OBM | Office of Internal Audit

Department of Administrative Services
Data Classification Audit

Audit Period: June through September 2018

Results Summary:

Objective	Conclusion
Data Classification	**Improvement Needed**

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

Report number: 2019-DAS-21 **Issuance date: September 20, 2018**

Executive Summary

Background

The Ohio Department of Administrative Services' (DAS) mission is to improve the effectiveness and efficiency of Ohio government by providing statewide leadership, oversight, products and services for activities related to information technology.

IT-13 Data Classification is the State of Ohio enterprise policy to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality. As part of the FY 2019 audit plan, OIA was engaged to perform a review over the data classification process implemented by DAS divisions and confirm compliance with IT-13.

During the audit, OIA identified opportunities for DAS to strengthen internal controls and improve business operations. A detailed listing of observations has been provided. This audit conforms to the *International Standards for the Professional Practice of Internal Auditing.* OIA would like to thank DAS staff and management for their cooperation and time in support of this audit.

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

Scope and Objectives

OIA staff were engaged to perform an assurance audit related to the agency's controls over data classification. This audit was performed between July and September 2018. The scope included a review of the data classification practices over the following areas:

- Data Classification Labels
- Data Classification Methodology
- Roles and Responsibilities
- Education and Awareness

Also, per DAS request, only DAS internal applications were included in our review. External or Enterprise applications managed by DAS were excluded from this review.

The following summarizes the objectives of the review:

- Evaluate the process for classifying data to ensure that it is in place, properly documented, and includes an accurate assessment of confidentiality and criticality of the data maintained at the agency.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. There were no low risk observations as part of this report.

Observation 1 – Data Owners and Data Custodians are Not Adequately Trained.

Per IT-13 section 2.3 agencies shall provide data classification education and awareness training that is designed to complement the roles and responsibilities outlined in section 2.3 of this policy.

Through review, OIA observed that data owners and data custodians are not required to take the current online data classification training. OIA reviewed the data classification course completion report for the online training and observed that, as of 7/30/2018, none of the data owners or custodians attended.

During our review, six data owners were interviewed and none of them were aware of their responsibilities as documented in policy IT-13, such as ensuring that users are trained on how to handle sensitive data and creating data access guidelines based on the need to access certain data. Also, two data custodians were interviewed and neither were aware of the data custodian responsibilities defined in IT-13, such as encrypting data or creating data backups.

Inadequate training of data owners and data custodians regarding the responsibilities for their roles can lead to lack of or improper classification of data, which may lead to exposure of confidential data.

Recommendation
Management needs to ensure that data owners and/or data custodians are required to complete online training and compliance reports should be used to monitor course completion.

Management Response
DAS Office of Information Security and Privacy (OISP) has developed data classification training which is currently available on ELM. OISP will work in collaboration with the DAS Applications Services Team to identify business owners and assign the required training.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CISO	March 2019

Observation 2 – Partial Compliance with the Data Classification Policy

IT-13 – Data Classification is the State of Ohio enterprise policy that provides data classification guidelines to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality. IT-13 also requires that agencies systematically go through the data classification process and document their classification decisions.

Through review, OIA noted the following gaps in procedures for classifying DAS data:

1. Per IT-13 Section 2.3, agencies are required to designate individuals who will be responsible for carrying out the duties associated with the roles of data owner, data custodian and data users. OIA examined the data classifications documentation for six internal applications and observed that the data custodian and data owner were identified. However, the data users were not identified.

2. Per IT-13 Section 2.5, agencies shall conduct regular compliance reviews with relevant staff of all data classification labels to ensure compliance with any state or agency policies, and with federal, state and local laws. During our review, OIA noted that DAS does not have policies and procedures in place for performing regular compliance reviews.

3. Per IT-13 Section 2.5, the data classification needs to be updated if the type of data used by an application is modified. In addition, agencies are required to ensure that data classification is determined during the design phase when planning a new IT system. Per discussion with management, we noted that DAS does not have a documented policy or procedures for incorporating data-classification into change requests and new projects.

4. During our review, OIA noted that DAS Internal data classification Policy 2100-04 was last updated in 2012. IT-13 which was created in 2015 established requirements for state agencies in relation to understanding and managing data. The DAS data classification internal policy 2100-04 has not been updated to incorporate the new guidelines established in IT-13.

OIA identified the following risks for the gaps noted above:

1. Not identifying the data users can prevent the agency from creating targeted rules, policies, and training that protect data from unauthorized access or misuse.

2. Lack of compliance reviews by DAS may lead to inconsistent implementation of policies and procedures or undetected deviations from the policy.

3. Lack of procedures for creating or updating data classification for changes or new projects may lead to improper classification of data, which may cause DAS to not have proper security controls over confidential data.

4. Inadequate documentation of procedures for guidelines established in IT-13 State of Ohio enterprise data classification policy may lead to inconsistent operations and inadequate compliance with the policy.

Recommendation

Management should create new procedures or update current policies and procedures to address the following:

1. List the data users in the data classification documentation for each application.

2. Develop procedures for regular data classification compliance reviews.

3. Incorporate and document the data-classification process for new development projects and change requests.

Update DAS Internal Policy 2100-04 to reflect requirements documented in IT-13.

Management Response

DAS Office of Information Security and Privacy (OISP) is planning a phase II DAS data classification initiative leveraging the automation of tools within the ServiceNow Governance Risk and Compliance module that will provide a mechanism for tracking the progress, timelines and clearly defining roles and responsibilities for implementing and managing data classification. OISP will work in collaboration with the DAS Applications Services Team to implement. In addition, the Office of Information Security and Privacy is establishing a security approval process for new DAS systems and services which includes data classification as a requirement before a system/service is approved to move forward with development or implementation. DAS Internal Policy 2100-04 is in the process of being updated to reflect requirements documented in IT-13. Updates will be implemented by year end 2018.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CISO	May 2019

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