn, Inspector General
Linda Champion, Deputy Commissioner, Finance and Operations
Martha Asbury, Assistant Deputy Commissioner, Finance and Operations
Andre Smith, Deputy Commissioner, Division of Technology and Innovation
Kevin Younger, Information Security Manager

FDOT

Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

JIM BOXOLD
SECRETARY

July 21, 2016

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

Dear Ms. Norman:

I am pleased to respond to the preliminary and tentative audit findings and recommendations concerning your audit of:

Department of Transportation – IT Operational Audit
Entitywide Information Technology Risk Assessment Process

As required by Section 11.45(4) (d), Florida Statutes, the department's responses to the Federal Awards audit findings are enclosed. The Department's response to Confidential Finding No. 1 will be separately provided by secure mean (FTA).

I appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact our Inspector General, Bob Clift, at 850-410-5800.

Sincerely,

Rachel D. Cone

for Jim Boxold
Secretary

JB: cm

Enclosures (2)

cc:
Rachel Cone, Assistant Secretary- Finance and Administration
April Blackburn, Chief Information Officer
Robert E. Clift, Inspector General
Kristofer Sullivan, Director of Audit

Response to Finding

Finding No. 3: Data Classification, Categorization of IT Systems, and Risk Mitigation

A comprehensive risk assessment includes data classification and categorization of IT systems based on the security objectives of confidentiality, integrity, and availability of information to effectively identify and prioritize IT security controls and IT security control deficiencies. For IT security control deficiencies identified during the risk assessment process, mitigation plans should be developed to resolve or reduce the risks.

For the 3-year risk assessment due March 31, 2015, AHCA, DCF, DEO, DOE, and DOT conducted a risk assessment that included identification of IT security controls and security control deficiencies. However, our examination of the agencies' risk assessment documentation disclosed that the agencies' did not complete the data classification and categorization of IT systems, thereby limiting the effectiveness of an ongoing risk management program and the development of security plans. Specifically, we found that the agencies':

- Specialized security awareness training was limited without the classification of data, including identification of confidential and exempt data that required specialized training.
- Audit logging and monitoring was limited without the identification of confidential and exempt data that requires logging and monitoring of access and transactions involving such data.
- Analysis of configuration management IT security controls for IT systems was ineffective without the classification of data and categorization of IT systems.
- Disaster recovery planning was less effective without the categorization of IT systems.
- IT security controls over backup resources were less effective without the identification of confidential and exempt data.
- Data loss prevention and incident response was limited without the identification of confidential and exempt data that should be monitored for loss or unauthorized access.

Additionally, AHCA, DOE, and DOT did not developed risk mitigation plans for all IT security control deficiencies identified in the risk assessment process. The lack of data classification and categorization of IT systems and risk mitigation plans may reduce the agencies' assurance that risks and all likely threats and vulnerabilities have been identified and evaluated, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to mitigate through appropriate IT security controls, and which residual risks to formally accept.

Recommendation: To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Agency Response and Corrective Action Plan:
Agree. A risk assessment for Fiscal Year 2016-2017 has been funded by the Legislature. During this risk assessment, the classification of data and the categorization of IT systems will be included in the project scope. FDOT is working to develop formal risk management processes and governance. Risk mitigation will be part of that project.

Estimated Corrective Action Date:
By June 30, 2017

Agency Contact and Telephone Number:
April Blackburn (850) 414-4771

Finding No. 4: IT Security Controls

IT security controls are safeguards and countermeasures prescribed for information systems or organizations that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems or organizations and satisfy a set of defined security requirements. According to the NIST framework, IT security controls include critical IT functions and activities. Such IT functions and activities include security awareness training, logging and monitoring, configuration management, standards for identification and authentication, disaster recovery planning, data loss prevention and incident response planning, and ongoing risk management.

Our review of selected IT security controls at AHCA, DCF, DEO, DOE, and DOT disclosed that some IT security controls need improvement. Specifically, we found that:

- While the DOT had implemented Office of Information Systems (OIS) Method and Practice documents for baseline hardening, written policies and procedures that enforced the use of the OIS Method and Practice documents were not in place. Additionally, while the DOT had a documented change control process that required configuration changes for systems and applications to be approved, the process did not require verification of the systems and applications configurations to the baseline prior to implementation.
- While the DOT had a DR plan for critical IT resources and annually tested the DR plan for the mainframe, annual testing of the DR plan was not always performed for other critical IT resources.
- The DOT had not developed system security plans for all DOT systems.
- Certain IT security controls related to audit logging and monitoring need improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising DOT data and IT resources. However, we have notified appropriate DOT management of the specific issue.

The lack of appropriate IT security controls increases the risk that the confidentiality, integrity, and availability of agency data and IT resources may be compromised.

Recommendation: To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

Agency Response and Corrective Action Plan:
Agree. The OIT will develop policies and procedures that enforce the use of the OIT methods and practices. By June 30, 2017.

Agree. The OIT is currently in the process of implementing a change control process that will include the verification of the systems and applications configurations to the baseline prior to implementation. This will be a multi-phased project with the first phase to be completed by June 30, 2017.

Agree. The Department agrees that some critical IT resources were not included in the DR plan testing, however, this was due to a lack of available funds and staff resources. If the resources needed are made available, the Department will develop a process for testing the DR plan that includes these critical IT resources. OIT is unable to provide a completion date at this time because it is not known when, if ever, the Legislature will approve the financial resources needed to complete the DR process.

Agree. The Department is currently working to identify those systems that currently have no security plan. Once identified, security plans will be developed for those systems. The initial phase of this project is the identification of those systems that currently have no security plan. This phase of the project is to be done by June 30, 2017.

Agree. The Department is working to correct items reported for logging and monitoring.

Estimated Corrective Action Date:
See individual dates above.

Agency Contact and Telephone Number:
April Blackburn (850) 414-4771