OBM | Office of Internal Audit

Department of Transportation
DOT IT General Controls Audit

Audit Period: July 2017 through June 2018

Results Summary:

Objective	Conclusion
IT Governance	Improvement Needed
Application System Development	Well-Controlled
Change Management	Improvement Needed
Security Management	Major Improvement Needed
Operations	Well-Controlled

* Refer to Appendix A for classification of audit objective conclusions.

Report number: 2019-DOT-20 **Issuance date: September 20, 2018**

Executive Summary

Background

The ODOT maintains and oversees Ohio's transportation infrastructure including: bicycle and pedestrian, aviation, highways, public, rail, water and commercial. A number of computer systems are used to help ODOT fulfill its charter and achieve its objectives. Between the months of July and September 2018, the OBM Office of Internal Audit (OIA) performed an IT General Controls audit of the financially significant applications operated and maintained by the agency's Department of Information Technology (DoIT).

The review of controls and transactions was performed between July and September 2018 and the audit period was fiscal year 2018. The Auditor of State is relying on OIA's work as part of their audit of the State of Ohio financial statements and Single Audit. OIA's objective summary results and detailed observations are shown on the following pages. The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

This report is solely intended for the information and use of agency management, the Auditor of State, and the State Audit Committee. It is not intended for anyone other than these parties.

ODOT's IT leadership team has demonstrated a proactive approach towards managing risks. IT staff and management involved in the IT General Controls audit were open and collaborative throughout the engagement. OIA would like to thank ODOT staff and management for their cooperation and time in support of this audit.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's IT general controls. This work was completed July through September 2018. The scope of this audit included the following areas:

- IT Layers: Application, Database, Operating System, and Operations
- Applications: Current Billing System, Appropriation Accounting, Site Manager, Structure Management System, and RIMS
- Testing Bridge and Pavement Condition Assessment Rating

The following summarizes the objectives of the review:

- **IT Governance** - IT is meeting the needs of the business; compliance requirements are adequately addressed; resources are appropriately deployed; and IT control environment is operating effectively.

- **Application System Development** - Software development life cycle and project management processes in place to help ensure that systems are developed based upon a consistent set of standards.

- **Change Management** - Changes to application and system functionality is consistent with business requirements, the system operates within specifications, changes are tested and approved prior to implementation, and production is not susceptible to unauthorized modification.

- **Security Management** – Administrative, logical and physical controls adequately protect the confidentiality, integrity and availability of computer resources per business requirements.

- **Operations** - Processes supporting the integrity and reliability of activities impacting the operation of the organization's computer resources are effective.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Seperated Employees Are Not Timely Disabled

State of Ohio IT Standard, ITS SEC-02, and SANS Top 20 Critical Controls state that a process should exist to revoke system access by disabling accounts immediately upon termination of an employee or contractor.

OIA noted that when an employee is terminated, Human Resources (HR) opens a termination ticket in ServiceNow. Once the ticket is complete, a confirmation email is generated to the requestor. OIA selected a sample of terminated employees for testing and noted the following:

- 14of 40 (35%) separated employees with an Active Directory account were not disabled timely after separation from the agency.

- 2of 40 (5%) separated employees with an Active Directory account had an enabled account after separation from ODOT.

- 1 of 77 (1.3%) separated employees had an active mainframe administrator account. This administrator account is being used by another individual at DAS/OIT. The password to this account has been changed. The corresponding Active Directory account was disabled at the time of separation.

- 1 of 12 (8%) Appropriation Accounting administrators and 1 of 8 (13%) Current Bill administrators had enabled accounts, however, both employees changed positions during FY18 and no longer needed this access. Per inquiry by auditor, access was disabled.

At this time, the ODOT Division of Information Technology is in process of implementing a Separation Process that remedies this observation. The failure to disable, delete or reconcile user accounts in a timely manner after separation increases the risk of unauthorized access to systems and data.

Recommendation

Management should identify the issues causing delays in the deprovisioning process or the reason these accounts are not disabled timely. Also, management should consider implementing a reconciliation process of separated employees to ensure that errors are caught and corrected timely. Results of the reconciliation should be approved and maintained as evidence per agency retention policy. This process should focus on centralizing the process and working with the districts to ensure uniform compliance.

Management Response

IT is working with HR to ensure timely separations. Central Office HR discussed the issue with District HR personnel and sent a follow up communication on 9/25/18 outlining the process HR (District/CO) needs to follow to ensure timely separations. Central Office IT sent out a communication to District IT Managers dated 9/24/18 stating procedures to be followed for on and off boarding, which included a review of the separation list by the IT Manager or their designee to ensure timely separations. If a ticket has not been submitted by HR for an employee separation, IT is to request the ticket submittal in Service Now. A 10 percent review will be conducted by CO IT of separations based upon the bi-weekly listing sent out by HR.

A group is being put together to discuss the on & off boarding of consultants and contractors. Recommendations from this group should be expected by 12/31/18 and implementation/training of the process to follow. Full implementation should be expected no later than April 1, 2019.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
High	CIO	April 1, 2019

Observation 2 – Inappropriate Level of Approval for Account Access

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standard, AC-2 Account Management, states that the organization "requires approvals (by agency defined personnel) for requests to create information system accounts".

Network access requests are initiated by HR or the district hiring manager completing a ServiceNow new user request. This request process includes supervisor approval within the ServiceNow tool.

Per review of the ServiceNow account request process, 4 of 40 (10%) new hire samples tested did not have supporting approvals documented in ServiceNow.

Without evidence of the appropriate level of approval for account access, the risk increases that individuals are given inappropriate access or unintentional modifications are made to systems and data.

Recommendation

Each of the twelve districts within the State has their own HR and IT departments that manage ServiceNow requests for new users. Central Office should continue to stress the importance of management oversight to district leadership. Central Office should also assess the risk of errors and omissions at the district offices and, as deemed appropriate, perform periodic reviews of established controls to determine whether they are functioning properly.

Management Response

A revised hiring questionnaire has been created and is currently being utilized by the Central Office Service Desk. This questionnaire for new hire access is to be attached to the ServiceNow request.

Communications about the questionnaire have been submitted to the District IT Managers for their use on 9/27/18. Additional discussion to be held at the next IT Manager's meeting in November.

Discussion to be held with Central Office HR to determine procedures to institute a periodic review of new hire documentation. Procedures will be documented and review to begin in the spring of 2019.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	March 31, 2019

Observation 3 – No Formal Process for RIMS User Access Reconciliations

State of Ohio IT Standard ITS-SEC-02 policy identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standard, AC-2 – Account Management, states the agency should "actively manage the life-cycle of system and application accounts - their creation, enabling, modifying, and disabling, and removing accounts" - in order to minimize opportunities for attackers to leverage them.

For the Roadway Inventory Management System (RIMS), no user account reconciliations were performed during FY18. As users onboard or offboard, the RIMS manager notifies the Oracle DBA and the Application Administrator through a Service Now ticket. Since the number of users with access to the application is small, management has performed the function manually and informally.

The risk of not developing or maintaining strong controls over management of user accounts could result in inappropriate access, modifications, or exposure to the application's data.

Recommendation

Recommend creating formal, documented policy for reconciling user accounts in RIMS. Steps in the process should identify the scope of the account reviews, how often accounts are reviewed, who conducts the reviews, how to ensure the state of user accounts is appropriate, and how to remedy identified issues.

Management Response		
The Department of Information Technology at ODOT has worked with the division of Technical Services in order to create a formal process for reconciling user accounts within the RIMS system. ODOT provided OIA with the new process and the results of the reconciliation.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
Moderate	CIO	August 31, 2018

Observation 4 – Domain Administrator Accounts Are not Periodically Reviewed

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standard, AC-2 Account Management, states that agencies should require accounts with elevated privileges to "specify authorized users of the system and ensure required approvals for requests to create accounts." The agency should manage "creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles)."

During review, there were 35 enabled domain administrator accounts. Four of these were service accounts, nine belonged to ODOT staff/contractors, and 22 belonged to DAS/OIT staff. ODOT management verified the service accounts and ODOT staff/contractor accounts, however, DOT could not verify some of the DAS/OIT administrator accounts for appropriateness or if the administrator account was still needed. There is no agreement in place between OIT and ODOT on how to handle and communicate OIT staff's creation and disabling of domain administrator accounts on ODOT's systems.

Administrator or privileged accounts have elevated rights to systems and data. The failure to periodically verify these accounts are appropriate and required increases the risk to the confidentiality, integrity, and availability of systems and data.

Recommendation
ODOT and DAS/OIT management should work together to agree how to handle creation and disabling of domain administrator accounts on ODOT's systems. When DAS/OIT needs to create a domain admin account, ODOT should be notified. The corresponding domain administrator account should be disabled on the separation date. As part of ODOT's review

procedures, in the quarterly meeting held by ODOT IT and DAS/OIT management, domain administrator accounts should be discussed and reviewed for appropriateness.

Management Response
ODOT IT discussed this finding with DAS/OIT at our joint FY18 Quarterly Review meeting on 9/25/18. OIT has indicated that moving forward, they will more regularly review OIT membership to ODOT's Domain Administrator group. Additionally, ODOT will be submitting a list of all current Domain Admins to DAS/OIT one (1) week previous to future Quarterly Review meetings, so that (as a permanent addition to the meeting agenda), both agencies can review and remediate membership as needed. ODOT has also implemented alerting in such a way that when any person is added to this group, an alert is generated and emailed to ODOT IT personnel, just in case OIT fails to notify ODOT of the addition at the time it takes place.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	January 31, 2019

Observation 5 – Security Awareness Training is Not Provided to Contractors

The State of Ohio IT Standard, IT-SEC-02, Enterprise Security Controls Framework, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implemented for the State of Ohio. NIST 800-53r4 AT-2 provides guidance that the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes; and the organization provides refresher security awareness training in accordance with the organization-defined frequency.

Department of Administrative Services (DAS) directive IT-15 IT Security Awareness and Training requires information technology (IT) security awareness and training for the State of Ohio information system users, which includes employees, contractors, temporary personnel and other agents of the State.

Securing Ohio - Security and Privacy Training is the DAS-prescribed security training for cybersecurity awareness. Ohio Department of Transportation (ODOT) provides this training to full-time employees; however, it is not administering the required DAS training to its contractors. ODOT's rationale for not complying with the training requirements is contractor's descriptors (i.e. job codes) were not included in the ODOT Learn System employee population. Additionally,

Human Resources has limited or no access to DAS' Enterprise Learning Management (ELM), which is the statewide eLearning system.

Providing security awareness training for all employees helps to eradicate risky behaviors that could potentially lead to a network compromise. Lack of time dedicated to employee security awareness training and the lack of communication security exception are key reasons organizations' cybersecurity awareness programs fail to meet their objectives. Furthermore, uninformed users may increase the exposure to security attacks such as phishing emails, malware from inappropriate websites and social engineering.

Recommendation

Management should require security awareness and training be completed at onboarding and annually thereafter by all ODOT employees to include contractors, temporary personnel and other agents of the State. Consider alternative means to ensure security awareness training is completed by all employees, such as utilizing DAS ELM as a means of distribution. Furthermore, management should define and implement procedures for monitoring, reporting, and establishing escalation and service level performance resolution methods for service level issues.

Management Response

ODOT agrees that security awareness and training is essential to all employees including contractors, temporary personnel and other agents of the State. ODOT will be working in coordination with the Office of Information Security and Privacy (OISP) to require contractors, temporary personnel and other agents of the State to use the DAS ELM security awareness and training solution. Processes and procedures will be adopted to monitor new employees who are not included in the ODOT Learn training and reporting processes are being established to notify OISP to add them to the DAS ELM solution. As the processes and procedures are finalized, reports of the training status and escalation of personnel not completing the training will be addressed and established. This solution will be implemented by December 31, 2018 and re-evaluated on an annual basis and will be addressed as part of the onboarding requirements.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	December 31, 2018

Observation 6 – Policies and Procedures Need to be Periodically Reviewed and Updated

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standards state that the agency should "develop and document procedures to facilitate the implementation of security controls," the policies should be "reviewed and updated" at an "agency defined frequency." Procedures should address "scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance." It also states, "the organizational risk management strategy is a key factor in establishing policy and procedures."

Per discussion with management, DOT is conducting a risk-based annual review and approval of agency policies. During our review, OIA noted the following issues:

1. DOT's Policies, Standards and Procedures references DAS policies for password standards. However, there is no approved DAS password policy in place applicable to agencies for FY18. DOT is in the process of creating their own password policy, which is currently in draft form and awaiting DOT management approval.

2. Within the IT Service Desk policy dated May 2014, the escalation procedure contains references to employees who have since separated from the agency.

3. The SDLC policy, the DOT Schedule Task Environment Overview policy and the IT Release Management policy do not have a periodic review process in place. These policies were last updated in 2012 and 2011, with no evidence they have been reviewed by management since then for accuracy.

A lack of accurately documented IT security policies and procedures may lead to ineffective security control implementation and monitoring, leaving the agency vulnerable to compromise. Failure to implement and enforce a standard policy review process can prevent policies from being approved by the appropriate level of senior management and prevent tactical procedures, standards, or guidelines from supporting the objectives of those policies.

Recommendation

Management should continue working toward getting the DOT password policy approved by management. Controls in the approved password policy should be implemented on DOT systems. For instances where parameters may not be implemented due to password limitation requirements, exception reports should be created and approved by management.

The escalation procedures in the IT Service Desk policy should be updated to include those responsible for escalating service issues. If appropriate, rather than listing employee names within the direct policy, consider referencing titles, designations, or a central contact sheet that

management can update as needed without constant updates to the policy to reflect personnel changes.

All policies and procedures should be formally reviewed on a regular basis, as defined and documented by agency management, to ensure the policies continue to reflect the agency's objectives and actual practices in place.

Management Response

IT Service Desk Manager is in the process of re-writing procedures for the Service Desk that include all after-hours escalation processes. An additional document that is noted in the procedure will list employee names and phone numbers for escalation rather than including that information in the procedure itself. Documentation for executive management review is set to be completed by December 31, 2018 and implemented after approval.

In addition, in order for ODOT to continue to be compliant with required State of Ohio security controls, an implementation of new policies that are in alignment with current State of Ohio IT ITS-SEC-02 standards will be created, approved and reviewed bi- annually for compliance to State of Ohio IT security standards and policies. These policies will assist in keeping ODOT more secure from compromises and fulfilling the OBM OIA audit recommendations found in the DOT FY19 IT General Controls Review.
A bi-annual standard policy review process will be created in order to strengthen tactical procedures, standards, or guidelines in support of the business objectives of ODOT. During this review, policy gaps will be identified, and timeframes identified for implementing the new policies or changes to policies.

Currently, two (2) policies (Information Technology Resource Policy, Password Policy) and two (2) standards (Password Standard for Organizational Users, Password Standard for Non-Organizational Users) have been submitted for final approval with the Director's office and have been approved by District Deputy Directors. An additional six (6) policies (Access Controls, Security Education and Awareness, Data Classification, Mobile Computing, Malicious Code Defense, Risk Assessment) have been submitted to the Communication Office for approval. Once the Communication Office approves these policies, the District Service Managers will review and comment on the policy content. When finalized, these six (6) new policies will be submitted to the District Deputy Directors for approval. ODOT plans on implementing these eight (8) policies and two (2) standards by December 31, 2018. In addition, twelve (12) new policies will be added to this same process with the goal of adoption by June 30, 2019.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	June 30, 2019

Observation 7 – Testing is not Consistently Performed Prior to Releasing Changes into Production

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standards state that the agency should implement "separation of duties which addresses the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion." Additionally, ODOT has a release management process in place to help ensure changes are documented, tested, and implemented based upon a consistent set of standards. ODOT's IT Release Management v1.5 states "if users accept the tested changes, they need to sign-off on the changes prior to moving to the next step".

Release management forms reviewed did not consistently evidence the required testing acceptance prior to releasing changes to the production environment. During our review of the change management process, OIA testing noted the following:

- Two of the fourteen (14%) change request release forms reviewed lacked evidence to support testing was appropriately approved prior to releasing changes into production. One release form was missing testing information including the tester name, while the other contained a supervisor authorization that was dated after the release date.

The lack of evidence to support testing being completed and authorized prior to releasing changes into production increases the risk of incomplete deliverables and/or unauthorized changes applied to production environments. Furthermore, failure to evidence who performs the change testing leads to an increased risk of inadequate segregation of duties in the release management process.

Recommendation

Ensure that managers and employees are aware that documentation of change testing is required in all instances. Completion of the release management procedures should be evidenced through signature of the tester and approver names, date(s), and any explanation, if necessary, within the IT release management form. If a particular step is determined to be unnecessary, the proper approvals and justification should be appropriately documented and dated in the release management form.

Management Response

ODOT is in the process of deploying the Change Management module in its ServiceNow instance. This tool will help not only with Release Management, but also other changes to the environment here. The target date for initial implementation is 12/31/2018. Once deployed, we

will be working through modification of the workflows to make it work with ODOT's Software Development Lifecycle for cohesion. Once training is complete, we should have a fully useable system. We expect to complete these aspects by 3/31/2019.

In the meantime, we will follow up periodically with staff to ensure that they are aware that documentation of change testing is required in all instances, and to follow existing release management procedures.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	March 31, 2019

Observation 8 – Disaster Recovery plan is not in place

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standard, CP-2: Contingency Plan, CP-4: Contingency Plan Testing, CP-6: Alternate Storage Site, CP-7: Alternate Processing Site refer to developing a contingency plan, identifying essential missions and business functions, providing recovery objectives and metrics, developing test scenarios and testing them at a secure off-site location to help ensure its effectiveness. Disaster recovery and contingency planning help ensure an entity can accomplish its mission and has the capability to process, retrieve, and protect information maintained in its systems in the event an interruption or disaster leads to temporary or permanent loss of the computer facilities.

During the audit period, ODOT's hardware and system/application software were maintained and administered at the State of Ohio Computer Center (SOCC) by the DAS/OIT. However, no agreement exists between DAS/OIT and ODOT regarding how disaster recovery operations are to be handled. Through review, OIA noted the following:

1. A service level agreement between ODOT and DAS/OIT to define the DR responsivities for each party did not exist.

2. Duplicate data services or redundant data center locations were not identified for the non- mainframe ODOT operations.

3. There was no approved agency-level disaster recovery/business resumption plan to provide comprehensive detailed agreed-upon data and business recovery guidance for both DAS/OIT and ODOT personnel.

4. Disaster recovery testing of the SiteManager, Appropriation Accounting, Current Billing, RIMS, or Structure Management System applications did not occur at an alternate processing facility during the audit period.

Without an approved plan to document and delineate agreed-upon data and business recovery functions between two separate agencies, timely and effective recovery of IT operations may not occur according to management's expectations. In the absence of a secure, redundant processing environment, recovery functions may not occur effectively. Failure to regularly test and maintain disaster recovery and business resumption plans could result in slow or ineffective recovery if recover testing lessons are not learned and applied for actual disaster occurrences.

Recommendation

ODOT and DAS/OIT should implement a service level agreement between the two agencies to clearly define the disaster recovery services provided by DAS/OIT for the agency. In addition, ODOT should implement agency level disaster recovery plans to cover the areas not covered by the service level agreement between ODOT and DAS/OIT. Because disaster recovery and business resumption is an area of shared responsibility between the agency and the service provider (DAS/OIT), ODOT personnel will have involvement in the disaster recovery process, and the agency-level disaster recovery plan should identify key agency personnel, prioritized applications and datasets, and define ODOT responsibilities and resources to be engaged in the
event of a disaster.

In addition, once the plan is implemented, DAS/OIT and ODOT management should perform periodic testing of the DR plan. Any weaknesses noted during testing must be evaluated and corrective action taken to ensure the DR plan provides adequate and current business recovery and system availability. Going forward, a testing schedule should be created to facilitate the continued monitoring and testing of the DR plan. Also, a redundant off-site location must be established to provide both testing and alternate processing facilities in the event of a disaster.

Management Response

ODOT is well aware of the issue with the lack of a DR plan for IT Operations. As has been stated in previous responses to the same issue, although we understand that the responsibility resides with ODOT from a legal point of view, from a practical view, ODOT cannot, by itself, create, nor execute a DR plan successfully. DAS/OIT now owns the core infrastructure components necessary to operate ODOTs technical operations, and to successfully test the same.

ODOT has reached out to DAS/OIT on several occasions in order to cooperatively create a DR Plan. We consider a DR Plan to be a set of instructions, with an order of execution, such that if

properly performed, would result in successful technical operations of ODOT systems. While things like DR sites/services, and system redundancies could play parts within a DR Plan, these things, in and of themselves are not a DR Plan, nor could they become one.

We will continue to reach out to DAS/OIT in order to reach agreement on creation of a plan and its testing plan. ODOT has no choice but to simply create the outline of the plan, and their order of execution. It will not be possible to execute the plan, nor to test it without the assistance of DAS/OIT. We will endeavor to have ODOT's part of the plan created by March 31, 2019.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	March 31, 2019

Observation 9 – Security Assessment and Authorization Not Completed for RIMS

The State of Ohio IT Standard, IT-SEC-02, Enterprise Security Controls Framework, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation in the State. The NIST 800-53 security assessment and authorization (CA) control family provides guidance that agencies develop an agency-defined frequency for updating security authorization.

ODOT's established Privacy Impact Assessment Policy 28-016 reads that departments shall create privacy impact statements prior to the implementation of any information technology data system. Privacy impact statements consist of a Privacy Threshold Assessment (PTA), a Privacy Impact Assessment (PIA), or both. OIA noted during testing that ODOT was unable to provide a copy of the PTA for the Roads Inventory Management System (RIMS) for the current audit period, FY18.

The compliance process begins with a PTA or PIA, which serves as the official determination to whether a department program or system has privacy implications to mitigate privacy risks. Not completing the appropriate assessment may lead to the improper identification of systems with sensitive data and lack of proper security controls over those systems.

Recommendation
Management should complete a privacy threshold analysis on all systems to include but not be limited to the Roads Inventory Management System (RIMS) in order to be compliant with NIST 800-53 and the ODOT Privacy Impact Assessment Policy 28-016. Ensure the completed privacy threshold analysis and privacy impact assessment forms are maintained, periodically reviewed, and updated in accordance with policy.
Management Response
RIMS-PTA was submitted to OBM OIA on August 30, 2018. No Privacy Impact Assessment (PIA) was required. According to the ORC, an updated PIA or PTA is required for major enhancements or upgrades. If there are no changes, there is no requirement for a new PIA or PTA.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	August 30, 2018

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Refer to Appendix A for classification of audit observations.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee