Office of the Auditor General
Follow-Up Report on Prior Audit Recommendations

# IT Equipment Surplus and Salvage

Department of Technology, Management, and Budget

November 2023

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

071-0515-19F

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

# Report Summary

## *Follow-Up Report*

## *IT Equipment Surplus and Salvage*

## *Department of Technology, Management, and Budget (DTMB)*

**Report Number:**
**071-0515-19F**

**Released:**
**November 2023**

We conducted this follow-up to determine whether DTMB had taken appropriate corrective measures in response to the two material conditions noted in our January 2020 audit report.

| Prior Audit Information | Follow-Up Results | | |
|---|---|---|---|
| | **Conclusion** | **Finding** | **Agency Preliminary Response** |
| Finding 1 - Material condition<br><br>Controls needed to ensure sanitization and disposal.<br><br>Agency agreed. | Partially complied | Reportable condition exists.<br>See Finding 1. | Partially agrees |
| Finding 5 - Material condition<br><br>Improved physical security controls needed.<br><br>Agency agreed. | Partially complied | Reportable condition exists.<br>See Finding 5. | Disagrees |


**Obtain Audit Reports**

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

**Doug A. Ringler, CPA, CIA**
Auditor General

**Laura J. Hirst, CPA**
Deputy Auditor General

This Page Left Intentionally Blank

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

November 9, 2023

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Director Lange and Chief Information Officer Clark:

This is our follow-up report on the two material conditions (Findings 1 and 5) and the two corresponding recommendations reported in the performance audit of IT Equipment Surplus and Salvage, Department of Technology, Management, and Budget. That audit report was issued and distributed in January 2020. Additional copies are available on request or at audgen.michigan.gov.

Your agency provided the preliminary responses to the follow-up recommendations included in this report. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during our follow-up. 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

## TABLE OF CONTENTS

## IT EQUIPMENT SURPLUS AND SALVAGE

## INTRODUCTION, PURPOSE OF FOLLOW-UP, AND PROCESS DESCRIPTION

**INTRODUCTION**

This report contains the results of our follow-up of the two material conditions* (Findings 1 and 5) and the two corresponding recommendations reported in our performance audit* of IT Equipment Surplus and Salvage, Department of Technology, Management, and Budget (DTMB), issued in January 2020.

**PURPOSE OF FOLLOW-UP**

To determine whether DTMB had taken appropriate corrective measures to address our corresponding recommendations.

**PROCESS DESCRIPTION**

IT equipment is regularly purchased and used by State of Michigan (SOM) employees to process and store data for State government operations. As this equipment becomes surplus, obsolete, or out of warranty, the State must dispose of these items in a safe and secure manner. DTMB contracted with a third-party vendor for the sanitization* or disposal* of surplus IT equipment, including desktop computers, laptop computers, servers, storage and networking devices, smart phones, hard drives, and tablet computers.

The State's primary method for disposing of equipment is DTMB's Automated Asset Recovery Program* (AARP) System. State employees use the AARP System to notify DTMB of unneeded IT equipment, which is then evaluated to determine if it is fit for reuse or should be disposed of via a vendor. Retired equipment is removed from DTMB's official inventory of record. Workstations fit for reuse are stored at the DTMB Depot* as agency stock. DTMB Delivery, Warehouse, and Surplus Services primarily handles the transfer and storage of equipment by assigning a pallet number to track IT equipment identified for disposal within the AARP System and by creating a manifest so the equipment can be scanned during pickup by the vendor at the Depot location.

** See glossary at end of report for definition.*

## PRIOR AUDIT FINDINGS AND RECOMMENDATIONS; AGENCY PLAN TO COMPLY; AND FOLLOW-UP CONCLUSIONS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

### FINDING 1

Audit Finding Classification: Material condition.

Summary of the January 2020 Finding:
DTMB did not fully establish controls to ensure its vendor properly sanitized and disposed of all surplus and salvage IT equipment. Specifically, we noted the following:

a. DTMB did not have procedures to:

   (1) Monitor disposal records for stand-alone storage devices and network equipment for which the pallet number was left blank.

   (2) Review all devices assigned to a pallet number and ensure the devices were included on the appropriate manifest for pickup.

   (3) Use a manifest to track network equipment sent to the vendor.

b. DTMB did not establish procedures to reconcile vendor disposal certificates with its equipment disposal records.

c. DTMB did not track smart phones, non-Windows tablets, and individual hard drives at a detailed level in the AARP System.

Recommendation Reported in January 2020:
We recommended that DTMB fully establish controls to ensure its vendor properly sanitizes and disposes of all surplus and salvage IT equipment.

### AGENCY PLAN TO COMPLY*

On September 18, 2020, DTMB stated it:

- Updated internal procedures in December 2019 to include tracking network equipment and standalone storage devices.
- Developed internal procedures in December 2019 to validate the existence of disposal or sanitization certificates.
- Developed an internal procedure in January 2020 to ensure all devices assigned to a pallet are also assigned to a shipping manifest.

** See glossary at end of report for definition.*

- Will implement controls in December 2020 to increase the chain of custody documentation for these devices as part of the disposal process.

Also, DTMB utilizes additional controls to reduce the risk of unauthorized disclosure of State data. These controls include:

- An automated system to administer data security* for SOM owned and managed smart devices.
- Encrypting hard drives for SOM-owned and managed computers in accordance with State standard 1340.00.170.03.
- As of November 2019, DTMB ensured smart devices and individual hard drives are secured in locked bins once the devices are received at the State's IT-Depot.
- Sanitizes physical server hard drives as part of the decommissioning process. Smart devices are sanitized or shredded by the vendor.

In addition, DTMB delegated the purchase and issuance of smart devices to State agencies. DTMB will continue to work with State agencies in clarifying the roles and responsibilities for sanitizing various media* when using the AARP System.

**FOLLOW-UP CONCLUSION**

DTMB partially complied. A reportable condition* exists.

DTMB updated its tracking procedures to ensure the vendor picked up all devices. Also, DTMB established disposal certificate reconciliation procedures to help ensure it receives disposal certificates for all equipment provided to the vendor. In addition, DTMB implemented tracking for smart phones, non-Windows tablets, and individual hard drives within the AARP System to ensure all equipment with data is properly sanitized. The National Institute of Standards and Technology* (NIST) states organizations should sanitize digital media using approved methods, and the sanitization should be tracked, documented, and verified. NIST also states, following sanitization, a certificate of media disposition should be completed for each piece of media which has been sanitized.

Our follow-up noted DTMB:

a. Complied.

   (1) In January 2020, DTMB began including stand-alone storage devices and network equipment in monitoring reports it uses to ensure each device is assigned a pallet number.

** See glossary at end of report for definition.*

(2) DTMB implemented procedures to ensure it assigned all devices to a pallet number and the devices were included on the appropriate manifest for pickup. We reviewed records between October 2022 and May 2023 for retired or salvaged devices in the Information Technology Asset Management System* (ITAM) and the Configuration Management Database* (CMDB) to verify each device had an associated AARP System request with an assigned pallet number and was included on the appropriate manifest. We sampled AARP System disposal requests with blank pallet numbers and determined the blank pallet numbers were appropriate because these devices were not sent for disposal, for example, warranty replacements.

(3) DTMB used manifests to track network equipment, which includes switches, routers, and firewalls, which were sent to the vendor. We reviewed records between October 2022 and May 2023 for salvaged network equipment in the CMDB and verified each device was included on a manifest.

b. Partially complied.

DTMB established some procedures to reconcile vendor disposal certificates with its equipment disposal records. However, our review of disposal certificates noted DTMB did not:

(1) Receive certificates for 2 (5%) of 43 sampled AARP System disposal requests. Also, DTMB did not timely receive 35 (85%) of 41 certificates, in accordance with contract requirements.

(2) Timely receive certifications for all 43 sampled ITAM records for retired desktop computers, laptop computers, and Windows tablets, in accordance with contract requirements.

(3) Receive certificates for 3 (7%) of 43 sampled CMDB records for salvaged servers, stand-alone devices, and network equipment. Also, DTMB did not timely receive 34 (85%) of 40 certificates, in accordance with contract requirements.

DTMB relies on the vendor to determine whether an internal hard drive or stored data is on each device. Currently, no procedure exists for DTMB, or the agency which owns the data on the device, to validate the

** See glossary at end of report for definition.*

accuracy of the vendor's assertion regarding whether the device contains a hard drive or stored data. DTMB informed us the vendor made the assertion for the devices missing certificates in our samples. Without a validation procedure, DTMB cannot ensure all State data was properly sanitized or destroyed.

Although DTMB received most of the certificates for sampled records, DTMB did not obtain the certificates in a timely manner. The vendor typically provides monthly certificate reports for devices sanitized or disposed of since the prior certificate report. Of 124 received sampled certificates, 112 (90%) were acquired more than 61 days after the vendor picked up the equipment from the Depot. DTMB's contract requires the vendor to provide disposal certificates within 30 days of equipment pickup. The risk of exposing confidential State data increases when devices are not timely sanitized or disposed. The table below shows the time between the date the vendor picked up the equipment and the date DTMB received disposal certificates for the sampled records:

Summary of Timeliness of Obtaining Certificates
Days Between Manifest Date and Certificate Received Date

| | Timeliness of Certificates Received System | | | |
|---|---|---|---|---|
| Days | AARP System (Part b. (1)) | ITAM (Part b. (2)) | CMDB (Part b. (3)) | Total |
| 0 to 30 | 3 | 0 | 0 | 3 ( 2%) |
| 31 to 60 | 3 | 0 | 6 | 9 ( 7%) |
| 61 to 70 | 5 | 5 | 12 | 22 ( 18%) |
| 71 to 80 | 11 | 5 | 15 | 31 ( 25%) |
| 81 to 90 | 8 | 17 | 6 | 31 ( 25%) |
| 91 to 100 | 9 | 8 | 1 | 18 ( 15%) |
| 101 to 110 | 2 | 8 | 0 | 10 ( 8%) |
| Total | 41 | 43 | 40 | 124 (100%) |

| | |
|---|---|
| Total over 61 days | 112 |
| Total certificates received | 124 |
| Percentage over 61 days | 90% |

Complete reconciliation controls for disposal certificates would help DTMB validate whether stored data exists on devices sent to the vendor and ensure timely receipt of certificates for SOM IT equipment.

c. Complied.

DTMB implemented tracking for smart phones, non-Windows tablets, and individual hard drives within the AARP System. We reviewed the AARP System disposal requests between October 2022 and May 2023 and noted each smart phone, non-Windows tablet, and individual hard drive had a unique serial number or system-

generated tracking number to maintain chain of custody documentation throughout the disposal process.

**FOLLOW-UP RECOMMENDATION**

We again recommend that DTMB fully establish controls to ensure its vendor properly sanitizes and disposes of all surplus and salvage IT equipment.

**FOLLOW-UP AGENCY PRELIMINARY RESPONSE**

DTMB provided us with the following response:

*Finding 1, Subpart 1b*

*DTMB disagrees with the need to establish additional procedures related to whether a device contains a hard drive or stored data. The processes implemented by the State of Michigan reduce the risk to an acceptable level or do not necessitate the development of such a process as the risk is not applicable.*

*The State computers, laptops, and tablets are encrypted at the hardware level which prevents accessing data even if the hard drive is separated and accessed by another device; this reduces the risk to an acceptable level.*

*DTMB agrees DTMB did not always receive the certificates from the vendor within 30 days of equipment pickup as required in the contract. DTMB will review and update contract language to ensure timely receipt of equipment sanitization certificates.*

**AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE***

SOM Technical Standard 1340.00.110.01 states, when required based on data classification, the organization tracks, documents, and verifies media sanitization and disposal. Without procedures to determine whether devices contain hard drives or stored data, DTMB cannot ensure compliance with this Standard. While DTMB asserts the devices are encrypted, this Standard does not eliminate or change the requirement based on whether or not devices are encrypted.

As noted in the finding, the contract already contains a requirement for timely receipt of the certificates, which DTMB is not currently enforcing.

Given DTMB provided no persuasive information to counter the facts of the finding, it stands as written.

** See glossary at end of report for definition.*

## FINDING 5

Audit Finding Classification: Material condition.

Summary of the January 2020 Finding:
DTMB did not fully implement physical security controls* over the State's surplus and salvage IT equipment, which could lead to unauthorized employees gaining access to IT equipment, undetected theft of equipment, or unauthorized disclosure of sensitive or confidential information.

Our review disclosed DTMB did not:

a. Restrict access to the surplus and salvage storage area beyond general building access.

b. Securely store untracked devices, such as smart phones, non-Windows tablets, and hard drives, within the designated surplus and salvage storage area.

Recommendation Reported in January 2020:
We recommended that DTMB fully implement physical security controls over the State's surplus and salvage IT equipment.

### AGENCY PLAN TO COMPLY

On September 18, 2020, DTMB stated it:

- Established an internal procedure, as of January 2020, to review access rights and hours employees are allowed to access the building.

- Agreed with the need to ensure building access is appropriate. Also, DTMB acknowledged access had not been fully restricted because doing so would require considerable changes to the existing building, impact Depot operations and other operations within the building, and require additional funds. DTMB will consider the OAG's recommendation when additional funding becomes available.

- Started storing smart devices along with hard drives and loose media in locked bins since November 2019 and July 2019, respectively.

- Utilizes additional existing controls including security cameras and security guards at the loading dock gate to reduce the risk of unauthorized access to SOM data.

### FOLLOW-UP CONCLUSION

DTMB partially complied. A reportable condition exists.

DTMB gathers surplus and salvage IT equipment from State agencies and stores the equipment in an open designated area within a warehouse building. DTMB stores smart devices, hard

** See glossary at end of report for definition.*

drives, or loose media in locked bins with restricted access. Also, employees must be granted approval to access the building. DTMB established internal procedures to review access rights to the building.

Our follow-up noted:

a. Not complied.

   DTMB did not restrict access to the surplus and salvage storage area beyond general building access.

   SOM Technical Standard 1340.00.110.01 requires media to be physically protected within controlled areas using safeguards prescribed for the highest system security level of information ever recorded or contained on it until destroyed or sanitized. Also, SOM Technical Standard 1340.00.120.01 requires physical access to be authorized based on role and a restricted area to be used to control access to sensitive information, such as personally identifiable information. Although DTMB implemented and completed monthly reviews of access rights, these reviews did not always determine whether an individual's access to the building was still needed or properly authorized, particularly when the employee worked for a different department or division. DTMB's review focused on changes to access; therefore, if access did not change but should have, there is a risk DTMB's review would not identify the error.

   We sampled 47 of 393 employees with building access to review for the principle of least privilege* and proper granting of approvals by DTMB. We noted:

   (1) 37 (79%) of 47 employees did not require access to the State's surplus and salvage IT equipment storage area for their job responsibilities.

       Also, DTMB maintained 4 access cards not assigned to specific employees. We sampled 1 of these 4 cards to review for the principle of least privilege and DTMB approval. DTMB informed us this card should not have access to the IT equipment surplus and salvage storage area and removed the access for this card.

   (2) 12 (26%) of 47 employees did not have approval for at least one access right.

       Also, DTMB did not maintain access approvals for the sampled access card not assigned to specific employees. DTMB informed us this card allowed

** See glossary at end of report for definition.*

access to the IT equipment surplus and salvage storage area and removed the access for this card.

(3) DTMB's process for assigning access ensured all 37 users with approved access for at least one access right had access to the building during approved time frames.

b. Complied.

SOM Technical Standard 1340.00.110.01 requires media to be protected until destroyed or sanitized. We noted DTMB securely stored previously untracked devices in locked bins, including smart phones, non-Windows tablets, and hard drives. Also, access to those locked bins is restricted to individuals requiring access to those bins based on their job responsibilities.

**FOLLOW-UP RECOMMENDATION**

We again recommend that DTMB fully implement physical security controls over the State's surplus and salvage IT equipment.

**FOLLOW-UP AGENCY PRELIMINARY RESPONSE**

DTMB provided us with the following response:

*DTMB disagrees with the need to further restrict access to the building beyond the existing restrictions and processes which are in place. As DTMB noted in the prior audit response, the cost to restrict the access to the Surplus and Salvage area of the building beyond general building access would exceed the cost benefit of doing so.*

*DTMB implements the following controls to reduce risk:*

- *The building itself is secured by gates, security guards, and the need to use an access card to enter the building. DTMB restricts the access to the building to individuals who have a business need to access the building for their job responsibilities.*

- *The State computers, laptops, and tablets are encrypted at the hardware level which prevents accessing data even if the hard drive is separated and accessed by another device; this reduces the risk to an acceptable level.*

- *Additionally, State network infrastructure devices (routers, switches, firewalls) do not possess internal data storage. Furthermore, as part of a separate secure disposal process, the hard drives from servers hosted in the State's hosting center are sanitized and shredded.*

- *DTMB has security cameras at entry points and throughout the surplus and salvage IT equipment area.*

*DTMB Central Control monitors the video which may be utilized for forensic analysis.*

- *As noted in the OAG's audit report, DTMB secures smart devices, hard drives, and loose media in locked bins.*
- *Visitors are escorted within the building.*

**AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE**

DTMB's disagreement with the need to further restrict building access and the controls in place do not fully align with the Technical Standard. SOM Technical Standard 1340.00.110.01 states agencies are to physically control and securely store digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded or contained on it and protects this media until it is destroyed or sanitized. The Standard does not eliminate this requirement based on whether or not devices are encrypted.

We acknowledge DTMB secures smart devices, hard drives, and other loose media in locked bins. However, laptops, PCs, and other larger devices which may contain confidential information are stacked on pallets, unsecured in the salvage area of the warehouse.

Therefore, the finding stands as written.

## FOLLOW-UP METHODOLOGY, PERIOD, AND AGENCY RESPONSES

**METHODOLOGY**

We reviewed DTMB's corrective action plan and SOM standards, policies, and procedures. Specifically, for:

- Finding 1, we:
  - Interviewed DTMB staff to obtain an understanding of DTMB's processes and procedures to:
    - Reconcile vendor's disposal certificates with DTMB's equipment disposal records.
    - Track IT equipment by assigning pallet numbers and creating manifests.
  - Reconciled AARP System disposal records with the No Pallet Report to determine if network equipment was included.
  - Compared the IT equipment recorded in ITAM and CMDB with the manifests to ensure all retired and salvaged equipment was assigned to a pallet and included on a manifest.
  - Reviewed the contract between DTMB and the third-party vendor responsible for IT equipment sanitization and disposal.
  - Determined whether certificates of disposal were provided by the vendor and maintained by DTMB by randomly sampling:
    - 43 of 16,365 disposal records from the AARP System. We also randomly and judgmentally selected 12 additional records from a subpopulation of 119 records in which the pallet number field was blank.
    - 43 of 12,540 retired equipment records from ITAM.
    - 43 of 549 salvaged records from CMDB.
  - Assessed DTMB's process for validating the receipt of sanitization or disposal certificates for all assets sent to the vendor for salvage.
  - Evaluated DTMB's tracking of smart phones, non-Window tablets, and hard drives within the AARP System.

- Finding 5, we:
    - Met with DTMB staff to obtain an understanding of the changes implemented to improve physical security controls over the State's surplus and salvage IT equipment.
    - Obtained and reviewed DTMB's internal procedures for reviewing employee building access to ensure the effectiveness of the process.
    - Randomly and judgmentally sampled 3 DTMB monthly building access reviews completed between January and May 2023 to determine implementation and effectiveness of the review process.
    - Randomly selected a sample of 47 of 393 employees and judgmentally selected 1 of the 4 access cards not assigned to specific employees with access to DTMB's building where surplus and salvage IT equipment is stored to evaluate for the principle of least privilege and proper building access authorization.
    - Observed the third-party vendor's process for picking up equipment from the Depot.
    - Observed physical controls over the smart devices, non-Windows tablets, and hard drives to ensure they were properly secured in the State's surplus and salvage storage area.

**PERIOD**

Our follow-up generally covered October 1, 2022 through July 31, 2023.

**AGENCY RESPONSES**

Our follow-up report contains 2 recommendations. DTMB's preliminary response indicates it partially agrees with 1 recommendation and disagrees with 1 recommendation.

The agency preliminary response following each follow-up recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

## GLOSSARY OF ABBREVIATIONS AND TERMS

| | |
|---|---|
| **agency plan to comply** | The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan. |
| **auditor's comments to agency preliminary response** | Comments the OAG includes in an audit report to comply with *Government Auditing Standards*. Auditors are required to evaluate the validity of the audited entity's response when it is inconsistent or in conflict with the findings, conclusions, or recommendations. If the auditors disagree with the response, they should explain in the report their reasons for disagreement. |
| **Automated Asset Recovery Program (AARP) System** | The system provided by DTMB to process State agency IT equipment disposal requests. |
| **Configuration Management Database (CMDB)** | The system used by DTMB to inventory servers, stand-alone storage devices, and network equipment. |
| **Depot** | An area within a State-owned warehouse where surplus IT equipment is stored prior to disposal or redeployment. |
| **disposal** | Removal or release of media from organizational control following the decision it does not contain sensitive data because the media never contained sensitive data or sanitization techniques were applied. |
| **DTMB** | Department of Technology, Management, and Budget. |
| **Information Technology Asset Management System (ITAM)** | The system used by DTMB to inventory desktop computers, laptop computers, and Windows tablets. |
| **IT** | information technology. |
| **material condition** | A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our |

| | |
|---|---|
| | assessment of materiality is in relation to the respective audit objective. |
| **media** | Material on which data is or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. |
| **National Institute of Standards and Technology (NIST)** | An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs. |
| **performance audit** | An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. |
| **physical security control** | A control restricting physical access to computer resources and protects them from intentional or unintentional loss or impairment. |
| **principle of least privilege** | The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes. |
| **reportable condition** | A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud. |
| **sanitization** | A process rendering access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media. |
| **security** | Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. |
| **SOM** | State of Michigan. |

This Page Left Intentionally Blank

This Page Left Intentionally Blank


**Report Fraud/Waste/Abuse**

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070