OBM | Office of Internal Audit

Bureau of Workers' Compensation

IT - Cybersecurity - Identify & Recover Controls Audit

Audit Period: June through September 2018

Results Summary:

Objective	Conclusion
Cybersecurity Identify Controls	**Well-Controlled with Improvement Needed**
Cybersecurity Recover Controls	**Well-Controlled**

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

Report number: 2019-BWC-20 **Issuance date: September 20, 2018**

Executive Summary

Background

The Ohio Bureau of Worker's Compensation is responsible for providing workers' compensation insurance to all public and private employees except those that qualify for self-insurance. With assets of approximately $27 billion, BWC is the largest state-funded insurance system in the U.S. In addition, BWC is one of the top 10 largest underwriters of workers' compensation insurance in the nation. Insuring 244,000 Ohio employers, BWC provides insurance coverage to approximately 60 percent of Ohio's workforce.

Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks. To perform the engagement, OIA will leverage the Framework for Improving Critical Infrastructure Cybersecurity, which was produced by the National Institute of Standards and Technology (NIST). There are five categories to the framework including: Identify, Protect, Detect, Respond, Recover. This engagement will focus on the Cybersecurity Identify & Recover controls. The Identify function includes understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The Recover function develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that may be impaired due to a cybersecurity event.

During the audit, OIA identified opportunities for BWC to strengthen internal controls and improve business operations. A detailed listing of observations has been provided. This audit conforms to the International Standards for the Professional Practice of Internal Auditing. OIA would like to thank BWC 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 agency's controls over Cybersecurity Identify and Recover controls. The audit was performed between July and September 2018. The scope of this audit was a focus on the following functional areas of cybersecurity identify and recover: asset management, governance, risk assessment, risk management strategy, and recovery improvements and communications.

The following summarizes the objectives of the review:

- Evaluate the effectiveness of BWC’s Cybersecurity Identify and Recover Controls.

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 – Inadequate Communication and Maintenance of IT Policies

According to the NIST Cybersecurity Framework, GV-1, an organization's information security policy needs to be implemented and communicated appropriately to staff. Individuals with security responsibilities should review security policies when they join an organization and review updates to the information security policy when made.

OIA noted that new IT staff are not required to review IT information security policies when they join BWC. In addition, IT users are not notified when these policies are updated. The BWC IT policies do not show the name and role of the approver. Further, policies do not exist that formally govern the creation, approval, and review of IT policies.

Unless policies are reviewed by IT staff, individuals may not be fully aware of their responsibilities pertaining to information security. Further, without a formal process for creating, approving and reviewing IT policies, IT policies may not be maintained appropriately.

Recommendation

Management should ensure that all new IT employees review the IT policies for information security when they join BWC. A mechanism should be established that will track an acknowledgement that employees have reviewed the IT policies when they take a role in IT. Further, an acknowledgement should also be required when updates are made to existing IT policies.

In addition, management should ensure that IT policies document the name and role of the person approving them. When policies are reviewed, policies should include the date reviewed and a summary of changes made.

A documented process governing policy creation should be created that formally outlines roles and responsibilities for creating and reviewing policies. The frequency of policy reviews should be included in the process.

Management Response		
Management agrees and we will publish the IT policies to all employees again this month. In addition, we will update our onboarding process to formalize the communication of IT policies to all new IT employees and consultants.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
Moderate	CIO	November 2018

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