Office of the Auditor General
Preliminary Survey Summary

Statewide Data Classification Management

Department of Technology, Management, and Budget

September 2020

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

071-0514-20

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General
Doug A. Ringler, CPA, CIA
Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

September 29, 2020

Mr. Brom Stibitz
Acting Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Elliott-Larsen Building
Lansing, Michigan

Dear Mr. Stibitz:

This is our preliminary survey summary of Statewide Data Classification Management, Department of Technology, Management, and Budget. Because we did not identify significant concerns that would warrant the additional use of our audit resources, we have decided to terminate this performance audit.

We appreciate the courtesy and cooperation extended to us during our preliminary survey. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

PRELIMINARY SURVEY SUMMARY

STATEWIDE DATA CLASSIFICATION MANAGEMENT

RESULTS

Our preliminary survey did not identify significant concerns that would warrant the additional use of our audit resources to complete a performance audit. Therefore, we have terminated this project and did not conduct sufficient testing to conclude on the overall effectiveness and efficiency of Statewide Data Classification Management.

FACTORS IMPACTING AUDIT TERMINATION

The Department of Technology, Management, and Budget (DTMB):

- Implemented State of Michigan (SOM) Technical Standard 1340.00.150.02 and Technical Procedure 1340.00.150.02.01 to provide enterprise-level guidance to all State agencies on how to identify and classify their data based on sensitivity, criticality, and risk. The Standard and Procedure were consistent with industry best practices.

- Implemented and required State agencies to use a Governance, Risk, and Compliance (GRC) tool, in late 2016, as part of the Michigan Security Accreditation Process (MISAP). MISAP requires the approval of data classification within the GRC tool for a system to receive an Authority to Operate (ATO), before moving from development into production. In addition, SOM Technical Standard 1340.00.150.01 requires that State agencies update the ATOs for their systems at least every 3 years, including reevaluating data classification (see Exhibit #1 for an overview of MISAP).

- Provided training and guidance to State agencies in the form of classes and instructional videos. The three State departments we judgmentally sampled indicated that the training and guidance was sufficient to enable them to identify and properly classify data.

Selected State departments:

- Properly identified and assigned data classification roles and responsibilities to department staff.

- Properly documented and approved the classification of data for 6 (100%) of 6 randomly and judgmentally sampled systems in accordance with the data classification processes outlined in SOM Technical Standard 1340.00.150.02.

BACKGROUND

Description: Data classification is a process to identify and categorize information and information systems based on their sensitivity, criticality, and risk. This categorization provides a common framework for effective management and oversight of information security controls for IT resources. Without proper data classification, an agency has an increased risk of implementing inadequate controls that may lead to a security incident or data breach. State agencies that experience a security incident or data breach can suffer reputational damage, operational downtime, and loss of customer or public confidence and may incur costs associated with managing the incident and notifying the affected parties.

DTMB's Michigan Cyber Security (MCS) established enterprise-wide guidance in the form of SOM Technical Standard 1340.00.150.02 and SOM Technical Procedure 1340.00.150.02.01 that requires State agencies to document data classification as part of the MISAP on either the DTMB-3544 Agency Business Owner Data Classification Declaration form or in the GRC tool. Information system owners at the various State agencies work with business relationship managers (BRMs) from DTMB's Agency Services to document data classification for all data elements in a complete and accurate manner (see Exhibits #2 through #4 for an overview of the State's data classification processes and levels and potential impact level definitions for security objectives).

SCOPE

Our preliminary survey generally covered October 1, 2017 through August 31, 2020 and included a limited review of the State's data classification processes.

PURPOSE

Within a performance audit, we design the preliminary survey to obtain an understanding of the core activities within an entity or program and to identify potential program improvements and/or deficiencies that could impair management's ability to conduct its operations in an effective and efficient manner. If the results of a preliminary survey do not identify significant concerns, our practice is to terminate the planned performance audit.

Preliminary survey procedures are limited in nature and should not be considered a completed performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. In addition, our preliminary survey procedures would not necessarily disclose the presence or absence of any material conditions and/or reportable conditions. Given that the procedures we employed did not constitute a performance audit, we will not issue a performance audit report and we do not express conclusions regarding the effectiveness or efficiency of Statewide Data Classification Management.

SUPPLEMENTAL INFORMATION

UNAUDITED
Exhibit #1

STATEWIDE DATA CLASSIFICATION MANAGEMENT
Department of Technology, Management, and Budget

Overview of MISAP
As of August 31, 2020

The following is a high-level overview of the State's security accreditation process (which includes data classification) within the State's GRC tool that was implemented in late 2016 by DTMB's MCS. In 2018, the data classification process was automated within the GRC tool to provide consistent baseline guidance. The yellow highlighted boxes indicate the review and approval of data classification for a system.

MISAP Workflow Process

System Registration and Documentation of Data Classification Assessment and System Hardware/Security Controls:

1. System Registration
Register system profile in the GRC tool and identify responsible parties, such as information system owner, agency security officer, data custodian, BRM, and MCS liaison.

2. Documentation of Data Classification Assessment
Identify the data classification level (Exhibit #3), potential impact level for security objectives (Exhibit #4), and overall security categorization (low, moderate, or high) according to Federal Information Processing Standard Publication 199.

3. Documentation of System Hardware/Security Controls
Document the system architecture, network diagram, disaster recovery plan, and business impact analysis which identifies system criticality and scoping of appropriate security controls.

System Registration Approval and Documentation of Risk Assessment and Plan of Action and Milestone (POAM):

4. System Registration Approval
Agency security officer and BRM approve the system registration from steps 1 through 3, **including initial approval of data classification.**

5. Documentation of Risk Assessment
Evaluate the security control needs necessary for control effectiveness. Secure the minimum baseline control configurations to National Institute of Standards and Technology (NIST) Moderate.

6. Documentation of POAM
Identify control gaps and actions required to mitigate or remediate the gaps and any milestones to meet the actions including targeted completion dates.

Final MISAP Approvals and Documentation of Authority to Operate (ATO):

7. Final MISAP Approvals
Approve the overall MISAP processes to obtain ATO, **including evaluation of data classification**. Approvals include BRM, agency security officer, MCS, chief security officer, and chief information officer.

8. Documentation of ATO
Obtain reaccreditation which includes an evaluation of data classification and all MISAP steps. This is required when major system updates occur or when the ATO expires, whichever occurs first.

Source: The OAG prepared this exhibit based on information obtained from DTMB personnel during the preliminary survey.

STATEWIDE DATA CLASSIFICATION MANAGEMENT
Department of Technology, Management, and Budget

Overview of Data Classification Processes
As of March 10, 2020

STEP 1 - IDENTIFY INFORMATION SYSTEMS AND DATA

The agency identifies data that is collected, processed, stored, and/or transmitted.

STEP 2 - IDENTIFY AND UNDERSTAND APPLICABLE LEGAL AND REGULATORY REQUIREMENTS

The agency identifies applicable State and federal laws and regulations, policies, procedures, standards, and privacy compliance requirements required for data protection.

STEP 3 - DETERMINE THE DATA CLASSIFICATION LEVEL

The agency determines the classification level of the data being classified as restricted, confidential, internal, or public (see Exhibit #3 for definitions of data classification levels).

STEP 4 - DETERMINE THE DATA IMPACT LEVEL

The agency determines the data impact level by assigning a potential impact level of high, moderate, or low to each security objective: confidentiality, integrity, and availability (see Exhibit #4 for definitions of impact levels).

STEP 5 - DETERMINE THE SECURITY CATEGORIZATION

The agency establishes the security categorization by selecting the highest value from the impact designations given to the security objectives in Step 4.

STEP 6 - DOCUMENT THE DATA CLASSIFICATION

The agency documents the outcome of the data classification process by completing a DTMB-3544 Agency Business Owner Data Classification Declaration form and/or enters the information into the DTMB GRC tool.

STEP 7 - DETERMINE SECURITY CONTROLS AND SAFEGUARDS

DTMB's MCS assists the agency in selecting the minimum security controls and control enhancements to protect the data.

STEP 8 - MONITORING AND EVALUATION

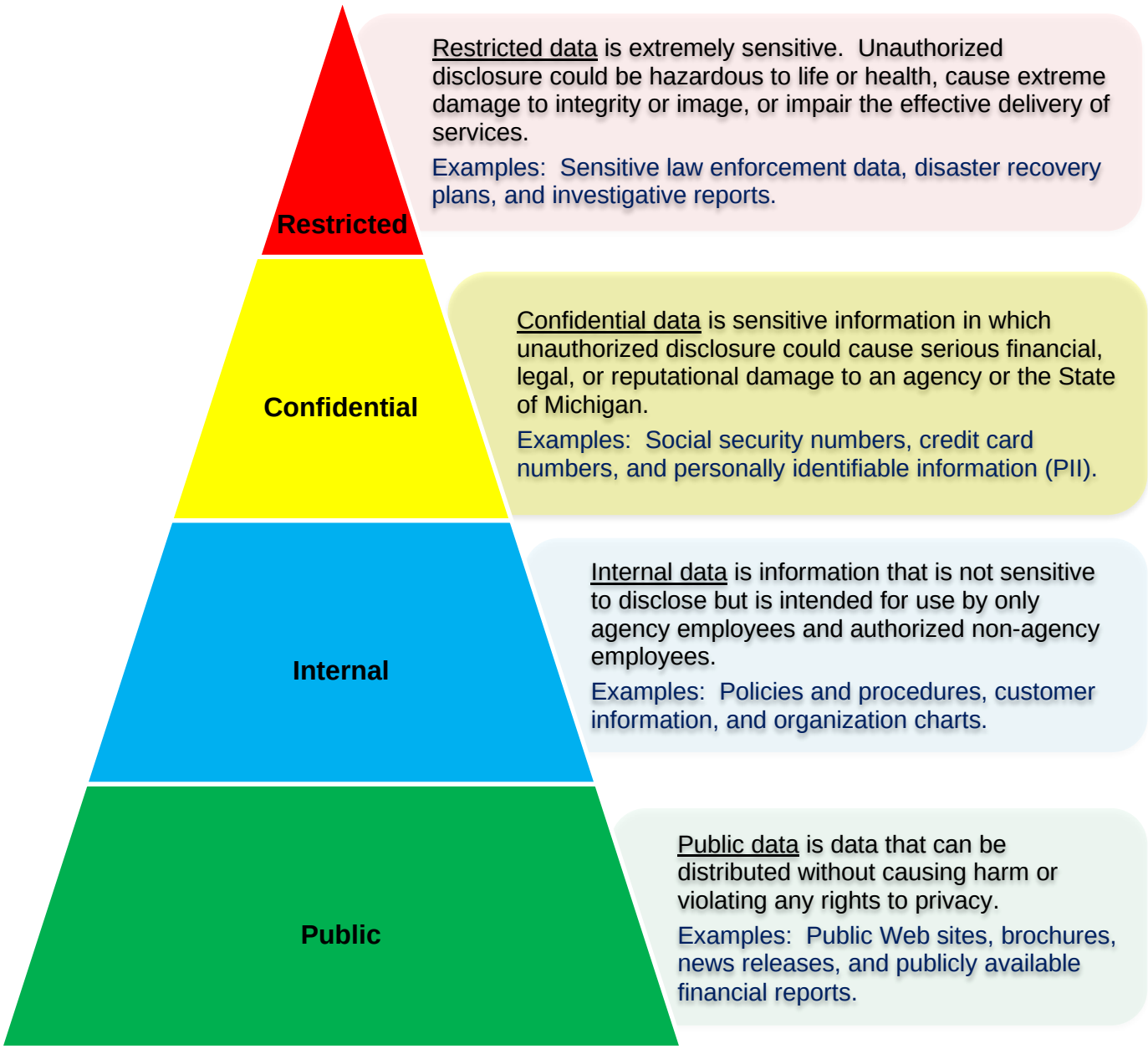
The agency continually monitors and periodically evaluates data classification. The agency reevaluates data classification at least every 3 years in accordance with MISAP (see Exhibit #1 for an overview of MISAP).

Source: The OAG prepared this exhibit using information from SOM Technical Standard 1340.00.150.02.

UNAUDITED
Exhibit #3

STATEWIDE DATA CLASSIFICATION MANAGEMENT
Department of Technology, Management, and Budget

Overview of Data Classification Levels
As of March 10, 2020



Source: The OAG prepared this exhibit using information from SOM Technical Standard 1340.00.150.02.

UNAUDITED
Exhibit #4

STATEWIDE DATA CLASSIFICATION MANAGEMENT
Department of Technology, Management, and Budget

Potential Impact Level Definitions for Security Objectives
As of March 10, 2020

Security Objective	Potential Impact Level		
	Low	**Moderate**	**High**
Confidentiality Defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The unauthorized disclosure of information could be expected to have a:	**Limited** adverse effect on organizational operations, assets, or individuals.	**Serious** adverse effect on organizational operations, assets, or individuals.	**Severe or catastrophic** adverse effect on organizational operations, assets, or individuals.
Integrity Defined as guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could be expected to have a:			
Availability Defined as ensuring timely and reliable access to and use of information. The disruption of access to or use of information or an information system could be expected to have a:			

Source: The OAG prepared this exhibit using data from SOM Technical Standard 1340.00.150.02.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650