Office of the Auditor General
Performance Audit Report

Statewide Integrated Governmental Management Applications (SIGMA) - Selected Application Controls and Service Level Requirements

State Budget Office

March 2019

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

071-0595-18

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

SIGMA - Selected Application Controls and Service Level Requirements
State Budget Office (SBO)

Report Number:
071-0595-18

Released:
March 2019

Statewide Integrated Governmental Management Applications (SIGMA) is an enterprise resource planning (ERP) solution for the State of Michigan. SIGMA was implemented in modules during fiscal years 2017 and 2018. SIGMA administration and security are the responsibility of the SIGMA team in conjunction with the Office of Financial Management and the various State agencies. SIGMA fully or partially replaced over 60 State government IT systems, including accounting (MAIN), timekeeping (DCDS), procurement (Buy4Michigan), and other agency-specific applications. As of October 19, 2018, SBO expended more than $150 million on the development and implementation of SIGMA, with a total budget of $175.3 million, since project inception in fiscal year 2013.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of selected access controls over SIGMA.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Improvements to user account management controls are needed. We noted that 207 users had SIGMA access after departing State employment and that State agencies did not monitor when transaction approvals were bypassed (Finding #1).		X	Agrees
SBO did not implement workflow controls for all document codes that should require approval. Users created Expense Adjustment Manual Disbursement transactions totaling a net credit amount of $36.2 million that were not subject to approval within SIGMA (Finding #2).		X	Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of the State's efforts to ensure the completeness and accuracy of selected data within SIGMA.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Five (11%) of 46 interfaces reviewed did not have a reconciliation process, and 11 (24%) of 46 did not have sufficient documentation that the reconciliation was performed (Finding #3).		X	Agrees
SBO should improve the completeness and accuracy of its vendor master data because we could not determine the legitimacy of 5 (12%) of 43 randomly and judgmentally sampled vendors (Finding #4).		X	Agrees

Audit Objective	Conclusion
Objective #3: To assess the State and vendor's compliance with the service level requirements within the SIGMA contract.	Partially complied

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Improvements were needed in monitoring and documenting compliance for 14 (93%) of the 15 service level requirements that the SIGMA vendor agreed to provide to the State (Finding #5).		X	Partially agrees
SBO did not sufficiently assess the level of coverage obtained in the Annual Security Review service level requirement. We identified potential deficiencies in the agreed-upon nature and scope of the System and Organization Controls (SOC) engagements (Finding #6).		X	Partially 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 28, 2019

Mr. Chris Kolb, State Budget Director
State Budget Office
George W. Romney Building
Lansing, Michigan

Dear Mr. Kolb:

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

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Director upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

SIGMA - SELECTED APPLICATION CONTROLS AND SERVICE LEVEL REQUIREMENTS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

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.

Statewide Integrated Governmental Management Applications* (SIGMA) consists of various modules, implemented during fiscal years 2017 and 2018, that users are approved to access depending on their job responsibilities. SIGMA modules include:

- Administration, which allows users to centrally manage security, approvals, and batch administration for the Financial and Human Resource Management modules.

- Budget, a data repository for entering and analyzing data that supports the key components for developing the Executive Budget recommendation.

- Business Intelligence (BI), a reporting solution that provides a data warehouse for Financial, Budget, and Human Resources Management data. BI provides single-point access to SIGMA information, allowing users to choose from over 300 SIGMA supported reports or to create custom queries.

- Employee Self Service (ESS), which is used by State employees to enter time and submit leave, overtime, expense reimbursement, and travel requests.

- Financial (FIN), which allows users to control financial resources using the chart of accounts; general ledger; accounts payable; accounts receivable; cost allocation; agency procurement; asset, cash, inventory, and grant management; and project accounting. This module is used by State employees to create the State's accounting entries.

- Human Resource Management (HRM), which is used by the State for time entry, leave and overtime requests, expense reimbursements, and labor distribution.

- Manager Self Service (MSS), which is used by supervisors and managers to approve employee time sheets, leave and overtime requests, travel, and expense reimbursement.

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

- Vendor Self Service (VSS), which is used by vendors to respond to solicitations for goods and services; to view grant opportunities, payments, and pending payments; and to submit progress reports, status reports, and invoices. State employees use VSS for some of the State's management and administration of vendor information.

As of May 30, 2018, the number of active users with access to at least one module consisted of:

Modules	State Employees	Non-State Employees	Total
ESS only	34,933	0	34,933
ESS and other SIGMA modules	13,874	516	14,390
Total	48,807	516	49,323

Note: Non-State employees include contractors, Michigan Economic Development Corporation (MEDC) staff, college and university staff, and local and federal government employees.

Access controls are the responsibility of the State Budget Office (SBO), in conjunction with State agencies. 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 and workflow. State agencies are responsible for approving user access within their areas; reviewing agency transactions via established workflow controls*; and monitoring certain user activity, such as the bypass of approvals.

AUDIT OBJECTIVE

To assess the effectiveness* of selected access controls over SIGMA.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Automated workflow controls within SIGMA were operating as intended to ensure that transactions are subject to approval.

- SBO had implemented some procedures related to user account management.

- Two reportable conditions* related to improving user account management controls and implementing workflow controls for all document codes that should require approval (Findings #1 and #2).

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

FINDING #1

Improved user account management controls needed.

SBO, in conjunction with State agencies, should improve its user account management controls to help ensure that SIGMA access is secure and that controls are properly designed and implemented in accordance with State of Michigan (SOM) technical standards.

SOM Technical Standard 1340.00.040.01 defines the audit and accountability security controls required for SOM executive branch information systems. The standard requires that information systems be monitored for inappropriate or unusual activity, use of privileged access*, use of administrative privileges, and user account management activities. The standard also requires management to review the types of events being audited annually or when there is a change in the threat environment. In addition, SOM Technical Standard 1340.00.020.01 requires State agencies to notify SBO within 24 hours of when users are terminated or transferred so that access can be removed in a timely manner.

Our review disclosed:

a. SBO and the State agencies did not always remove SIGMA user access in a timely manner. Specifically:

(1) After departing State employment, 207 users had access to at least one SIGMA module. Fourteen (7%) of the 207 users had a last log-in date that was an average of 13 days after the date they left State employment. These users had access to SIGMA modules as follows:

Modules	Number of Users	Number of Users With Log-In After Leaving State Employment
ESS only	145	10
ESS and other SIGMA modules	62	4
Total	207	14

Note: See Objective #1 background section for total number of SIGMA users and explanations of user capabilities within the various SIGMA modules.

Of the 207 users, 145 (70%) had access to only the ESS module, which is used by employees to enter time and to submit travel or leave requests. We could not develop an efficient testing methodology to determine if any of these users utilized their access after departure.

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

(2) One contracted help desk employee had SIGMA access for approximately one month after his/her State employment departure. Removing this access would help ensure that inappropriate transactions are not input into SIGMA.

b. All 35 (100%) State agencies reviewed did not formally monitor the bypass of transaction approvals (both financial and nonfinancial) for appropriateness because the SIGMA team had not provided guidance to State agencies to do so. Subsequent to our review, SBO issued the needed guidance.

c. Users with privileged access were not adequately monitored. SBO implemented some procedures; however, additional monitoring would increase system security and ensure the appropriateness of application configuration changes, modifications to approved document workflows, and data fixes that do not require approval within SIGMA.

SBO informed us that it was creating new security procedures, as necessary, to meet the State's standards and needs, and that current procedures had been evolving since SIGMA implementation.

RECOMMENDATION

We recommend that SBO, in conjunction with State agencies, improve its user account management controls to help ensure that SIGMA access is secure and that controls are properly designed and implemented in accordance with SOM technical standards.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees that continual improvement of user account management controls help ensure that SIGMA access is secure and controls are properly designed and implemented in accordance with SOM technical standards. Regarding the specific parts of the finding:

- *The users noted in part a. were in a pending status for final timesheet and payroll processing. Access was timely and systematically removed once the final termination status was complete. SIGMA will review the systematic removal of access to determine if changes are needed.*

- *The guidance noted in part b. was issued in August 2018. SIGMA completes monitoring centrally and in coordination with State agencies to ensure bypassed approvals are monitored weekly.*

- *The monitoring noted in part c. will continue to evolve as needed to meet State standards and needs.*

FINDING #2

SBO did not implement workflow controls for all document codes that should require approval to help ensure the reasonableness and propriety of SIGMA transactions.

Workflow controls needed for EAMD transactions.

SIGMA is a document-driven system with all transactions having a document code that acts as the basic control for what the transaction can do. This includes controlling workflows to establish the necessary approvals, required fields, and dollar amount limitations.

The U.S. Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual* (FISCAM) recommends that organizations implement controls to ensure that transactions are complete, accurate, and valid and that an automated workflow exists to initiate the approval process. These controls would provide assurance that transactions are reviewed and approved by authorized individuals.

We reviewed 19 (11%) of the 175 SIGMA document codes without an established workflow control to assess whether it was appropriate for the transactions to not require approvals. One (5%) of the 19 document codes, the Expense Adjustment Manual Disbursement (EAMD) code, should require supervisor approval because of the financial statement impact of the transactions.

EAMD transactions are used to cancel and adjust expense transactions. SIGMA users created 4,281 EAMD transactions, with a net credit amount of $36.2 million. Without proper approvals to ensure that EAMD documents are appropriate, the risk of financial statement misstatement increases.

SBO informed us that, because EAMD was misclassified as a non-general accounting document during SIGMA implementation, it did not believe that a workflow was warranted at the time.

RECOMMENDATION

We recommend that SBO implement workflow controls for all document codes that should require approval.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees with this recommendation. Workflow was tested and then added to the EAMD document in production in February 2019. The remaining document codes are not believed to require workflow for one of the following reasons:

- *The document code is not being used in SIGMA and has been inactivated to prevent its use.*

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

- *The document code is systematically generated after a different document code received all required approvals and became final.*

- *The document code is created from an interface where the approvals are documented in the initiating system.*

SBO is reanalyzing all 175 document codes without workflow based on 1-year plus of operations to confirm that EAMD was the only document code requiring the addition of workflow.

COMPLETENESS AND ACCURACY OF SELECTED DATA

BACKGROUND

According to FISCAM, controls should be implemented to provide reasonable assurance of the completeness and accuracy of data within a system.

Interface controls* ensure the accurate, complete, and timely processing of data between systems and the complete and accurate migration of data during system conversion. SIGMA has more than 300 outbound and inbound interfaces with more than 100 other systems.

SIGMA fully or partially replaced more than 60 State government legacy computer systems. Data was converted from the legacy systems and reconciled as part of the conversion process. The systems converted to SIGMA include:

- Michigan Administrative Information Network (MAIN) - Statewide accounting, purchasing, and financial management system.
- Data Collection and Distribution System (DCDS) - State employee time and expense capture.
- Buy4Michigan - State procurement functions.
- Other agency-specific applications.

Master data is core data that is used entity-wide and is essential for business operations. To conduct business with a specific vendor, a record must be active and approved in the SIGMA vendor master data table. Upon implementation of SIGMA, existing vendor data was converted from MAIN. A vendor may initiate the process to be added to SIGMA using the VSS module, or authorized State agency users may register the vendor with the necessary documentation attached to the request.

Ensuring that SIGMA contains complete and accurate data is the responsibility of SBO, in conjunction with State agencies.

AUDIT OBJECTIVE

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

CONCLUSION

Moderately effective.

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

FACTORS IMPACTING CONCLUSION

- State agencies and SBO implemented procedures related to interface reconciliation controls for most of the interfaces reviewed.

- We were able to validate that 40 (87%) of 46 interfaces reviewed reconciled between SIGMA and the source system.

- Most vendor master data reviewed was complete and accurate.

- SBO's and State agencies' efforts to ensure the completeness and accuracy of data converted to SIGMA from legacy systems were generally sufficient.

- Two reportable conditions related to fully establishing and implementing interface controls and improving the completeness and accuracy of vendor master data (Findings #3 and #4).

FINDING #3

Fully established and implemented interface controls needed.

SBO, in conjunction with State agencies, did not fully establish and implement interface controls over the SIGMA application to ensure that all data exchanged between SIGMA and other State information systems was processed completely, accurately, and timely.

SIGMA exchanges data with more than 100 information systems via interface files, including vendor payments, cash receipts from customers, State employee payroll, tax refunds, and payment cancellations.

SBO, as the owner and central control agency of SIGMA, is responsible for establishing guidance for State agencies to follow in regard to the reconciliation of interfaces to and from the application. State agencies, as the data owners, are responsible for the implementation of interface reconciliation controls.

According to FISCAM, interface controls should be established and implemented to reasonably ensure that data transferred from a source system to a receiving system is processed accurately, completely, and timely. Also, effective interface reconciliation procedures should include the use of control totals, record counts, or other logging techniques.

We reviewed interface controls for 46 (14%) of 318 judgmentally sampled interfaces and determined:

a. Five (11%) of the 46 interfaces did not have a reconciliation process in place and were not being reconciled. Because a process did not exist, sufficient evidence was not readily available for us to verify that these interfaces reconciled.

b. An additional 5 (11%) of the 46 interfaces did not have formally documented interface reconciliation procedures.

   SBO developed interface design documentation describing the implementation requirements for high-level groups of SIGMA interfaces. This documentation was not designed to contain information specific to the reconciliation of individual interfaces, which State agencies should develop in the form of documented procedures. This will help ensure consistency in the reconciliation process, promote best practices, and facilitate knowledge transfer.

c. Eleven (24%) of the 46 interfaces did not have sufficient documentation that the reconciliation was performed. For example, State agencies did not always maintain reports or logs of record counts and control totals from the source and receiving systems. Because reconciliation processes existed for these interfaces, we were able to validate that 10 (91%) of the 11 interfaces reconciled. However, for the remaining one, a potential system defect affecting the reporting of payroll data precluded us from performing the reconciliation.

State agencies and SBO informed us that, because SIGMA is a new system and miscommunication occurred regarding the responsibility for interface reconciliations, processes and procedures had not been fully implemented or were still being developed at the time of our review.

RECOMMENDATION

We recommend that SBO, in conjunction with State agencies, fully establish and implement interface controls over the SIGMA application.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees with the recommendation that State agencies, in conjunction with SIGMA, fully establish and implement interface controls over the SIGMA application.

SIGMA developed the Interface Feedback Report to provide detailed record status, record counts, and control totals to assist agencies with interface reconciliation. In addition, SIGMA Vendor / Customer Update data, EFT and Warrant Payment Status, EFT Payment Return and Notice of Change (NOCs), and Converted Warrant Status Update data is available to agencies on a daily basis through the Extract Management Layer (EML) for reconciliation purposes. Agencies are responsible for leveraging this data and similar data from interfacing systems in order to complete reconciliation activities and are responsible for documenting their reconciliation procedures as these procedures may differ by agency and by interfacing system.

SIGMA issued Temporary Operating Policy & Procedure 0007 on November 9, 2018, providing guidance to the agencies regarding interface reconciliation.

As noted in part c., there is a potential software defect related to the display of payroll reconciliation data online. This has been logged with the software vendor and is being researched. SIGMA is printing the balanced screens and attaching the information to the reconciliation documentation to ensure that the reconciliations can be recreated and relied upon after subsequent cycles are processed.

FINDING #4

Improvements needed to vendor master data.

SBO should improve the completeness and accuracy of its vendor master data to help ensure that all SOM payments are made to legitimate entities.

According to FISCAM, master data serves as the basis for transaction processing; therefore, it is critical that controls exist over the integrity and quality of data. To reasonably ensure an appropriate level of control, an organization should have effective auditing and monitoring capabilities to allow changes to master data records to be recorded and reviewed where necessary. Ideally, monitoring should be built in to normal, recurring responsibilities to identify data integrity problems more quickly.

Our review of SIGMA vendor master data disclosed that SBO did not:

a. Sufficiently monitor vendor taxpayer identification numbers (TINs) for completeness.

   SBO requires that vendors, unless considered a tax-exempt entity, have a TIN to be considered active. However, under specific circumstances, a TIN is not always required to be entered if the vendor self-registers in SIGMA. We identified 71 active vendors who did not have a TIN and were not tax-exempt entities.

b. Implement sufficient processes to determine the legitimacy of all vendors.

   We compared the legal name and TIN of 43 randomly and judgmentally sampled active vendors to SOM tax records and LexisNexis*. We could not match this combination for 5 (12%) vendors and, therefore, could not determine whether the vendors were legitimate. Also, SIGMA has an online IRS TIN matching process. For the 5 vendors that we could not match, we noted:

   (1) Two (40%) vendors did not have a TIN issued by the IRS.

   (2) One (20%) vendor's name and TIN combination did not match IRS records.

   (3) Two (40%) vendor records were not sent to the IRS for a match by SBO.

SBO informed us that formal procedures had not been developed to address these items and that processes are continually evolving to ensure the completeness and accuracy of vendor master data since system implementation.

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

RECOMMENDATION

We recommend that SBO improve the completeness and accuracy of its vendor master data to help ensure that all SOM payments are made to legitimate entities.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO agrees with the recommendation to improve the completeness and accuracy of vendor master data and the related processes, and has taken corrective action regarding the issue that caused missing TINs. SIGMA is in the process of updating and creating procedures to improve the use of the TIN matching process to help ensure accurate and complete vendor data.

SBO (SIGMA and OFM) complies with IRS requirements for obtaining TIN information, issuing B-notices as directed by the IRS, and applying backup withholding when appropriate. In addition, SBO requires W8 or W9 information from registered vendors and this serves as a safe harbor with the IRS regarding the accuracy of vendor information. With the implementation of SIGMA, SBO elected to use a nightly IRS TIN match process to further ensure the accuracy of TIN information as reported by vendors. Although these processes were used to help ensure accurate and complete vendor data, a formal process for steps to take regarding mismatches identified in the process had not been established.

COMPLIANCE WITH SERVICE LEVEL REQUIREMENTS

BACKGROUND

In 2014, SBO contracted with a software technology vendor for the acquisition and implementation of SIGMA, including hosting, application maintenance and support, and disaster recovery. The contract contains a service level agreement (SLA) consisting of 15 requirements (see summary of the status of service level requirements, presented as supplemental information). The vendor is required to maintain and provide monthly reports to SBO showing its performance against all aspects of the SLA. The contract allows SBO to assess service level credits (reductions in payments against quarterly invoices) if the vendor fails to provide the promised services and/or deliverables in the manner specified in the SLA. The aggregate amount of service level credits cannot exceed 10% of managed services fees (application maintenance and support) paid annually to the vendor. The vendor's compliance with the service level requirements is monitored by SBO.

AUDIT OBJECTIVE

To assess the State and vendor's compliance with the service level requirements within the SIGMA contract.

CONCLUSION

Partially complied.

FACTORS IMPACTING CONCLUSION

- SBO implemented some processes to monitor the vendor's compliance with the service level requirements within the SIGMA contract, including assessing all service level credits allowable under the contract for instances of noncompliance in fiscal year 2018 (see supplemental information).

- The vendor had not complied with various service level requirements within the SIGMA contract.

- Two reportable conditions related to sufficiently managing the service level requirements within the SIGMA contract and sufficiently assessing the level of coverage obtained in the annual security review (Findings #5 and #6).

FINDING #5

Service level requirements not sufficiently managed.

SBO should improve management of the service level requirements within the SIGMA contract to help ensure that services provided by the vendor meet the level of performance agreed to with the State.

The SIGMA contract includes 15 service level requirements that define the acceptable terms and deliverables for items such as system availability, online response time, completion times for critical batch jobs, and monitoring of system security (see summary of the status of service level requirements, presented as supplemental information). The contract allows for service level credits to be assessed against the vendor for not meeting certain requirements.

According to Control Objectives for Information and Related Technology* (COBIT), organizations should manage service level requirements by regularly monitoring performance, including deviations from agreed-upon values, such as system availability and response time. COBIT also states that service level requirements should be reviewed and revised when needed.

Our review disclosed:

a. SBO should improve its SLA monitoring and documentation of compliance for 14 (93%) of the 15 service level requirements. Specifically, for these 14 requirements, SBO did not:

(1) Completely and accurately track the vendor's compliance with 3 (21%) of the requirements. We noted:

(a) For 6 (86%) of 7 randomly sampled critical issues, the vendor did not provide the required root cause remedy. Also, 2 (3%) of 64 critical issues reoccurred 3 times, resulting in noncompliance with the issue recidivist rate requirement. However, SBO's compliance tracking spreadsheet incorrectly indicated that the vendor complied with these requirements for 6 (100%) of 6 months reviewed.

(b) For 3 (17%) of 18 randomly sampled days, a critical or serious issue occurred; however, the associated job ticket was not monitored for resolution time in SBO's compliance tracking spreadsheet. On these 18 days, 47 job tickets were created because critical or serious issues occurred.

(c) The vendor provided service level requirement reporting; however, it did not include the details deemed necessary by the State. SBO incorrectly tracked this requirement as complied for 6 (100%) of 6 months reviewed.

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

(2) Create and maintain sufficient documentation to support the vendor's compliance with 4 (29%) of the 14 requirements. We noted:

(a) For 2 (9%) of 23 randomly and judgmentally sampled days, SBO did not have a formal job ticket or correct information in the compliance tracking sheet to document system downtime.

(b) For 2 (9%) of 23 randomly and judgmentally sampled days, the job ticket did not accurately track system downtime.

(c) For 2 (13%) of 15 randomly and judgmentally sampled days, SBO did not record details of offline batch processing in the compliance tracking spreadsheet.

(d) For 2 (5%) of 43 randomly sampled days, details of critical batch job completion were not recorded in the compliance tracking spreadsheet.

(3) Fully establish and implement an effective process for monitoring compliance with 9 (64%) of the 14 requirements. For example, there was no process to track the creation of disaster recovery backup files.

b. SBO should amend the contract or formally establish additional agreed-upon procedures for 7 (47%) of the 15 service level requirements. Specifically, for these 7 service level requirements:

(1) The vendor did not provide sufficient or agreed-upon documentation to support compliance with 5 (71%) of the 7 requirements. For example, the vendor did not provide supporting documentation to support that the antivirus scanning requirement had been met.

(2) SBO did not sufficiently define and obtain vendor agreement on how it will measure compliance with 4 (57%) of the 7 requirements. For example, the specific transactions to be used for measuring online response time had not been defined.

(3) Descriptions in the contract were inaccurate or unclear for 4 (57%) of the 7 requirements. For example, the description of the security compliance requirement stated that compliance will be measured against 5 performance indicators; however, only 4 indicators were listed in the contract.

c. SBO should consider the cost benefit of implementing internal processes or contracting with a third party to independently verify the service level requirements within the contract. We determined that SBO only partially completed an independent verification for 8 (53%) of the 15 service level requirements.

SBO informed us that some deficiencies in managing the service level requirements were due to unclear expectations between the vendor and State, along with a lack of formal processes.

RECOMMENDATION

We recommend that SBO improve management of the service level requirements within the SIGMA contract to help ensure that services provided by the vendor meet the level of performance agreed to with the State.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO partially agrees with the recommendation.

SBO agrees that additional details in the reporting against the standards and associated formal processes for monitoring were necessary. A change notice to the contract was executed in December 2018 to address this. This change notice resulted in further detailing of the service level requirements from 15 to 26 and included clarifications to calculations and reporting requirements.

SBO disagrees that improved management of the service level requirements is necessary to ensure the vendor meets the level of performance agreed to with the State. In addition, SBO disagrees with some of the details contained in the finding. SIGMA extensively and thoroughly monitors and enforces service level requirements. The failure to meet the requirements was not the result of the level of management and monitoring performed by SBO. Except for Standard 14, the OAG-Determined Status of the Service Level Standards (as presented in the supplemental information) matches the status that was determined by SBO. All contractual provisions were properly enforced. It is SBO's position that Standard 14 was met based on the contractual requirements, however, increased detail in the report was needed. As noted above, a change notice to the contract was executed in December 2018 and additional details are now included in the monthly reports.

As with any new system, particularly one of this size and complexity, numerous adjustments and tuning efforts have been done and continue to be done to improve the level of service received by the vendor. SBO is conducting a cost benefit analysis regarding additional monitoring processes and third-party monitoring options.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE*

As stated in the finding, it is an industry best practice to manage service level requirements through performance monitoring, and SBO has implemented such a process. The finding does not indicate that SBO is responsible for the contractor's failure to meet the requirements; it merely identifies areas in the process that could benefit from increased monitoring and documentation to help ensure that SBO has every advantage when holding the contractor accountable.

The OAG obtained a thorough understanding and conducted other audit procedures related to the management of service level agreement compliance to ensure that the details of the finding are accurate. SBO acknowledged that its established policies, procedures, and processes require updates or additional details.

Therefore, the finding stands as written.

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

FINDING #6

Need to assess coverage obtained from annual security review.

SBO did not sufficiently assess the level of coverage obtained in the Annual Security Review service level requirement. This assessment would help ensure that adequate consideration had been given to controls over SIGMA financial reporting and security that are managed by the vendor.

The Annual Security Review service level requirement within the SIGMA contract calls for an appropriately scoped assurance engagement under the American Institute of Certified Public Accountants' (AICPA's) System and Organization Controls* (SOC) reporting framework.

SOC reports are internal control reports on the services provided by a service organization. The reports provide valuable information that users need to assess and address the risks associated with an outsourced service. A SOC 1, type 2 engagement is conducted by an independent auditor to report on management's description of a service organization's system and the suitability of the design and operating effectiveness of the controls over financial reporting. A SOC 2, type 2 engagement provides an assessment of the operational controls over areas such as system security, availability, processing integrity, confidentiality, and privacy.

SBO and the vendor formally agreed that the vendor would undergo annual SOC 1, type 2 and SOC 2, type 2 engagements. The agreed-upon nature and scope of both engagements included enterprise and end-user computing and the network environments. The SOC 2 engagement would include controls over security and availability. In 2017, the vendor underwent and provided the results of these agreed-upon engagements to the State.

We reviewed the SOC reports and other SIGMA security assessments and identified potential deficiencies in the agreed-upon nature and scope of the SOC engagements and other security assessments. For example:

a. The control areas of confidentiality and privacy were not included in the SOC 2 scope, primarily because the State conducted an information security risk assessment (the DTMB-170) and underwent annual penetration testing and security control assessments. Also, the vendor's infrastructure was Federal Risk and Authorization Management Program* (FEDRAMP) certified.

   Although the State completed the DTMB-170, it did not test the operating effectiveness of controls as would be done in a SOC 2 engagement. Also, the annual security controls assessment did not include the controls over the vendor's infrastructure or the controls provided by SBO. In addition, although the vendor annually undergoes an

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

independent assessment of its FEDRAMP compliance, SBO did not formally review the results of this assessment and was not fully aware of how the results, including identified vulnerabilities and control deficiencies, could impact the security posture of SIGMA.

b. The control area of processing integrity was not included in the SOC 2 scope primarily based on the State and vendor having the shared responsibility for managing SIGMA, including the service level requirements within the contract. Processing integrity helps ensure system processing is complete, valid, accurate, timely, and authorized. Our review identified deficiencies in monitoring and compliance with the service level requirements that relate to processing integrity (see Finding #3).

c. The SOC 1 and SOC 2 engagements did not include an assessment of database administration controls. These controls were the primary responsibility of the vendor and should be independently reviewed and reported to the State.

d. SBO had not formally assessed whether processes were established for complementary user-entity controls and whether the controls were operating effectively. The SOC 1 and SOC 2 engagements relied on the operating effectiveness of complementary user-entity controls. These controls exist within SBO, in conjunction with State agencies, and should be implemented in order to achieve the control objectives covered by the SOC engagement. SBO informed us that processes existed to cover some areas of the complementary user-entity controls.

We requested from SBO any detailed assessments that it had performed, such as an analysis of the points of focus of each SOC trust service criteria to the other agreed-upon security assessments. However, SBO could not provide evidence to support that this type of an assessment was completed. Conducting a formal assessment of the coverage obtained in the Annual Security Review service level requirement will help ensure that SBO identifies control deficiencies and that future engagements provide the necessary level of assurance to the State.

RECOMMENDATION

We recommend that SBO sufficiently assess the level of coverage obtained in the Annual Security Review service level requirement.

AGENCY PRELIMINARY RESPONSE

SBO provided us with the following response:

SBO partially agrees with the recommendation.

SIGMA agrees with the need to continually assess the level of coverage obtained in the annual security review service level requirement. In addition, the formal assessment of complementary user-entity controls began with the preliminary Top Down Risk Assessment effort that is a precursor to the biennial internal control evaluation which will be completed by May 2019.

SBO disagrees with the assertion that the level of coverage obtained was not sufficiently assessed. Extensive analysis was conducted jointly by SIGMA, the Office of Internal Audit Services, and DTMB Agency Services with advisement from the Office of the Auditor General to identify and define the scope (level of coverage) of the annual security review (SOC report). We agree that a more formal assessment of complementary user-entity controls needs to be completed and that additional formalized processes to review the results of the examinations are needed. The scope of coverage from the SOC engagements and additional required penetration and vulnerability testing will be continually evaluated.

SIGMA has multiple informal processes in place including processes published in Temporary Internal Policies and Procedures (TIPPs), Temporary Operational Policies and Procedures (TOPPs), and the Operational Framework. In addition, SIGMA leverages multiple weekly and twice daily meetings to review issues, discuss upcoming activities, coordinate support needs, and review Plan of Action & Milestone (POAM) security vulnerabilities.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE

Prior to the commencement of the audit, SBO sought advisement from the OAG on the scope of the security review, and the OAG provided concerns with that scope. After conducting more extensive audit procedures, the OAG determined that, in addition to some new concerns, some of the original concerns still existed.

Although SBO expressed disagreement in its response, it plans to continually assess the level of coverage obtained in the annual security review service level requirement and implement formal assessment procedures through the biennial internal control evaluation process.

Therefore, the finding stands as written.

SIGMA - SELECTED APPLICATION CONTROLS AND SERVICE LEVEL REQUIREMENTS
State Budget Office

Summary of the Status of Service Level Requirements
January 1, 2018 Through June 30, 2018

<table>
<tr><th>Standard 1</th><th colspan="2">Scheduled Hours of On-Line Availability for Non-Public Facing Components</th></tr>
<tr><th></th><th>Service Level Requirement</th><th>OAG-Determined Status</th></tr>
<tr><td><b>Description</b></td><td>For software that has been implemented for non-public facing components, the system must be accessible by users for the scheduled hours listed below for the purpose of measuring the performance standards:
<table>
<tr><th>Environment</th><th>Scheduled Hours of On-Line Availability</th></tr>
<tr><td>Development and test environments</td><td>6 a.m. - 6 p.m., Monday - Friday*
6 a.m. - 6 p.m., Saturday*</td></tr>
<tr><td>Development report distribution</td><td>6 a.m. - 12 midnight, 7 days per week*</td></tr>
<tr><td>Production and production quality assurance (QA)</td><td>7 a.m. - 6 p.m., business days
7 a.m. - 4 p.m., Saturday**</td></tr>
<tr><td>Production and production QA report distribution</td><td>7 a.m. - 6 p.m., business days
7 a.m. - 4 p.m., Saturday**</td></tr>
</table>
* Times listed are exclusive of notified maintenance windows. Standard maintenance window is as defined in Section 3.0 of Attachment 2.
** During the year-end close or other testing processes, these scheduled hours of online availability may be extended (as requested by the State).
Availability of environment includes redundant IP based router and network from Lansing to the Contractor's hosting center.</td><td></td></tr>
<tr><td><b>Measurement</b></td><td>Downtime is measured from the time a problem record is opened and the outage has been coded until the problem has been resolved and service has been restored. Tracking tools approved by the State must be used to track and measure the availability objective.</td><td>SBO uses a compliance tracking spreadsheet to measure availability of each non-public facing component of SIGMA. Measurement data within the spreadsheet is based on batch cycle completion reports and job tickets that track issues causing system downtime. We identified deficiencies related to monitoring for compliance and documentation of compliance with this requirement (see Finding #5).</td></tr>
<tr><td><b>Target Performance</b></td><td>99.5% compliance with target service level</td><td>Not met for 6 (100%) of 6 months reviewed.</td></tr>
<tr><td><b>Period of Review</b></td><td>Monthly</td><td>Completed.</td></tr>
</table>

This summary continued on next page.

<table>
<tr><td><b>Service Level Credit</b></td><td>$25,000 per month in which Target Performance level is not met.
$50,000 if the Target Performance level is not met in a subsequent consecutive month.
If Target Performance is met 3 successive months, the Service Level Credit is $15,000 per month in which Target Performance level was not achieved.</td><td>SBO assessed $145,680 in service level credits against this requirement. The maximum allowable service level credit was reached in April 2018, which prevented additional credits from being assessed.</td></tr>
<tr><td><b>Standard 2</b></td><td colspan="2"><b>Scheduled Hours of On-Line Availability for Self-Service Components</b></td></tr>
<tr><td></td><td><b>Service Level Requirement</b></td><td><b>OAG-Determined Status</b></td></tr>
<tr><td><b>Description</b></td><td>For software that has been implemented for Self-Service components (employee and vendor), the system must be accessible by users for the scheduled hours listed below for the purpose of measuring the performance standards:
<table>
<tr><th>Environment</th><th>Scheduled Hours of On-Line Availability</th></tr>
<tr><td>Development and test environments</td><td>6 a.m. - 6 p.m., Monday - Friday*
6 a.m. - 6 p.m., Saturday*</td></tr>
<tr><td>Production and production QA</td><td>7 x 24*</td></tr>
</table>
* Times listed are exclusive of notified maintenance windows. Standard maintenance window is as defined in Section 3.0 of Attachment 2.
Availability of environment includes redundant IP based router and network from Lansing to the Contractor's hosting center.</td><td></td></tr>
<tr><td><b>Measurement</b></td><td>Downtime is measured from the time a problem record is opened and the outage has been coded until the problem has been resolved and service has been restored. Tracking tools approved by the State must be used to track and measure the availability objective.</td><td>SBO uses a compliance tracking spreadsheet to measure availability of each self-service component of SIGMA. Measurement data within the spreadsheet is based on job tickets that track issues causing system downtime. We identified deficiencies related to documentation of compliance with this requirement (see Finding #5).</td></tr>
<tr><td><b>Target Performance</b></td><td>99.5% compliance with target service level</td><td>Not met for 3 (50%) of 6 months reviewed.</td></tr>
<tr><td><b>Period of Review</b></td><td>Monthly</td><td>Completed.</td></tr>
<tr><td><b>Service Level Credit</b></td><td>$25,000 per month in which Target Performance level is not achieved. Amount rises to $50,000 if the Target Performance level is not met in a subsequent consecutive month.
If Target Performance is met for 3 successive months, the Service Level Credit is $15,000 per month in which Target Performance level was not achieved.</td><td>SBO assessed $125,000 in service level credits against this requirement.</td></tr>
</table>

This summary continued on next page.

Standard 3	On-Line Response Time	
	Service Level Requirement	**OAG-Determined Status**
Description	Both online inquiry and online update of mutually agreed upon and selected single transactions must be achieved within the cumulative transaction response times specified below: **Environment** — **Scheduled Hours of On-Line Availability** Production — <2.0 seconds - 91% <3.0 seconds - 93% <4.0 seconds - 95% <5.0 seconds - 97%	
Measurement	Response times must be measured at the server.	SBO did not fully establish and implement an effective process for measuring compliance with this requirement and had not selected any transactions for measurement (see Finding #5).
Target Performance	100% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor self-reported compliance with this requirement; however, SBO had not independently verified the status (see Finding #5).
Period of Review	Monthly	Completed.
Service Level Credit	$25,000 per month in which Target Performance level is not met. $50,000 if the Target Performance level is not met in a subsequent consecutive month. If Target Performance is met 3 successive months, the Service Level Credit is $15,000 per month in which Target Performance level was not achieved.	SBO had not assessed any service level credits related to this requirement as the Target Performance had been met.

Standard 4	Network Response Time	
	Service Level Requirement	**OAG-Determined Status**
Description	The Contractor must perform the processing services in accordance with the Network Response Time Performance Standard measured as the network response time from the server at the Contractor's hosting center to the Lansing based vendor router and back to the server host.	
Measurement	Average network response time must be <0.125 seconds.	SBO did not fully establish and implement an effective process for measuring compliance with this requirement (see Finding #5).

This summary continued on next page.

Target Performance	100% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor self-reported compliance with this requirement; however, SBO had not independently verified the status (see Finding #5).
Period of Review	Monthly	Completed.
Service Level Credit	$25,000 per month in which Target Performance level is not met. $50,000 if the Target Performance level is not met in a subsequent consecutive month. If Target Performance is met for 3 successive months, the Service Level Credit is $15,000 per month in which Target Performance level was not achieved.	SBO had not assessed any service level credits related to this requirement as the Target Performance had been met.

Standard 5	**Off-Line Batch Processing**	
	Service Level Requirement	**OAG-Determined Status**
Description	All scheduled output from normal nightly batch processing must be delivered to the specified State end user in the manner elected by such end user. For the purposes of this section, the term "delivered" shall mean with respect to end users who are connected to the ERP application software and who elect to receive their output in electronic format, the Contractor must have such output available by 7 a.m. each business day. The Contractor must initiate production 'on-request' jobs within two (2) hours of receipt of an approved request, subject to the design limitations of the ERP application software, in no case shall initiation of such processing be delayed beyond the current night's batch processing cycle.	
Measurement	The parties must develop a mutually acceptable tracking and reporting process for this service level objective. The specific, final batch processing requirements and the identification of critical batch jobs will be agreed upon during performance benchmarking that takes place as part of the ERP Implementation project.	SBO uses a compliance tracking spreadsheet to measure completion time of off-line batch processing. Measurement data within the spreadsheet is based on batch cycle completion reports. We identified deficiencies related to documentation of compliance with this requirement (see Finding #5).
Target Performance	100% compliance with target service level	Not met for 6 (100%) of 6 months reviewed.
Period of Review	Monthly	Completed.

This summary continued on next page.

Standard 6	**Completion Times for Critical Batch Jobs**	
	Service Level Requirement	**OAG-Determined Status**
Description	The Contractor must complete normal nightly batch processing through the report cycle of the ERP application software within the batch processing window of 6 p.m. - 7 a.m. business days. The Contractor will work with the State to develop a table of critical batch jobs prior to implementation in any ERP project phase that includes: job, job description, and critical completion time. All jobs listed in that table shall be subject to the following standard in relation to the listed critical completion time: The Contractor must perform the processing services in accordance with the performance standard identified below: < 2 missed completions in previous 3 months. For purposes of this section, a 'missed completion' is defined as a designated batch job completing beyond the specified "critical completion time." The jobs listed in the table will include the following as well as others that will be identified as part of production planning: Payment and Warrant Request Interfaces Outbound Bank Interfaces Inbound Bank Interfaces EFT and Wire Transfer Jobs Report Distribution Jobs Final nightly batch or syncpoint jobs (that must be completed prior to the beginning of a new online day) Processing of EDI or eInvoice interface Time and attendance and employee travel and expense reimbursement interfaces (bi-weekly) Warrant Writing Interfaces and/or Jobs	
Measurement	The parties must develop a mutually acceptable tracking and reporting process for this service level objective. The specific final batch processing requirements and the identification of critical batch jobs will be agreed upon during performance benchmarking that takes place as part of the ERP Implementation project.	SBO uses a compliance tracking spreadsheet to measure completion time of critical batch jobs. Measurement data within the spreadsheet is based on batch cycle completion reports. We identified deficiencies related to documentation of compliance with this requirement. Also, the final identification of critical batch jobs should be formally agreed to (see Finding #5).
Target Performance	100% compliance with target service level	Not met for 6 (100%) of 6 months reviewed. The vendor should provide additional supporting documentation for its level of compliance with this requirement, such as details of critical batch job completion times in its monthly compliance reporting (see Finding #5).
Period of Review	Monthly	Completed.

This summary continued on next page.

Service Level Credit	The Service Level Credit amount is $50,000 per failure to meet the required service level.	SBO assessed $150,000 in service level credits against this requirement. The maximum allowable service level credit was reached in April 2018, which prevented additional credits from being assessed.

Standard 7	**Daily Disaster Recovery Backups**	
	Service Level Requirement	**OAG-Determined Status**
Description	The Contractor must ensure that disaster recovery backups are complete, encrypted, prepared and either moved to the off-site storage facility on a daily basis per the mutually agreed schedule or replicated to the 'hot site' or 'warm site' as required by this agreement.	
Measurement	The parties must develop a mutually acceptable tracking and reporting process for this service level objective.	SBO did not fully establish and implement an effective process for measuring compliance with this requirement (see Finding #5).
Target Performance	100% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor self-reported that it complied with this requirement, but it has not provided sufficient supporting documentation. SBO did not independently verify the vendor's level of compliance (see Finding #5).
Period of Review	Monthly	Completed.

<table>
<tr><th>Standard 8</th><th>Issue Response and Resolution Time</th><th></th></tr>
<tr><td></td><td><b>Service Level Requirement</b></td><td><b>OAG-Determined Status</b></td></tr>
<tr><td><b>Description</b></td><td>The Contractor must respond to and resolve issues that have been designated as Contractor-owned issues within the times below, unless otherwise agreed upon by the State and the Contractor:
<table>
<tr><th>Issue Severity</th><th>Response Time</th><th>Resolution Time</th></tr>
<tr><td>Critical</td><td>10 minutes</td><td>24 hours</td></tr>
<tr><td>Serious</td><td>1 hour</td><td>48 hours</td></tr>
<tr><td>Moderate</td><td>1 day</td><td>Per the Contractor's Patch Set obligations in Section 20.0</td></tr>
</table>
</td><td></td></tr>
<tr><td><b>Measurement</b></td><td>The parties must develop a mutually acceptable tracking and reporting process for this service level objective.</td><td>SBO uses a compliance tracking spreadsheet to measure issue resolution time. Measurement data within the spreadsheet is based on job tickets that track critical and serious issues and weekly meetings to discuss other outstanding issues. We identified deficiencies related to monitoring for compliance with this requirement, including issue response time not being measured (see Finding #5).</td></tr>
</table>

This summary continued on next page.

Target Performance	100% compliance with target service level	Not met for 6 (100%) of 6 months reviewed.
Period of Review	Monthly	Completed.
Service Level Credit	$25,000 per month in which Target Performance level is not met. $50,000 if the Target Performance level is not met in a subsequent consecutive month. If Target Performance is met 3 successive months, the Service Level Credit is $15,000 per month in which Target Performance level was not achieved.	SBO assessed $125,000 in service level credits against this requirement. The maximum allowable service level credit was reached in April 2018, which prevented additional credits from being assessed.

Standard 9	**Incident Resolution - Issue Triage, Closure and Recidivist Rate**	
	Service Level Requirement	**OAG-Determined Status**
Description	Incident Triage, Closure and Recidivist Rate will be determined by monitoring compliance with the following four key performance indicators (KPI): Incident Triage: Contractor to indicate high-level diagnosis and estimate to remedy to the State within 30 minutes of acknowledgement. Incident Closure: Incident to be documented with root cause remedy, (where root cause is within Contractor's control), and procedures to eliminate repeat of incident within 24 hours of incident closure. Incident Recidivist Rate: Closed incidents not to reappear across all in-scope services no more than two times following incident closure. Incident means any critical incident where the services for which the Contractor is responsible under the Statement of Work (SOW) are unavailable.	The description indicates that compliance should be measured against four KPI; however, only three are listed (see Finding #5).
Measurement	Total Priority 1 Incidents for which Contractor is responsible under the SOW, where solution services are unavailable - number of incidents where the KPI was not in compliance.	SBO uses a compliance tracking spreadsheet to review critical incidents to ensure that they do not reappear more than twice after closure. We identified deficiencies related to monitoring for compliance with this requirement. Also, SBO did not fully establish and implement an effective process for measuring compliance with the other KPI in this requirement. In addition, SBO had not determined the types of tickets which should count toward this measurement (see Finding #5).

This summary continued on next page.

Target Performance	100% compliance with target service level	Not met for 5 (83%) of 6 months reviewed. The vendor self-reported compliance with this requirement for 6 months, but it did not provide sufficient supporting documentation. SBO had not fully independently verified compliance (see Finding #5).
Period of Review	Monthly	Completed.
Standard 10	**Capacity Monitoring and Planning**	
	Service Level Requirement	**OAG-Determined Status**
Description	Capacity Monitoring and Planning - Capacity utilization flag will be determined by monitoring compliance with the following five key performance indicators (KPI): Contractor Service Delivery Center CPU capacity not to exceed 95% aggregate sustained utilization by supported server class (compute, file, web, etc.) for a period of 4 hours or 80% aggregate sustained utilization for a period of 8 hours. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents. Contractor Service Delivery Center disk capacity (online) not to exceed 80% utilization as measured by both available disk space and available I/O by server class for period of 5 days. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents. Contractor Service Delivery Center memory usage not to exceed 95% aggregate sustained utilization by server class for period of 4 hours. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents. Data center LAN and wide area connectivity elements not to exceed 90% aggregate sustained utilization on primary network backbone. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents. Flag, for the purposes of this Service Level, means a Contractor notification to the State as set forth in the Process Interface Manual or other supporting documents.	
Measurement	Number of instances where individual KPI's were not in compliance	SBO did not fully establish and implement an effective process for measuring compliance with this requirement (see Finding #5).

This summary continued on next page.

Target Performance	99.5% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor has self-reported compliance with this requirement as being met, but this has not been independently verified by SBO (see Finding #5).
Period of Review	Monthly	Completed.
Standard 11	**Security Compliance**	
	Service Level Requirement	**OAG-Determined Status**
Description	Security Compliance will be determined by monitoring compliance with the following five key performance indicators (KPI): Material compliance with the State IT and federal (FISMA) security policies for the classification of data contained in the systems Check the antivirus signatures every 12 hours and update of antivirus signatures when new signatures are available 100% of environments (inclusive of memory, disk and other file structures) to be actively scanned for viruses, trojan horses, rootkits and other malware every 24 hours 100% of environments to be reviewed for inactive/suspended user accounts every 30 days	The description indicates that compliance should be measured against five KPI; however, only four are listed (see Finding #5).
Measurement	Total number of individual KPI's performed per month that were in compliance / Total number of individual KPI's performed per month	SBO did not fully establish and implement an effective process for measuring compliance with this requirement and did not sufficiently define for all of the KPI (see Finding #5).
Target Performance	99.5% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor has self-reported that it complied with this requirement, but it has not provided sufficient supporting documentation. SBO only partially independently verified the vendor's level of compliance (see Finding #5).
Period of Review	Monthly	Completed.
Standard 12	**Annual Security Review**	
	Service Level Requirement	**OAG-Determined Status**
Description	An appropriately scoped assurance engagement under the AICPA's SOC reporting framework is required. Details regarding scope and control objectives to be established at a later date. Contractor will assist and cooperate with this effort by providing Third Party or the State security personnel with appropriate access to Contractor's facilities and personnel as required to conduct these reviews.	

This summary continued on next page.

Measurement	Number of instances where individual KPI's were not in compliance	SBO used a compliance tracking spreadsheet to record the annual security review being obtained.
Target Performance	100% compliance with target service level	Not determined. Deficiencies were identified related to SBO's assessment of coverage with this requirement (see Finding #6).
Period of Review	Annually	Not completed as of June 30, 2018.
Standard 13	**Monitoring and Auditing Security Breach**	
	Service Level Requirement	**OAG-Determined Status**
Description	Physical, Network, System Security Breach Detection will be determined by monitoring compliance with the following two key performance indicators (KPI): Compliance with all Michigan breach notification laws and requirements including incident response procedures. Physical, Network, and System Security Breach Detection will be determined by monitoring compliance with the following two KPI: Remote logging access (and system configuration/policy reviews) for SOM systems and their related networking and security systems.	The description should be made clear to help ensure that compliance with this requirement can be accurately determined (see Finding #5).
Measurement	Number of instances where notification requirements are met	SBO did not fully establish and implement an effective process for measuring compliance with this requirement (see Finding #5).
Target Performance	100% compliance with target service level	Met for 6 (100%) of 6 months reviewed. The vendor self-reported that it complied with this requirement, but it has not provided sufficient supporting documentation. Also, the level of compliance has not been fully independently verified by SBO (see Finding #5).
Period of Review	Monthly	Completed.
Service Level Credit	$25,000 per month in which Target Performance level is not met. $50,000 if the Target Performance level is not met in a second or subsequent consecutive month.	SBO had not assessed any service level credits related to this requirement as the Target Performance had been met.
Standard 14	**SLA Reporting Timeliness**	
	Service Level Requirement	**OAG-Determined Status**
Description	Meeting mutually agreed delivery dates related to completion of application maintenance tasks requiring coding changes, new coding, or application configuration.	The description should be made clear to help ensure that compliance with this requirement can be accurately determined (see Finding #5).

This summary continued on next page.

Measurement	Number of instances where agreed upon delivery dates were met	SBO uses a compliance tracking spreadsheet to indicate when the vendor provides self-reporting of service level requirement compliance. We identified deficiencies related to monitoring for compliance with this requirement (see Finding #5).
Target Performance	100% compliance with target service level	Not met for 6 (100%) of 6 months reviewed.
Period of Review	Monthly	Completed.

Standard 15	**Asset Management Refresh – Asset Inventory Accuracy**	
	Service Level Requirement	**OAG-Determined Status**
Description	Asset Inventory Element Accuracy will be determined by comparing the Contractor-provided and maintained Asset Management Tracking system records against the State system generated record of Asset Inventory Elements. The scope of this comparison is all hardware (physical and virtual) including equipment and software procured, operated and supported by the Contractor for use by the State. Contractor will not be responsible for accuracy errors that are not caused by the Contractor. Given use of a leveraged platform, the Contractor will provide and maintain a tailored Asset Management Inventory such that it would be applicable and accurate should the State want hosting to be undertaken at the State or other location, per Section 2.U of Attachment 2.	
Measurement	Element Accuracy = Total Accurate Asset Inventory Elements / Total Asset Inventory Elements	SBO did not fully establish and implement an effective process for measuring compliance with this requirement (see Finding #5).
Target Performance	98% compliance with target service level	Not determined. The level of compliance has not been fully independently verified by SBO (see Finding #5).
Period of Review	Annually	Not completed.

Source: The OAG created this summary using data obtained from SBO's Procurement Contract No. 071B4300137.

SYSTEM DESCRIPTION

SIGMA is an enterprise resource planning (ERP) solution for the State of Michigan. SIGMA administration and security are the responsibility of the SIGMA team in conjunction with the Office of Financial Management and the various State agencies. SIGMA fully or partially replaced over 60 State government IT systems.

SIGMA consists of various modules, such as Financial, Human Resource Management, Administration, and Business Intelligence, and is capable of cost accounting and cost allocation, grant lifecycle management, asset and inventory management, and performance budgeting. In 2014, SBO contracted with a software technology vendor for the acquisition and implementation of SIGMA. As of October 19, 2018, SBO expended more than $150 million on the development and implementation of SIGMA, with a total budget of $175.3 million, since project inception in fiscal year 2013.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the system and other records related to selected application controls* and service level requirements 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2016 through September 30, 2018.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of SIGMA in order to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Obtained an understanding of SIGMA and its various modules that make up the application.
- Reviewed applicable policies, standards, and procedures for State information systems.
- Interviewed management and staff responsible for administering and securing SIGMA.
- Analyzed job tickets to gain an understanding of known system issues and defects.
- Reviewed system documentation and the vendor contract.

OBJECTIVE #1

To assess the effectiveness of selected access controls over SIGMA.

To accomplish this objective, we:

- Randomly and judgmentally sampled 105 of 14,390 user accounts as of May 30, 2018 for proper approvals, principle of least privilege*, and segregation of duties*.

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

- Reviewed the State's process for removing user access after departure from the State.

- Evaluated the State's processes for monitoring user access and activity.

- Identified and analyzed controls implemented to protect against incompatible user roles and enforce the segregation of duties.

- Assessed the reasonableness of 19 of 175 randomly and judgmentally sampled document codes as of May 4, 2018 that did not have workflow controls to require approval.

- Judgmentally sampled 15 of 143 document codes that require workflow as of May 4, 2018 to determine whether the workflows were working as intended by reviewing the approvals for 186 processed transactions.

- Created 23 test transactions to put through the workflow process to ensure that workflow controls were functioning appropriately.

We sampled user accounts and document codes using a risk-based approach. Our random samples were selected to eliminate any bias and enable us to project the results to the population. For our judgmental samples, we could not project our results to the respective populations.

OBJECTIVE #2

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

To accomplish this objective, we:

- Judgmentally sampled and reviewed interface design documentation and reconciliation procedures for 46 of 318 system interfaces as of May 17, 2018 for compliance with industry best practices.

- Judgmentally sampled 46 of 318 system interfaces as of May 17, 2018 to assess whether State agencies, in conjunction with SBO, reconciled the interfaced data for completeness. We also evaluated the sufficiency of supporting documentation maintained by the agencies.

- Analyzed vendor master data tables to ensure the completeness and accuracy of significant vendor data.

- Tested the appropriateness of the creation and modification of vendor records in SIGMA for a judgmental and random sample of 43 of 8,471 high-risk vendors as of June 25, 2018.

- Analyzed cash payment transactions and miscellaneous vendor transactions for irregularities.

- Reviewed SOM tax data, LexisNexis, and IRS records to determine the legitimacy of a judgmental and random sample of 43 of 8,471 high-risk vendors as of June 25, 2018.

- Judgmentally and randomly sampled records and balances from the following areas to assess the completeness and accuracy of data conversion from the legacy systems to SIGMA. Specifically, we:

  - Reconciled all fiscal year 2017 ending balance sheet accounts at the fund level from MAIN to SIGMA fiscal year 2018 beginning balances. Also, we randomly sampled 43 of 1,044 SIGMA fiscal year 2018 beginning balance sheet account coding roll ups to verify the ending balance on the fiscal year 2017 *State of Michigan Comprehensive Annual Financial Report (SOMCAFR).*

  - Reconciled all fiscal year 2017 ending warrants outstanding at the vendor level from MAIN to SIGMA fiscal year 2018 beginning balances. Also, we randomly sampled 43 of 104,621 MAIN fiscal year 2017 ending warrants outstanding balances to verify detailed payment information in SIGMA fiscal year 2018 beginning balances.

  - Randomly sampled 21 of 540 Project Accountability and Billing (PAB) conversion files which contain detailed records from this system. We then randomly sampled 1 or 2 records (40 total) from each conversion file to verify the information in SIGMA as of the beginning of fiscal year 2018.

  - Randomly sampled 43 of 55,783 MAP Financial Obligation System (MFOS) detailed records to verify the information in SIGMA as of the beginning of fiscal year 2018.

  - Randomly sampled 43 of 7,552 cost accounting conversion error records to verify that the information was uploaded into SIGMA correctly as of the beginning of fiscal year 2018.

  - Judgmentally and randomly sampled 43 of 445 grant program profiles to verify detailed program funding information in SIGMA as of the beginning of fiscal year 2018.

  - Randomly sampled 43 of 21,641 fixed asset balances to verify the detailed information in SIGMA fiscal year 2018 beginning balances.

  - Randomly sampled 40 of 6,269 electronic account profiles (EAPRO) and 40 of 6,662 electronic account addresses (EAAD) to verify the detailed information in SIGMA as of the beginning of fiscal year 2018.

- Evaluated SBO and the State agencies' data conversion and validation efforts for selected systems.

Our random samples were selected to eliminate any bias and enable us to project the results to the population. For our judgmental samples, we could not project our results to the respective populations.

OBJECTIVE #3

To assess the State and vendor's compliance with the service level requirements within the SIGMA contract.

To accomplish this objective, we:

- Reviewed the vendor's compliance with the 15 service level requirements within the SIGMA contract.

- Evaluated the sufficiency of the State's processes for monitoring compliance with the 15 service level requirements.

- Assessed the service level credits that the State has deducted from payments to the vendor as a result of noncompliance.

- Assessed the measurability and clarity of service level requirements as described in the SIGMA contract.

- Reviewed the vendor's Federal Risk and Authorization Management Program* (FEDRAMP) certification information, including compliance assessments.

- Reviewed the SOC 1 and SOC 2 reports and other security assessment reports on SIGMA.

- Assessed the complementary user entity controls described in the SOC 1 and SOC 2 reports.

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

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 6 findings and 6 corresponding recommendations. SBO's preliminary response indicates that it agrees with 4 recommendations and partially agrees with 2 recommendations.

The agency preliminary response that follows 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* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Director upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

SUPPLEMENTAL INFORMATION

Our audit report includes a summary of the status of service level requirements, presented as supplemental information. This information supported the conclusion to our third objective.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

auditor's comments to the agency preliminary response

Government auditing standards require auditors 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. Therefore, when this situation arises, the OAG includes auditor's comments to comply with this standard.

access controls

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

AICPA

American Institute of Certified Public Accountants.

application controls

Controls that are directly related to individual computer applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

Control Objectives for Information and Related Technology (COBIT)

A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over IT.

DCDS

Data Collection and Distribution System.

DTMB

Department of Technology, Management, and Budget.

DTMB-170

information security risk assessment.

EAMD

Expense Adjustment Manual Disbursement.

EDI

electronic data interchange.

effectiveness

Success in achieving mission and goals.

ERP

enterprise resource planning.

ESS

Employee Self Service.

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.*

Federal Risk and Authorization Management Program (FEDRAMP)

A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

interface controls

Controls that ensure the accurate, complete, and timely processing of data exchanged between information systems.

IP

Internet Protocol.

IRS

Internal Revenue Service.

IT

information technology.

KPI

key performance indicator.

LexisNexis

A research tool that allows a user to search a database of public records for information on individuals and businesses.

MAIN

Michigan Administrative Information Network.

material condition

A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.

performance audit

An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

principle of least privilege

The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.

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.

QA

quality assurance.

reportable condition

A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.

SBO

State Budget Office.

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.

SLA

service level agreement.

SOM

State of Michigan.

SOW

statement of work.

Statewide Integrated Governmental Management Applications (SIGMA)

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

System and Organization Controls (SOC) report

Designed to help organizations that provide 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 that need 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 that affect the security, availability, or processing integrity of the systems a service organization employs to process user entities' information, or the confidentiality or privacy of that information, but do not have 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.

VSS Vendor Self Service.

workflow controls Controls within SIGMA used to define the approval path that documents must follow before being finalized and the users who can approve such documents.

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) 334-8060, Ext. 1650