Office of the Auditor General
Performance Audit Report

Statewide Integrated Governmental Management Applications (SIGMA) - Selected Security and Application Controls

State Budget Office

March 2026

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

171-0595-25

> 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

Statewide Integrated Governmental Management Applications (SIGMA) - Selected Security and Application Controls

State Budget Office

Report Number:
171-0595-25

Released:
March 2026

SIGMA is an enterprise resource planning solution for the State of Michigan and is managed by the State Budget Office (SBO) SIGMA team. SIGMA consists of several modules which standardize Statewide accounting activities, procurement and vendor management, time and expense processes, budgeting processes, payment processing, cost accounting, bids and grant opportunities, and financial reporting. As of June 2025, SIGMA had approximately 283,300 active vendors, 52,200 State employees completing biweekly time and travel entries, and 11,400 core application users with access to complete financial, budget, procurement, human resource, and reporting functions. In fiscal years 2024 and 2025, SIGMA processed $86.4 billion and $91.1 billion in expenditures, respectively, and $88.6 billion and $91.8 billion in revenues, respectively.

Audit Objective	**Conclusion**
Objective 1: To assess the effectiveness of SBO's efforts to ensure completeness and accuracy of selected vendor data within SIGMA.	Moderately effective

Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
SBO does not have sufficient processes to identify and disable inactive vendor accounts. As of August 25, 2025, 131,596 (46%) of 287,510 active vendors had not received a payment since at least October 3, 2017 (Finding 1).		X	Agrees
An Internal Revenue Service (IRS) taxpayer identification number match was not completed for 6 (10%) of 61 sampled newly registered vendors, which may increase the risk of potential improper payments and fraudulent vendors (Finding 2).		X	Agrees

Observations Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Miscellaneous vendors could be further scrutinized to improve the accuracy of the procurement and vendor payment processes (Observation 1).	Not applicable for observations.		

Audit Objective	Conclusion
Objective 2: To assess the sufficiency of selected SBO SIGMA access controls.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Explanations and support were not sufficiently documented for 9 (75%) of 12 agencies who moved transactions past one or more levels of defined approval paths before the transaction was finalized (Finding 3).		X	Agrees
SIGMA application level access was not revoked promptly for 6 (10%) of 60 sampled terminated users, increasing the risk of unauthorized access, use, and modification of SIGMA data (Finding 4).		X	Agrees

Audit Objective	Conclusion
Objective 3: To assess the sufficiency of selected SBO SIGMA workflow controls.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
SBO should periodically reevaluate SIGMA transaction codes without required workflows or compensating controls to prevent modified transactions from being inadvertently processed without the appropriate approvals (Finding 5).		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

March 19, 2026

Jennifer L. Flood, State Budget Director
State Budget Office
George W. Romney Building
Lansing, Michigan

Director Flood:

This is our performance audit report on Statewide Integrated Governmental Management Applications (SIGMA) - Selected Security and Application Controls, State Budget Office.

We organize our findings and observations by audit objective. Your agency provided the 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

SIGMA - SELECTED SECURITY AND APPLICATION CONTROLS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

COMPLETENESS AND ACCURACY OF SELECTED VENDOR DATA

BACKGROUND

According to Federal Information System Controls Audit Manual* (FISCAM), controls should be designed and implemented to provide reasonable assurance of the completeness and accuracy of data within a system. Ensuring Statewide Integrated Governmental Management Applications* (SIGMA) contains complete and accurate data is the responsibility of the State Budget Office (SBO), in conjunction with State agencies.

Master data is referential data which provides the basis for ongoing business activities, for example, vendor data. A vendor may initiate the process to be added to SIGMA using SIGMA Vendor Self-Service (VSS), or authorized State agency users may register the vendor if provided with the required documentation. As part of SBO's vendor registration process, the associated taxpayer identification number (TIN) is included in a weekly automated exchange with the Internal Revenue Service (IRS) to validate a match.

Once the vendor is added to SIGMA, they can contact the SIGMA Helpdesk* for assistance. The Helpdesk has various controls to authenticate the vendor to ensure the individual providing information and accessing the vendor's account is the appropriate, authorized individual.

AUDIT OBJECTIVE

To assess the effectiveness of SBO's efforts to ensure completeness and accuracy of selected vendor data within SIGMA.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- SBO implemented effective controls to ensure SIGMA Helpdesk staff properly validated the contact's identity.

- SBO implemented generally effective controls to ensure vendor information matches between the SIGMA Financial (FIN) and VSS modules.

- Two reportable conditions* related to implementing sufficient data management controls over SIGMA vendor data (Finding 1) and ensuring all State of Michigan (SOM) registered vendors have a TIN matching an IRS record (Finding 2).

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

FINDING 1

Improvements needed over vendor file data management controls.

SBO did not implement sufficient data management controls over SIGMA vendor data. Failure to maintain accurate and current vendor data increases the risk of improper vendor payments and inefficiencies in the procurement and payment processes.

The U.S. Government Accountability Office's FISCAM recommends entities design and implement business processes and corresponding application controls to reasonably ensure master and transaction data records are complete, accurate, and valid. Business processes and application controls are configured to prevent or identify potential duplicate master data records as well as to detect data anomalies. The completeness, accuracy, and validity of data should be periodically assessed.

We analyzed 287,510 active SIGMA vendor records, as of August 25, 2025, and noted SBO did not:

a. Implement sufficient processes to identify and disable inactive vendor accounts. We analyzed vendor payment records and determined 131,596 (46%) active vendors had not received a payment since at least October 3, 2017. Of the 131,596 active vendors, 70,054 (53%) were converted from the prior accounting system and transitioned into SIGMA:

Last Payment	Converted Vendors	Vendors Registered by State Agencies	Vendors Self-Registered	Totals	Percentage of Total Vendors
Prior to October 3, 2017	70,054	3,763	57,779	131,596	46%
October 3, 2017 through September 30, 2019	14,599	1,082	6,322	22,003	8%
October 1, 2019 through September 30, 2021	11,548	2,030	8,074	21,652	8%
October 1, 2021 through September 30, 2023	11,983	5,743	14,760	32,486	11%
October 1, 2023 through August 25, 2025	39,446	6,504	33,823	79,773	28%
Totals	147,630	19,122	120,758	287,510	100%

The table below depicts the vendor creation dates for the 131,596 vendors who never received payments in SIGMA, of which 70,347 (53%) vendors were created prior to SIGMA implementation:

Years	Total	Percentage of Total Vendors
Prior to October 1, 2007	20,896	16%
October 1, 2007 through October 2, 2017	49,451	37%
October 3, 2017 through September 30, 2023	40,708	31%
October 1, 2023 through August 25, 2025	20,541	16%
Totals	131,596	100%

SBO is working with the third-party service provider to design and implement a process to archive inactive vendors after a designated period of inactivity. Because vendors must register to submit proposals on solicitations, there are valid active vendors without payments which should be considered in a data management strategy. SBO indicated compensating controls are in place to limit a vendor's ability to access and update account information which could be indicative of fraudulent activity. However, these controls do not prevent vendors from receiving payments. Also, SBO indicated payment transactions are subject to agency workflow which should include vendor validation.

b. Sufficiently monitor the vendor file to ensure selected vendor data is unique, complete, and accurate. Our review identified:

    (1) Potentially duplicative vendor records. We compared combinations of the legal name, address, and TIN of active vendors and noted multiple vendor records with the same address and TIN with similar legal names, for example, adding a middle initial to an individual's name or spelling out an abbreviation in the name. Also, we noted multiple vendors with the same legal names with similar TINs which appeared to be transposition errors.

The table below depicts examples of potentially duplicative vendor records:

Examples of Potential Duplicate Vendors	Vendor Code	Vendor Legal Name	TIN	TIN Type	Address
Same TIN and address, similar vendor legal name	Vendor Code 1	Company Name, Inc	123456789	EIN	ABC Street
	Vendor Code 2	Company Name, Incorporated	123456789	EIN	ABC Street
	Vendor Code 3	COMPANY NAME INC	123456789	EIN	ABC Street
Same vendor legal name and address, different TIN	Vendor Code 4	Business Name, Inc	987654321	EIN	123 Lane
	Vendor Code 5	Business Name, Inc	897654321	EIN	123 Lane
Same vendor legal name, TIN, and address, different TIN type	Vendor Code 6	Individual Name	123123123	EIN	XYZ Drive
	Vendor Code 7	Individual Name	123123123	SSN	XYZ Drive

(2) The vendor legal name was composed of only numeric characters for 15 vendors. Specifically:

(a) 12 vendors' legal names were the vendors' TIN.

(b) The remaining three vendors used numeric strings as legal names; however, the numbers do not appear to represent legitimate business names.

We first commented on potential risks within the vendor file master data elements during the fiscal year 2021 *State of Michigan Annual Comprehensive Financial Report* (*SOMACFR)* and discussed similar issues with SBO regarding the accuracy and completeness of vendor data. The fiscal year 2022 and 2024 *SOMACFRs* identified the need for improved vendor file controls. During this time, SBO implemented some enhanced vendor controls. However, as noted above, risks associated with vendor data still exist which necessitate the need for additional data management controls. SBO informed us formal procedures had not been developed to perform a comprehensive analysis to ensure the completeness and accuracy of vendor master data.

RECOMMENDATION

We recommend SBO implement sufficient data management controls over SIGMA vendor data.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees to continue to develop data management controls over SIGMA vendor data. SBO is working with the third-party service provider to design and implement a process to archive inactive vendors after a designated period of inactivity. SBO is developing additional reviews of the vendor file to ensure selected vendor data is unique, complete, and accurate.

FINDING 2

Improvements needed for vendor verification.

SBO did not ensure all vendors registered with the State had a TIN match performed with the IRS. TIN matches help safeguard the State from IRS penalties and may reduce the risk of improper payments and fraudulent vendors.

SIGMA Temporary Internal Policy and Procedure (TIPP) No. 0018 requires SBO to validate the vendor taxpayer and TIN information by using the automated IRS TIN match process. The TIN and taxpayer name must match the existing records on file with the IRS. Weekly, SBO sends all TIN and taxpayer information to the IRS for verification. The automated match determines if the name correctly matches the TIN and then returns a file with the status of the name and TIN number combination as a match or a reason code if the combination does not match its files.

We reviewed 10 of 60 weekly TIN matches from May 2, 2024 to June 25, 2025 and noted 6 (10%) of 61 newly registered vendors were not sent to the IRS for a TIN match; 3 of these 6 vendors received payments from the State during fiscal years 2024 and 2025 totaling $900 and $4,400, respectively.

SBO indicated taxpayer information for these vendors was already on file from prior payments made when they were classified as miscellaneous vendors. When registering as a vendor with the State, a document with the provided vendor taxpayer information is created. When a vendor with existing taxpayer information registers an additional document to flag the vendor for IRS TIN validation is required. Once both of these documents are approved, the vendor should be flagged to send for the IRS weekly TIN matching process. In these noted instances the modification document was not created. As a result, when these vendors registered with the State, SBO did not identify them as newly registered vendors and therefore did not include them in the weekly TIN matching process.

RECOMMENDATION

We recommend SBO ensure all vendors registered with the State have a TIN match performed with the IRS.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees to ensure all vendors registered with the State have a valid TIN match performed with the IRS. SBO performs TIN matching as a safe-harbor for tax reporting. While the TIN match process may provide additional assurances regarding accuracy of vendor data its purpose is not part of SBO's internal controls surrounding vendor data and associated payments. SBO is updating procedures to ensure that registered vendors who were previously miscellaneous vendors have a TIN match completed as part of a routine process.

OBSERVATION 1

Implementing processes over the use of miscellaneous vendor codes may improve the accuracy of payments and reduce the risk of fraud.

Vendors conducting business with the SOM receive payments through SIGMA. A vendor code is generated in SIGMA when a vendor either self-registers through the SIGMA VSS application or is added by a State agency through the SIGMA FIN application. As of August 25, 2025, SIGMA contained 287,510 active vendors.

Occasionally, payments in SIGMA are not linked to a vendor code and are processed as a miscellaneous vendor payment. These payments may contain only limited information such as name, address, and/or banking information. Vendors can register in SIGMA after receiving a miscellaneous vendor payment, but the payment(s) received prior to the vendor registration will not retroactively link to the vendor's newly assigned vendor code. During fiscal years 2024 and 2025, the State issued payments to approximately 408,000 miscellaneous vendors totaling $2.3 billion and $1.9 billion, respectively. Individual payments issued ranged from less than a dollar to $152.5 million during fiscal years 2024 and 2025.

SBO informed us certain payment types have established processes to authorize payments made to miscellaneous vendors and may be a suitable substitute to the TIN matching process. For example, lottery payments require presentation of a government issued photo ID and social security card prior to payment issuance. The table below depicts examples of payments made to miscellaneous vendors using established processes:

	Fiscal Year Payments		
Payment Type	2024	2025	Total Payments
Lottery prizes	$267.8 million	$284.1 million	$551.9 million
Taxes, refunds, garnishments, and levies	$ 1.1 billion	$ 1.2 billion	$ 2.3 billion
Adult services, child development and care, and other health and human services programs	$430.7 million	$476.2 million	$906.9 million
Retirement services	$ 48.5 million	$ 48.1 million	$ 96.6 million

In addition to the payments in the table, SBO identified 15,838 miscellaneous vendor payments totaling $44 million which may not relate to an established process.

During the vendor registration process, SIGMA uses a weekly automated exchange with the IRS to validate the legitimacy of the vendor's TIN. Miscellaneous vendors are not subject to the weekly TIN validation process.

At calendar year-end, SBO will identify miscellaneous vendors who received greater than $600 of 1099* reportable payments.

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

These miscellaneous vendors who received enough 1099 reportable payments are subject to a yearly TIN validation process. While the year-end TIN validation is a control to help reduce IRS penalties assessed against the State, it provides an additional benefit by identifying the correct vendor and potentially reducing the risk of fraudulent vendor payments. Because SBO performs the additional TIN validation only once per calendar year a significant amount of time may pass before a TIN validation occurs, increasing the risk of making payments to potentially illegitimate vendors.

SBO should consider the following for all payments made to miscellaneous vendors:

- Analyze the type, frequency, and dollar amount of payments to miscellaneous vendors to determine if dollar limits should be placed on these payments.

- Analyze miscellaneous vendor details (e.g., name, address, or bank account information) to identify patterns and recurring transactions with the same vendor details to help identify potential fraud or control circumvention.

- Periodically review payments issued to miscellaneous vendors to identify potential anomalies or irregularities.

- Consider additional TIN validation processes for miscellaneous vendors in addition to the current procedures.

SELECTED ACCESS CONTROLS

BACKGROUND

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.

According to the SOM Financial Management Guide (Part VII, Chapter 1, Section 900), SBO has primary responsibility for establishing, maintaining, and monitoring internal control* over its critical IT applications. Support for SIGMA consists of three primary areas: End User Support, Centers of Excellence, and Business Operations and New Development. The End User Support area deals with the central aspects of SIGMA security.

The SIGMA Security and Workflow team, within the End User Support area, provides administration, configuration, and monitoring of access to SIGMA to help ensure compliance with the State's internal control and data security policies. Also, it develops and configures security roles and workflow roles, and it works with the agency security administrators to develop and assign business roles. SIGMA users obtain core application and/or time and travel related business roles. Core application business roles allow the end user to complete financial, budget, procurement, human resources, and reporting functions. Time and travel related business roles allow State employees to submit biweekly time sheets and travel reimbursement requests.

SIGMA issues temporary operating policies and procedures (TOPPs) to provide SIGMA users with information to ensure the implementation of appropriate internal control and segregation of duties to prevent incompatible roles.

AUDIT OBJECTIVE

To assess the sufficiency of selected SBO SIGMA access controls.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- SBO established and implemented procedures related to SIGMA users' semiannual and annual recertifications in accordance with State policies and standards.

- SBO established and implemented procedures related to reviewing users with privileged access.

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

- Two reportable conditions related to improving bypass and override review guidance (Finding 3) and improving controls to ensure timely SIGMA access removal (Finding 4).

FINDING 3

Improved guidance needed to ensure errors and approvals have proper support and documentation.

SBO should improve its guidance to ensure overridden errors and bypassed approvals have the proper supporting documentation and help prevent potential misuse.

Error messages are defined within SIGMA to alert users to an error or warning condition prior to submitting transactions. Each error message requires specific security roles to allow a user to override error messages and submit the transaction.

Bypassing approvals moves a submitted transaction past one or more levels of the defined approval path before the transaction is final. Select security roles allow a user to bypass approvals on specific types of transactions.

SOM Technical Standard 1340.00.040.01 requires information systems to be monitored for inappropriate or unusual activity, use of privileged access*, use of administrative privileges, and user account management activities. Also, the Standard requires management to review the types of events being audited annually or when there is a change in the threat environment. TOPP No. 0006 requires agencies to develop specific expectations about the nature and timing of bypass and override usage by user, document type, and/or error message. SBO provides only a standard template which agencies may use to document their review of weekly bypasses and overrides. Typically, agencies would indicate if the bypass or override was routine, often, expected, or no additional review needed.

SBO performs weekly and monthly reviews of agencies' bypasses and overrides. Our review of the supporting documentation provided to SBO by 19 different agencies noted 12 of the 19 agencies bypassed approvals during the selected months, of which 9 (75%) of the 12 agencies did not document a sufficient explanation to support the bypasses.

SBO informed us TOPP No. 0006 defines bypass and override monitoring requirements, and each agency is responsible for the internal control regarding when and how bypasses should be applied. The level of maintained documentation should be defined by the agency, and not SBO, as the documentation available would vary across agencies.

While the TOPP instructs agencies to develop specific expectations for bypass and override usage, SBO performs the bypass and override review. Therefore, SBO would be the appropriate team to determine and provide guidance regarding the level of explanation and necessary documentation agencies should maintain.

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

RECOMMENDATION

We recommend SBO improve its guidance to ensure overridden errors and bypassed approvals have the proper support and documentation.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees to improve its guidance to departments to ensure overridden errors and bypassed approvals have the proper supporting documentation according to department internal controls. SIGMA TOPP NO. 0006 will be updated to reflect the additional guidance.

FINDING 4

Improved user access controls needed.

SBO should improve user access controls to ensure agencies remove SIGMA core access, in a timely manner, when it is no longer required. Ineffective access controls increase the risk of unauthorized access, use, and modification of SIGMA data.

SOM Technical Standard 1340.00.020.01 requires State agencies to remove user access when accounts are no longer required or when users depart State employment. In May 2025, the Standard was revised removing the three business day time-frame requirement; however, this requirement was in place for most of the audit period.

We sampled 60 SIGMA users whose access privileges were terminated between October 1, 2023 and July 19, 2025 and noted 6 (10%) users departed State employment between 5 and 139 days prior to the date core access was removed. SIGMA has a systematic process in place to remove all access upon final payroll processing, but the timing of this removal is several weeks after an individual departs. If an agency has not timely removed access prior to the systematic process taking place, departed employees retain access to perform their previous job duties, which may include processing accounting transactions.

SBO informed us because State agencies should submit access removal requests within SIGMA prior to systematic removal, there is potential for a lack of timely removal of user access.

While we acknowledge the agencies share responsibility for timely removing SIGMA access, our audit focused on SBO's access removal process.

RECOMMENDATION

We recommend SBO improve user access controls to ensure agencies remove SIGMA core access when it is no longer required in a timely manner.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees to update guidance to help ensure agencies timely remove SIGMA core access when it is no longer required. SIGMA Agency Security Administrator training will be updated to reflect the additional guidance.

SELECTED WORKFLOW CONTROLS

BACKGROUND

SBO, in conjunction with State agencies, is responsible for SIGMA workflow controls*. Workflow controls define the approval path, determine the users who can approve transactions before finalization, and ensure transactions are complete, accurate, and valid.

Workflow controls in SIGMA can be designed to trigger approvals based on specific fields within a transaction, such as unit code, department code, transaction amount, and last user ID. Also, these workflow controls can be designed not to require approvals unless specific criteria are met, referred to as conditional workflows. Some interface transactions do not have a workflow in SIGMA because approvals are performed in the originating systems. However, if a transaction is modified once it is interfaced into SIGMA, a conditional workflow could be used to require approval for the modification.

Some SIGMA transactions do not need workflow controls. For instance, a transaction related to a preceding or succeeding transaction which receives approval may not require a workflow.

AUDIT OBJECTIVE

To assess the sufficiency of selected SBO SIGMA workflow controls.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- Workflow controls operated as intended to ensure sampled transactions were subject to approval.

- Controls within SIGMA prevented the use of inactive transaction codes reviewed.

- SBO implemented some compensating controls over transaction codes without workflows.

- One reportable condition related to periodically reevaluating internal control over transactions not requiring approvals (Finding 5).

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

FINDING 5

Improvements needed to SIGMA workflow controls.

SBO should periodically reevaluate internal control over transactions which do not require approvals to ensure the completeness and accuracy of transactions processed in SIGMA.

Workflows are assigned to specific transaction codes to define document approval requirements before they are finalized in SIGMA.

FISCAM recommends organizations implement controls, such as approval workflows, to ensure transactions are complete, accurate, and valid. These controls provide assurance transactions and modifications are reviewed and approved by authorized individuals.

As of June 26, 2025, SIGMA had 213 active transaction codes, of which 74 did not have established workflow controls. We sampled 10 of these transaction codes and noted SBO did not:

a. Require workflows or compensating controls for 4 (40%) of 10 transaction codes which allow users to modify the transaction after submission by interface or batch user accounts. These transactions are used to record, reclassify, and accrue expenditures within SIGMA. In both fiscal years 2024 and 2025, approximately $3.3 billion net credits were processed using these transaction codes.

   SBO informed us these transactions are interfaced into SIGMA from other systems where the initial approval and reconciliations are documented, or system generated in SIGMA via a batch process, therefore no workflows were established. However, we noted users can modify the transactions after interfacing into SIGMA without subsequent approval.

b. Ensure implementation of compensating controls for 1 (10%) of 10 transaction codes which allows users the ability to transfer budget authorization between appropriations. In fiscal year 2024, approximately $282.8 million in transfers were processed on this transaction code.

   SBO informed us a report was developed for monitoring these transactions; however, prior to August 28, 2025, monitoring was not performed using this report since SIGMA's implementation in October 2017. After bringing this matter to management's attention, SBO indicated a review was completed to confirm all related transactions have been properly entered and it will implement a review process going forward.

RECOMMENDATION

We recommend SBO periodically reevaluate internal control over transactions which do not require approvals.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees to periodically reevaluate transactions that do not have workflow established. Development of the review methodology has begun with anticipated completion date of June 2026 aligned with SIGMA agile operations. This review will be conducted periodically thereafter with the frequency to be determined based on the results of the first review.

SYSTEM DESCRIPTION

SIGMA is an enterprise resource planning solution for the SOM. SIGMA consists of several modules which standardize Statewide accounting activities, procurement and vendor management, time and expense processes, budgeting processes, payment processing, cost accounting, bids and grant opportunities, and financial reporting. As of June 2025, SIGMA contained 283,300 active vendors, 52,200 State employees completing biweekly time and travel entries, and 11,400 core application users with access to complete financial, budget, procurement, human resource, and reporting functions. In fiscal years 2024 and 2025, SIGMA processed $86.4 billion and $91.1 billion in expenditures, respectively, and $88.6 billion and $91.8 billion in revenues, respectively.

VSS is a web-based component of SIGMA in which vendors can apply to register to do business with the SOM. VSS allows vendors to identify the commodities and services the company provides, scan for opportunities, respond to solicitations, submit invoices, and query financial information.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the system and other records related to selected security and application controls of SIGMA. 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.

Our audit did not include a direct review of the human resource management (HRM), budget, or business intelligence (BI) SIGMA modules.

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 August 31, 2025.

METHODOLOGY

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

- Obtained an understanding of SIGMA and its various application modules.
- Reviewed SBO and SOM policies and procedures related to SIGMA security.
- Interviewed SBO staff to obtain an understanding of SIGMA and processes related to user access, workflows, interface, change controls, and vendor file management.
- Analyzed expenditures and revenues for transaction codes without an established workflow.
- Obtained an understanding of SBO's key processes and internal control significant to the potential audit objectives.
- Assessed the SIGMA complementary user entity controls from the System and Organization Controls* (SOC) 1 and SOC 2 reports.

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

OBJECTIVE 1

To assess the effectiveness of SBO's efforts to ensure completeness and accuracy of selected vendor data within SIGMA.

To accomplish this objective, we:

- Analyzed 287,510 active SIGMA vendor file records as of August 25, 2025 to ensure the completeness and accuracy of selected vendor data. Specifically, we:

  - Judgmentally selected significant vendor file data fields to ensure data was complete and accurate.

  - Reviewed SBO's process to identify and deactivate vendors after a defined time period.

  - Identified possible duplicate vendor records.

- Reviewed SBO's process to ensure vendor data from SIGMA FIN and VSS were in sync and free of discrepancies as of July 7, 2025.

- Randomly and judgmentally sampled 43 of 14,169 resolved SIGMA Helpdesk tickets from September 27, 2024 through May 29, 2025, to determine whether Helpdesk staff properly validated the caller's identity.

- Randomly sampled 10 of 60 weeks from May 1, 2024 through July 1, 2025 to determine whether TIN validations were performed for newly created vendors. Subsequently, we identified the vendors subject to a TIN validation and judgmentally selected one vendor and randomly subsampled six vendors from each of the 10 sampled weeks.

We selected random samples to eliminate any bias and enable us to project our testing results to the respective populations. We selected other samples judgmentally to ensure representativeness or based on risk, and could not project those results to the respective populations.

OBJECTIVE 2

To assess the sufficiency of selected SBO SIGMA access controls.

To accomplish this objective, we:

- Judgmentally sampled 3 of 10 months, from October 1, 2024 through July 31, 2025, to ensure SBO maintained proper supporting documentation from its weekly and monthly bypass approval and override error monitoring reviews.

- Reviewed SBO's process to recertify privileged and nonprivileged user access to determine if semiannual and annual recertifications were performed as required by SOM Technical Standards.

- Reviewed SBO's process to ensure all changes to users with privileged access are regularly reviewed for appropriateness.

- Randomly sampled 60 of 9,721 terminated users from October 1, 2023 through July 19, 2025 to determine if core access was revoked within three business days for terminated or transferred users.

- Reviewed SIGMA data to determine if State employees terminated between October 1, 2023 and August 2, 2025 had active SIGMA access.

We selected random samples to eliminate any bias and enable us to project our testing results to the respective populations. We selected other samples judgmentally to ensure representativeness or based on risk, and could not project those results to the respective populations.

OBJECTIVE 3

To assess the sufficiency of selected SBO SIGMA workflow controls.

To accomplish this objective, we:

- Identified 139 active transaction codes in SIGMA with workflows as of June 26, 2025 and performed the following testing:

  - Randomly and judgmentally sampled 15 transaction codes and selected a sample of 45 of 70,923 processed transactions with those 15 transaction codes, from June 1, 2024 through May 31, 2025, to determine if workflows followed proper approval paths.

  - Randomly and judgmentally sampled 15 of the remaining 124 transaction codes and analyzed approval data for all processed transactions with those sampled transaction codes, from June 1, 2024 through May 31, 2025, to verify no missing or duplicate approvals.

- Randomly and judgmentally sampled 3 of 13 inactive transaction codes with workflows as of June 26, 2025 to verify transactions could not be created.

- Randomly and judgmentally sampled 10 of 74 active transaction codes without workflow controls as of June 26, 2025 to determine if not requiring workflow controls was reasonable.

- Randomly and judgementally sampled 15 transaction codes and created 34 transactions in a SIGMA test environment to review the workflow process and ensure workflow controls were appropriately designed and functioning as intended.

We selected random samples to eliminate any bias and enable us to project our testing results to the respective populations. We selected other samples judgmentally to ensure representativeness or based on risk and could not project those results to the respective populations.

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.

AGENCY RESPONSES

Our audit report contains 5 findings and 5 corresponding recommendations. SBO's preliminary response indicates it agrees with all of the recommendations.

The agency preliminary response following each 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* 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.

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

PRIOR AUDIT FOLLOW-UP

Following is the status of the reported findings from our March 2019 performance audit of the Statewide Integrated Governmental Management Applications (SIGMA) - Selected Application Controls and Service Level Requirements, State Budget Office (071-0595-18):

Prior Audit Finding Number	Topic Area	Current Status	Current Finding Number
1	Improved user account management controls needed.	Rewritten*	3 and 4
2	Workflow controls needed for EAMD transactions.	Rewritten	5
3	Fully established and implemented interface controls needed.	Not in scope of this audit.	
4	Improvements needed to vendor master data.	Rewritten	1
5	Service level requirements not sufficiently managed.	Not in scope of this audit.	
6	Need to assess coverage obtained from annual security review.	Not in scope of this audit.	

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

GLOSSARY OF ABBREVIATIONS AND TERMS

1099

A group of IRS tax forms which document payments made during the tax year by an individual or business which typically is not the individual's or business's employer.

access controls

Controls protecting data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

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.

effectiveness

Success in achieving mission and goals.

Federal Information System Controls Audit Manual (FISCAM)

A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.

FIN

SIGMA financial module.

internal control

The plan, policies, methods, and procedures adopted by management to meet its mission, strategic plan, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.

IRS

Internal Revenue Service.

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.

observation

A commentary highlighting certain details or events which may be of interest to users of the report. An observation may not include all of the attributes (condition, effect, criteria, cause, and recommendation) presented in an audit finding.

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.

privileged access

Extensive system access capabilities granted to persons responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.

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.

rewritten

The recurrence of similar conditions reported in a prior audit in combination with current conditions warranting the prior audit recommendation to be revised for the circumstances.

SBO

State Budget Office.

SIGMA Helpdesk

Provides general support services and assistance related to SIGMA Financial and Vendor Self-Service.

SOM

State of Michigan.

SOMACFR

State of Michigan Annual Comprehensive Financial Report.

Statewide Integrated Governmental Management Applications (SIGMA)

The State's enterprise resource planning business process and software implementation which support budgeting, accounting, purchasing, human resource management, and other financial management activities.

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.

TIN	taxpayer identification number.
TIPP	temporary internal policy and procedure.
TOPP	temporary operating policy and procedure.
VSS	Vendor Self-Service.
workflow controls	Controls within SIGMA used to define the approval path which transactions must follow before being finalized and the users who can approve such transactions.

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud
Hotline: (517) 334-8070