



Office of Budget and Management Supplier Operations - Supplier Portal Audit

Audit Period: July through September 2018

Results Summary:

Objective	Conclusion
Security of Sensitive Supplier Information once received through the Supplier Portal	Major Improvement Needed

* Refer to Appendix A for classification of audit objective conclusions.



Executive Summary

Background

The Office of Budget and Management (OBM) has the authority to operate a shared services center for the purpose of consolidating common business functions, including establishing methods to ease operations for suppliers dealing with the State. Suppliers or agencies can submit a request to Ohio Shared Services (OSS) to add new supplier information or to edit existing supplier information. The OSS Supplier Operations team is responsible for processing and maintaining supplier records in accordance with the standards and processes defined by OBM and providing supplier registration and maintenance services.

The Supplier Portal is a self-service application designed to provide suppliers with convenient access to information about their financial interactions with the State of Ohio. Users of the Supplier Portal can register to do business with the State or if the user's business is already registered, request to have a OH|ID associated with the business to view dashboards, view pending purchase orders, invoices and payment totals. The Supplier Portal was launched on July 9, 2018. As of September 11, 2018, 1,189 suppliers have self-registered and there are 2,080 unique users with those suppliers.

During the audit, OIA identified opportunities for OBM to strengthen internal controls and improve business operations. OIA conforms with the *International Standards for the Professional Practice of Internal Auditing*. OIA would like to thank OBM staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's Supplier Operations - Supplier Portal. This work was completed September through December 2018. The scope of this audit was Supplier Operations processes to include security of sensitive information.

The following was the objective of the review: Evaluate the design and effectiveness of controls to secure sensitive supplier information once received through the Supplier Portal.

Audit Period: September through December 2018.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. There were no low risk observations.



Observation 1 – Supplier Tracker Access

Effective business processes include documented policies and procedures, defining roles, determining appropriate access for the roles, assigning roles to employees, and periodically reviewing assigned roles. Management should review and update the policies and procedures to ensure they are current and relevant. Agencies should only collect, maintain, and use sensitive information that is necessary and relevant to functions that the agency is required or authorized to perform.

The Supplier Operations team verifies suppliers have entered their registration data completely and accurately through the Supplier Portal. The data has sensitive information including tax identification numbers and bank account numbers. The data is transmitted electronically to OAKS and to an internal SharePoint site, Supplier Tracker. Other sections of Shared Services provide support for supplier registrations, including call center operations and quality assurance reviews, necessitating access to the Supplier Tracker. However, OBM does not have controls in place to ensure access to supplier sensitive information is limited to employees that must access it to perform job duties. Specifically:

- All employees assigned access roles to the Supplier Tracker can view all sensitive information stored within the tracker, regardless of whether their work requires access to the sensitive information. As of November 2018, there were 43 employees with access to the Supplier Tracker.
- There are no periodic reviews of the employees with Supplier Tracker access to verify the employees still require access and the roles assigned to the employees are aligned with their job functions. One employee with access to the Supplier Tracker is no longer employed by OBM. The employee had been off-boarded upon leaving OBM and no longer has an active directory account, prohibiting the employee from accessing the Supplier Tracker. Another employee with access to the Supplier Tracker has changed jobs within OBM and no longer requires access.

Semi-annually, OAKS FIN Assurance requires agencies to review the OAKS FIN roles assigned to the agencies' employees. OAKS FIN Assurance provides the agencies a spreadsheet listing each agency's employees with OAKS FIN access and the assigned roles. However, the list of roles is not complete. OIA compared the roles assigned to Supplier Operations staff to the spreadsheet provided by OAKS FIN Assurance and six of 13 roles were not included in the spreadsheet. Therefore, OBM cannot rely on the spreadsheet to completely review employees' FIN access roles for appropriateness.

Failure to properly safeguard sensitive information and limit access to employees that need it to perform job duties may result in loss, theft, or unauthorized disclosure of sensitive



information. Lack of periodic reviews of access to sensitive information increases the risk of sensitive information being lost or stolen.

Recommendation

Limit access to supplier sensitive information in the Supplier Tracker to employees that need access to sensitive data to perform job duties. Implement periodic reviews of the assigned access and access roles to ensure the employees assigned access require continued assignment of the access and access role assigned to them. Remove employees' access if no longer needed to perform job duties. Periodically review procedures developed to determine if effectively ensuring the safety of the sensitive information maintained in the Supplier Tracker.

Consider implementing an additional periodic review of OAKS FIN roles to ensure all roles assigned to staff members are appropriate. Document lists of standard roles the agency's sections should be assigned and verify the roles assigned agree with the standard roles. Document performance and results of the review, including explanations for roles assigned in addition to the standard roles.

Management Response

OBM agrees with the recommendation and is taking steps to limit access to supplier sensitive information in the Supplier Tracker to employees that need access to sensitive data to perform job duties. We will also put in place a procedure that provides for periodic reviews of the assigned access and access roles to ensure the employees assigned access require continued assignment of the access and access role assigned to them and remove employees' access if no longer needed to perform job duties as well as a process to ensure we periodically review the procedures developed to determine if effectively ensuring the safety of the sensitive information maintained in the Supplier Tracker.

We will also discuss and consider the recommendation of implementing an additional periodic review of OAKS FIN roles to ensure all roles assigned to staff members are appropriate.

Risk*	Remediation Owner	Estimated Completion Date
High	Interim Deputy Director of OSS	January 25, 2019

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Please refer to Appendix A for classification of audit objective conclusions.



Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee