CONSENT AGENDA ITEM

#11

protiviti
Risk & Business Consulting. Internal Audit.

MEMORANDUM

TO: CFX Board Members

FROM: Jeff Tecau, Protiviti

DATE: December 15, 2016

SUBJECT: Internal Audit Reports

Attached, please find the following Internal Audit reports as reviewed and accepted by the Audit Committee on December 15, 2016.

A. Public Records Review

B. DHSMV Data Security Assessment

Reviewed by: _____

Central Florida Expressway Authority

2017 Public Records Review

November 4, 2016

protiviti®

Face the Future with Confidence

Table of Contents

protiviti

Executive Summary

Background

As a public agency, the Central Florida Expressway Authority (CFX) is required to comply with Chapter 119 of the Florida Statute, Florida Public Records Law. The law provides that any records made or received by any public agency in the course of its official business are available for inspection, unless specifically exempted by the Florida Legislature. Public records include all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by CFX.

The CFX Records Management department consists of a Records Specialist and a Manager of Public Records, who also serves as the agency's Records Management Liaison Officer (RMLO) with Florida's Division of Library and Information Services. CFX selects Record Coordinators within each department to work with Records Management. The Records Management function and Record Coordinators are jointly responsible for maintenance, retention, preservation, and destruction of public records as required by the Public Records Law. CFX manages public records in various forms, including paper records, electronic documents, electronic mail (email), and text messages. CFX engages a document imaging vendor to microfilm permanent public records for preservation and an offsite storage vendor to store records with long-term or permanent retention. CFX uses a combination of the offsite storage vendor and a shredding vendor for public records destruction.

In accordance with the FY 2017 Internal Audit Plan, Internal Audit performed a review of CFX's process to manage public records, including electronic records management, record collection and document retention.

Objectives

The objectives of this review were to:

(1) Evaluate CFX's public records management policy and procedures to comply with public records laws surrounding custodial requirements, maintenance, preservation, retention, and destruction of public records;

(2) Assess the data retention processes, technologies, and software utilized to capture electronic records, such as mobile phone, email, and voice mail;

(3) Evaluate the Records Management and Coordinator training program;

(4) Benchmark CFX public records management policy and procedures with local industry practices.

Summary of Project Scope, Approach, and Results

Internal Audit evaluated CFX's public records management processes and internal controls for design effectiveness based on the requirements of the Florida Public Records Law. Based upon the work performed, Internal Audit identified eight opportunities that would strengthen CFX's overall public records management process and internal control environment. The table below provides an overview of the areas reviewed and opportunities identified.

Key Areas Reviewed	Procedures Performed	Number of Observations	Observation Reference
Policies and Procedures	✓ Reviewed CFX's public records management process to comply with the Florida Public Records statues surrounding custodial requirements, maintenance, preservation, retention, exemptions, and destruction of public records. ✓ Benchmarked CFX's public records policy and procedures, including training requirements, with other Florida-based tolling agencies.	1	1
Training & Awareness	✓ Determined how public records requirements are communicated to Authority employees, committee members, and the board of directors. ✓ Evaluate the public records management training procedures.	1	2
Technology	✓ Determined what technologies are currently utilized to retain electronic communication via mobile phone, email, and voice mail at CFX. ✓ Reviewed the configurations of identified technologies to determine how electronic communication is stored within each. ✓ Reviewed the processes in place to review the records that are captured and stored within CFX's environment.	2	3,4
Records Collection and Retention	✓ Reviewed CFX's records management process for organizing, identifying, and tracking offsite storage records.	2	5,6
Records Destruction	✓ Reviewed CFX's process and internal controls for destroying public records that have met retention requirements.	2	7,8
	TOTAL:	**8**	

Recommendations for Improvement

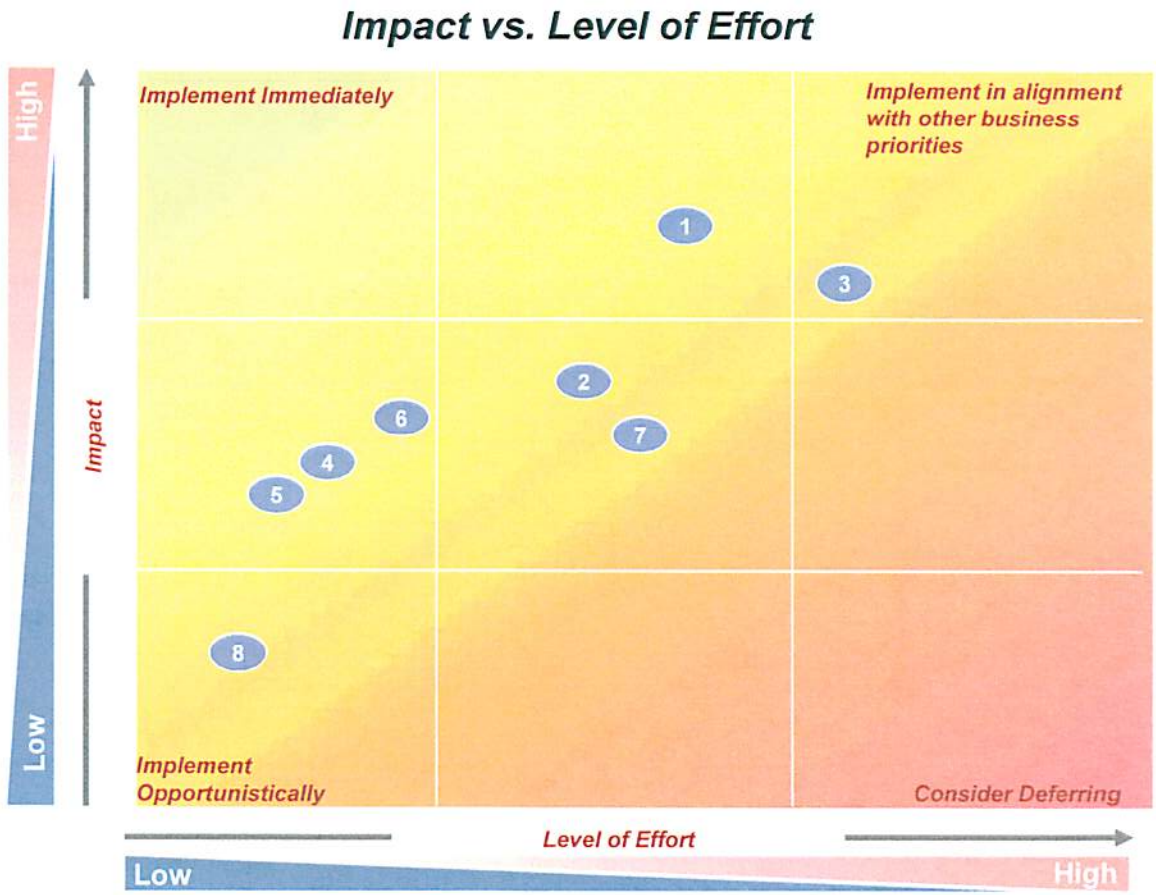
I. **Define Records Management Policy and Procedures**
   1. Revise records management policy and create desktop procedures

II. **Enhance Training & Awareness Program**
   2. Annual Record Coordinator training

III. **Enhance Technology**
   3. Update or replace outdated records management database
   4. Implement additional layers of protection for text message collection

IV. **Improve Records Collection and Retention Processes**
   5. Issue CFX electronic mail account to non-public board and committee members
   6. Develop a barcode tracking reconciliation

V. **Develop Records Destruction Processes**
   7. Limit record retention to required term
   8. Enforce offsite storage vendor contract compliance



Impact versus level of effort was judgmentally evaluated through joint discussions between CFX management and Internal Audit.

protiviti

Detailed Observations

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 1 – Records Management Policy and Procedures

CFX has a records management policy in place and a records management plan, which was created in 2011 by a third-party consultant to provide long-term, forward-looking guidelines and recommendations for governing CFX's records management program. The CFX records management policy contains portions of the records management plan.

CFX does not have a records management procedural document that provides the detailed records management practices that are currently in place.

Policies should contain clear, simple statements of how an organization or entity intends to conduct its operations and provide a set of guiding principles to help management with decision making, while procedures should help govern the actions necessary to fulfill the organization's policies for operations. Procedures containing an appropriate level of detail can help reduce misunderstanding and increase distribution of pertinent information to those involved in the process.

Recommendation

CFX should consider revising the records management policy to clearly state the direction of the Records Management function and create separate "desktop" procedures that clearly define and document key aspects of CFX's records management activities that are currently in place, including, but not limited to the following:

- Record Coordinator procedures by department
- Frequently used GS1-SL Retention Schedules by department and any departures from the GS1-SL Retention Schedule for specific records
- Barcode and database tracking process for offsite storage of records
- Public records request tracking and quality control review process
- Use of the records management database and email search tool for public records requests
- Exemptions to public records law that are frequently used and/or relevant to CFX's business
- Examples of confidential information that should not be disclosed in response to a public records request
- Methods for electronic records retention
- Preservation process for permanent public records
- Public records destruction process

Continued on the following page...

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 1 – Records Management Policy and Procedures

Management Response
Concur.

Management Action Plan
CFX will develop a revised policy and desktop procedures based on the recommendations in this report and the new records management plan from the third-party consultant.

Action Plan Owner / Due Date
Michelle Maikisch, Chief of Staff /
Policy revision – June 30, 2017
Desktop procedures – June 30, 2018

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 2 – Record Coordinator Training

CFX policy requires that all employees complete an annual public records training, which is currently accomplished in conjunction with Ethics and Sunshine Law training provided by the CFX Legal department. The Manager of Public Records receives additional training to ensure the employee has the appropriate knowledge and skills to serve as the Records Management Liaison Officer.

In addition, CFX selects Record Coordinators within each department to work with the Manager of Public Records to ensure departmental public records are managed in compliance with Florida Public Records Law. The Record Coordinators perform a key role in the organization's public records management processes. However, specialized training for Record Coordinators is not in place.

Recommendation

Management should implement an annual public records management training program for the Record Coordinator role. The training should include the following, at a minimum:

- Internal processes and expectations for Record Coordinators
- Application of Florida Public Records Law to accomplish assigned responsibilities
- Exemptions and confidential information per Florida Public Records Law as applicable to the individual departments
- Upcoming public records related projects
- Opportunities to discuss challenges and questions related to the Record Coordinator role

Management Response

Concur.

Management Action Plan

CFX will develop a formalized training process for the Record Coordinators with the assistance of the records management consultant. Training will be in addition to the basic public records training for all employees and will include detail specific to their role and responsibilities as Record Coordinators.

Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff / December 31, 2017

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 3 – Records Management Database

Although CFX's IT department built a custom Access Database for the Records Management department to store and retrieve location data for hard copy public records, it is no longer supported or maintained by the IT department (although it is stored on the Network File Share and subject to normal backup processes). Due to this, the Records Management department, the users of the database, have experienced issues and errors accessing the information contained within the database including:

- Reliance on web search results in order to troubleshoot problems with the database.
- Orphaned data that points to records that no longer exist, or have already been destroyed.
- Data integrity issues, such as the incorrect modification of the retention schedule of all records (which was changed to "retain permanently" for all documents).
- Unnecessary custom queries, tables, and search forms built approximately 10 years ago that affect the user interface and performance of the Access Database

Recommendation

CFX should consider migrating the current Access Database to a records management tool designed for this purpose. The selected tool should be provisioned and managed by the IT department, and should include a user-friendly interface, such as a web-based front end application to allow the Records Management department to access the information needed to fulfill public records requests. CFX should also consider contacting the offsite storage vendor to determine if they have a records management tool that can be leveraged to query, retrieve, and maintain records.

Management Response

Concur.

Management Action Plan

CFX will research solutions to replace the records management database and will include the procurement of a new database in the budget for next fiscal year.

Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff and Corey Quinn, Chief Technology/Operations / June 30, 2018

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 4 – Text Message Collection

CFX utilizes the Smarsh application to collect and store text messages sent to or from CFX cellular telephones. Due to the configuration of Apple devices, any text message sent between two Apple devices (e.g. iPhone to iPhone), whether the message is between two CFX employees or between CFX and an external party, is not captured in the Smarsh application. This is due to the manner in which the iMessage communication platform was designed by Apple.

Once the issue of record retention specific to Apple device messaging was identified, CFX's IT department quickly escalated the concern with the Smarsh application vendor. The solution provided by Smarsh included turning off the iMessage feature on each enrolled Apple device so that messages are forced to use Short Message Service (SMS) or Multimedia Messaging Service (MMS) instead of iMessage. The request to make this configuration change has been distributed to CFX's user base, and at the time of the audit, was completed for all iPhone users within the environment.

Recommendation

Management should update user procedures for CFX connected devices to include the requirement to keep iMessage turned off. Management should also enhance the current mobile phone provisioning process and related procedures to include a step for turning off iMessage on Apple devices before they are issued to the user.

Management should consider the following options to monitor compliance with the procedures and ensure collection of text message records:

- Develop a manual process to periodically review user settings on enrolled Apple devices
- Implement "parental controls" on enrolled devices with a password known by two CFX IT employees
- Implement a mobile device management (MDM) tool to automate the control process

Continued on the following page...

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 4 – Text Message Collection

Management Response
Concur.

Management Action Plan
Management is completely confident that due to the redundancy of safeguards currently in place that all text messages are retrievable. Notwithstanding, management agrees to implementing additional layers of safeguards.

Action Plan Owner / Due Date
Corey Quinn, Chief of Technology/Operations /
Turn off iMessage capability – complete as of November 30, 2016
Procedure updates – June 30, 2017
Review vendor MDM capabilities – March 31, 2017

protiviti

Detailed Observations

- Policies and Procedures
- Training & Awareness
- Technology
- Records Collection and Retention
- Records Destruction

Observation 5 – Electronic Mail Collection

The CFX Board is comprised of government employees and three gubernatorial appointed citizens. The gubernatorial appointed citizens serving on the CFX Board have been provided CFX electronic mail (email) addresses, which helps with record collection and retention for compliance with Florida Public Records law. However, Board members do not serve on committees, and instead appoint representatives to serve in their place. The non-government citizens serving at the Committee level have not been provided with CFX email addresses, creating greater opportunity for emails regarding agency business to be sent outside of CFX's Exchange deployment, leaving them absent from the public records files or CFX-established records retention schedules.

Recommendation

CFX should assign a CFX email address to each non-government Committee member and should communicate the expectation that all agency business be conducted using this email address. If this is not possible, CFX should consider requiring that any email messages related to agency business conducted outside of a CFX email address be forwarded to a designated CFX address for collection and retention.

Management Response

Concur.

Management Action Plan

CFX will issue email addresses to the non-government committee members and will require committee members to utilize the email address for agency business or to forward all related emails to the address for collection and retention.

Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff / December 31, 2017

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 6 – Records Barcode Tracking

To aid in tracking the movement, storage, and retrieval of paper records, when records are ready to be sent to the offsite storage vendor for retention, barcodes are issued to Record Coordinators or custodians by the Records Management department. The Record Coordinator or custodian completes and returns a box inventory form to Records Management, which identifies the records within the box, attaches the barcode, and sends the box to offsite storage. The Records Management department enters the detailed box contents into the records management database, by barcode, for record tracking and retrieval purposes. All available and issued barcodes are tracked by Records Management in Excel, but Records Management does not currently follow up on the status of barcodes where no box inventory form was returned and does not confirm receipt of the box by the offsite storage vendor.

During the audit, one instance was identified in which a barcode was issued to a Record Coordinator ten months prior but could not be located in the records management database, indicating that the box inventory form was not returned to Records Management. The box was subsequently located onsite; however, inadequate tracking of barcodes, box inventory forms, and receipt of boxes by the offsite storage vendor increases the risk of undetected loss and an inability to subsequently comply with any public records request specific to those records.

Recommendation

To improve the tracking process of public record boxes, Records Management should perform a monthly reconciliation of the barcodes issued, box inventory forms received, and boxes received by the offsite storage vendor. CFX may consider including a barcode tracking tool in the records management database and developing reports to facilitate and formalize the tracking and reconciliation processes for records sent to the offsite vendor for storage.

Management Response

Concur.

Management Action Plan

CFX will implement the monthly reconciliation process as recommended.

Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff / March 31, 2017

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 7 – Electronic Public Records Destruction

Although a records retention schedule is clearly defined in policies, electronic records are not being destroyed according to the retention schedule. Currently, CFX is permanently retaining records for the following digital technologies with no defined procedures or technology in place to guide destruction beyond the required retention limits:

- Microsoft Exchange (electronic mail, calendar, and contacts)
- Smarsh (text messages)
- Network Shared Drive (electronic documents and other records)
- SharePoint (electronic documents and other records)

CFX's Records Management Policy and Public Records Training are documented and establish the records retention schedule. The training states that "a public record may only be destroyed or disposed of in accordance with the retention schedules", and "after the retention period, public records that are no longer needed must be systematically disposed".

Florida Administrative Code 1B-24.003(1)(a) states that "Retention periods are determined by the content, nature, and purpose of records, and are set based on their legal, fiscal, administrative, and historical values, regardless of the format in which they reside or the method by which they are transmitted." This means that certain emails or text messages may need to be retained longer than others based on their content.

Recommendation

Review existing policies and procedures surrounding the disposition or destruction of documents to ensure they provide sufficient detail around record retention and destruction.

Develop an approach to destroy records from the systems they are stored within (such as Smarsh, Exchange, SharePoint, Shared Drives, etc.) once their retention schedule has been met. To facilitate this, consider developing a method within each digital technology instance to classify records and document their associated destruction date according to the retention schedule and Authority policy.

The timely destruction of public records once retention is met would help reduce electronic and manual resource requirements and associated costs to store records. In addition, public records held beyond the retention period would need to be produced in the event of a public record request. Timely destruction of records could reduce labor requirements for the discovery of items that should have been destroyed in the event of a sizeable public record request.

Continued on the following page...

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 7 – Electronic Public Records Destruction

Specific to Microsoft Exchange, CFX should consider the following actions to assist in managing email correspondence so emails can be categorized and destroyed when necessary:

- Set mailbox limits that automatically delete messages after a pre-determined period of time
- Restrict the creation of .PST files so that all messages reside within user's inbox (and not on their local machine)
- Create a "vault" to store important emails that must be kept for a certain number of days on each user's inbox, and outline the type of content within emails that would warrant the message to be placed within the "vault". This "vault" would not be subject to the automatic delete processes outlined above so that all messages that must be kept are secured and can be retrieved when necessary.

CFX may consider implementing an email management tool that does the above and allows for categorization of emails by retention schedule.

Management Response
Concur.

Management Action Plan
CFX will establish a systematic destruction process for each type of electronic technology. The process will be documented in the policies and desktop procedures. CFX will explore email management tools available to assist with the destruction process.

Action Plan Owner / Due Date
Michelle Maikisch, Chief of Staff / June 30, 2018

protiviti

Detailed Observations

Policies and Procedures

Training & Awareness

Technology

Records Collection and Retention

Records Destruction

Observation 8 – Offsite Public Records Destruction

Florida Regulation 1B-24.003(10) requires all destruction of public records be conducted in a manner that safeguards the interests of the state and safety, security and privacy of individuals. The current CFX process is to have a witness present during onsite or offsite destruction of public records, which helps ensure compliance with the statute. Per CFX's contract with its offsite storage vendor, the vendor must complete a Certificate of Destruction each time records are destroyed, which is to include the name of the person performing destruction and the name of the witness. However, during the audit, upon inspection of these Certificates of Destruction, the names of the people performing the destruction and the name of the witness were not consistently documented on the Certificates of Destruction submitted to CFX.

Recommendation

CFX should contact its offsite storage vendor and request compliance with the contract terms through timely submission of complete Certificates of Destruction. In addition, CFX should implement a consistent management review control to check the completeness of Certificates of Destruction as received to verify the information provided is in accordance with the contractual requirements.

Management Response

Concur.

Management Action Plan

CFX will review the contractual requirements with the offsite storage vendor and will review future certificates to ensure the person performing destruction and the name of the witness are included.

Action Plan Owner / Due Date

Michelle Maikisch, Chief of Staff / March 31, 2017

protiviti

DHSMV Data Security Assessment

Central Florida Expressway Authority

September 2016

Executive Summary

protiviti
Risk & Business Consulting
Internal Audit

Overview

During the period of August 8, 2016 to September 12, 2016, Internal Audit performed a Data Security Assessment of the Department of Highway Safety and Motor Vehicles (DHSMV) data within the Central Florida Expressway Authority (CFX) environment. The objectives of the assessment were to review internal controls for gaps in design related to the requirements set forth in *Section V – Safeguarding Information*, of the DHSMV Drivers License or Motor Vehicle Record Data Exchange Memorandum of Understanding (MOU).

The summarized objectives of Section V are:

- Information exchanged will not be used for any purposes not specifically authorized by the MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purposes, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.
- Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.
- Access to the information will be protected in such a way that unauthorized persons cannot review or retrieve the information.
- All personnel with access to the information exchanged under the terms of the MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).
- All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).
- All access to the information must be monitored on an on-going basis by the Requesting Party (CFX). In addition, the Requesting Party (CFX) must complete an annual audit to ensure proper and authorized use and dissemination.

Executive Summary

protiviti
Risk & Business Consulting. Internal Audit.

Scope & Approach

Internal Audit conducted an assessment of the process used for safeguarding DHSMV data in the CFX environment. In order to complete this review, the following procedures were performed:

- Reviewed policies and procedures related to the safeguarding of electronic and physical data transfers, data storage, and data access.
- Conducted interviews with key personnel to understand the *Drivers License or Motor Vehicle Record Data Exchange* process.
- CFX Management approved the scope of work and believed it to be sufficient to meet the requirements of the MOU. Conducted testing of controls related to the following areas:
    - Policies and Procedures
    - Application Access
    - Segregation of Duties
    - Change Control
    - Data Storage
    - Data Transfer
    - Network Firewall
    - Network Architecture
    - Active Directory
    - Physical Security
- After testing was completed, analysis was performed to compare the results of testing to the control objectives outlined in the MOU.

Executive Summary

Summary of Results

As a result of this review, Internal Audit identified zero (0) observations that should be addressed in order to enhance CFX's Drivers License or Motor Vehicle Data Exchange process.

Appendix A – Controls Tested

protiviti
Risk & Business Consulting. Internal Audit.

	Control Objective	Control Description	Testing Results
1	Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.	**Policies and Procedures:** CFX implements company-wide policies and procedures that enforce the safeguarding of company data and other sensitive customer data whether or not it is currently being used or accessed.	**Control Effective**
2	All personnel with access to the information exchanged under the terms of the Drivers License or Motor Vehicle Record Data Exchange MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the requesting party.	**Training:** CFX requires in the hiring process that all users sign an acknowledgement after reviewing either the employee or contractor security guidelines handbook which covers the safeguarding of data. These acknowledgments must be maintained for all current/active users.	**Control Effective**
3	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access:** System access to the TRIMS applications for new users is appropriately administered through the submission of a New User Authorization Form. This form is completed by the new user's Manager and the proper approvals/signatures are obtained. Access to the applications is then administered by IT support.	**Control Effective**
4	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access - Terminated Users:** System access to the TRIMS application and company network is appropriately revoked in a timely fashion for terminated users. Upon receipt of a termination notification (email, authorization form, phone call, etc.) from HR or a Manager responsible for the terminated user, the user's system account is disabled immediately.	**Control Effective**
5	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Database-level Access:** Database-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**

Appendix A – Controls Tested

protiviti
Risk & Business Consulting
Internal Audit

	Control Objective	Control Description	Testing Results
6	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Server-level Access:** Server-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**
7	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**FTP Gateway Access:** All individuals / user accounts with access to the FTP Gateway are authorized and appropriate.	**Control Effective**
8	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Host (HT250) Access:** All individuals / user accounts with access to the Host (HT250) are authorized and appropriate.	**Control Effective**
9	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Oracle DB Access:** All individuals / user accounts with access to the Oracle DB are authorized and appropriate.	**Control Effective**
10	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**DOCPRD1 Access:** All individuals / user accounts with access to the DOCPRD1 server are authorized and appropriate.	**Control Effective**
11	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Infoview Crystal Reports (RPTPRD4) Server Access:** All individuals / user accounts with access to the Infoview Crystal Reports (RPTPRD4) server are authorized and appropriate.	**Control Effective**
12	Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.	**DHSMV Data Access:** Management performs a periodic review of user access across each of the in-scope entities to ensure that the assigned access level is commensurate with his/her job function.	**Control Effective**

Appendix A – Controls Tested

protiviti
Risk & Business Consulting
Internal Audit

	Control Objective	Control Description	Testing Results
13	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** Dedicated Test environments exist for the testing of changes and patches, where practical. CFX appropriately documents and tests each change.	**Control Effective**
14	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** All changes and patches are authorized, executed, and documented according to stated procedures.	**Control Effective**
15	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Data Encryption:** Driver's license number as it is obtained from the DHSMV is encrypted when stored in the Oracle database. Also test encryption methods at all other transmission points, including at network, application, and database layers (if applicable).	**Control Effective**
16	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Firewall:** CFX has an operational firewall in place to restrict access to the internal network.	**Control Effective**
17	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Active Directory:** All individuals with Active Directory credentials are current, active users and all rights granted through Active Directory are commensurate with their current job responsibilities.	**Control Effective**
18	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Data Center:** Access to the data center(s) is restricted to appropriate personnel and is provided through the use of a physical key, key card, biometric, or other form of physical security.	**Control Effective**

Appendix A – Controls Tested

protiviti
Risk & Business Consulting
Internal Audit

	Control Objective	Control Description	Testing Results
19	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Work Areas:** Access to the work areas is restricted to appropriate personnel and is provided through the use of a physical key, key card, biometric, or other form of physical security.	**Control Effective**
20	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Logging & Monitoring:** Logging and auditing functions are enabled on all in-scope entities. In addition, all system logs are monitored for unauthorized access and irregular activity.	**Control Effective**
21	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Vulnerability Scanning / Penetration Testing:** CFX performs periodic external vulnerability scans and penetration tests.	**Control Effective**