Office of the Auditor General
Performance Audit Report

Selected Department of Military and Veterans Affairs IT Systems

Department of Military and Veterans Affairs and
Department of Technology, Management, and Budget

February 2026

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

511-0590-25

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

Performance Audit
Selected Department of Military and Veterans Affairs IT Systems
Department of Military and Veterans Affairs (DMVA) and Department of Technology, Management, and Budget (DTMB)

Report Number:
511-0590-25

Released:
February 2026

The Michigan Veteran Homes (MVH) within DMVA is responsible for delivering long-term care services to eligible veterans and their dependents. Our scope includes the review of four IT systems used within MVH: Point Click Care (PCC), OnShift, BD Pyxis, and RxPertise. MVH uses these systems to maintain patient medical records, schedule nursing staff, review patient medication plans, and track and dispense medication. DMVA has the primary responsibility for establishing, maintaining, and monitoring internal control over its IT applications and the operational environment. DTMB is charged with providing centralized administrative purchasing services, including support for IT purchases. MVH operated three homes and served 481 members during fiscal year 2025.

Audit Objective			Conclusion
Objective 1: To assess the sufficiency of DMVA and DTMB's efforts to administer selected veteran home IT system contracts.			Not sufficient
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DMVA, in conjunction with DTMB, used a process for procuring IT systems which did not include some of the State's critical data security and contractual requirements. Their actions increased the risk of unauthorized access, misuse, and disclosure of confidential veteran and State data (Finding 1).	X		Partially agrees

Audit Objective	Conclusion
Objective 2: To assess the effectiveness of DMVA's security and access controls over PCC.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DMVA did not authorize or monitor 21 PCC vendor user accounts with all 121 available privileged and non-privileged roles (Finding 2).	X		Partially agrees
DMVA could not validate the vendor's current security configuration settings for PCC complied with the State's technical standards or perform effective user account management (Finding 3).		X	Partially agrees

Audit Objective	Conclusion
Objective 3: To assess the sufficiency of DMVA and DTMB's monitoring of selected veteran home third-party service organizations.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DMVA did not sufficiently review the third-party service organizations' complementary user entity controls (CUECs) in the System and Organization Controls reports for PCC and OnShift. Without evaluating the CUECs, DMVA cannot fully determine if it can rely on the vendors' controls to protect veteran home and State data (Finding 4).		X	Agrees

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

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

February 26, 2026

David Henry, Chair
Michigan Veterans' Facility Authority
and
Anne Zerbe, Executive Director
Michigan Veteran Homes
and
Major General Paul D. Rogers, Director
Department of Military and Veterans Affairs
3411 North Martin Luther King Jr. Boulevard
Lansing, Michigan

Kyle Guerrant, Acting Director
Department of Technology, Management, and Budget
and
Eric Swanson, Acting Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Chair Henry, Executive Director Zerbe, General Rogers, Acting Director Guerrant, and Acting Chief Information Officer Swanson:

This is our performance audit report on the Selected Department of Military and Veterans Affairs IT Systems, Department of Military and Veterans Affairs and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agencies provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* require an audited agency to develop a plan to comply with the recommendations and submit it to the State Budget Office (SBO) upon audit completion. State administrative procedures require the audited agency to develop the plan as early as practicable and within 60 days after report issuance and submit the plan to the Office of Internal Audit Services (OIAS), SBO. Within 30 days of receipt, OIAS will 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 this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

SELECTED DEPARTMENT OF MILITARY AND VETERANS AFFAIRS IT SYSTEMS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ADMINISTERING SELECTED IT SYSTEM CONTRACTS

BACKGROUND

IT includes software the State uses to store, manage, access, communicate, send, and receive information. The Department of Technology, Management, and Budget (DTMB) has implemented policies and processes concerning IT systems, including the procurement of systems hosted or supported by third-party service organizations (TPSOs), for all State agencies. TPSOs are entities which provide services on behalf of the State, such as software providers, and may collect, process, transmit, store, organize, and maintain the State's hard-copy and electronic data. Contracts involving TPSOs require additional controls to manage risk, including ongoing monitoring, to ensure contractual obligations and data protection requirements are met.

The Michigan Procurement Policy Manual* (MPPM) is designed to provide a transparent and standardized procurement policy and process for all State agencies. MPPM instructs an agency to coordinate with various areas within DTMB when it believes it may need an IT solution. DTMB Agency Services works with the agency to assess the need and perform market research, and then the purchase will be moved to either DTMB Financial Services or DTMB Central Procurement Services (CPS) depending on the cost over the lifespan of the contract. CPS is primarily responsible for large IT purchases where the overall contract value is over $500,000. Contracts under $500,000, including orders from the Michigan Master Computing Program* (MMCP), are facilitated by DTMB Financial Services.

The MMCP consists of four resellers with established contracts, who can be leveraged for the purchase of hardware or software. Two resellers provide only services which allow the State to purchase software licenses and renewable maintenance and support as needed. The State may enter into software license agreements, commonly referred to as end user license agreements* (EULAs), with specific publishers procured under the MMCP reseller. EULAs are a legal contract between the user and the software publisher to detail the terms and conditions for using the software.

The Department of Military and Veterans Affairs (DMVA) procured its applications for patient medical records (Point Click Care [PCC]) and nurse staffing (OnShift) through the MMCP and procured its narcotics dispensing system and medication review tool (BD Pyxis and RxPertise) directly with the software providers.

AUDIT OBJECTIVE

To assess the sufficiency of DMVA and DTMB's efforts to administer selected veteran home IT system contracts.

CONCLUSION

Not sufficient.

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

FACTORS IMPACTING CONCLUSION

- One material condition* related to communicating and agreeing upon the State's standard data security* and contractual requirements with the selected veteran home TPSOs (Finding 1).
- DMVA and DTMB maintained EULA documentation for PCC, OnShift, and BD Pyxis.
- DMVA and DTMB identified data stored on-premises at the State or within the continental United States for OnShift, BD Pyxis, and RxPertise.

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

FINDING 1

Procurement deficiencies increase risk to data security and State interests.

DMVA, in conjunction with DTMB, did not ensure the State's standard data security and contractual requirements were communicated and agreed to by the selected veteran home TPSOs when utilizing the MMCP to procure PCC and OnShift. Without specified and required critical security, confidentiality, and performance expectations that are clearly defined or enforceable, DMVA and DTMB have increased the risk of unauthorized access, misuse, and disclosure of confidential veteran and State data.

DMVA and DTMB did not ensure critical State data security and contractual requirements were included in the current agreements with selected veteran home TPSOs.

MPPM requires the State and a vendor to execute a contract which encompasses the entire agreement prior to a vendor's performance, creating a legal obligation to perform the specified activities and set expectations for the parties. CPS provides guidance on contracting practices, including standardized contract terms and IT specific guidance, for parties involved in IT purchasing.

State of Michigan (SOM) Policy 1340.00 requires all entities authorized to access, store, or transmit State data to protect the confidentiality*, integrity*, and availability* of the data in accordance with all State enterprise IT policies, standards, and procedures. CPS IT Procurement Reference Guide defines State data as any information the contractor receives from the State or derives from information received, including personally identifiable information* (PII) and personal health information or protected health information* (PHI). The guide strongly encourages strict adherence to security language in contract terms and schedules, which are derived from regulatory requirements, accepted best practices, and State policies to ensure the safeguarding of State data.

Our review of applications for medical records (PCC) and nurse staffing (OnShift) disclosed DMVA, in conjunction with DTMB, did not procure the systems using a contract directly with the applications' TPSOs. DMVA informed us these applications were procured from a reseller participating in the MMCP using EULAs to establish the terms between the State and the TPSOs. DMVA and DTMB relied on vendor EULAs which did not incorporate the State's specific data security standards and contractual requirements included in State IT contracts.

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

DMVA, in conjunction with DTMB, did not ensure the EULAs or other documentation for PCC and OnShift contained needed language. We noted:

Missing or Incomplete Language	EULA Language	Criteria	Potential Impact
Specifications or statements of work* (SOWs), including service level agreements*.	PCC EULA contains service level specifications; however, it does not establish a framework for payment when a requirement is not met or goods and services have not been provided. Not included in OnShift EULA.	MPPM states SOWs clearly define the scope of the work to be performed or provided by the vendor and the State, responsibilities to the parties, deliverables, time line for performance, acceptance criteria, and service level agreements. The National Institute of Standards and Technology* (NIST) states organizations should document the basis of vendor relationships so the relationships can be monitored and the level of control is established by the contracts.	Without these items defined and agreed upon, DMVA cannot perform effective* monitoring of TPSOs and problems cannot be remedied if service levels are not met.
Contract terms, including initial contract terms with fixed start and end date, the renewal process, and contract price.	Fixed subscription periods and pricing are not specified within PCC EULA. Fixed subscription periods are not specified within OnShift EULA. Both PCC and OnShift subscription periods and pricing are defined in purchase orders issued to the MMCP reseller when DMVA obtains a new, annual purchase order.	MPPM defines essential components of standard State contracts to include the contract term, including renewal process, and contract price.	Without defined contract periods and pricing directly established with the TPSOs, there is an increased potential of risks such as automatic renewals, service continuation beyond the intended scope, overpayments, vendor disputes, and the inability to determine financial damages in the event of breach.
Requirement to comply with all State physical and IT security policies and standards.	PCC and OnShift EULAs state appropriate technical measures or safeguards will be maintained to protect against the destruction, loss, unavailability, or unauthorized access of customer data.	The CPS IT Procurement Reference Guide states all IT contracts are required to have a data security schedule which includes contractual requirements reflecting State policy and law.	The current EULAs do not define and enforce measures which are in line with, or more restrictive than, State established policies and standards.
Data ownership requirements.	PCC EULA states upon termination, the PCC TPSO will retain only PHI necessary to continue proper management and administration to carry out its legal responsibilities. Unless otherwise agreed to by the parties, the vendor, at its option, will return or destroy the remaining PHI maintained. OnShift EULA states the TPSO is not obligated to retain any customer data if the State has materially breached the agreement or failed to cure the breach within a specific period. Both PCC and OnShift EULAs do not include requirements of the TPSOs to provide State data upon request.	Section 750.491 of the *Michigan Compiled Laws (MCL)* defines State data as property owned by the State. State standard contract terms detail State data is and will remain the sole and exclusive property of the State, including requirements to provide an extract of data when requested and return data upon termination or expiration of the relationship.	The current EULAs do not require TPSOs to provide State data upon request and allow the TPSOs to either maintain State data after termination or delete State data, including confidential PII and PHI.

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

Table continued on next page.

Missing or Incomplete Language	EULA Language	Criteria	Potential Impact
Contractor storage of State data.	PCC EULA states PCC will host the customer's production database in the customer's country of residence. However, this does not specify where data stored with the subservice cloud storage provider* is maintained. Not included in OnShift EULA; however, third-party assurance reports indicate data is stored in the United States.	State standard contract terms require the contractor to keep and maintain State data in strict confidence and keep and maintain State data in the continental United States. Also, SOM Technical Standard 1340.00.160.01 requires the outsourcing of information system services outside the continental United States to be authorized by the State chief information officer and chief security officer.	DMVA informed us they did not receive a response from PCC indicating where the confidential data stored with the subservice cloud storage provider was hosted, despite the EULA specifying it should be stored in DMVA's country of residence, the United States. Storing data within the continental United States helps mitigate cybersecurity risks by keeping data within trusted jurisdictions.
Obligation of confidentiality.	PCC and OnShift EULAs allow TPSOs to aggregate anonymized State data with data of other customers for analytics.	State standard contract terms require the parties to agree to hold all confidential information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give, or disclose confidential information to third parties. Also, CPS guidance warns of clauses within license agreements that give a licensor the right to collect or use data processed by the software, as this could put sensitive State data at risk.	Current EULAs are in contradiction of both CPS guidance and State standard contract language and do not specify which types of data may be anonymized.
Remedies for data breach.	PCC and OnShift EULAs state the vendors shall not be liable for damages in excess of the amount paid by the State for services provided in the last 12-month period preceding an event.	CPS guidance states data loss language in contracts is critical, as without those protections the cost of remedying security breaches falls on the State and its taxpayers.	DMVA paid $291,543 and $22,860 for PCC and OnShift subscriptions, respectively, covering October 1, 2024 through September 30, 2025. Amounts the State would be remedied may not be sufficient to address potential breaches. The ramifications of State data loss may have profound economic impact if systems hosting State data were to be breached.
Audit by contractor.	PCC EULA states PCC will obtain third-party security audits; however, it does not require any audit results be provided to the State. Not included in OnShift EULA.	State standard contract terms require the contractor to conduct a comprehensive independent third-party audit of its data privacy and information security program and provide such audit findings to the State.	DMVA cannot ensure third-party assurance reports will always be obtained from TPSOs. As noted in Objective 3 factors impacting conclusion, DMVA obtained System and Organization Controls* (SOC) reports covering recent reporting periods for PCC and OnShift.
Right of audit by the State.	Not included in PCC or OnShift EULAs.	Standard contract terms affirm the State has the right to review the contractor's data privacy and information security program prior to and during the contract term.	DMVA cannot independently assess data security requirements managed or implemented by TPSOs hosting confidential data (see Finding 4).
Right to terminate.	PCC and OnShift EULAs include specifications to terminate if notifications required by the vendor are provided.	Standard contract language allows the State, at its sole election, to immediately terminate a contract without limitation and without liability.	DMVA is required to terminate EULAs in accordance with the vendor's terms, not the State's.

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

We consider this to be a material condition because:

- The EULA's terms, which are insufficient, will control the entire relationship between the State and its TPSOs who store confidential and sensitive State data and veteran health data.
- The EULAs are legally binding documents which limit the State's ability to audit vendor systems, restrict data ownership rights, or impose automatic liability disclaimers.
- The EULAs do not align with the State's data security; contractual, legal requirements; or *MCLs.*

RECOMMENDATION

We recommend DMVA, in conjunction with DTMB, ensure the State's standard data security and contractual requirements are communicated to and agreed upon by the selected veteran home TPSOs.

AGENCY PRELIMINARY RESPONSE

DMVA and DTMB partially agree. Given the length of DMVA and DTMB's preliminary response, the response and our auditor's comments to Finding 1 are presented on page 25.

SECURITY AND ACCESS CONTROLS

BACKGROUND

Security* controls are the management, operational, and technical controls designed to protect the availability, confidentiality, and integrity of an IT system and its information.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting the resources from unauthorized modification, loss, and disclosure. For access controls to be effective, they should be properly authorized, implemented, and maintained.

In early 2020, DMVA and DTMB engaged a TPSO for use of the PCC application. PCC is a software-as-a-service* (SaaS), cloud-based software application hosted and maintained by the vendor. In the SaaS model, DMVA management is limited to user-specific application configuration* settings and does not manage or control the underlying cloud infrastructure, which typically includes the network, servers, operating systems*, storage, or individual applications. The shared responsibility of access control is a consideration in the SaaS model; however, DMVA is ultimately responsible for the security of its cloud-based data, including who has access to it.

DMVA uses PCC as the electronic medical records system in all three veteran homes, allowing DMVA to maintain and communicate patient information among healthcare providers and retain medical record data for long-term inpatient care services. The primary users of PCC consist of State and contracted employees working in the veteran homes. As of July 2, 2025, PCC had 819 active user accounts.

AUDIT OBJECTIVE

To assess the effectiveness* of DMVA's security and access controls over PCC.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DMVA established and implemented some procedures related to user account authorization and recertifications in accordance with State policies and standards.
- Some access controls were implemented in accordance with State policies and standards.
- Some security configuration parameters were implemented in accordance with SOM Technical Standards.
- One material condition related to PCC vendor user accounts' excessive access rights in PCC (Finding 2).
- One reportable condition* related to fully establishing and implementing user access controls over PCC (Finding 3).

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

FINDING 2

Improvements needed in monitoring PCC vendor staff access to veteran health information.

All 21 PCC vendor user accounts had access to all of the roles in the system.

DMVA did not ensure PCC TPSO vendor accounts were granted appropriate access or conduct monitoring of vendor account activity. As a result, inappropriate access to sensitive and confidential veteran health data may occur, increasing the risk of unauthorized use or compromised data integrity.

We identified 21 active PCC user accounts as of August 26, 2025 associated with TPSO vendor employees, with all 121 roles assigned, including privileged roles, and noted DMVA did not:

a. Authorize access for the vendor's user accounts in PCC.

   SOM Technical Standard 1340.00.020.01 requires approvals from appropriate individuals for new account requests. Also, agencies are required to document valid access authorizations and intended system usage before granting access to the system.

   DMVA informed us no specific authorization form exists for vendor accounts, and the TPSO will create accounts to provide technical support services as needed and specified in agreements with the State.

b. Enforce the principle of least privilege*.

   SOM Technical Standard 1340.00.020.01 requires the assignment of access rights based on the principle of least privilege, allowing only authorized access for users necessary to perform assigned job duties. With all 121 available roles assigned to the PCC vendor accounts, it is possible for these users to create, edit, and disable accounts, including their own, perform accounting tasks such as billing, and view/edit veteran health data.

   DMVA informed us the vendor required access to all available roles in PCC to replicate potential issues identified by PCC users and provide support as needed.

   National Institute of Standards and Technology* (NIST) states when system users include external system service providers, access control processes apply the principle of least privilege to precisely define what information is accessible, for what duration, at what frequency, using what access methods, and by whom. NIST recommends entities establish baseline configurations for development, testing, and operational environments to protect systems from unplanned or unexpected events related to development and testing activities. Configurations in the test environment mirror configurations in the operational environment, therefore testing and troubleshooting could occur in a non-operational environment.

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

c. Monitor TPSO vendor account activity.

SOM Technical Standard 1340.00.040.01 requires agencies implement an audit log report which supports efficient, timely, and effective audit log analysis to search for events of interest. NIST recommends entities implement additional monitoring on privileged user accounts* who have access to more sensitive information, including security-related information.

DMVA informed us during medical record audits there have been no indications of any modification by any PCC user log-in, and if there had been, it would have triggered additional actions. However, these reviews are performed on an ad hoc basis of individual member's medical information and would not provide sufficient monitoring of all potential actions performed by PCC vendor accounts.

We consider this to be a material condition because of the number of PCC vendor accounts granted excessive access rights and DMVA's insufficient monitoring of the actions performed in PCC containing confidential veteran health data.

RECOMMENDATION

We recommend DMVA ensure PCC TPSO vendor accounts are granted appropriate access and monitor vendor account activity.

AGENCY PRELIMINARY RESPONSE

DMVA partially agrees. Given the length of DMVA's preliminary response, the response and our auditor's comments to Finding 2 are presented on page 27.

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

FINDING 3

Improvements needed to PCC access and security controls.

DMVA did not fully establish and implement access controls over PCC, which could lead to unauthorized access, disclosure, or modification of veteran health data.

SOM Technical Standard 1340.00.020.01 defines the access control baselines for access to information systems, including those used, managed, or operated on the agency's behalf by a vendor.

Our review of PCC disclosed DMVA did not:

a. Fully establish a formal process to grant PCC application access to align with the users' job responsibilities. DMVA did not:

   (1) Identify all groups or functions on user access requests or always have complete user access supporting documentation.

   We randomly sampled 30 of 374 active PCC users created within the audit period as of July 2, 2025, and reviewed access authorization communication to determine whether access was appropriately authorized and noted DMVA did not:

   (a) Specify the groups or functions to which the users should be assigned for 26 (96%) of 27 users. E-mail communication to request access to PCC contained the user's job position which did not always equate to a specific role within PCC. However, we noted common job positions within the veteran homes, such as a certified nursing assistant, generally aligned with a consistent role in PCC.

   SOM Technical Standard 1340.00.020.01 requires State agencies to establish a process to control and document the assignment of access rights based on valid access authorization and intended system usage. Without a formalized process or guidance to map job positions to specific PCC roles, access decisions are made based on interpretation of job titles provided in e-mail communications.

   (b) Maintain complete supporting documentation for the access granted to the remaining 3 (10%) of 30 users.

   SOM Technical Standard 1340.00.020.03 affirms the agency is responsible for maintaining documentation of authorized users from the initial request to the deregistration of users who no longer

require access to State protected IT resources.

(2) Assess and document incompatible roles or excessive access rights to ensure effective segregation of duties* and access based on the principle of least privilege. Identifying incompatible roles is a key control in effective segregation of duties. Inadequate segregation of duties increases the risk of malicious activity.

SOM Technical Standard 1340.00.020.01 requires agencies implement separation of duties by identifying and documenting the separate duties of individuals and defining system access authorization to support separation of duties.

DMVA informed us customized roles have been created in PCC to assign access rights in alignment with job responsibilities in the veteran homes. Individuals administering access to PCC will internally discuss the purpose or function of new employees to determine the appropriate customized roles to assign.

b. Always perform effective user account management. We noted DMVA did not:

(1) Remove an anonymous test account utilized in the production environment.

We identified one PCC test account active as of July 2, 2025 not associated with a unique individual.

SOM Technical Standard 1340.00.020.01 allows use of test accounts with information system owner approval; however, the Standard further states anonymous accounts are prohibited. If not properly managed, an anonymous test account in production environments may create a security risk because the account may, inadvertently, be granted inappropriate application access and may not be disabled when no longer needed or properly monitored.

DMVA informed us the test account is used within one veteran home to review what a user with different customized roles assigned will have access to within PCC.

(2) Perform annual and semiannual recertifications of PCC users for 2 of the 3 veteran homes. SOM Technical Standard 1340.00.020.01 requires reviewing access rights periodically for

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

appropriateness. In May 2025, the Standard was revised to no longer require semiannual recertification of privileged user accounts. However, the prior version was applicable for the majority of the audit period during which semiannual reviews were required.

DMVA informed us the two veteran homes have recently begun recertification reviews which had not been previously completed because of a lack of awareness regarding the requirement or temporary staffing adjustments to cover employee leave.

(3) Disable separated employees' user accounts.

We determined 2 (5%) of 43 randomly sampled PCC user accounts as of July 2, 2025 were not disabled within 24 hours of employee separation. User access was removed between 6 and 59 days after the separation date.

SOM Technical Standard 1340.00.020.01 requires disabling or removing user access when accounts are no longer required and when users are terminated or transferred.

DMVA informed us it relies on notifications from contractors when contracted nursing staff are no longer employed.

c. Ensure selected security configurations were appropriate.

SOM Technical Standard 1340.00.080.01 defines the identification and authentication security controls required for State information systems. This Standard is applicable to all information systems, including vendor managed systems.

For all tested security configurations managed by the PCC vendor, DMVA did not obtain documentation to demonstrate the current settings implemented comply with SOM Technical Standards. DMVA informed us the vendor was unwilling to provide documentation beyond the SOC reports. DMVA confirmed the selected security configurations were not documented within the available SOC reports and provided documentation which did not indicate whether the vendor implemented what was described at the time of our review.

Because of the confidentiality of these configurations, we summarized our testing results for presentation in this finding and provided the underlying details to DMVA management.

RECOMMENDATION	We recommend DMVA fully establish and implement access controls over PCC.
AGENCY PRELIMINARY RESPONSE	DMVA partially agrees. Given the length of DMVA's preliminary response, the response and our auditor's comments to Finding 3 are presented on page 28.

MONITORING SELECTED TPSOs

BACKGROUND

DMVA utilizes various vendor hosted or supported solutions, including on-premises commercial off-the-shelf* software and SaaS solutions to administer skilled nursing care to members in Michigan veteran homes. These services include maintenance of electronic medical records, nursing staff scheduling, member medication plan review, and medication tracking and administration.

According to the State of Michigan Financial Management Guide* (FMG) (Part VII, Chapter 1, Section 1000), each department is required to establish and maintain a sound internal control* system over activities, including those managed by TPSOs. The department should consider the TPSO's significance to department operations, gain an understanding of its controls, and obtain assurance the controls are present and functioning as intended to ensure the State's interests are protected in an acceptable fashion.

An effective risk management process occurs throughout the lifecycle of the relationship with a TPSO and includes ongoing monitoring of its activities and performance. Independent reviews and evaluations of performance allow management to determine the TPSO's controls are effectively managed and provide regular and formal reporting of TPSO performance in accordance with contract requirements, including deviations from the agreed service.

SOC reports can be obtained to provide the departments with an opinion, conclusion, or findings regarding the reliability of controls related to services. To rely on the vendor's controls, DMVA must have complementary user entity controls* (CUECs) which are properly designed and implemented. These controls help ensure the vendor's system and services work securely and effectively and complement the TPSO's controls.

AUDIT OBJECTIVE

To assess the sufficiency of DMVA and DTMB's monitoring of selected veteran home TPSOs.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- DMVA obtained SOC reports covering recent reporting periods for PCC and OnShift.
- DMVA appointed an agency security officer* to manage risk and help ensure agency information security.

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

- One reportable condition relating to improving TPSO SOC report oversight and the monitoring and implementing of controls to manage risks associated with outsourced services (Finding 4).

FINDING 4

Monitoring improvements needed for TPSOs.

DMVA needs to improve its monitoring of selected TPSOs to include sufficiently reviewing TPSO SOC reports and designing and implementing required CUECs. Strengthened monitoring would increase DMVA's assurance regarding the security and management of veteran home and State data.

SOC reports are internal control reports on the services provided by a TPSO and provide valuable information users need to assess and address the risks associated with an outsourced service. The FMG (Part VII, Chapter 1, Section 1000) prescribes guidelines for departments to assess and manage risk associated with third-party relationships and requires each department to establish and maintain a sound internal control system over activities and transactions, including those managed by TPSOs.

According to the FMG, departments need to understand the controls each TPSO designs, implements, and operates for their assigned operational processes and evaluate how the TPSO's internal control system impacts the department's internal control system. Also, the FMG requires departments to obtain SOC reports within 60 days of the report issue date and complete a review, which includes using the SOC report review template to evaluate and document the auditor's opinion, management's assertion of control environment, reporting period, use of subservice organizations, and an evaluation of the effectiveness of CUECs.

We reviewed DMVA's monitoring controls of its PCC, OnShift, BD Pyxis, and RxPertise TPSOs and noted:

a. DMVA did not sufficiently review and document the assessment of PCC and OnShift SOC reports.

   DMVA informed us the SOC reports for PCC and OnShift were reviewed during the Michigan Security Accreditation Process* (MiSAP) in conjunction with DTMB to ensure the State's adopted NIST security controls are met. However, its review did not evaluate all FMG requirements, including CUECs which must be implemented by DMVA to ensure the service organization's control objectives are achieved. Without reviewing the FMG requirements and evaluating the effectiveness of CUECs, DMVA is unable to fully determine the reliability of controls related to services provided as measured against suitable and available criteria, such as NIST.

CUECs were not evaluated to ensure the reliability of the vendor's controls.

b. DMVA did not obtain the PCC and OnShift SOC reports within 60 days after the report date. Reports were obtained between 124 and 232 days after the date of issuance.

   DMVA informed us it is not always aware of when a new SOC report is issued, as DMVA's purpose to obtain the SOC report is to complete the biennial MiSAP process.

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

Timely receipt is essential to ensure the SOC report does not identify weaknesses which require immediate attention.

When the State outsources tasks and functions, many of the service organization's risks become the State's risks. High risk activities, such as safeguarding and preventing unauthorized disclosure of confidential and sensitive information, demand greater attention and oversight by the department. SOC reports include valuable information which add credibility and trust to the information users need to manage risk associated with outsourced service providers.

RECOMMENDATION

We recommend DMVA improve its monitoring of selected TPSOs to include sufficiently reviewing TPSO SOC reports and designing and implementing required CUECs.

AGENCY PRELIMINARY RESPONSE

DMVA agrees. Given the length of DMVA's preliminary response, the response and our auditor's comments to Finding 4 are presented on page 29.

AGENCY PRELIMINARY RESPONSES

SELECTED DEPARTMENT OF MILITARY AND VETERANS AFFAIRS IT SYSTEMS
Department of Military and Veterans Affairs and
Department of Technology, Management, and Budget

Finding 1 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DMVA and DTMB's preliminary response to Finding 1 and our auditor's comments providing further clarification and context where necessary.

Overall Auditor's Comment

The language contained in the PCC and OnShift EULAs was insufficient and did not align with State standard contracting requirements. Key terms were not clearly defined, leaving critical obligations open to interpretation by the vendor. This lack of clarity increases the State's risk related to data security, confidentiality, and enforceability of performance standards.

Finding 1: Procurement deficiencies increase risk to data security and State interests.

DMVA and DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
DMVA and DTMB partially agree with the finding. While we acknowledge that the End User License Agreements (EULAs) used did not explicitly reference the State of Michigan Technical Security Standards, we disagree that this implies the State's data was inherently less secure. EULAs are legally binding agreements, and those executed for PCC and OnShift included provisions addressing security, confidentiality, and performance. The EULAs were reviewed by DTMB from a technical and legal perspective.	As noted in Finding 1, State standard contract language absent in the EULAs leaves the SOM vulnerable to the vendors interpretation of the provisions, which may differ from the State's expectations or statutory requirements. Without clear alignment to the State's contracting standards, enforcement becomes difficult and ambiguities can favor the vendor in the event of a dispute. While security and confidentiality were addressed, the vendor's language did not incorporate State required security controls and specific language regarding handling, storage, and destruction of State data. The absence of State-defined requirements increases the risk of insufficient data protection, unclear responsibilities, and limited recourse in the event of noncompliance.
Both systems were procured through approved contracting vehicles under State policy. DTMB conducted technical and legal reviews of the EULAs, and additional compensating controls were implemented, including: • *Alignment with State security standards through EULA review, System Security Plans, and Risk Assessments.* • *A signed Business Associate Agreement (BAA) with PCC for Health Insurance Portability and Accountability Act (HIPAA) compliance.* • *Biennial internal control evaluations of select security controls.*	DTMB did not mention nor provide documentation of a technical or legal review. The compensating controls listed by DMVA and DTMB in the internal control evaluations and biennial reporting processes are point in time assessments utilized by State agencies.
The agencies will continue to enhance controls for monitoring third-party service providers and have matured IT risk assessment processes over the past 18 months.	

Detail contained in the audit report table includes provisions commonly found in the State's standard contract terms. However, the MMCP program allows for these provisions to be addressed within EULAs and associated documents. EULAs and associated documents may address contractual provisions contained within the State's standard contract terms, though specific language may not be stated verbatim.

While the provisions could be addressed within EULAs, the table in the finding details those provisions missing or incomplete in the current PCC and OnShift EULAs. State procurement guidance is clear that a complete understanding between parties be defined in writing, and any issues which may arise can be resolved using only the terms contained in the agreement. The important concepts should be covered by the license or agreement, with no assumptions.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 1

Go to Finding 2

Finding 2 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DMVA's preliminary response to Finding 2 and our auditor's comments providing further clarification and context where necessary.

Finding 2: Improvements needed in monitoring PCC vendor staff access to veteran health information.

DMVA provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
In regard to (a) and (b), the Agency disagrees that vendor access was not authorized nor assigned according to the principle of least privilege. PCC is MVH's electronic medical record (EMR) system, a critical tool in the provision of care to our patients. As an organization providing 24/7 medical care, timely technical support – including outside 9-5 business hours – is essential. Technical support personnel (TSP) are required to assist any and all users who encounter system issues. Therefore, they must have access to all system roles to validate the user's experience and provide resolution.	The fact remains no documentation exists to support DMVA approved access to a SOM application for the vendor user accounts. Also, DMVA did not determine whether the accounts with access to all 121 roles available were appropriate to the job responsibilities and technical support required. Access by vendor users to the DMVA production environment, which contains confidential veteran PII and PHI, should be controlled, temporary, and logged with clear justification documented.
The assignment of select authorized TSP to all security roles is crucial to provide agreed upon services and does not negate the signed terms and conditions that clearly prohibit improper access to the vendor-managed system. DMVA is satisfied with PCC's documented procedures for authorizing and assigning TSP access. PCC was hired with the expectation they would provide 24/7 software support and these selected TSP need access to all roles to do so. The likelihood and risk to patient health and safety associated with delayed resolution of EMR technical issues greatly outweighs the likelihood and risk associated with the TSP improperly accessing the system. *In regard to (c), the Agency agrees with the finding and has implemented a procedure and schedule for monitoring activities related to the vendors' user accounts.*	Vendor user accounts were not only assigned to all security roles, but were assigned to all roles within the system, including roles to perform billing, physician, psychiatrist, and pharmacist activities. PCC vendor users do not have a business need to perform accounting tasks or disable SOM user access within an application managed by DMVA. Enforcing the principle of least privilege would eliminate PCC users from having access to those areas. DMVA's process to allow PCC to assign and authorize users in DMVA's production environment does not follow the requirements in SOM Technical Standard 1340.00.020.01. The Technical Standard requires the agency to document and retain approvals by appropriate individuals for new account requests, valid access authorization, and intended system usage before granting access to the system. The SOM Technical Standard applies to all agency information systems, including those used, managed, or operated by a vendor on the agency's behalf. We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 2

Go to Finding 3

Finding 3 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DMVA's preliminary response to Finding 3 and our auditor's comments providing further clarification and context where necessary.

Finding 3: Improvements needed to PCC access and security controls.

DMVA provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
In regard to (a), the Agency agrees it has not "fully established a formal process" insomuch as user access requests are not submitted on a specific document. However, the Agency contends individual user access is granted in accordance with employee licensure and that State healthcare licenses serve as supporting documentation for the specific roles and responsibilities an employee shall be assigned. Granting access based on licensure is industry standard and will continue to be the Agency's approach. For some positions, multiple PCC roles exist within the scope of practice to reflect typical duties within MVH (e.g. an RN may typically act as a wound nurse at MVH, but is licensed to pass meds and perform other patient assessments as needed, which may require additional roles in PCC). Role assignments within scope of practice will be made as operational needs of the facility necessitate. This is not a failure to sufficiently segregate duties nor to enforce the principle of least privilege. Furthermore, non-licensed staff have defined roles and access that reflects limited duties according to State law.	DMVA's statements are contradictory as it states role assignments are based on having a State healthcare license and based on operational needs, which vary within the MVH. A State license does not provide information to dictate the level of access necessary in PCC. SOM Technical Standard 1340.00.020.01 states the agency must document the type of users that should have access to the system, the groups or roles they can be assigned to, and the privileges assigned to each group, role, or account. If role assignments are made within scope, as operational needs facilitate, DMVA should ensure this is documented appropriately. As noted in the Finding, DMVA did not assess and document incompatible roles or excessive access rights, which is a failure to sufficiently segregate duties and enforce the principle of least privilege.
In regard to (b), the Agency agrees with the findings as written and has (1) removed the test account and (2) implemented processes that meet the current standard. Regarding (3), the Agency asserts it will not be able to meet the new State Technical Standard (which was changed during the audit period), nor does it intend to implement corrective action. Not all departures come with timely notice. In some cases, they are preceded by leaves of absence, failures to report for duty, or suspensions; all of which may lead to eventual termination backdated to the employee's last day of attendance. DMVA makes every effort to revoke system access as soon as possible and will continue to do so within 24 hours of notification of termination yet contends there are circumstances that make compliance with the new Technical Standard impossible.	If DMVA cannot meet the new SOM Technical Standard, it should request a Technical Review Board exception stating as such.
In regard to (c), the Agency agrees we could not demonstrate the vendor's security configurations with screenshots of their internal system environment. DMVA has received formal exceptions and is now in compliance.	It is unclear how DMVA can claim formal exceptions were obtained when it acknowledges it was unable to obtain evidence of current configuration settings during the audit. Without proof of deviations from SOM Technical Standards, the basis for any formal exceptions remains unclear. We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 3

Go to Finding 4

Finding 4 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DMVA's preliminary response to Finding 4 and our auditor's comments providing further clarification and context where necessary.

Finding 4: Monitoring improvements needed for third-party service organizations.

DMVA provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
The Agency agrees with this finding and acknowledges improvements could be made to better monitor third-party service organizations and more intentionally evaluate required complementary user entity controls (CUECs). However, both systems received all necessary DTMB approvals required to be considered compliant with SOM Technical Standards. Security controls are reviewed triennially as part of the Michigan Security Accreditation Process (MiSAP) and biennially as part of Internal Controls Evaluation (ICE). Over 240 NIST controls for PointClickCare and over 130 NIST controls for OnShift are assessed and each TPSO's SOC report is analyzed, even if not documented on the recommended template. *DMVA will continue to strengthen TPSO monitoring practices. For the two material systems, DMVA has acquired 2025 SOC documentation and completed the recommended SOC Review Template within 60 days of the report publish date.*	A control or security assessment performed on a biennial and triennial basis is not sufficient to address vendor-related risk that can emerge at any time. Threat landscapes and vulnerabilities evolve rapidly and limiting assessments to only every two or three years leaves significant gaps in oversight. The MiSAP and ICE processes do not take the place of SOC report reviews, which are more often issued annually. During our audit fieldwork, we asked DMVA for evidence of a control assessed during the MiSAP process. DMVA informed us that the System Security Plan (SSP) indicated the control was set in accordance with SOM Technical Standards; however, the particular control did not have evidence attached in the SSP. The assessment of controls may not be sufficient if supporting evidence is not retained at the time of the review. As noted in Finding 3, DMVA was unable to receive a response from the vendor indicating the current configuration settings. Therefore, there is no assurance the control is implemented as intended or remained effective during the assessment period. We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 4

AGENCY AND SYSTEM DESCRIPTION

DMVA synchronizes strategic, legislative, and fiscal initiatives to build and sustain military readiness, care and advocate for veterans, and cultivate purposeful partnerships. DMVA branch operations include MVH, State Operations, Michigan National Guard, Michigan Veterans Affairs Agency, and the Michigan Youth Challenge Academy.

MVH provides nursing care and domiciliary services to military veterans, widows, spouses, former spouses, and parents of Michigan veterans. Currently, the MVH operates homes in Grand Rapids, Marquette, and Chesterfield Township. During fiscal year 2025, each of the homes served approximately 160 veterans. DMVA primarily uses 26 IT systems to provide long-term skilled nursing care and services within the homes. We conducted an assessment and identified four systems to review based on risk factors such as whether the service is hosted on State or vendor systems, impact on veterans' health and safety, and data confidentiality. Our scope included the following MVH systems:

- PCC is used to capture and maintain veterans' patient data, including medical record data for long-term care inpatient services and the facilitation of billing for qualifying services. PCC maintains data which includes both PII and PHI.

- OnShift is used as scheduling software for nursing staff within the veteran homes. Reports generated from OnShift are submitted to the Centers for Medicare and Medicaid Services to meet federal reporting requirements on the level of staff in long-term care facilities. OnShift maintains data which includes PII.

- BD Pyxis is used as a narcotics dispensing system which administers and tracks medications within all veteran homes.

- RxPertise is used as a medication regimen review software used to electronically review veterans' medications for potential drug interactions and create the most effective pharmaceutical outcomes for each veteran. Currently, the system is used only in the Grand Rapids facility.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the records and processes related to DMVA's IT system contracts administration, TPSO monitoring, and IT system access controls. We conducted this performance audit* 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As part of the audit, we considered the five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2023 through July 31, 2025.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of DMVA's and DTMB's processes and internal control to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed DMVA and DTMB management to obtain an understanding of the IT systems used to care and advocate for veterans.
- Examined fiscal years 2024 and 2025 appropriation acts to identify DMVA's budgeted IT services and projects.
- Reviewed DMVA and SOM policies and procedures related to system security and access.
- Analyzed DMVA expenditures and revenues from January 1, 2024 through April 30, 2025.
- Reviewed Michigan Veterans Trust Fund Board meeting minutes from January 2024 through March 2025 and Michigan Veterans' Facility Authority meeting minutes from February 2024 through February 2025.
- Examined DTMB's active contract list as of May 14, 2025 and then again as of June 5, 2025 to identify DMVA IT system contracts.

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

- Interviewed DMVA and DTMB staff to obtain an understanding of processes related to user access.
- Reviewed FMG and industry best practices for establishing relationships with TPSOs and monitoring them.

OBJECTIVE 1

To assess the sufficiency of DMVA and DTMB's efforts to administer selected veteran home IT system contracts.

To accomplish this objective, we:

- Examined MMCP's intranet and MPPM to gain an understanding of State IT security contract language and the DTMB divisions involved with MMCP.
- Interviewed CPS, DTMB Financial Services, and Chief Technology Office staff to gain an understanding of each division's responsibility in the process to procure software and hardware under MMCP.
- Reviewed selected DMVA IT systems' EULAs to determine whether standard State contract language, including data security and privacy requirements, were included.
- Reviewed selected DMVA IT systems' data hosting information to confirm whether data was hosted outside of the United States.

OBJECTIVE 2

To assess the effectiveness of DMVA's security and access controls over PCC.

To accomplish this objective, we:

- Interviewed DMVA's management and staff to obtain an understanding of the implemented security and access controls.
- Selected users with active PCC accounts to better understand, evaluate, and form conclusions on the design and implementation of DMVA's internal control procedures against State policy and industry best practices for granting and removing access. Specifically, we:
    - Identified 374 of 819 active user accounts created between October 1, 2023 and July 2, 2025 and randomly sampled 30 of 374 active user accounts to determine if DMVA maintained user access initial authorization documentation.
    - Randomly sampled 43 of 818 active user accounts associated with unique individuals as of July 2, 2025 to evaluate users' employment status.

- Reviewed monthly and quarterly recertifications of all PCC user accounts for one veteran home.
- Reviewed last log-in dates for all 819 active user accounts as of July 2, 2025 in PCC to verify user accounts were being disabled in accordance with SOM technical standards.
- Interviewed DMVA management and examined documentation to obtain an understanding of the segregation of duties in PCC.
- As of August 26, 2025, reviewed the appropriateness of 21 vendor user accounts having access to PCC data.
- Tested the end-user account security configurations against State policy and industry best practices.

OBJECTIVE 3

To assess the sufficiency of DMVA and DTMB's monitoring of selected veteran home TPSOs.

To accomplish this objective, we:

- Interviewed DMVA management to determine if organizational oversight and user roles and responsibilities were defined regarding external system services.
- Interviewed DMVA's and DTMB's management and staff to obtain an understanding of the SOC report receipt and review process.
- Reviewed and assessed PCC and OnShift SOC reports.
- Examined RxPertise to ensure data was stored on a local computer within the Michigan Veterans Home in Grand Rapids.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions or reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality of security configurations, we summarized our testing results for presentation in the report and provided the underlying details to DMVA management.

AGENCY RESPONSES

Our audit report contains 4 findings and 4 corresponding recommendations. DMVA's preliminary response indicates it agrees with 1 of the recommendations and partially agrees with 2 of the recommendations. DMVA and DTMB partially agree with 1 recommendation.

The agency preliminary response following each recommendation in our report was taken from the agencies' written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* requires an audited agency to develop a plan to comply with the recommendations and submit it to SBO upon audit completion. The State of Michigan Financial Management Guide (Part VII, Chapter 3, Section 100) requires the audited agency to develop the plan as early as practicable and within 60 days after report issuance and submit the plan to OIAS, SBO. Within 30 days of receipt, OIAS will either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls	Controls protecting data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
agency security officer	An agency official with operational authority for security agency information and establishing controls for its generation, collection, processing, dissemination, and disposal. Assists the agency information system owner and information owners in ensuring information systems have adequate security controls in place to meet all applicable State and/or federal laws, rules, and regulations.
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.
availability	Timely and reliable access to data and information systems.
commercial-off-the-shelf	Hardware or software IT products that are ready-made and available for purchase by the general public.
complementary user entity controls (CUECs)	Controls the service organization has included within its system and rely on the user entity (department) to implement in order to achieve the service organization's control objectives.
confidentiality	Protection of data from unauthorized disclosure.
configuration	The setup of a system. Configuration can refer to either hardware, software or a combination of both.
CPS	Central Procurement Services.
DMVA	Department of Military and Veterans Affairs.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.

end user license agreements (EULAs)	Software license agreement representing a contractual agreement between the licensor of the software and the licensee. Defines the relative rights between the licensor and licensee, gives a licensee the legal right to use a given software application, and documents the formal granting of permission to use, including clearly describing the rights and restrictions on use.
integrity	Accuracy, completeness, and timeliness of data in an information system.
internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.
IT	information technology.
material condition	A matter, in the auditor's judgment, which 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.
MCL	*Michigan Compiled Laws.*
Michigan Master Computing Program (MMCP)	Consists of a group of resellers, with established contracts, that can be leveraged for the purchase of hardware or software under $500,000 as well as certain Standard IT Hardware and Software that cannot be purchased directly (Adobe, Microsoft, etc.). MMCP is supported by a bidding process facilitated by DTMB Financial Services.
Michigan Procurement Policy Manual (MPPM)	Designed to provide various stakeholders, including procurement professionals, end users, contractors, and taxpayers, a transparent and enterprise-wide standardized procurement policy and process. MPPM is the official source of policy for all purchases made pursuant to Public Act 431 of 1984.
Michigan Security Accreditation Process (MiSAP)	A Statewide IT application security plan and remediation methodology for assessing risk, identifying and documenting application controls, remediating identified control gaps, and obtaining an authority to operate within the State IT environments.

MVH	Michigan Veteran Homes.
National Institute of Standards and Technology (NIST)	An agency of the U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum-security requirements for federal programs.
OIAS	Office of Internal Audit Services.
operating system	The essential program in a computer which manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
PCC	Point Click Care.
performance audit	An audit which 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.
personally identifiable information (PII)	Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, social security number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.
principle of least privilege	The practice of limiting access to the minimal level which will allow normal functioning. Applied to employees, the principle of least privilege translates to giving employees 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.
privileged user accounts	Extensive system access capabilities granted to the person(s) responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
protected health information (PHI)	Individually identifiable health related information which is collected by a HIPAA-covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

reportable condition	A matter, in the auditor's judgment, 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.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
service level agreements	Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination.
software-as-a-service (SaaS)	Application accessible from various devices through either a thin client interface, such as a web browser, or a program interface. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or individual applications.
SOM	State of Michigan.
State of Michigan Financial Management Guide (FMG)	A consolidation of State financial management policies and procedures.
statement of work (SOW)	Clear definition of the scope of the work to be performed or provided by the contractor and the State, the responsibilities of the parties, the deliverables, the milestones and time line for performance, acceptance criteria, applicable service level agreements, and the associated payment stream.
subservice cloud storage provider	A third-party vendor which a primary organization relies on to deliver part of its services, specifically cloud infrastructure including network, servers, operating systems, or storage.
System and Organization Controls (SOC) report	Designed to help organizations providing services to user entities build trust and confidence in their delivery processes and controls through a report by an independent certified public accountant (CPA).

Each type of SOC report is designed to meet specific user needs:

- SOC 1 (Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting) - Intended for user entities and the CPAs auditing their financial statements in evaluating the effect of the service organization's controls on the user entities' financial statements.

- SOC 2 (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy) - Intended for a broad range of users needing information and assurance about a service organization's controls relevant to any combination of the five predefined control principles.

  There are two types of SOC 1 and SOC 2 reports:

  - Type 1 - Reports on the fairness of management's description of a service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description, as of a specified date.

  - Type 2 - Includes the information in a type 1 report and also addresses the operating effectiveness of the controls to achieve the related control objectives included in the description, throughout a specified period.

- SOC 3 (Trust Services Report for a Service Organization) - Intended for those needing assurance about a service organization's controls affecting the security, availability, or processing integrity of the systems a service organization employs to process user entities' information, or the confidentiality or privacy of information, but not having the need for or the knowledge necessary to make effective use of a SOC 2 report.

- SOC for Cybersecurity - Intended to communicate relevant information about the effectiveness of an organization's cybersecurity risk management programs.

TPSO third-party service organization.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070