bakertilly

State of Idaho
Luma IT Audit

June 2024



Table of contents

Executive Summary	**3**
Background	4
Approach	5
Current State Perspectives	6
Summary Results	7-9
Key Risks & Perspectives	**10**
Appendices	**17**

Luma IT Audit

Executive Summary

Background

Baker Tilly performed an assessment of 101 relevant IT General Controls (ITGCs) identified within the FISCAM framework over the Luma system; as well as assessed the reliability of key data across 62 sampled interfaces into 21 identified modules within Luma from adjacent systems. While ITGCs tend to operate in a homogenous manner across a system, interface controls were scoped based on the identification of key financial data necessary for financial reporting; including, but not limited to, the following Luma modules:

- General Ledger
- Cash Management
- Accounts Payable
- Accounts Receivable
- Payroll
- Benefits

Approach

1. Conducted control interview and walkthrough procedures to evaluate the design and implementation (D&I) for key controls in-scope, captured in testing workpapers against the FISCAM framework
2. Executed tests of operating effectiveness (TOE) for key controls in-scope, captured in testing workpapers
3. Developed recommendations to address identified control gaps, design / operating effectiveness issues and control improvement opportunities
4. Supported LSO in evaluating control deficiencies, identified severity both individually and on the aggregate, and prepared the summary of aggregated deficiencies (SAD), including the results of relevant audit activity performed in response to identified deficiencies
5. Provided periodic updates to LSO as to the status of testing activities, specific to controls testing results



Current State Perspectives and Overview

SCO has relied upon a reactive approach to break fixes. Their efforts to remediate issues are largely driven by individual issues that are identified and reported from end users, rather than proactively identifying gaps and addressing issues more holistically.

Security and privacy controls are largely informal and undefined. Data validation controls are not currently established or owned by the State Controller's Office, and interface specifications are inconsistently documented and configured.

While critical security configurations and infrastructure have been implemented and managed effectively by the State Controller's Office, the SCO acknowledges the need for stronger governance controls, such as the design and documentation of updated policies and procedures and performance of key security and privacy processes.

Summary Results

Baker Tilly performed tests of design and implementation and operating effectiveness for 101 relevant IT General Controls (ITGCs) scoped in by the Legislative Services Office. The in-scope controls were categorized into the following control areas according to the classifications outlined in the FISCAM framework:

Security Management	Access Controls	Configuration Management (including implementation/"go-live" activities)	Segregation of Duties
Contingency Planning	Application Level General Controls	Interface Controls	Data Management System Controls

Baker Tilly determined there to be **sixty (60)** identified control deficiencies that are largely comprised of gaps in the design and implementation of in-scope controls against the FISCAM control framework and illustrative procedures. See the following slide for additional details with further summarization of identified deficiencies.

Deficiency Summary – Table Legend

Baker Tilly issued a conclusion for each control objective area after considering the severity and volume of deficiencies noted within each control area. Each control deficiency was given a low, medium, or high severity rating to encapsulate the perceived likelihood or impact from the deficiencies noted during design and implementation or operating effectiveness testing. Further refer to the "Summary of Aggregated Deficiencies" document for further granularity with each identified control deficiency.

Conclusion Legend

Conclusion	Rating Description
Unsatisfactory	Systemic design or operating effectiveness issues exist with a large volume of deficiencies or several high severity deficiencies noted. This categorization indicates a control objective area that needs several priority remediation items.
Needs Improvement	Key controls require improvements or remediation to improve the organization's security and privacy posture but are not indicative of systemic issues or were determined to be an aggregate of high severity deficiencies that require significant remediation efforts.
Satisfactory	Controls are largely designed and operating effectively with some level of expected failure, and are not factors of systemic design or operating effectiveness issues.

Deficiency Severity Legend

Rating	Deficiency Severity Description
L	Low severity indicates a slight likelihood for material loss or misstatement, compliance concerns, reputational risk, availability and completeness of critical management information, or misappropriation of company assets or data.
M	Moderate severity indicates a moderate likelihood for material loss or misstatement, compliance concerns, reputational risk, availability and completeness of critical management information, or misappropriation of company assets or data.
H	High severity indicates significant likelihood for material loss or misstatement, compliance concerns, reputational risk, availability and completeness of critical management information, or misappropriation of company assets or data.

Deficiency Summary

Deficiencies identified throughout Baker Tilly's testing procedures largely fall into two key risk areas:

1. High and moderate severity deficiencies related to a lack of data validation procedures, determined to have contributed to a lack of confidence in the integrity/reliability of system and interfaced data.
2. Moderate and low severity deficiencies that were indicative of informally implemented security and privacy functions with design or documentation gaps.

Control Objective Area	Control Count	Deficiencies			Failure Rate	Conclusion	Notes
		H	M	L			
Security Management	17	0	11	4	88%	Unsatisfactory	A large volume of deficiencies were noted, and deficiencies were largely a result of key security or privacy processes that have not been formalized or fully implemented to the requirements outlined within the FISCAM framework.
Segregation of Duties	5	0	4	0	80%	Unsatisfactory	
Access Controls	16	0	4	2	38%	Needs Improvement	The severity of identified deficiencies were determined to be of only moderate or low risk.
Interface Controls (Business Process)	28	15	7	0	79%	Unsatisfactory	Deficiencies were largely a result of inconsistent configurations, incomplete or informally managed specification documentation, and a lack of established data validation controls.
Contingency Planning	3	0	0	2	67%	Needs Improvement	Deficiencies were largely a result of informalized and unmanaged policies and procedural documentation or were a result of key security or privacy processes that have not been formalized or fully implemented to the requirements outlined within the FISCAM framework. The severity of identified deficiencies were determined to be of only moderate or low risk.
Application General Controls (Business Process)	21	0	6	4	48%	Needs Improvement	
Configuration Management	4	0	0	0	0%	Satisfactory	
Data Management (Business Process)	7	1	0	0	14%	Satisfactory	One noted deficiency surrounding the lack of a validation control to reconcile master/transactional data (non-specific to interfaces).
Overall	**101**	**16**	**32**	**12**	**59%**	**Unsatisfactory**	**According to in-scope controls within the FISCAM framework, BT determined that key data validation, security, and privacy controls were inadequately designed and implemented.**

** Refer to Appendix III for table legend and descriptions related to deficiency severity and conclusions.

Luma IT Audit

Key Risks and Perspectives

Summary of Key Risks

Based on the results of procedures performed, Baker Tilly has identified a total of **sixty (60)** control deficiencies related to the Luma information system. The deficiencies identified during the review can be attributed to two main areas of risk which are summarized below and explained in more detail on the following slides.



Lack of Data Validation Controls (23 deficiencies)



Informally Managed Security and Privacy Program (37 deficiencies)

Lack of Data Validation Controls

Data validation controls, primarily within the interface controls and data management objective areas, were not effectively designed or implemented throughout the testing period. Issues in data integrity and reliability related to interface processing and system data processing were determined by Baker Tilly to be symptoms of design deficiencies noted through preponderance of testing conclusions and interviews with key stakeholders. See below for key observations:



Lack of Data Validation Controls

- Management (SCO) does not operate or own data validation or reconciliation processes to periodically assess the completeness and accuracy of interfacing data.
- No reporting capabilities are being utilized to aid in the reconciliation of data source systems.
- Design documentation and build specifications are informally reviewed and maintained, and do not consistently document expected processes and procedures related to interfaced data handling.

Baker Tilly's Perspective on Luma Data Validation and Integrity

Interfaces are inconsistently configured, and specification documentation does not consistently capture information related to error handling, unit and/or user acceptance testing performed, interface custodians or owners, etc. However, technologies and processes have been implemented to **reactively** respond to issues as SCO is made aware.

Automated mechanisms for ensuring data validity are not consistently implemented or documented within specification documentation or system configurations.

SCO does not own or currently assume ownership over processes for data validation and reconciliations that leverage reporting capabilities of the system. Detective controls to **proactively** identify issues with interfacing data and/or system functionality in processing are not currently established.

Informally Managed Security and Privacy Program

The next key risk area identified relates to the informal design and implementation of key security and privacy processes, including the lack of updated or managed policies and procedures and inadequately designed security and privacy controls. While the volume of deficiencies attributed to this key risk is high, Baker Tilly determined the severity of deficiencies attributed to these objective areas to be lower comparatively against the lack of data validation controls. See below for key observations:



Informally Managed Security and Privacy Program

- A formal security and privacy management program has not been established through updated policies and procedures.
- Critical security processes (i.e., a formal risk assessment, access reviews and restriction of privileged access, incident response program, business continuity and disaster recovery plan, etc.) have not been formally designed, implemented, or documented.
- Security and privacy controls that currently exist within the control environment are largely informal, unoptimized, and performed on an ad-hoc basis.

Baker Tilly's Perspective on the Security and Privacy Program

Management has not formally designed and documented policies and procedures with relation to the security and privacy program for Luma to be maintained and updated on a periodic basis.

While a role-based access model is utilized, management has not implemented controls to periodically and continuously evaluate potential segregation of duties conflicts and enforce the principle of least privilege when allocating permissions to users.

Key security processes, such as an Incident Response Program, Business Continuity Plan / Disaster Recovery Plan, IT Risk Assessment, and Audit Logging/Monitoring capabilities have not been designed or implemented to the expected level of maturity outlined in the FISCAM framework.

Summarized Implementation Roadmap

The immediate priority for management is to address the lack of data validation controls and gauge whether initial functional and technical requirements were appropriately implemented as expected. Management should stagger the implementation of our detailed recommendations in order to provide assurance that expected functionality is appropriately implemented and data validation controls are established and defined prior to shifting focus to recommendations in strengthening the overall security and privacy posture of the system. This may require a shift in priority to performing a **proactive** requirements mapping exercise as opposed to continuing with reactive break fixes and change requests. Baker Tilly believes this would be a more efficient method to restore confidence in the system's data integrity prior to addressing other key recommendations. See below for a summarized implementation timeline:



Appendices

Appendix I

Interview Participants

Baker Tilly conducted onsite and virtual interviews with the SCO office and LSO auditors to gain an understanding of the control environment and processes around the Luma system. See below for key employees inquired with, including, but not limited to:

- Patrick Hodges, Deputy Controller, Division of Accounting
- Scott Smith, Deputy Controller
- Rocky Bencken, IT Info Security Engineer IV
- Brett Richardson, CIO
- Greg Schenk, Business Intelligence Analyst
- Steven Trevaskis, It Info Sys And Infr Eng III
- Chris Cullen, Bureau Chief
- Chris Minter, Bureau Chief
- Phil Varrick, LUMA Finance Team Member
- Jason Skelton, Luma Procurement Lead

Appendix II

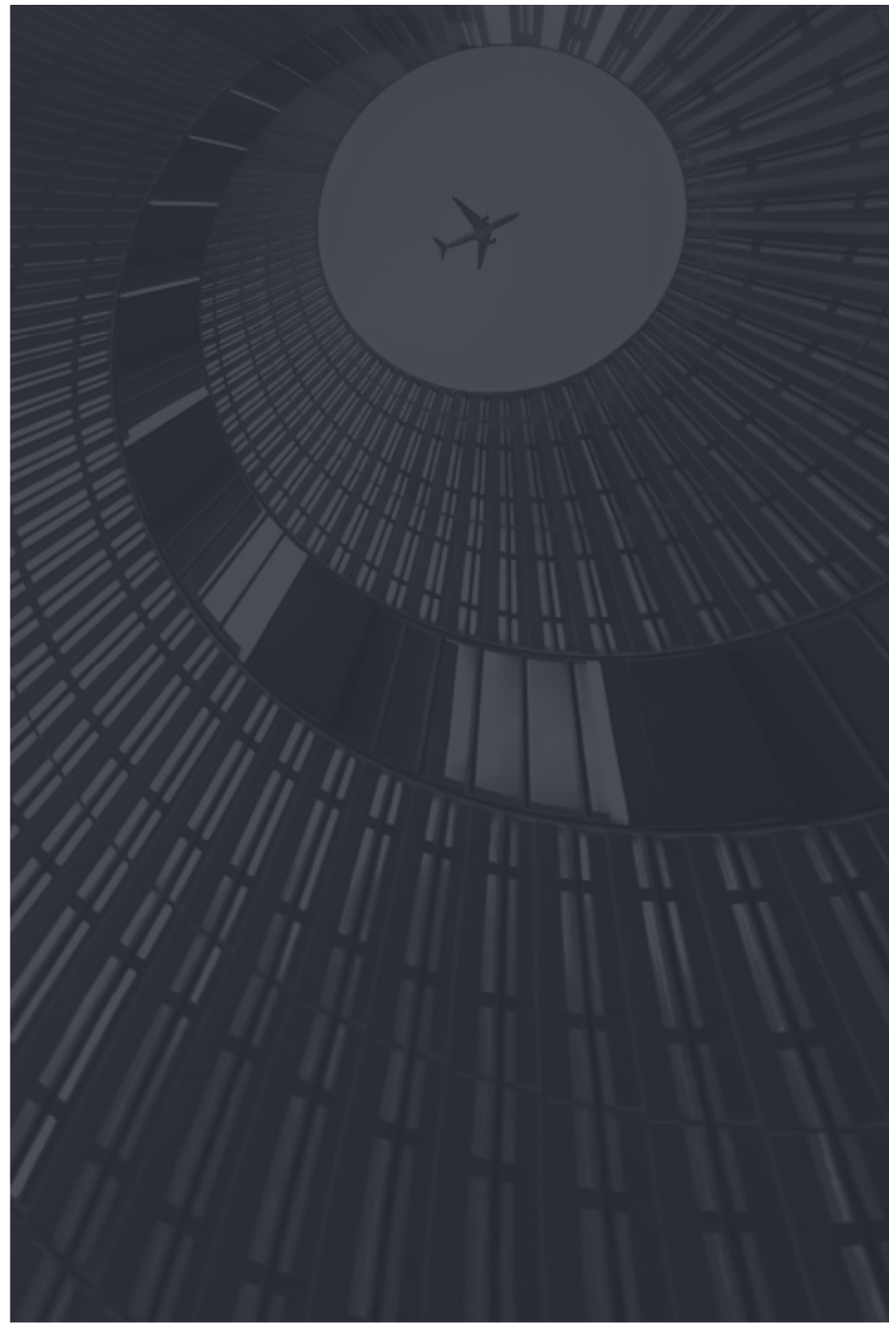
Engagement Timeline



Contact Information

Joe Shusko
Partner
Joe.Shusko@bakertilly.com
585.201.2439

Derek Biliskov
Manager
Derek.Biliskov@bakertilly.com
765.661.6472



Baker Tilly US, LLP, trading as Baker Tilly, is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2023 Baker Tilly US, LLP.

Management's View and Corrective Action Plan
Auditor's Responses

Terri Kondeff
Director

Legislative Services Office
Idaho State Legislature

Serving Idaho's Citizen Legislature

State of Idaho Luma IT Audit

Management View and Corrective Action Plan with Auditor's Responses

The State of Idaho Luma IT Audit report was completed by Baker Tilly, through a contract with the Legislative Services Office, Legislative Audits Division. As part of that audit, we requested that the Office of the State Controller (SCO) provide us with responses and corrective action plans for the 14 summarized recommendations encompassing the 60 deficiencies identified. The following information includes the summary issue title, prioritized rating, summary of the recommendation, management's view on the issue, management's corrective action plan with timeline, and an auditor's response. The management view and corrective actions with timeline are included verbatim from the document received from the SCO on October 10, 2024. Our auditor responses are included to provide any clarity to the management responses provided and address concerns we have with either the management view or the corrective action plan.

SUMMARY ISSUE #1: Validate implementation of interfacing data and expected functionality

PRIORITIZATION RATING: High

SUMMARY OF RECOMMENDATION: Management should coordinate an exercise to proactively reconcile functional and technical requirements of interfacing data to the implemented solutions, including a corresponding unit and user acceptance test scenario, and test execution in order to ensure that all required functionality and configurations are appropriately configured. During this process, business process documentation and interface specification documents should be updated and

supported with systematic evidence that provide additional assurance that the design of interfaces and system configurations are controlled, defined, and established.

Specific requirements with relation to duplicate entries or data should be validated through unit and user acceptance testing during the exercise and ensure that such mechanisms are functioning as expected in accordance with functional and technical requirements as noted by business teams.

During this process, the existing service ticket and email alerting methods that the SCO have established over most of the sampled interfaces should be enforced where possible and documented within the specification guides that are established for each individual interface, including sign-offs and approvals from relevant business personnel who interact with the interface.

Discrepancies in the error alerting capabilities should be identified across all required interfaces and reconfigured to consistently alert and prompt resolution of identified errors.

MANAGEMENT VIEW: *The recommendation appears to identify two distinct areas that need to be addressed. The first revolves around the reconciling of interfacing data. The second appears to identify a need for addressing the business process documentation and interface specifications. For the first recommendation, this is a net new requirement for the State. In the legacy environment and during the requirements development stage, the State retained the federated management of data with the agencies. Within Idaho Code and GAAP policies, the agencies are required to validate the data sources from their systems and ensure Luma is accurately reflecting their transactions. This is further refined by the existing ACFR requirements where agencies are responsible for attesting to the accuracy of the data. As a net new requirement, the State must build out the process requirements and establish the procedures/expectations for Luma and every interface owner (approximately 165) in order to achieve acceptable data reconciliation processes. This may result in additional workload of significance that could require a case study on additional resources requiring approval from the Legislature. The second recommendation requires a formalization of the business process and interface specification documentation. Much of the process was defined and already documented. The gap revolves around the formalization and documentation of agreement between Luma and the interface owners. This recommendation highlights the need to achieve a mature documentation and reconciliation process. Given our current experience with agencies completing the reconciliation process, we acknowledge the entries within Luma are meeting the State requirements. This recommendation enables us to ensure our documentation reflects the realities of the current processes.*

CORRECTIVE ACTIONS WITH TIMELINE:
CORRECTIVE PLAN #1:

- *Build a roadmap with major milestones no later than October 1, 2024.*
- *Establish data reconciliation process no later than 1 December, 2024,*
- *Complete data reconciliation process no later than 30 June, 2025*

CORRECTIVE PLAN #2:

The initial goal is to get the process documentation formalized and published. With approximately 164 interfaces in production, we are tackling this is two phases.

- *Phase 1: any new interface requests will conform to the approved process which will ensure we have systemic evidence of design approval, validated testing, and guidelines for error handling. Completion by October 31, 2024.*
- *Phase 2: all existing interfaces will need to be reviewed to achieve conformance with this approved documentation. With 164 existing interfaces, we project a review of a maximum of 10 interfaces per month (maximum) with larger, complex interfaces reducing the availability. The goal to achieve a full review of all interfaces is projected for 31 December, 2025.*

Note: Correction Action Plan #2 is dependent upon the resources available within agencies and the State Controller's Office. Should the resource model require advocacy with the Legislature, the formal adoption process could be delayed until resources are secured (2026).

ANTICIPATED DATE OF REMEDIATION: *Varied with full completion December 31, 2025*

Auditor's Response: We thank the State Controller's Office for corporation and assistance throughout the audit. We would like to clarify that this recommendation is aimed at validating the actual implementation of the interfacing process and expected functionality to ensure that business process needs were appropriately addressed and tested, not just reconciling the data. The recommendation includes suggesting the SCO reconcile functional and technical requirements of the interfacing data to the implemented solutions, including appropriating testing to ensure required functionality is achieved. Completing data reconciliations to validate the financial information in Luma is important, and addressed in Summary Issue #2, but the focus of this issue is ensuring that the interface processes designed by the SCO adequately meet the needs of the agencies utilizing them and is appropriately documented.

Idaho Code 67-1001 states that "It is the duty of the state controller: (1) To superintend the fiscal concerns of the state, with its accounting, informational, payroll, and related data processing services." In addition, 67-1001(5) states that the State Controller is "To keep and state all funds in which is interested." A team approach between State agencies and the SCO is necessary to fulfill these Idaho code requirements and this report specifically addresses recommendations for the SCO. Further, the statement that "Within Idaho Code and GAAP policies, the agencies are required to validate the data sources from their systems and ensure Luma is accurately reflecting their transactions." is misleading. It is the agencies responsibility to ensure that they maintain appropriate supporting documentation and implement internal controls to ensure accurate processing of financial transactions. However, without appropriate tools such as adequate financial reports, it is not the agencies responsibility, nor even within their capabilities, to ensure that Luma captures the data entered accurately. Additionally, GAAP does not only apply to the agencies but also to SCO as the owner of Luma and the preparer of the State's financial statements. Ultimately responsibility for the accuracy of financial statements rises to management, and as the preparer of the ACFR, management is considered to be the SCO.

While Corrective Action Plan #1 addresses the concerns raised in Summary Issue #2 more so than this issue, complete data reconciliation processes by June 30, 2025, increases the risk that errors could occur in interfacing processes and would not be detected.

We are also concerned about the length of time planned for the final implementation of Corrective Plan #2. It will be at least 24 months, depending on available resources, since Luma went live to when the SCO reviews all existing interface processes to achieve conformance with documentation of design approval, validated testing, and guidelines for error handling. This extends the risk that interfaces do not process correctly, errors are not resolved timely, and data may not reported correctly in Luma and by the State.

While we understand the constraints of limited resources, it is critical that procedures be implemented as quickly as possible to ensure that the agencies' multiple interfaces are operating correctly and providing complete and accurate financial data to the State.

SUMMARY ISSUE #2: Implement proactive data validation and reconciliation controls to be owned and executed by the SCO

PRIORITIZATION RATING: High

SUMMARY OF RECOMMENDATION: Management should ensure that formal processes for data validation controls and reconciliation practices are established and owned by the State Controller's Office, even when the agencies are the authorities with access to the source data for reconciliation.

Management should first begin by identifying whether the reporting capabilities from Luma are configured appropriately to aggregate output data and ease the effort for the reconciling parties to compare against source data in aggregate. Once the reporting capabilities have been assessed and evaluated by management, there should be some initial design workshops to ensure that a reconciliation process with each agency for interfaces that they have designed and requested can be validated on a periodic basis through a reconciliation that is supported by Luma reporting capabilities. Further, an overarching reconciliation process for master and transactional data records maintained in the database (if feasible to obtain from Infor) are complete, accurate, and valid.

The process should be periodic and should be owned by the State Controller's Office (SCO) and reporting from Luma may need to be generated and provided by the SCO to individual agencies per the agreed upon frequency for data reconciliation efforts.

Management should implement a detective control to review system data processing logs relevant to the significant business processes on a periodic basis commensurate with the frequency of processing activities.

As no current processes exist to automatically reconcile output data against source data, management should evaluate whether any automated processes for data reconciliations are able to be configured or requested to be implemented by Infor.

MANAGEMENT VIEW: *This is a net new requirement for the State. In the legacy environment and during the requirements development stage, the State retained the federated management of data with the agencies. Within Idaho Code and GAAP policies, the agencies are required to validate the data sources from their systems and ensure Luma is accurately reflecting their transactions. This is further refined by the existing ACFR requirements where agencies are responsible for attesting to the accuracy of the data. As a net new requirement, the State must build out the process requirements and establish the procedures/expectations for Luma and every interface owner (approximately 165) in order to achieve acceptable data reconciliation processes. This may result in additional workload of significance that could require a case study on additional resources requiring approval from the Legislature.*

CORRECTIVE ACTIONS WITH TIMELINE:
CORRECTIVE PLAN #1:

- *Build a roadmap with major milestones no later than October 1, 2024.*
- *Establish data reconciliation process no later than 1 December, 2024,*
- *Complete data reconciliation process no later than 30 June, 2025*

Note: Should the resource model require advocacy with the Legislature, the formal adoption process could be delayed until resources are secured (2026).

An additional recommendation is to implement a detective control method for reviewing processing log on a periodic basis as well as designing an automated reconciliation process. At this time, both of these recommendations are process improvements that would enhance our current processes or seek efficiencies. These improvements would take considerable time and, as these are categorized as efficiencies, recommend this not to be a condition required to meet the acceptable standards. As future processes gain more efficiency, Luma will explore these opportunities and implement at a future date independent from this audit. This recommendation highlights the need to achieve a mature documentation and reconciliation process. Given our current experience with agencies completing the reconciliation process, we acknowledge the entries within Luma are meeting the State requirements. This recommendation enables us to ensure our documentation reflects the realities of the current processes.

ANTICIPATED DATE OF REMEDIATION: *June 30, 2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. As noted in Summary Issue #1, we believe that a team approach between State agencies and the SCO is necessary to fulfill the SCO's Idaho code requirements. We are also concerned with the comment that *"*As a net new requirement, the State must build out the process requirements and establish the procedures/expectations for Luma and every interface owner (approximately 165) in order to achieve acceptable data reconciliation processes*."* Our concern is that this is not a "net new" requirements but rather should have been factored into the implementation process when the system was being designed and configured to incorporate interface processes. We are also concerned that this response does not properly address of the equal importance of both data reconciliation and documenting policies and procedures to ensure the process accomplishes the goal of reconciliation.

We would like to clarify that the suggestion to evaluate if there are any automated processes for data reconciliation from Infor could be a possible cost saving way of completing these reconciliations, not an efficiency enhancement. We agree that there are a variety of ways the SCO could design reconciliation processes but also continue to assert that data validation and reconciliation is a requirement for any system that includes multiple sources of data used to build financial statements. This is not a new requirement, but rather an overlooked requirement by the SCO. Because the SCO had not taken ownership of reconciliation practices, the report recommended at a minimum, a reconciliation process and a detective control utilizing data processing logs that should already be available, and a suggestion that the SCO could also investigate the viability of an automated reconciliation process from Infor to assist in these processes, and potentially reduce costs.

Also, noted in Summary Issue #1, we are concerned about the length of time planned for the final implementation of Corrective Plan #1. This extends the risk that data is not reported correctly in Luma and by the State and it is critical that this risk be addressed timely.

SUMMARY ISSUE #3: Strengthen maintenance practices for specification documentation and configurations

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management should establish a periodic (at least annual) review for all implemented interfaces in alignment with requirements to be stated in updated policies and procedural documentation. The review should not only be performed over the design specifications, but should include a review of the implementation as configured within the system and be performed as such:

1. Process owner generates a complete and accurate listing of all key interfaces (including screenshot of how the listing was generated) from the application.
2. Process owner formally sends the interface listing and/or screenshots to the appropriate reviewer.
3. Reviewer properly documents and performs the appropriate level of detail to ascertain whether configuration settings, parameters, and tolerances for input data validations against specified definitions for input data format and content are appropriate.
4. Reviewer further documents their understanding of how the population of interfaces was generated, and their determination of whether the resulting population is both complete and accurate in generating all of their responsible interfaces.
5. Reviewer formally documents “approval” whether it be by an email confirmation, ticketing system, or signature. OR determines issues with interface configurations or input data validation to be remediated.
6. Review was performed by appropriate management personnel with proper segregation of duties enforced.
7. Configurations are appropriately modified in a timely manner for users flagged as exceptions during the review.
8. Timeliness – If this is an annual review then happens once a year, if it is a semi-annual twice a year and so on.

Management should ensure that a formal review of specification documentation, including templates and data mapping documents, occurs on a periodic basis (and updated as changes occur) for all (key) interfaces associated with the Luma platform. Change requests related to interfaces should be linked within the specification documentation and version histories and timestamps of changes should be recorded within the documents to create an audit trail of updates to the design documentation.

MANAGEMENT VIEW: *This recommendation builds from the formalization of the business process and interface specification documentation outlined in RECOMMENDATION #1. In concert with the formalization of the business process and interface specification documentation, an additional maintenance schedule will be added.*

CORRECTIVE ACTIONS WITH TIMELINE: *The initial goal is to get the process documentation formalized and published and complete a review of all existing interfaces (approximately 165) by 31 December 2025. Once that is complete, an annual schedule will be established to collaborate with interface owners to ensure requirements, documentation, and existing processing parameters continue to meet expectations.*

- *Establish annual schedule no later than 31 December 2025.*

ANTICIPATED DATE OF REMEDIATION: December 31, 2025

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. Also, noted in Summary Issue #1 and Summary Issue #2, we are concerned about the length of time planned for the final implementation of the Corrective Action Plan. This extends the risk that data is not reported correctly in Luma and by the State and it is critical that this risk be addressed timely.

SUMMARY ISSUE #4: Review the existing access model and evaluate potential segregation of duties conflicts for administrative users; implement a periodic review for point-in-time recertification of user access and permissions

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management should establish a periodic (at least annual) access review for all critical systems and infrastructure in alignment with requirements to be stated within the organization's access management policy. Ideally, the review should assess all users, unless a separate review over privileged users is implemented, and be performed as such.

With respect to the identifying Segregation of Duties conflicts, management should incorporate an element into the review where role-based access is identified and reviewed for conflicts that users may have the ability to perform.

This may require the generation of an additional definitions document to explain the various access permissions associated with roles, and where potential conflicts can be identified and assessed.

The first performance of this review should serve to justify the reallocation of administrator permissions. Management should assess whether it is possible to implement more automated controls to prohibit potential segregation of duties conflicts from occurring at a transactional level.

If not feasible, manual processes to periodically review and identify potential instances of incompatible duties occurring should be implemented to detect and address any instances of an authorized user performing an incompatible duty.

MANAGEMENT VIEW: *All security access request forms are informally audited when there is an update to the form. By informally, I mean that there are no "management approved" policy or procedures. When a SAR form is created, the fulfillment teams which are application subject matter experts review the requests for reasonableness. Should the person have that access, is it too much for their position, is it too little for their position. There are limits to this; however, as not every position in the state has a well-defined job description that is available to SCO. A "staff accountant" at one agency may have very different job requirements as another "staff accountant" at the same agency let alone another agency. When there is a change to a SAR form the same process is reviewed as it goes through each fulfillment team it is again reviewed for reasonableness. The missing link for this is the formality and the review for segregation of duties issues.*

CORRECTIVE ACTIONS WITH TIMELINE: *This will be completed by formalizing the processes and policy and with the full implementation of the Infor Governance, Risk and Compliance (GRC) modules within Luma. GRC was already purchased and planned to be used for these reasons at the time of the audit Interview and was so communicated to the Auditors. There was some hold up from Infor because the modules were not available in the FedRAMP (higher security) version of Infor where Luma resides. These are net new activities and current staffing levels have not been able to complete the tasks required to implement these tools. Staffing may need to be augmented to complete the required tasks based on the plan when complete.*

GRC has two modules that apply to this control set. Certification Manager and Authorization Insights. SCO is currently in the planning phase for Authorization Insights so that known segregation of duties (SoD) issues are cleaned up first. The planning phase should be completed by Oct, 1 2024 and active processing of SoD violations well underway by Dec, 1 2024. Certification Manager planning phase should also be completed by Oct, 1 2024. This will take significant communication with the agencies but the goal is to start processing certifications in the Jan, 1 2025 timeframe.

Certification Manager is for the validation of user access. Certification Manager starts a review process of each user's access requirements to the Luma application. It begins by generating a list of access roles for an individual and then send a confirmation to the employee's listed supervisor for approval. The supervisor either approves or adjusts the required access that the employee needs and this is returned to the State Controllers Security Team for further actions. If accesses are being increased

the Security Team will use a "What-If" tool in the GRC module to check for segregation of duties issues that the new access might create. If it does the added access will be denied or a mitigating control will have to be agreed on. If no change the certification will be accepted and no further action will be required until the next round. If access is to be removed the SCO Security Team will prompt the agency's Security Request Administrator, SRA, to update the employee's Security Access Request form so that the accesses will get promptly removed. Timeliness: it is intended that this will be an annual review.

Authorization Insights is a tool within GRC that identifies and notifies via reports any segregation of duties issues that may exist in the system. Violation reports will be created and reviewed on a weekly basis. When issues arise the violation research will be assigned to a functional team member for review as to whether the employee need the accesses or not. If no then this will need to be forwarded to the Agency SRA for role adjustment. If the employee needs the access, then a mitigating control will be required to prevent the employee from potential fraudulent actions. This is partially in place at the time of the audit review.

ANTICIPATED DATE OF REMEDIATION: *SoD violations underway Dec 2024. Certifications begin Jan. 2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. We would like to address the comment from the SCO that "*GRC was already purchased and planned to be used for these reasons at the time of the audit Interview and was so communicated to the Auditors. There was some hold up from Infor because the modules were not available in the FedRAMP (higher security) version of Infor where Luma resides*." While it is important to note that the SCO acquired the GRC tool, it is also important to note that planned actions do not provide current security nor guarantee implementation and are not auditable. The go-live date had been planned for July 1, 2021, and then July 1, 2022, for the FSM system and neither of those planned events happened. Auditors cannot evaluate planned actions, but only review policies and procedures that are in place during the audit period. Also, there is no indicated date of completion on response.

SUMMARY ISSUE #5: Formalize and implement organizational policies to establish a security and privacy program for the Luma system

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management should perform a formal review of all security and privacy-related policies and ensure that an up-to-date approval and signoff are included, formalizing the implementation of these expectations and requirements across the organization, as well as establish a governing document that acts as the formal implementation of an entity-wide security management plan related to Luma; and ensure that the details within include considerations for security practices and strategy, and are aligned with the entity's strategic plan. Policies should also include considerations for privacy and outline the application characteristics as appropriate.

Policies and procedures established should appropriately:

- consider risk;

- address data management, including data validation and error resolution, in accordance with the entity's data strategy or applicable guidelines established by the entity's data governance body, data integrity board, or management;
- address changes to business process application functionality through modifications to application software or changes to configurable controls within application software;
- address purpose, scope, roles, responsibilities, coordination among business or organizational units with external entities, and compliance;
- identify and describe the relevant processes;
- consider information system general and application controls;
- consider information system general and application controls;
- ensure that users can be held accountable for their actions.
- consider segregation of duties controls; and
- help ensure that users can be held accountable for their actions through appropriate logging and monitoring activities.

Policies should be reviewed annually for appropriateness through a formal documented review and approval process by an appropriate authority with relevant oversight over the business unit or organizational policy in review.

These policies should be retained in a central location and made available to all employees to access at their convenience. Employees should receive notifications when a policy document has been updated and be required to reacknowledge key policies after an update is made and on a periodic basis.

Management should formalize and update all Luma security and privacy documentation that currently exists and ensure that the details within include considerations for security and privacy and outline the application characteristics as appropriate. Policies should be reviewed annually for appropriateness through a formal documented review and approval process by an appropriate authority with relevant oversight over the business unit or organizational policy in review. These policies should be retained in a central location and made available to all employees to access at their convenience. Employees should receive notifications when a policy document has been updated and be required to reacknowledge key policies after an update is made and on a periodic basis.

MANAGEMENT VIEW: *Historically SCO has followed ITA policies for Legacy. ITA policies are not adequate for the requirements of Luma and new policies were in process at time of auditor's interview. A sample template of the new policy was uploaded for the Auditors review. It is unclear if the Auditors reviewed the ITA policies which are in force until new policies are approved by SCO Management.*

An updated and approved Privacy Policy has been published to the SCO Web Site.

CORRECTIVE ACTIONS WITH TIMELINE: *The new policies are being written based on NIST, IRS Special Publication 1075 and now they are being updated to include FISCAM requirements. Due to this is a new requirement, the estimated first draft of this policy is November, 1 2024 and will be very generic in nature. A detailed*

standards document will follow with first draft in the Jan, 1 2025 timeframe.

ANTICIPATED DATE OF REMEDIATION: *First draft of comprehensive plan due Jan. 2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. We would like to note that the auditors reviewed all documents requested and provided and that review supports recommendations. The ITA policies authorizing legislation specifically exempts elected constitutional officers such as the State Controller, so at a minimum the SCO would need to create a policy that states they are adopting the ITA policies and identify which of those policies are included in the SCO policies. Additionally, we agree that the ITA policies alone are inadequate to address the needs of a financial system intended to include many interfaces and provide reliable financial statements for the state, and as such, the SCO should have documented policies and procedures to address that.

Finally, it is important to point out that FISCAM requirements are based off NIST standards and should not add to the workload, they are not new requirements. Below is an example of the relationship between FISCAM and NIST:

FISCAM CONTROL ACTIVITY	NIST	Audit Procedures	Deficiency
•BP01.03.01 Input data validation errors are researched to identify and remediate the cause(s) of the errors •This control activity references to NIST SP 800-53, SI-10 •Included in Summary Recommendation #1	•NIST SP 800-53, SI-10 Information Input Validation-Resolution of Errors •The organization ensures that input validation errors are reviewed and resolved in a defined time period	•Obtain an understanding of the entity's processes and methods for researching and remediating input data validation errors through: •Inquiry of personnel •Inspection of documentation	•Management has <u>not consistently documented the error handling and resolution approach</u> for all interfaces and has <u>not appropriately configured all interfaces to log errors and notify personnel appropriately</u>. •There is a lack of transparency for error handling in which an email alert is not configured, and an error log is saved to a shared folder on the back-end of the system needing an IT staff to triage it appropriately.

SUMMARY ISSUE #6: <u>Implement an audit logging and monitoring program and consider the implementation of a SIEM tool to aggregate security events for investigation and resolution</u>

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION:
Short Term Recommendation: Management should identify which native logging and alerting mechanisms Luma offers with relation to potential security events and incidents (i.e., unsuccessful login attempts, unrecognized IP addresses or suspicious activity) and implement formal detective processes and controls for IT Technicians and personnel to export activity logs and system event notifications for a periodic review over those events (based on a frequency commensurate with the amount of activity that occurs).

Long Term Recommendation: Management should implement a formalized and aggregated SIEM tool for monitoring by dedicated IT personnel. The aggregated tool will ensure that all appropriate events are monitored and analyzed daily by the tool and IT personnel for potential risks, flagging high risk or critical events for IT personnel to investigate to resolution. The SIEM tool should aim to be integrated with all of management's current systems and tools in order to log events in a centralized location for ease-of-monitoring and incident detection, however, should specifically aggregate events from Luma.

For both recommendations, a formalized review process should be instituted, and an "Audit Logging and Monitoring Policy" should be established to document the appropriate procedures for generating reports of log activity or suspicious events for review, roles and responsibilities for reviewers, and when to enact the incident response plan.

MANAGEMENT VIEW: *At time of audit interview, all SCO on-premises devices, servers and workstations, export logs to a log aggregation system that has great searchability, SIEM light if you will. It ingests about 10.5 million records a day. We were also already planning to use an additional module, Process Insights, in the Infor GRC suite to monitor and alert on possible fraudulent transactions within the Luma system. We were waiting for that module to get FedRAMP Authorization which it did recently.*

CORRECTIVE ACTIONS WITH TIMELINE: *We have begun a process of reviewing the Duo authentication logs on a daily basis and all actions are documented in SNOW tickets. This is the most efficient way to review authentications of our systems. If failures are found then the Luma TS Security team runs them to ground to validate no malicious behavior is observed. Several possible conditions such as account lock outs and someone choosing a fraudulent Duo attempt directly create SNOW tickets. There have only been a few attempts marked as fraud and all have proven to be false alarms. These are followed to the point that if we cannot trace the "fraudulent" attempt to a known good IP address where the user has authenticated successfully from, we call the user and follow up. This does usually result in IPs being blocked in our upstream firewalls as we see malicious attempts on an almost daily basis in our VPN access but not in Luma Access.*

As for GRC, Process Insights, we will begin review and planning in the Oct, 1 2024 timeframe unless we can get some staff augmentation to accelerate the planning an implementation of this tool. Expected implementation by end March 2025.

ANTICIPATED DATE OF REMEDIATION: *Process insights in place 3/1/2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit.

SUMMARY ISSUE #7: Establish a formal Incident Response Plan and program to prepare, detect, analyze, contain, eradicate, recover from, and assess security and privacy-related incidents over the Luma system

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: The organization should start by ensuring that their draft Incident Response Plan includes the following components, at a minimum:

Preparation for Incidents: SCO should define roles and responsibilities for key personnel involved in Incident Response, what tools are in use to detect incidents, the processes for reporting incidents and how to classify incidents.

Detection and Analysis: SCO should document how they identify, triage, and assess the nature and scope of the incident. How does SCO define an incident and attribute it to the classifications they've previously defined.

Containment, Eradication, and Recovery: Procedures and personnel responsible for the isolation of compromised machines, resources, or data, removal of the compromise, and restoration of the affected systems and data.

Post-Incident Activity: How are incidents evaluated after resolution to improve processes moving forward? A template for lessons learned should be established as well.

Further, the incident response plan should be reviewed annually for appropriateness through a formal documented review and approval process by an appropriate authority with relevant oversight over the incident response capability.

The plan should be retained in a central location and made available to all employees to access at their convenience. Employees should receive notifications when a policy document has been updated.

MANAGEMENT VIEW: *This is an issue of not having a formal "management approved" Incident Response Plan in place, and not that there was no incident response. SCO agrees that to be a mature organization we need to have this in place and it was in process at the time of the audit interview and was uploaded to the BT tool as "G-30 SCO Cybersecurity_Incident_Response_Plan.docx".*

CORRECTIVE ACTIONS WITH TIMELINE:
A draft Incident Response Plan that contains the stated items is in the management approval pipeline.

ANTICIPATED DATE OF REMEDIATION: *Already in approval process.*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. Again, we are not disputing that the SCO provided a draft document to the auditors, however draft documents are not final implemented and practiced plans, so they do not meet the requirements of the control activity. Additionally, "already in approval process" provides no indication of when the plan will be approved, in place, and provided to the appropriate employees. If we assume that the document uploaded to the auditors was also "in approval process" at that time, as the SCO states, then it has been almost 5 months between the audit and receipt of responses and it has still not been approved and placed in service.

SUMMARY ISSUE #8: Establish a formal Risk Assessment process that includes the Luma system and associated risks

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management (SCO) should formally implement a Risk Assessment process that includes the Luma system as a critical technology to assess, to be performed at least annually. The organization should ensure that information risk management components are based on a standard-aligned framework that is comprehensive in relation to the nature of the business's systems and operations. We recommend utilizing the NIST SP 800-30's guidance on performing risk assessments. Management should ensure that the assessment performed results in the update or creation of a risk register. The risk register should be maintained on a continuous or frequent basis to ensure that updates are made to formally define risks to the organization through a process that identified internal and external threats, asset vulnerabilities, likelihood of a threat event, and the impact of a potential threat event (with consideration to Luma, especially).

SCO should lead the effort on ensuring an integrated information risk assessment is performed on an annual basis that incorporates the reliance upon third parties and internal teams with respect to a standard-aligned framework. A third party consultant can be utilized to assist with the completion of the assessment, but there are several resources available to assist the SCO with coordinating the assessment, such as the NIST 800-30 special publication on completing risk assessments. The results of the assessment should be documented and a register should be maintained to track remediation efforts or action plans in relation to identified risks.

Risk assessment results, including validation and mitigation, should be documented, analyzed, and approved by the SCO prior to finalizing and commencing action plans. Risks should be reassessed periodically or to address changes to the system, its environment of operation, or other conditions that may affect the security or privacy state of the system.

Further, management should design and document a formal risk management policy that details the organization's risk tolerance. The policy should be reviewed and approved on an annual basis.

Tolerance levels for risk should be classified and given stringent requirements in terms of risk acceptance procedures and key stakeholders that must be present in order to sign off on a risk. For example, risks that are determined to have a specific level of impact or likelihood would either require a sign-off from Luma or IT stakeholders, or if more severe, require a documented approval from the leadership team.

MANAGEMENT VIEW: *SCO has completed several partial informal Risk Assessments to include a few informal communication related events. Most notable is the when creating the single sign on Enterprise Dashboard we informally analyzed the risk of having a single source that depended on statewide resources solely or to deploy a second source, also in the AWS GOV cloud to be as closely tied to the Infor tenant that Luma resides in. We went with the latter.*

CORRECTIVE ACTIONS WITH TIMELINE: *SCO has begun the process of risk analysis using Consequence-driven Cyber-informed Engineering (CCE) Accelerate methodology. This is developed by Idaho National Laboratory in conjunction with Battelle Energy and the United States Department of Energy and deployed via the Idaho Military Division as a statewide initiative. The scope of "Luma" is far too vast to do a single risk analysis so it will be broken down into Critical Functions and then each will get its own risk analysis. Even at that it is proving to be a very large scope so prioritization will be brought into the mix so that we can focus on most likely events first. The first outputs should not be expected before Jan, 1 2025 as this will take significant staff time required and that is in scarce supply at this time. Again, staff augmentation may be required to get a timely output.*

ANTICIPATED DATE OF REMEDIATION: *First outputs Jan. 2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit.

SUMMARY ISSUE #9: Establish and document an internal controls framework

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management should formally establish an internal controls framework, in which they identify all relevant risks to the organization (specifically in the lens of the Luma platform and business functions that operate through it) and any controls implemented to mitigate those risks (including what authoritative frameworks they were sourced from, if applicable).

The FISCAM framework may be the best place to start, and Baker Tilly recommends that system-level monitoring activities are implemented to ensure that controls are continuously evaluated for operating effectiveness and remediation efforts, where needed, are tracked through resolution.

Once established, a formal 'findings management' or 'issues management' policy and procedural document should be established to formally outline the procedure for identifying, analyzing root causes, responding to, and remediating control deficiencies, audit findings, and improvement opportunities.

MANAGEMENT VIEW: *As per Idaho Technology Authority (ITA) policy "P4140 – CYBERSECURITY FRAMEWORK", NIST is the accepted as the statewide Framework. SCO is interested in completing the transition from Legacy to Luma and maturing our position by adding the additional layers of the FISCAM framework.*

SCO does formally document the lifecycle of audit findings via ServiceNow incident tickets. This goes back to legacy applications but this is the first audit of the Luma application so there were no formal findings to document yet. This is a deficiency in the formal policy and procedures.

CORRECTIVE ACTIONS WITH TIMELINE: *The new Comprehensive Cybersecurity Policy will include this reference to FISCAM being the new framework going forward. SCO will also Formalize a policy and supporting procedures for identifying, analyzing root causes, responding to, and remediating control deficiencies, audit findings, and improvement opportunities.*

ANTICIPATED DATE OF REMEDIATION: *6/30/2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. The ITA is not specifically applicable to the SCO, as explained in the auditor's response to Summary Issue 5, and the SCO would need to specifically include those policies or a reference to them in the SCO policies. Additionally, we continue to assert that FISCAM requirements are all based on NIST standards so the comment that this is a more complex requirement is inaccurate and these standards should not add to the workload.

SUMMARY ISSUE #10: Enhance documentation of deprovisioning activities during the offboarding process, and consider implementing a periodic review process to ensure all terminations were deprovisioned in a timely manner

PRIORITIZATION RATING: Medium

SUMMARY OF RECOMMENDATION: Management should ensure that termination events reconcile to the listed dates within Luma and that deprovisioning activities occur within a timely manner following the listed termination date.

Management should also consider a detective process in order to reconcile whether terminated employees have had their access removed and their termination statuses appropriately updated. For example, a periodic review in which a listing of all users with a termination date within the calendar month, then manually validated by management to have been appropriately deprovisioned and the details of those activities are documented appropriately within the user's account records.

MANAGEMENT VIEW: *SCO uses the Security Access Request (SAR) form application as the "should-be" state of user access. Every time there is an update to a SAR form there is an audit of the status of the user and roles. SCO CSC Operations staff are the first stop in the processing of a SAR and at that time they have extensive procedures to follow that include validation that the subject of the SAR is in fact an Active employee in the Luma system. If not, then the SAR is sent back with notes saying such. This has been in place since shortly after go live.*

As far as off boarding when an employee reaches a status of Term-Final, all escalated Luma roles are removed such that the employee is only able to access W2 and historic paystub information. The employee's Luma "actor" is also disabled which will remove access from all Financial, Purchasing and Human Capital Management processing as well.

Process has begun as INC0127564. No due date assigned yet.

CORRECTIVE ACTIONS WITH TIMELINE: *The recommendation is to get employees deprovisioned in a timelier manner. There is an initiative to move the offboard from the "Term Final" status to the "Term Pending" status which will make deprovision timelier. There is a meeting for technical to introduce the solution to functional on 8/6/2024 to plan implementation and set timeline.*

ANTICIPATED DATE OF REMEDIATION: *This is in process and will be tracked as SNOW INC0127564. Should be complete before Jan 1 2025*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. We would like to point out that the activities described in Management View are primary activities that occur at the time of termination, not review (control) procedures intended to ensure that the expected activities occurred as intended. We are concerned that this is still a risk with no control feature included.

SUMMARY ISSUE #11: Establish a Business Continuity Plan and Disaster Recovery Plan(s)

PRIORITIZATION RATING: Low

SUMMARY OF RECOMMENDATION: Management should formally establish a Business Continuity Plan that cover business operations as whole. As part of the development of a business continuity plan, resources (i.e., hardware, devices, data, time, personnel, and software) should be classified and analyzed for criticality and business value in order to best develop business continuity plans. The plan should further establish redundancies in personnel and address the procedures for enacting the plan in case of disaster events and scenarios. Additionally, a process should be established to regularly review and approve the plans to ensure they remain aligned to business processes and goals. The BCP and DR plan should be tested on at least an annual basis, and incorporate a formally designed lessons learned process to assess whether any changes to existing plans should be made following the test performed.

Further, management should ensure that security incident recovery strategies are formally defined, well documented, and aligned to business continuity strategies. These recovery strategies should be reviewed regularly to identify areas for improvement and capture previous lessons learned during recovery exercises when evaluating improvements to the plan.

MANAGEMENT VIEW: *While there is not currently a formalized business continuity plan, SCO has experienced a couple of DR tests already. In one case, the ITS Agency lost connectivity to the internet taking the entire state network down from the Luma perspective. In another case, INFOR/AWS had an outage where the entire system was down. Unfortunately, neither outage was documented well enough to show our processes to the Auditors as both came very early on while Luma was still in "hyper care". ServiceNow tickets were opened and Service Tickets were opened with both ITS and Infor respectively; however, what lacked was documentation of root cause analysis from the "vendors".*

CORRECTIVE ACTIONS WITH TIMELINE: *SCO is developing a new Business Continuity Plan based on the changes as a result of moving to a cloud-based software solution. With such a radical change in business operations, the process required additional time to fully understand our goals, lessons learned, and potential recovery strategies. SCO maintained an extensive business continuity plan under the previous systems environment and is committed to ensuring the services are established and enacted for future disaster events. In many aspects, the selection of a cloud-based service provider was influenced by the improved business sustainment options available versus an on-premise solution. Expected completion of plan is no later than 31 December 2025.*

ANTICIPATED DATE OF REMEDIATION: *12/31/2024*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. It should be noted that the SCO should clarify the expected date of completion as both 2025 and 2024 are identified.

SUMMARY ISSUE #12: Implement and re-evaluate potential for information spills and data losses with relation to the Luma system

PRIORITIZATION RATING: Low

SUMMARY OF RECOMMENDATION: Management should identify and determine whether implementing data loss prevention solutions or information spill protection within the Luma platform is necessary, or if there are any considerations for information loss.

If so, management should research data loss prevention solutions or additional security measures to protect against sensitive information leaks and spills.

MANAGEMENT VIEW: *SCO is implementing a DLP solution via Cisco Umbrella for SCO employees. SCO also utilizes full disk encryption on all SCO endpoints. Some other agencies do as well.*

SCO does not currently have access to the statewide network nor the does SCO have access to workstations statewide so there are limits as to what data loss prevention can be put into place.

SCO will work with Infor to identify options for data loss prevention tools that will work in conjunction with the Cloud suite product.

CORRECTIVE ACTIONS WITH TIMELINE: *SCO will work the based on priorities*

ANTICIPATED DATE OF REMEDIATION: *SCO will work this based on priorities*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit.

SUMMARY ISSUE #13: Establish data flow diagrams and strengthen documentation to describe the flow of data to, through, and from the Luma platform

PRIORITIZATION RATING: Low

SUMMARY OF RECOMMENDATION: Management should establish data flow diagrams and information exchange documentation (sourced from Interface specification documentation or architectural diagrams) that are reviewed and updated on an annual basis, or as major changes occur. Alternatively, the understood data flow should be documented within one of the newly developed policies or existing policies, and can be reviewed as changes to the expected data flows are made.

MANAGEMENT VIEW: *This recommendation builds from the formalization of the business process and interface specification documentation outlined in RECOMMENDATION #1. In concert with the formalization of the business process and interface specification documentation, the effort will seek to include data flow diagrams and included as part of the annual review.*

CORRECTIVE ACTIONS AND TIMELINE: *The initial goal is to get the process documentation formalized and published and complete a review of all existing interfaces (approximately 165) by 31 December, 2025. Once that is complete, an annual schedule will be established to collaborate with interface owners to ensure requirements, documentation, and existing processing parameters continue to meet expectations.*

- *Establish annual schedule no later than 31 December 2025.*

ANTICIPATED DATE OF REMEDIATION: *Establish annual schedule no later than 31 December 2025.*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit.

SUMMARY ISSUE #14: Establish a SOC Report Review process with relation to the Luma platform as hosted and provided by Infor

PRIORITIZATION RATING: Low

SUMMARY OF RECOMMENDATION: Management should perform a formal SOC report review over the Infor SOC2 report on an annual basis (in accordance with issuance dates by the service organization). The scope of the review should be to perform the following:

1. Evaluation of any identified exceptions within the report or noted qualifications on the issued opinion.
2. Mapping of CUECs (Complementary User-Entity Controls) to existing controls or processes in the SCO environment.

The review should be documented and retained over a time period appropriate for management's requirements to reproduce such records as needed.

MANAGEMENT VIEW: *The request is to formalize and document the SOC review over the SOC2 reports for cloud service providers to identify and evaluate controls to make sure they are adequatly covered. This will be a new process.*

CORRECTIVE ACTIONS AND TIMELINE: *SOC review will begin by Oct 2024*

ANTICIPATED DATE OF REMEDIATION: *SOC reviews will begin by Oct. 2024*

AUDITOR'S RESPONSE: We thank the State Controller's Office for cooperation and assistance throughout the audit. The contracting audit firm offered a template to aid in the review of the SOC report and we encourage the SCO to take advantage of this tool.