CENTRAL FLORIDA EXPRESSWAY AUTHORITY

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti
Face the Future with Confidence

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

Information Security Risk Assessment – Phase I

May 2017

Internal Audit, Risk, Business & Technology Consulting

EXECUTIVE SUMMARY

Overview

This report represents the results of Phase I of the Information Security Risk Assessment conducted by Internal Audit ("IA") as outlined in Florida Statute 282.318, "Security of Data and Information Technology". This statute requires that an agency:

- *Use a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.*
- *Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency.*

The standard risk assessment methodology that IA used during this Information Security Risk Assessment was the National Institute of Standards and Technologies ("NIST") Special Publication 800-30.

This phase of the review focused only on Asset Identification. Additional phases will be conducted in the future to complete the Information Security Risk Assessment.

Scope

IA used the following approach in the delivery of Phase I of this project:

1. IA assigned categories and owners to assets by performing the following activity:
    - Developed an inventory of assets for in-scope business systems that create, receive, maintain, or transmit sensitive data. The inventory was accumulated through a combination of the following methods:
        - Interviewing IT administrators, business unit management, and other key personnel
        - Utilizing current asset management / identification data

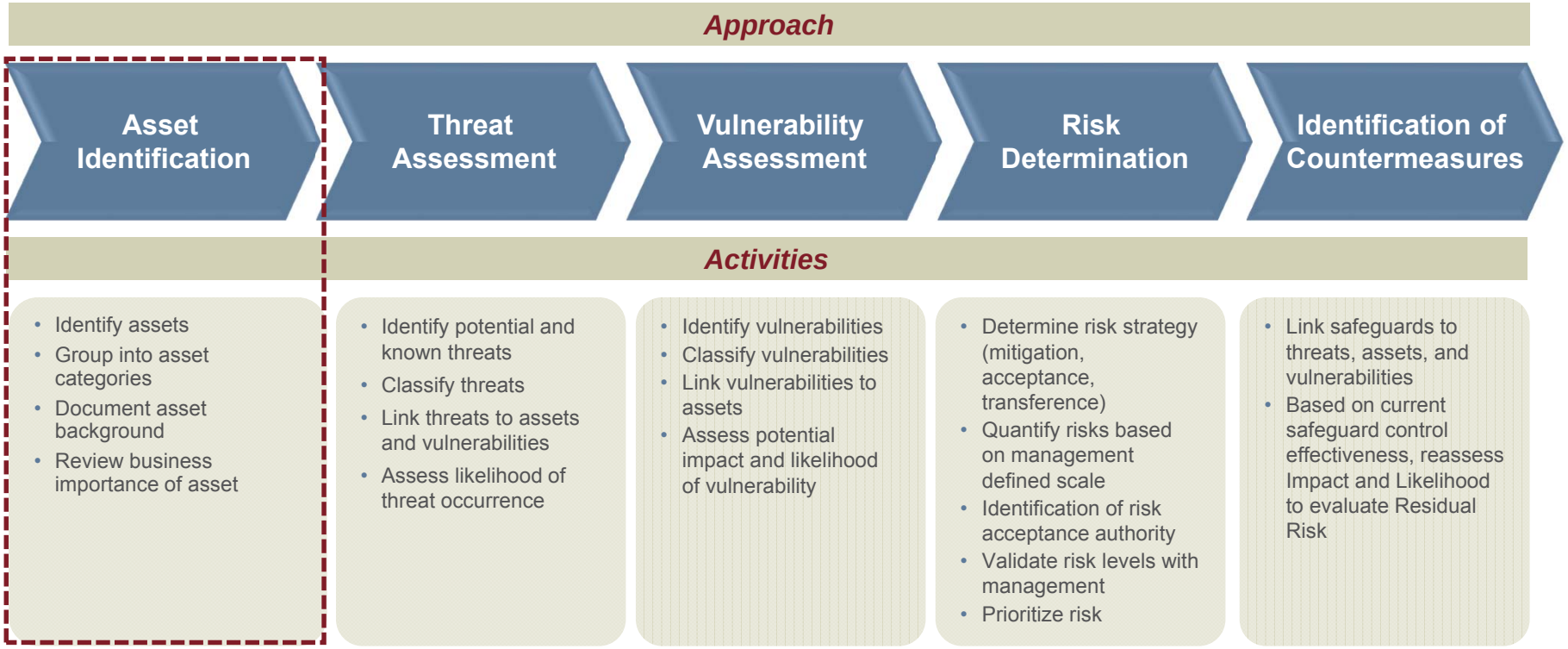
EXECUTIVE SUMMARY

Approach

IA reviewed documentation and interviewed key CFX and ITS personnel in order to:

1. Identify assets
2. Group assets within categories
3. Document asset descriptions
4. Review of the business importance of assets

As a result of this work, IA identified 13 assets that will be considered during the remaining phases of the Information Security Risk Assessment. These assets are listed on page 3 and 4.



ASSET IDENTIFICATION

#	Name	Description
1	Key Applications	Applications and databases crucial to business operation, including: • TRIMS – Customer support/account management application • TRAILS – Transponder retail and in-lane sales application • EDEN – Financial reporting system • VES – Violation Enforcement System • ARCS – Database and supporting infrastructure (sensors, controllers, hosts) that capture transponder activity • iMars/Special Viewer – Imaging software used to validate letters and digits on license plates • Helpdesk ticketing system • SAMS – Security & Access Management System for managing access to TRIMS and TRAILS. • 3rd party software applications – Microsoft Office, etc. • InfoView – Enterprise reporting utilizing Crystal Reports.
2	External Web sites	Websites managed by CFX that are internet facing and utilized by customers, vendors, and employees: • CFX FTP Site – Used by Vendors and Employees to exchange files • E-Pass / VES Web Sites – Customer service site • CFX Corporate Web Site – Informational site used to describe information about the organization • VIO Web – Law enforcement portal for toll violation information
3	Workstations	A single-user or shared computer either located at HQ or Toll Plazas used for everyday operation and tasks of CFX Employees. These may be desktops or laptops.
4	Servers	Computers supporting CFX applications that run operating systems such as Windows Server 2012 or OpenVMS
5	Phone Systems	Voice over Internet Protocol phones for at each location used for communication and mobile devices assigned to users for voice, text, and email communication. Includes Interactive Voice Response (“IVR”) system.
6	Email	Microsoft Exchange email server used for communication.
7	Network Infrastructure	Network systems such as Intrusion Detection Systems (“IDS”), firewalls, routers, core switches, aggregate switches, and end of line switches in plaza cabinets.

ASSET IDENTIFICATION (CONT.)

#	Name	Description
8	ITS Closed Circuit TV Cameras	Cameras and supporting infrastructure that allow CFX to view traffic on the roadways.
9	ITS Dynamic Message Signs	Systems and supporting infrastructure that displays warnings or estimated travel times.
10	ITS Data Collection and Traffic Monitoring Systems	Systems and supporting infrastructure that estimate speed, congestion, and travel times on the roadways.
11	ITS Wrong Way Driving Deployments	Systems and supporting infrastructure that detects and alerts upon drivers going the wrong way on a road.
12	Lenel Badge System	Access control system used for physical security throughout all CFX locations to allow access to CFX facilities.
13	Printers/Copiers	Copiers and Printers located at HQ, Service Centers, and Plazas.

Face the Future with Confidence

protiviti