OBM | Office of Internal Audit

Department of Developmental Disabilities Database Security Audit

Audit Period: October through December 2018

Results Summary:

Objective	Conclusion
Provide an independent assessment of the effectiveness of controls around database security and configuration	**Improvement Needed**

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

Report number: 2019-DDD-20 **Issuance date: December 13, 2018**

Executive Summary

Background

The Ohio Department of Developmental Disabilities (DDD) oversees a statewide system of supports and services for people with developmental disabilities and their families. DDD does this by developing services that ensure an individual's health and safety, encourage participation in the community, increase opportunities for meaningful employment, and provide residential services and support from early childhood through adulthood. The Division of Information and Technology Services (ITS) is responsible for creating and implementing the Department's IT security policy, developing and supporting business applications, managing the Department's IT infrastructure, and project and portfolio management for current and new IT projects. ITS services 88 county boards with more than 3,000 staff across six regions, and about $2.2 billion Medicaid benefits managed.

During the audit, OIA identified opportunities for DDD to strengthen internal controls and improve business operations. A summary, along with detailed observations, has been provided. OIA would like to thank DDD 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 DDD's database security process. This work was completed October through December 2018. The following summarizes the objectives of the review:

- Provide an independent assessment of the effectiveness of controls around database security and configuration

The scope of this audit included an evaluation of the following areas:

- Access authentication through unique user IDs and passwords.
- Password parameters meet industry standards.
- Authorization and restriction of privileged-level access.
- Appropriate implementation of the security configuration.

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.

Although the observations below are identified as high risk, OIA noted that these issues are not common across all databases. IT Management indicated that these databases are in the process of being migrated to a newer version and security controls will be tightened to align with best practices. As a result, the overall conclusion was "Improvement Needed" as indicated above.

Observation 1 – Inadequate Account Control and Monitoring - Offboarding

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-3 provides guidance that agencies should notify account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes.

During the audit, OIA noted that a former employee separated for approximately six months from DDD still had access to certain AD groups and elevated privileges.

The failure to disable or delete user accounts in a timely manner after separation increases the risk of unauthorized access to systems and sensitive data. Furthermore, insufficient routine reviews of user accounts increase the likelihood that inactive or inappropriate accounts will not be identified. Management should ensure that default accounts in all databases are disabled as part of standard procedures for creating databases. In addition, management should create documentation describing steps taken to create and maintain databases along with the responsibilities of specific roles.

Recommendation

When employees separate from DDD, ensure all access is revoked and their user account is properly removed from the database(s). Management should periodically reconcile user accounts to ensure correct access is maintained and revoked when needed.

Management Response
Identity Management practices continue to be enhanced as DODD migrates from its legacy domains to the State of Ohio domains. Once migrated to State of Ohio domains, as personnel is marked in OAKs, accounts are automatically disabled in ODX and downstream. Domains specific to DODD will be decommissioned. Additionally, the account in question has already been addressed as a part of INC2511784.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	June 30, 2019

Observation 2 – Lack of Data Encryption for Sensitive Information

The State of Ohio IT Standard, ITS-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. Per control SC-28 of the NIST 800-53 framework, information systems should protect the confidentiality and/or integrity of data at rest. One method of protecting sensitive data at rest is by using encryption.

OIA observed that DDD stores Health Insurance Portability and Accountability Act (HIPAA) data within certain databases. Through review, it was noted that data encryption is not enabled on these databases. Per discussion, DDD indicated that the systems are in the process of being migrated to a newer version, which resulted in encryption settings to not be enabled. HIPPA regulates consumers' Protected Health Information (PHI), which is individually identifiable health information. This includes, but is not limited to, consumer's vitals (name, phone number, address), and past, present, or future physical or mental health or condition of an individual.

Lack of encryption on sensitive information may lead to data being exposed in the event of a security breach. Date of birth Information could be leveraged, along with an individual's name, for identity theft. Unless PHI data is encrypted, dates of birth, social security numbers and other sensitive information could be accessed or viewed without a business need.

Recommendation
Management should ensure Protected Health Information (PHI) related data is encrypted. To increase the likelihood that sensitive data is adequately encrypted, management should develop

standards that provide written guidance on when encryption is required and periodically monitor that the procedures are being followed.

Management Response

DODD has encrypted most of its databases. The remainder are being encrypted as a part of completing the migration of all databases to its new environments. It is a part of project #2019248210.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	March 31, 2019

Observation 3 – Accounts have Excessive Database Role Access

The State of Ohio IT Standard, ITS-SEC-02, Enterprise Security Controls Framework, identifies the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the framework for information security controls implementation for the State of Ohio. According to control AC-6 of the NIST 800-53 framework, organizations should use the principle of least privilege, which allows only access for users that are necessary to perform tasks that are relevant to their business duties.

Individuals having database owner access have many privileges within the database including but not limited to creating, altering, and dropping tables or procedures, executing access, truncating tables, changing recovery model, and backing up or dropping the database as well as ability to modify database security. This role can also provide access to insert, update, and delete data in a database.

Through review of database roles granted, OIA identified certain roles and access levels that were not appropriate. The specific roles and access levels were provided to DDD IT management.

The risk of granting elevated access on database servers is that any individual with this access can perform any action on a server, including deleting and altering databases. Unless the database owner, data writer, and schema access are restricted appropriately, accounts without a business need for this access can make substantial changes to databases.

Recommendation

Management should ensure that role access is limited to only individuals with a key business need. In addition, only accounts with a need for database owner or data writer access should have this capability. Further, management should formally define roles and specific access that is required for IT staff in policies and procedures, based on the job functions that they perform. This information should include standards for database access, database owners, database owners of schemas, and data writers. These standards should be implemented for all DDD databases.

Management Response

ITS continues to review and enhance its databases as it migrates to its new environments as a part of project #2019248210. Prior to a database migrating to a new environment, central office user roles will be added into the identity management solution which includes user/role review and approval of access. Additionally, the items in question are being addressed as a part of INC2537141.

Risk*	Remediation Owner	Estimated Completion Date
High	CIO	June 30, 2019

Observation 4 – A Default Account was Enabled on a Database

The State of Ohio IT Standard, ITS-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. According to control AC-2 from the NIST 800-53 framework, accounts should be disabled in accordance with organization-defined procedures. A commonly used best practice for information systems is to disable accounts when not needed, such as 'default' accounts.

Through discussion, OIA observed that a default administrator account was enabled on the master database. The account is windows password policy enforced, but the password expiration date is not enforced. Moreover, we noted that the password for this account was last changed in May 2016. DDD advised the account should be disabled.

Allowing default accounts to be enabled in a database presents a risk of unauthorized access to data. Inadvertent or intentionally malicious actions, such as inappropriate access to data, could occur while a user is connected.

Recommendation

Management should ensure that default accounts in all databases are disabled as part of standard procedures for creating databases. In addition, management should create documentation describing steps taken to create and maintain databases along with the responsibilities of specific roles.		
Management Response		
ITS continues to review and enhance its databases as it migrates to its new environments as a part of project #2019248210. Prior to a database migrating to a new environment, account reviews will take place to ensure that only the necessary accounts and privileges which includes user/role review and approval of access. Additionally, the item in question is being addressed as a part of INC2537171.		
Risk*	**Remediation Owner**	**Estimated Completion Date**
High	CIO	June 30, 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