Ohio Department of Insurance
External Review System Audit

Audit Period: October through December 2018

Results Summary:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Review System Business Rules Process</td>
<td>Well-Controlled</td>
</tr>
<tr>
<td>User Access Security Controls</td>
<td>Well-Controlled with Improvement Needed</td>
</tr>
</tbody>
</table>

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

Background

The Ohio Department of Insurance (ODI) regulates the business of insurance in Ohio. Its mission is to serve and protect Ohio consumers through fair and efficient regulations, provide assistance and education to consumers, and promote a competitive marketplace for insurers. To carry out this mission, it licenses insurance agents and agencies, investigates allegations of misconduct by insurance agents or agencies, examines claims of consumer and provider fraud, and monitors the financial solvency and market conduct of insurance companies. The Department reviews insurance policies and forms used by insurance companies and the premiums they charge customers in the life, accident, health, managed care, and property and casualty insurance lines.

As of July 2018, ODI implemented Business Rules for the External Review (ER) System process for Independent Review Organizations (IRO) and Health Plan Issuers (HPI).

During the audit, OIA identified opportunities for ODI 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 ODI 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 External Review (ER) System process. This work was completed January through March 2019. The scope of this audit included the following areas:

- Independent Review Organizations (IRO) Reassignment of a Medical Case
- Resubmission of a Contractual External Review for Medical (IRO)
- External Community User Access and Security Roles

The following summarizes the objectives of the review:

- Evaluate the design and effectiveness of the business rules within the External Review System process.
- Evaluate the design and effectiveness of application security controls within the External Review System (related to user access and security roles)

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 – Periodic User Confirmation Review**

The State of Ohio IT Standard, IT-SEC-02, Enterprise Security Controls Framework, 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 800-53r4 AC-2 provides guidance that agencies should review accounts for compliance with account management requirements.

ODI Business Rules for External Review (ER) System External Community User Access Management states, “there is at least one Supervisory Contact established in the ER System for each HPI (Health Plan Issuer) and IRO (Independent Review Organization) Account. Supervisory Contacts are authorized by their organizations and have responsibility to provide new user access verification, including initial Role and Affiliation permissions (as applicable). Supervisory Contacts also have responsibility for notifying ODI of any changes to user information and access permissions (including user deactivation) for their organization.”

ODI utilizes Salesforce which is an external cloud-based customer relationship management application. Once a user has been verified and set up in Salesforce, they are granted indefinite access to Salesforce until the ER Administrator Support revokes access.

ODI currently does not perform a review of the contact user list within Salesforce to determine accuracy of user accounts to confirm active status of a HPI and IRO user account, ensure least privilege is implemented and user access is revoked when an employee is separated/transfered.

Lack of user confirmation for ER System user contacts increases the risk of users with improper access privileges beyond those necessary to perform their assigned duties. Furthermore, separated employees could potentially still have access to consumer CPI, PII and HIPPA data in the ER System. A single incident of compromised personal data can result in reputational damage to ODI, their affiliates, and the State of Ohio.

**Recommendation**

Develop additional Business Rule procedures to periodically confirm ER System user contacts along with their proper access and security role. Consider collaborating with ODI IT department to create a report using the Salesforce application that will allow user contacts to be sorted by their agencies, affiliations and other pertinent criteria for each HPI and IRO. Request each HPI and IRO Administrator Contact to perform an agency user confirmation and submit results to the ER Administrator Support when completed. Consider building upon the reconciliation procedures to ensure the process is performed in its entirety and any discrepancies discovered are corrected.

Also, consider creating a communication method (e-mail) to ensure all HPI and IRO Administrator Contacts are aware of procedures for submitting new requests, changes and updates for an ER
System user account. This will also allow ODI to emphasize the importance of the information housed within the ER System and how crucial revoking user access is when their employee no longer needs access.

These procedures should be reviewed by management on a periodic basis and updated when necessary to accurately reflect current practices.

### Management Response

ODI recognizes the need for periodic reverification of access to the ER System by IRO and HPI Account user contacts. The following activities are already in progress:

1. A “Periodic Account User Contact Reverification” procedure has been added to the current Business Rules for External Review (ER) System External Community User Access Management (see page 4-5 of Attachment A). Business Rules will be reviewed annually and updated as needed to reflect current practices.
2. Additional fields have been added to the HPI and IRO Account Detail pages in Sales Force to record the most recent user contact reverification date and the reverification calendar quarter assignment for each Account.
3. ODI IT Department has made extracted data available to the Business Unit to support efficient population of reverification worksheets with individual Account user contact information (including applicable access Roles and Affiliations).
4. Reports and dashboards are being developed in Sales Force by the Business Unit to monitor and validate reverification procedures.

ODI also recognizes the need to clearly communicate to HPI and IRO Administrator Account contacts procedures to notify ODI of updates to their ER System user contacts and the importance of maintaining current user contact information, especially with regard to deactivation when a user contact no longer needs access. The following activities are planned:

1. Management will work with the Business Unit to prepare an initial email communication for distribution to HPI and IRO Administrator Account Contacts.
2. Each newly designated HPI and IRO Administrator Account Contact will also receive the email communication.
3. The information provided in the email communication will also be added to online ER System user “Help” resources.
4. The link will also be included as a reminder in annual reverification communications to HPI and IRO Administrator Contacts.

Some of the remediation activities described above are already accomplished or in progress. ODI estimates that all planned remediation activities will be established and implemented as Business Unit procedures by April 30, 2019.

<table>
<thead>
<tr>
<th>Risk*</th>
<th>Remediation Owner</th>
<th>Estimated Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>ER System Business Unit Administrator</td>
<td>April 30, 2019</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Description of Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Well-Controlled</strong></td>
<td>The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.</td>
</tr>
<tr>
<td><strong>Well-Controlled with Improvement Needed</strong></td>
<td>The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.</td>
</tr>
<tr>
<td><strong>Improvement Needed</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Major Improvement Needed</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Classification of Audit Observations

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description of Factors</th>
<th>Reporting Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low</strong></td>
<td>Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.</td>
<td>Agency Management; State Audit Committee (Not reported)</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>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.</td>
<td>Agency Management and State Audit Committee</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.</td>
<td>Agency Management and State Audit Committee</td>
</tr>
</tbody>
</table>