STATE OF CONNECTICUT

AUDITORS' REPORT
DEPARTMENT OF REVENUE SERVICES
INTEGRATED TAX ADMINISTRATION SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF MAY 2015

AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN ❖ ROBERT M. WARD

Table of Contents

STATE OF CONNECTICUT

AUDITORS OF PUBLIC ACCOUNTS

JOHN C. GERAGOSIAN

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

ROBERT M. WARD

September 22, 2015

AUDITORS' REPORT
DEPARTMENT OF REVENUE SERVICES
INTEGRATED TAX ADMINISTRATION SYSTEM
INFORMATION TECHNOLOGY SECURITY
AS OF MAY 2015

We have audited certain operations of the Department of Revenue Services Integrated Tax Administration System (ITAS) in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to, the period ending May 2015. The objectives of our audit were to:

1. Evaluate the department's internal controls over significant management and financial functions;

2. Evaluate the department's compliance with policies and procedures internal to the department or promulgated by other state agencies, as well as certain legal provisions; and

3. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the department, as well as certain external parties; and testing selected transactions. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

The State Auditors' Findings and Recommendations in the accompanying report presents any findings arising from our audit of the Department of Revenue Services Integrated Tax Administration System.

COMMENTS

FOREWORD

The Department of Revenue Services (DRS) operates principally under the provisions of Title 12, Chapters 201, 202 and 207 through 229 of the General Statutes. The department is responsible for administering and ensuring compliance with applicable provisions of this title and certain other statutes related to the assessment and collection of taxes. Major functions of the department include collecting and processing tax revenues, developing tax regulations and providing information and services to taxpayers.

Records pertaining to sales taxes collected by the Department of Motor Vehicles but credited to the Department of Revenue Services are examined as part of our audit of the Department of Motor Vehicles.

Section 12-1a of the General Statutes provides that the department is under the direction of a commissioner. Kevin B. Sullivan was appointed commissioner, effective January 10, 2011, and served in that position throughout the audited period.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our review of the controls environment of the Department of Revenue Services Integrated Tax Administration System revealed certain areas warranting attention that are discussed in the following findings.

User Account Setup and Separation of Duties

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53).

Control AC-02, Account Management, requires the organization to create, enable, modify, disable and remove information system accounts in accordance with organization-defined procedures or conditions.

Control AC-06 (7), Least Privilege-Review of User Privileges, requires the organization to review the privileges assigned, validate the need for such privileges, and reassign or remove privileges, if necessary, to correctly reflect organizational mission/business needs.

Control AC-05, Separation of Duties, requires the organization to:

a. Separate organization-defined duties of individuals;

b. Document separation of duties of individuals; and

c. Define information system access authorizations to support separation of duties.

Condition: The department's policies governing how a user's level of access should be assigned are described in a two-page document. This document contains two sentences governing front-end access and one sentence governing back-end access.

We were informed that the help desk assigns access levels to users based on the access levels of similar employees.

We were also informed that while user activity is monitored, no periodic reviews of user access levels are performed.

The department does not have any formal, written separation of duties policies.

The department does not have the ability to identify the full extent of the authorized functions of each user class through the use of security configuration tables within the ITAS database. Authorized actions are only partially stored within the database, requiring programming code on every page to be analyzed in order to identify what users can access.

Effect: The department's lack of sufficient formal procedures governing the configuration, assignment, and review of user access levels increases the chances that inappropriate access could be assigned to users and could go undetected and repeated.

The department is unable to compare available configurations of user access levels with separation of duties policies because the department has not drafted such policies. The ability to quickly identify all capabilities of each user class, and therefore each user, is also inhibited by the fact that no single report can identify this information. Instead, programming code must be reviewed on an object by object basis.

The department is at an increased risk of configuring levels of access that are excessive for any one user. If such access were assigned to a user, the user could then carry out actions from start to finish that might benefit the user or other individuals.

The department is not in compliance with NIST SP 800-53 access controls AC-02, AC-05, or AC-06 (7).

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should develop formal, written procedures governing the configuration, assignment, and review of user access levels, and separation of duties policies for ITAS. (See Recommendation 1.)

Agency Response: "The department agrees with this recommendation and initiated implementation in January 2015."

Shared Use of Computers

Criteria: The National Institute of Standards and Technology (NIST) recommends various identification and authentication controls (IA) in its special publication 800-53 (SP 800-53). Control IA-02, Identification and Authentication, requires that the organization's information system uniquely identify and authenticate organizational users.

Condition: In our analysis of certain types of Internet activity of DRS employees, we found instances in which two or more employees shared the same computer while using the same Windows session. Specific results were distributed to the agency and investigated. While no questionable or shared ITAS activity occurred in the instances identified, these instances nevertheless represent violations of agency policy, which requires that employees not share their computers with other individuals.

As a secondary method of detecting possible instances of password sharing between employees, we compared ITAS login records with Core-CT attendance records for the period of January 2012 through September 2013 and found numerous situations in which an employee used ITAS on a day when attendance records show they were physically away from work.

Upon giving the results of this second analysis to the department for investigation, they confirmed one of the employees shared their password. The department reported to us that the other instances identified are most likely limited to time reporting errors on the employees' timesheets based on interviews with the employees involved.

Effect: When two or more employees use the same computer and the same Windows session, employees can use one another's ITAS credentials to carry out unauthorized actions. Because there is evidence of users sharing accounts, it appears that NIST SP 800-53 control IA-02, Identification and Authentication, has not been fully implemented; therefore, users are not being uniquely identified.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to clarify its policies relative to the shared use of computers and implement controls to detect violations. (See Recommendation 2.)

Agency Response: "The department agrees with and will implement this recommendation."

Least Privilege

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53).

Control AC-06, Least Privilege, requires the organization to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

It also states that organizations should “consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege.”

Role-based access control (RBAC) helps to achieve least privilege. NIST created an RBAC model to provide a standard definition of RBAC features, which was formally adopted by the International Committee for Information Technology Standards (INCITS) and codified as INCITS 359-2004.

One RBAC standard is that user-role and permission-role assignment can be many-to-many.

Condition: The department’s ITAS system does not allow for a many-to-many relationship between users and roles. Users can only be assigned to one role. Therefore, user access levels throughout the entire system are determined by a single value.

Through an analysis of user activity, we found significantly varied uses of ITAS, in terms of windows accessed, among employees coded to the same user class and having the same privileges. While it is not necessarily a security concern that an employee can see or use a window that is not required for the employee’s assigned tasks, this does conflict with the concept of least privilege.

Effect: The department’s system uses a rigid method of role-based access control that does not conform to RBAC standards as defined by INCITS 359-2004. The department is not able to limit user access as specifically or variably as it could if the system’s design adhered to the NIST RBAC model.

The department is not in compliance with NIST SP 800-53 control AC-06, Least Privilege, because several user classes authorize access to windows that are not actually used by many employees in their class.

Cause: We were informed by the department that ITAS was not designed to conform to RBAC standards. The extensive modification necessary to have ITAS conform to RBAC standards is not feasible. This functionality will not be available until a new system is purchased.

Recommendation: The Department of Revenue Services should work toward conforming to the NIST RBAC model, which would make the varied configurations needed within each class more attainable. (See Recommendation 3.)

Agency Response: "The department agrees with this recommendation. The department agrees it must provide access to IT systems based on the principle of least privileged. However, NIST does not require the department to adhere to RBAC standards. The department will consider a form of role-based access controls when a new tax administration system is purchased."

Timely Disabling of Access Privileges

Criteria: The National Institute of Standards and Technology (NIST) recommends various personnel security controls (PS) in its special publication 800-53 (SP 800-53).

Control PS-04, Personnel Termination, requires the organization to disable information system access within an organization-defined time period for each instance of an employee termination. It is good business practice for that action to be carried out on the employee's last day of work.

Condition: In our review of 90 employee separations that occurred between January 2012 and September 2013, we found that in 45 instances (50%), the employee's user account had not been disabled between 2 and 70 business days after the termination date. On average, these accounts were disabled 22 business days after the employee's termination date.

Effect: We were able to determine that none of these employee accounts were used to access ITAS after their dates of separation and other controls exist to prevent terminated employees from using the system, such as the disabling of the their access cards or removal of their computer. However, this particular control failed at a high frequency.

The department is not in compliance with NIST control PS-04, Personnel Termination.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to ensure that all ITAS user accounts are disabled in a timely manner. (See Recommendation 4.)

Agency Response: "The department agrees with and will implement this recommendation."

Ad Hoc Reporting

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) and audit and accountability controls (AU) in its special publication 800-53 (SP 800-53).

Control AC-06, Least Privilege, requires the organization to employ the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Control AU-06, Audit Review, Analysis, and Reporting, requires the organization to review and analyze information system audit records for inappropriate or unusual activity.

Condition: ITAS data is accessible in different ways: through the front-end application; through the back-end database; and users may also create ad hoc reports using Oracle Discoverer, a business intelligence application that can be used to visually construct queries against the database.

Out of 635 total ITAS users, we found that 119 have access to Oracle Discoverer and the ability to run ad hoc reports that have been made public or shared with them by other users. Out of the 119 users, 60 had access privileges with the ability to create or edit queries. Although only a few users within Discoverer can create joins between tables, the 60 users have the ability to query directly against individual tables within the database. These users can query against a few select tables and then join that information outside of Discoverer to piece together confidential taxpayer information.

These users have access to 457 database tables, some of which contain personally identifiable taxpayer information, such as Federal Employer Identification numbers (FEIN), Social Security numbers (SSN), names, addresses, and other information. Only limited knowledge of the table structure is required to access the confidential information because many of the table names identify what fields are likely included in each table.

In addition, the information accessed by ad hoc reports run through Discoverer is not monitored, while the same information when accessed in a different manner (through front end screens) is monitored.

Furthermore, if queries run through Discoverer do not hit any of the tables covered by the database logs, they are not logged at all.

Effect: The department has granted significant access to personally identifiable taxpayer information to some users through the Oracle Discoverer application, and when they use that application to access ITAS data, their activity is not monitored and very little of it is logged. The same information, when accessed in a different manner, is logged and monitored.

The department is not in compliance with NIST SP 800-53 control AC-06, Least Privilege and AU-06, Audit Review, Analysis, and Reporting.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should limit user access in Oracle Discoverer and ensure that user activity is logged and monitored. (See Recommendation 5.)

Agency Response: "The department agrees with this recommendation, in part. The department agrees to research the ability to increase logging capabilities. However, the department approves the existing list of employees who currently have access. The purpose of Ad Hoc reporting is to provide business users with information, based on set criteria, that enables them to perform their job responsibilities. Each of the current employees with access to Ad Hoc Reporting has a business need for that access."

Auditors' Concluding Comments: We are not questioning the business need for ad hoc reporting. We are concerned about the significant access to personally identifiable taxpayer information granted to these users without similar logging and monitoring that is applied to all users of the front-end application.

Documentation of User Access Authorizations

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53).

Control AC-02, Account Management, requires that organization-defined personnel approve requests to create information system accounts, and that each account's access to the information system be based on valid access authorization.

Condition: We requested documentation to support the current information system access levels of ten sampled employees. The department was able to substantiate current access levels with valid access authorizations for three of the ten employees. Access levels for seven of the ten employees were unsubstantiated by an access authorization. It is unclear whether the department ever documented the authorizations or misplaced the documentation.

Effect: The department's ability to review the authorization of assigned access levels for its employees is impeded by the lack of documentation indicating why each employee currently has the access that they do.

The department is not in compliance with NIST SP 800-53 control AC-02, Account Management.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to ensure that supporting documentation validating the authorization and need for system access is maintained for all information system access granted to employees. (See Recommendation 6.)

Agency Response: "The department agrees with and will implement this recommendation."

Logging of Changes to User Access Levels

Criteria: The National Institute of Standards and Technology (NIST) recommends various audit and accountability controls (AU) in its special publication 800-53 (SP 800-53).

Control AU-02, Audit Events, requires that the information system be capable of auditing organization-defined auditable events. The organization is to define those events that are significant and relevant to the security of the information system as audit events.

Changes to user access levels constitute events that are significant and relevant to the security of information systems.

Condition: The department's audit trail does not capture changes to logical access restrictions at the application or system level.

Effect: The department is not in compliance with NIST SP 800-53 control AU-02, Audit Events.

The department is unable to analyze logs of changes to user access levels for suspicious activity, such as multiple changes in the same day or in a short time frame, because such logs are not generated.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to expand the coverage of its audit trails to include changes made to user access levels. (See Recommendation 7.)

Agency Response: “The department agrees with this recommendation and already completed implementation on March 17, 2014.”

Monitoring of Database Access Logs

Background: Fine-grained audit logging, unlike standard database logging, allows organizations to capture structured query language (SQL) statements run by users based on defined policies related to the type of statement run, the objects accessed by the statement, and other factors. Standard database logging does not capture the SQL statements. This is a unique feature of fine-grained audit logs.

Criteria: The National Institute of Standards and Technology (NIST) recommends various audit and accountability (AU) controls in its special publication 800-53 (SP 800-53). Control AU-06, Audit Review, Analysis, and Reporting, requires the organization to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity and for those findings to be reported to organization-defined personnel.

Condition: The department has implemented fine-grained audit logging, which are provided to the Internal Audit Unit on a monthly basis. While some steps are performed to verify and review the logs on a monthly basis, the current process does not include an analysis of the SQL statements run by users.

Effect: This control does not allow for the detection of abuse by the 40 back-end users of ITAS because the logs are not reviewed for abuse unless abuse is detected elsewhere. These users can use the back-end database to access taxpayer personally identifiable information without oversight, because unless they accessed that same information through a different means, no one in the department would review the fine-grained audit log.

The department is not in compliance with NIST SP 800-53 control AU-

06, Audit Review, Analysis, and Reporting.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should strengthen its internal controls with respect to its review of fine-grained audit logs. (See Recommendation 8.)

Agency Response: “The department agrees with this recommendation and is in the process of implementation.”

Audit Log Configuration

Criteria: The National Institute of Standards and Technology (NIST) recommends various audit and accountability controls (AU) in its special publication 800-53 (SP 800-53).

Control AU-02, Audit Events, requires that the information system be capable of auditing organization-defined auditable events and that the organization review and update the audited events to account for necessary changes over time.

Condition: The Department of Revenue Services employs fine-grained audit logging (FGA) on its back-end ITAS databases. FGA logs are populated based on audit policies defined by the organization. The effectiveness of this logging functionality depends on the adequate configuration of those policies.

We found several weaknesses in our review of the FGA policies configured by DRS in its back-end databases. For confidentiality reasons, we cannot disclose those specific weaknesses in our public audit report, as it could compromise the department’s data security.

Effect: There are 40 employees who are able to access the ITAS data using the back-end databases, and these deficiencies enable them to obtain personally identifiable information of any taxpayer with minimal oversight or audit log records generated.

The department is not in compliance with NIST SP 800-53 controls AU-02, Audit Events.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should strengthen its controls over database audit logging and periodically review and update the

FGA audit policies. (See Recommendation 9.)

Agency Response: "The department agrees with this recommendation and is in the process of implementation."

Recording of User Logins

Criteria: The National Institute of Standards and Technology (NIST) recommends various audit and accountability (AU) controls in its special publication 800-53 (SP 800-53). Control AU-02, Audit Events, requires the organization to determine that the information system is capable of auditing failed login events.

Control AU-03, Content of Audit Records, requires the information system to generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Condition: Logins are not recorded, with respect to who logged in, who attempted to login, under what username, at what time, from what location, or for how long. This deficiency is present at the database level of the ITAS data.

Effect: The department is unable to analyze login records for suspicious activity because such records do not exist.

The department is not in compliance with NIST SP 800-53 controls AU-02, Audit Events, or AU-03, Content of Audit Records.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to implement the recording of all successful and failed logins at the database level. (See Recommendation 10.)

Agency Response: "The department agrees with this recommendation and already completed implementation on March 5, 2014."

Database Account Lockouts

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53). Control AC-07, Unsuccessful Login Attempts, requires the organization to define and enforce a limit of consecutive invalid login attempts by a user during a specified time period and automatically lock out the user for a specified time period when the maximum number of unsuccessful attempts is exceeded.

Condition: At the database level, users are not locked out for any period of time after a set number of failed login attempts.

Of the 635 ITAS users, 40, or approximately 6.3 percent, have access to the back-end database where this control deficiency exists.

Effect: Access controls at the database level are weakened.

The department is not in compliance with NIST SP 800-53 control AC-07, Unsuccessful Login Attempts.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to improve its database access controls by locking accounts after a set number of failed login attempts. (See Recommendation 11.)

Agency Response: "The department agrees with this recommendation and already completed implementation on March 11, 2014."

Public User Role

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53). Control AC-06, Least Privilege, requires the organization to employ the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Condition: In our review of the back-end database user roles and privileges, we found that the PUBLIC role had been granted access to execute data definition language (INSERT/UPDATE/DELETE) statements against 47 tables used by Oracle BI Discoverer, an application that is used by the department to allow certain employees to run reports summarizing a variety of information contained in ITAS.

Effect: All 40 back-end users, including many who are business users not involved in database or application development, have access to create, add, change, or delete data contained in the Oracle BI Discoverer application tables. If they were to do so, the functionality and accuracy of Oracle Discoverer could become compromised.

The department is not in compliance with NIST SP 800-53 control AC-06, Least Privilege.

Cause: We were informed that the department did not manually make these grants and that the application granted the privileges on its own during initial setup. The department did not realize these privileges had been granted to the PUBLIC role upon installation.

Recommendation: The Department of Revenue Service should identify a way to configure Oracle Discoverer to operate without relying on the PUBLIC role holding these privileges, and then revoke these privileges from the PUBLIC role. (See Recommendation 12.)

Agency Response: "The department agrees with this recommendation and already completed implementation in March 2014."

Database Passwords

Criteria: The National Institute of Standards and Technology (NIST) recommends various identification and authentication controls (IA) in its special publication 800-53 (SP 800-53). Control IA-05, Authenticator Management, requires the organization to:

a. Enforce minimum password complexity, including requirements for case sensitivity; number of characters; mix of upper-case letters, lower-case letters, numbers, and special characters; and include minimum requirements for each criteria;

b. Enforce a minimum number of changed characters when new passwords are created;

c. Enforce password minimum and maximum lifetime restrictions;

d. Prohibit password reuse for a defined number of generations.

Condition: At the database level, passwords may be reused any number of times; they do not expire and are not bound by any complexity requirements.

Out of the 635 ITAS users, 40, or approximately 6.3 percent of all users, have access to the back-end database where this control deficiency exists.

Effect: Password controls at the database level are weak and could easily be compromised.

The department is not in compliance with NIST SP 800-53 controls IA-05, Authenticator Management.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to strengthen its database password controls. (See Recommendation 13.)

Agency Response: "The department agrees with this recommendation and already completed implementation in March 2014."

Access Cards

Criteria: The National Institute of Standards and Technology (NIST) recommends various physical and environmental (PE) controls in its special publication 800-53 (SP 800-53). Control PE-02, Physical Access Authorizations, requires the organization to:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;

b. Issue authorization credentials for facility access;

c. Review the list detailing authorized facility access by individuals; and

d. Remove individuals from the facility access list when access is no longer required.

Condition: At the time of our testing, August 15, 2013, we found an access card that was actively assigned to an employee who had been terminated on May 13, 2009. The former employee's access card was not deactivated in the 1,555 days since the termination, as of the time of our testing. In addition, the agency could not provide documentation to confirm whether the card was collected from the employee at termination.

The department does not monitor or review, at any interval, those individuals who have physical access to the building.

Effect: The department's lack of periodic reviews of those having physical access to its facilities increases the risk that unauthorized individuals might gain access.

While the agency reviewed and confirmed that this employee did not reenter the building after termination, the risk of unauthorized access remained.

The department is not in compliance with NIST SP 800-53 controls PE-02, Physical Access Authorizations.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should perform a periodic review of all active access cards to ensure that only necessary access cards remain active. (See Recommendation 14.)

Agency Response: “The department agrees with this recommendation and already completed implementation in August 2013.”

Data Center

Criteria: The National Institute of Standards and Technology (NIST) recommends various physical and environmental controls (PE) in its special publication 800-53 (SP 800-53).

Control PE-18, Location of Information System Components, requires the organization to position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Condition: The department’s datacenter has three separate entrances, one of which has a manual lock rather than a key card lock, and is more prone to a breach as manual locks can be picked.

Effect: The department’s datacenter is vulnerable to unauthorized access.

The department is not in compliance with NIST SP 800-53 control PE-18, Location of Information System Components.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to limit the number of entrances to its datacenter and fully secure each entrance. (See Recommendation 15.)

Agency Response: “The department agrees with this recommendation and already completed implementation on July 3, 2014.”

Disaster Recovery Plan

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning controls (CP) in its special publication 800-53 (SP 800-53).

Control CP-02, Contingency Plan, requires the organization to review the contingency plan at an organization-defined frequency, and update the contingency plan to address changes to the organization, information system, or operating environment and to address problems encountered during contingency plan implementation, execution, or testing.

Condition: At the time of our testing in November 2013, we found that the department's disaster recovery plan was last updated in January 2011.

Aspects of the current disaster recovery plan are outdated.

Effect: The lack of a current disaster recovery plan increases the risk that the department may not be able to resume operations in a timely manner in the event of a disaster.

The department is not in compliance with NIST SP 800-53 control CP-02, Contingency Plan.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to frequently review its disaster recovery plan and update it where necessary at a fixed and regular interval. (See Recommendation 16.)

Agency Response: "The department agrees with this recommendation and already updated the DRS Disaster Recovery Plan in December 2013, May 2014, September 2014 and April 2015."

Testing of the Disaster Recovery Plan

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning controls (CP) in its special publication 800-53 (SP 800-53).

Control CP-04, Contingency Plan Testing, requires the organization to:

a. Test the contingency plan for the information system to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Review the contingency plan test results; and

c. Initiate corrective action, if needed.

Condition: The department has not tested its disaster recovery plan, and has not defined an interval at which to test the plan or the methods to be used to test the plan.

Effect: The disaster recovery plan's effectiveness is uncertain because it has never been tested. In the event of a disaster, it is unclear what the outcome might be.

The department is not in compliance with NIST SP 800-53 control CP-04, Contingency Plan Testing.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should develop tests of its disaster recovery plan and procedures to conduct those tests at a fixed and routine interval. (See Recommendation 17.)

Agency Response: "The department agrees with this recommendation and already implemented a DRS Disaster Recovery Test Plan in December 2013. The department performed successful tests of the DRS Disaster Recovery Test Plan on May 19, 2014, September 8, 2014 and April 27, 2015."

Backup Location

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning controls (CP) in its special publication 800-53 (SP 800-53).

Control CP-06, Alternate Storage Site, requires the organization to establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information, and to ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

It also indicates that the alternate storage site should be separated from the primary storage site to reduce susceptibility to the same threats and to avoid accessibility problems in the event of an area-wide disruption or disaster.

Condition: The department's primary facility and backup storage sites are located too close to one another.

Effect: Any disaster affecting the general area of the department's primary location is likely to affect the backup location as well.

In the event of a disaster, the risk for complete data loss is increased.

The department is not in compliance with NIST SP 800-53 control CP-06, Alternate Storage Site.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should obtain an alternate backup site or contract with a vendor to arrange for the secure storage of system backup information. (See Recommendation 18.)

Agency Response: "The department agrees with this recommendation and already completed implementation on February 28, 2014."

Backup Tape Verification

Criteria: The National Institute of Standards and Technology (NIST) recommends various contingency planning controls (CP) in its special publication 800-53 (SP 800-53).

Control CP-09, Information System Backup, requires the organization to conduct backups of user-level and system-level information contained in the information system and to protect the confidentiality, integrity, and availability of backup information at the storage location. It further states that the organization should test backup information to verify media reliability and information integrity.

Organizations that conduct backups using tapes must track the location of each tape and the data that each tape holds in order to successfully conduct restoration procedures in a reasonable period of time.

Condition: In our review of 26 backup tapes recorded in the department's tape database effective November 14, 2013, the date of our testing, we found a non-existent tape that was incorrectly entered into the database, and two tapes that were physically misplaced, resulting in our inability to verify they were at the recorded location.

Effect: Inaccuracies in the tape tracking database and the misplacement of tapes can lead to delays in the execution of restoration procedures.

The department is not in compliance with NIST SP 800-53 control CP-09, Information System Backup.

Cause: The cause could not be determined.

Recommendation: The Department of Revenue Services should take steps to improve the accuracy of its tape tracking database and to prevent the misplacement of backup tapes. (See Recommendation 19.)

Agency Response: “The department agrees with this recommendation and already completed implementation on February 28, 2014.”

RECOMMENDATIONS

1. **The Department of Revenue Services should develop formal, written procedures governing the configuration, assignment, and review of user access levels, and separation of duties policies for ITAS.**

   Comments:

   We found that the department lacks sufficient formal procedures governing the configuration, assignment, and review of user access levels. Also, the department is unable to compare available configurations of user access levels with separation of duties policies because the department has not drafted such policies.

2. **The Department of Revenue Services should take steps to clarify its policies relative to the shared use of computers and implement controls to detect violations.**

   Comments:

   In our analysis of certain types of Internet activity of DRS employees, we found instances in which two or more employees shared the same computer while using the same Windows session.

3. **The Department of Revenue Services should work toward conforming to the NIST RBAC model, which would make the varied configurations needed within each class more attainable.**

   Comments:

   We found that access controls within ITAS do not allow for the level of control that would limit user access to screens required for the user's specific job function.

4. **The Department of Revenue Service should take steps to ensure that all ITAS user accounts are disabled in a timely manner.**

   Comments:

   Our testing revealed that some employee user accounts were not disabled in a timely manner subsequent to their termination.

5. **The Department of Revenue Services should limit user access in Oracle Discoverer and ensure that user activity is logged and monitored.**

   Comments:

We found that 60 users had access privileges with the ability to create or edit queries directly against individual tables within the database, which may contain confidential information, and that this activity was not monitored.

6. **The Department of Revenue Services should take steps to ensure that supporting documentation validating the authorization and need for system access is maintained for all information system access granted to employees.**

   Comments:

   The department could not provide documentation to support the ITAS access levels of seven out of ten users sampled for testing. It is unclear whether the department never documented the authorizations or misplaced the documentation.

7. **The Department of Revenue Services should take steps to expand the coverage of its audit trails to include changes made to user access levels.**

   Comments:

   We found that the department's audit trail does not capture changes to logical access levels at the application or system level.

8. **The Department of Revenue Services should strengthen its internal controls with respect to its review of fine-grained audit logs.**

   Comments:

   We found that while some steps are performed to verify and review the fine-grained audit logs on a monthly basis, the current process does not include an analysis of the SQL statements run by users.

9. **The Department of Revenue Services should strengthen its controls over database audit logging and periodically review and update the FGA audit policies.**

   Comments:

   We found that there were some users who are able to access the ITAS data using the back-end databases, which could allow them to access the personally identifiable information of any taxpayer.

10. **The Department of Revenue Services should take steps to implement the recording of all successful and failed logins at the database level.**

    Comments:

    At the database level, login attempts are not logged or monitored.

11. **The Department of Revenue Services should take steps to improve its database access controls by locking accounts after a set number of failed login attempts.**

    Comments:

    At the database level, users are not locked out for any period of time after a set number of failed login attempts.

12. **The Department of Revenue Services should identify a way to configure Oracle Discoverer to operate without relying on the PUBLIC role holding these privileges, and then revoke these privileges from the PUBLIC role.**

    Comments:

    During the installation of Oracle Discoverer, certain privileges were assigned to the PUBLIC role, therefore also granting these privileges to all database users.

13. **The Department of Revenue Services should take steps to strengthen its database password controls.**

    Comments:

    At the database level, passwords may be reused any number of times, they do not expire, and they are not bound by any complexity requirements.

14. **The Department of Revenue Services should perform a periodic review of all active access cards to ensure that only necessary access cards remain active.**

    Comments:

    We found that an access card was actively assigned to an employee who had been terminated on May 13, 2009.

15. **The Department of Revenue Services should take steps to limit the number of entrances to its data center and fully secure each entrance.**

    Comments:

    The department's data center has three separate entrances, one of which has a manual lock rather than a key card lock.

16. **The Department of Revenue Services should take steps to frequently review its disaster recovery plan and update it where necessary at a fixed and regular interval.**

Comments:

At the time of our testing, the department's disaster recovery plan was outdated, with the most recent partial update completed in January 2011.

17. The Department of Revenue Services should develop tests of its disaster recovery plan and procedures to conduct those tests at a fixed and routine interval.

Comments:

The department's disaster recovery plans have not been tested.

18. The Department of Revenue Services should obtain an alternate backup site or contract with a vendor to arrange for the secure storage of system backup information.

Comments:

We found that the department's primary facility and backup storage sites are located too close to one another to avoid a disruption or disaster from the same threat.

19. The Department of Revenue Services should take steps to improve the accuracy of its tape tracking database and to prevent the misplacement of backup tapes.

Comments:

We found that the database used to control backup tapes has incorrect information and that two backup tapes were physically misplaced.

CONCLUSION

In conclusion, we wish to express our appreciation of the cooperation and courtesies extended to our representatives by the personnel of the Department of Revenue Services during the course of our examination.

Bruce C. Vaughan

Bruce C. Vaughan
Principal Auditor

Approved:

Robert M Ward

John C. Geragosian	Robert M. Ward
Auditor of Public Accounts	Auditor of Public Accounts