OBM | Office of Internal Audit

Department of Higher Education

Change Management Audit

Audit Period: June through September 2018

Results Summary:

Objective	Conclusion
Change Management	**Improvement Needed**

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

Report number: 2019-DHE-20

Issuance date: September 20, 2018

Executive Summary

Background

The Ohio Department of Higher Education is a cabinet level agency for the Governor of the State of Ohio that oversees higher education for the State. The agency's main responsibilities include authorizing and approving new degree programs, managing state-funded financial aid programs and developing and advocating policies to maximize higher education's contributions to the State and its citizens.

Change management is the process that ensures that all IT system changes are processed in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. The main purpose of change management is to enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

During the audit, OIA identified opportunities for DHE to strengthen internal controls and improve business operations. A summary, along with detailed observations, has been provided. This audit conforms to the *International Standards for the Professional Practice of Internal Auditing.* OIA would like to thank DHE 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 were engaged to perform an assurance audit related to the controls over the agency's change management process. This work was completed July through September 2018. The objective of this audit is as follows:

- Perform a review of the change management process to provide assurance that the process is controlled, monitored and is in compliance with good practices.

The detailed scope of the engagement is as follows:

- IT change requests submitted during FY18.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Developers Have Access to Production

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standards state that the agency should implement "separation of duties which addresses the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion."

During our review, we noted that limited controls are in place to restrict access between the development environment and the production environment. Developers are permitted to both develop changes and place the resulting code into production.

Lack of adequate controls regarding implementing changes to production can result in ineffective changes, functionality not meeting requirements/objectives, or a service disruption to the application.

Recommendation

Developer access to the production environment should be removed. Management should investigate the possibility of assigning production responsibilities to a dedicated resource. The individual promoting to production should not have responsibilities for development. The developer may write the script so another person who is not a developer may promote to production. As part of ensuring separation of duties, the responsibilities for promoting to production should be formally documented.

Also, management should ensure access to systems is documented via an approval process. Documentation should include the name of the user, the approver, the time/date that access was approved, and the rationale for granting access. In addition, a procedure describing the steps for provisioning users should be created.

Management Response
Management will investigate separation of duties developers have in the production environment. Management will add a new item to the change management SOP which accounts for identifying developer vs person responsible for deploying code; if these values are the same and exception from management must be approved with proper justification.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	December 2018

Observation 2 – Policies and Procedures

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standards state that the agency should “develop and document procedures to facilitate the implementation of security controls,” the policies should be “reviewed and updated” at an “agency defined frequency.” Procedures should address “scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.” It also states, “the organizational risk management strategy is a key factor in establishing policy and procedures.”

Through review, OIA noted the following:

1. The Change Management Standard Operating Procedure (SOP) is currently in the process of being developed by DHE management following a recent upgrade.

2. The SOP is limited in detail and does not allow for a person new to the process to adequately perform the function. Details such as how to assess risk, approve a change, prioritize changes, test a change, the Change Approval Board’s (CAB) role, when to obtain CAB approval, and criteria used to determine a change is an emergency are not addressed by the SOP.

Management does not have a formally approved change management policy since the ServiceNow upgrade. In the event of a change of staff, there would be no formal guidance on what processes to follow, potentially leading to activities not being performed or gaps in performance expectation. Without proper management of change management controls, there is a risk that changes are not being properly developed and implemented. Unless roles and responsibilities are formally defined, full accountability for change management responsibilities may not be possible.

Recommendation

Management should ensure policies and procedures for the change management function are clearly defined. This documentation should include more detail of each step in the process. Details should be added, such as the Change Approval Board's (CAB) role, how CAB assesses risk, prioritizes changes, and when changes require CAB approval.

Testing procedures should be documented in the change management procedure and include how tests are approved. Management should establish a policy review cycle so the policy is reviewed and (if necessary) updated on a regular basis to reflect any new business requirements. Evidence of review should be maintained. Once details have been finalized, the documentation should be approved.

Management Response

Management will ensure policies and procedures for the change management function are clearly defined in the new Change Management SOP. We will add more details such as the Change Approval Board's (CAB) role, how CAB assesses risk, prioritizes changes, and when changes require CAB approval.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	March 2019

Observation 3 – Lack of Formal Documented Testing Plans and Test Results

The State of Ohio IT Standard, ITS-SEC-02, identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls implementation for the State of Ohio. NIST standards state that the agency tests, validates, and documents changes tot he information system before implementing the changes on the operational system. The agency should "Plan the Change" and assure that the "Implementation Plan" document is completed. This document should include the back-out plan, test plans and results, customer notification list, and business owner approval.

During our review, OIA noted that the change management policy and procedures require documenting a test plan and test results as part of the implementation plan prior to implementing the changes on the production system. However, in the randomly selected sample of 17 (out of a population of 208) change requests evaluated, we noted that changes did not have formally documented test plans or test results that analyzed potential functional and security impacts.

Lack of adequate controls regarding documenting test plans and test results of changes prior to promoting to production can result in ineffective changes, functionality not meeting requirements/objectives, or a service disruption to the application.

Recommendation

Management should require test plans and test results to be included as part of the implementation plan document for all changes. Test plans should be in sufficient detail to enable comprehensive testing to be undertaken. Plans may also indicate the name of the person or department responsible for each test. Actual test results should be documented and compared against expected results. The test plans and test results should be referenced and attached to the change record in ServiceNow.

Management Response

Management will discuss with the CAB the options of creating test plans as part for each change and how those test results can be referenced within the change record in ServiceNow. Testing will require more involvement and accountability from the business owners as a result of this remediation plan.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	CIO	March 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.

* Refer to Appendix A for classification of audit observations.

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