Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Aug. 7, 2019

ISOAG Aug. 7, 2019 Agenda

I. Welcome and Opening Remarks	Mike Watson, VITA
II. Agency Head Training	Barry Davis, DSS
III. Social Engineering	Rob Reese, VSP
IV. Xerox Managed Print Services	Sean Lucas and Joe Chambers, Xerox
V. ECOS Made Easy	Debi Smith, VITA
VI. Archer Security Exceptions	Lourdes Lunsford, VITA
VII. FY20 New and Enhanced Security Services	Bill Stewart and Darrell Raymond, ATO
VIII. Upcoming Events	Mike Watson, VITA

Agency Head Security Awareness
a VDSS Experience

Presentation Objective: Create a shared awareness of preparing and delivering Agency Head training…

Barry Davis, CISSP
DSS Chief Information Security Officer

ISOAG 8/7/2019

Agenda

- Why Brief the Agency Head?
- How to do it
- Walk through of DSS Agency Head Slide Deck
- Q&A

Why brief the agency head?

- They have at least 11 explicit responsibilities from SEC 501 (Section 2.4)
- A chance to show what Information Security is doing for the agency
- Discuss challenges and issues related to information security
- Establish your relationship, get to know the boss
- If you have a new Agency Head, this is your chance to talk about:
  - Mission Essential Functions, Primary Business Functions
  - Your reporting structure
  - Non IT risk

How to do an Agency Head Brief

- For new Agency Head, get them on day one
- Desktop briefing, side-by-side
- Plan for 20 minutes (be flexible)
- Topics:
  - Cover SEC 501 responsibilities (high level)
  - Cover specific external (IRS, SSA, HIPAA, PCI, etc.) responsibilities
  - Discuss Mission Essential Functions
  - Discuss most recent critical findings
- Let your boss know what you're doing
- Get their input for future awareness sessions

Home Office Executive Leader Security Training

VIRGINIA DEPARTMENT OF SOCIAL SERVICES

Barry B. Davis

Barry.davis@dss.virginia.gov

801 E. Main Street, Commissioner's Office

Richmond, VA 23219

Mond 99, 2099~11:15AM ~ 12:00PM

Training Objective: Improved understanding of the Agency Head role in securing and documenting DSS systems to State and Federal Standards

Agenda

- Welcome
- 2019 Updates
- Data drives Security
- Federal Requirements (SSA-IRS-NDNH)
- FTI and Safeguards
- Risk Management Framework - intro
- RACI Chart
- Mobile Devices and IOT
- Q&A

Info Security 2019 updates

- Federal Reviews: IRS, SSA, DoJ, CMS
- State Reviews: APA
- New Executive Structure
- VDSS has four cloud hosted applications in use using MS Dynamics 365 for Constituent Relationship Management (CRM)

Agency at a glance

- Eight Mission Essential Functions
- 198 supporting Primary Business Functions
- 45 sensitive applications
- Mature Information Security Program
- Mature Security Awareness Program

It is all about the data….

Federal Data & Requirements

- SSA Data (SPIDeR, VaCMS, iAPECS…)
- IRS/FTI Data (iAPECS, DIS FTI Servers)
- National Directory of New Hires
- CMS hub data
- PII collected under state and federal authorities to determine benefit eligibility
  - Some with federal sharing restrictions
  - Consent is key for sharing with other agencies

Federal Tax Information

- FTI is any tax return or tax return information received from the IRS or secondary source like SSA or CMS
- FTI includes any information created by the recipient that is derived from Tax return or Tax return information
- FTI currently exists in DCSE's iAPECS, DIS FTI servers, and local office paper files for cases processed under ADAPT

Federal Tax Information

- Disclosure for Benefit Programs
  - Access to ***FTI*** is strictly **prohibited** for non-paid employees, such as student interns, volunteers, or any other type of non-paid employee
  - Legacy FTI in file folders is off-limits to contractors, volunteers, interns
  - Risk for Imaging Systems
- Disclosure for DCSE
  - Same non-paid prohibition as Benefit Programs
  - No contractor restrictions
  - Must notify 45 in advance of new contractor disclosures

Federal/COV Penalties

- IRS FTI unauthorized disclosure penalties
- Per disclosure, felony, 5 years prison, $5,000 fine + civil fine of $1,000
- SSA unauthorized disclosure
- $10,000 + 1 year prison per disclosure
- COV unauthorized disclosure
  - Misdemeanor for accessing the data
  - Class six felony if the data is shared with others or used in the commission of another crime

FTI and Safeguards Topics

- Recent updated IRS Requirements:
  - Shredding FTI 1mmx5mm
  - FBI background check for anyone with access to FTI, including IT staff that manage FTI devices
- Home Office Triennial Inspection (September 2019)
- DSS FTI Hosted environment move to CESC

Risk Management Framework (RMF)

- Set of processes developed by National Institute of Standards and Technology (NIST), and used extensively by state, federal government and DoD
- Mandated by VITA SEC 501/SEC525, Centers for Medicare and Medicaid Systems (CMS), used by IRS too
- A prescribed governance, process and controls for securing sensitive data and systems. 18 control families
- Process Overview, SEC501 pp 1-13
  - Business Impact Assessment
  - Data Classification
  - Risk Assessment
  - System Security Plan
  - Authority to Operate
  - IT Audits
  - Continuous Monitoring (scans, audit log reviews, access reviews, etc.)
  - Continuity Planning

Agency Head SEC 501 Responsibilities

Agency Head Artifact RACI Chart R=Responsible, A=Accountable/Authority, C=Consulted, I=Informed	Commissioner	VITA	Data or System Owner	VDSS ISO
Artifact/Action				
Security of agency IT Systems and Data, Designate System Owners	A	R/I	R	C
Designate an Information Security Officer at least Biennially	A/R	I	I	C
Maintain Agency Information Security Program	A	C/I	I	R
Review and Approve Business Impact Analysis	A	I	I	(R)
Review and Approve Continuity Plan & Disaster Recovery Plan	A/R	I	C	R
Review or Designate Review of System Security Plans for all Sensitive Agency Systems/Applications	A	I/C	C	R
Ensure Agency Complies with the VITA IT Security Audit Standard (SEC 502)	A	I	I	R
Ensure an Information Security Safeguards Program is established	A	I	I	R
Ensure Information Security Awareness and Training Program is in place	A/I	I	I	R
Provide resources to enable the Information Security Program	A/R	I	I	C/I
Prevent conflict of interest and adhere to separation of duties	A	I	C/R	R

RMF SEC 501 Responsibilities

Artifact RACI Chart R=Responsible, A=Accountable/Authority, C=Consulted, I=Informed	Commissioner	Directors and Managers	System Owner	Chief Information Officer	VDSS Chief Information Security Officer (CISO)
Artifacts					
Develop, Approve, Publish Business Impact Analysis	A	C	C	I	R
Develop, Approve, Publish, Test Continuity Plan	A	C	C	I	R
Develop, Publish, Test Disaster Recovery Plan	A	C	C	R	C
Perform Data Classification	I	A	A	I	(R)
Perform Risk Assessment	A/R	C	A	C	R
Develop System Security Plan	A/R	I	R/A	C	R/C
Approval to Operate	A/R	I	C	C	R
Perform IT Audit	A	C	C	C	R/A
Develop and Manage DSS Information Security Program	A/I	C/I	C/I	C/R	R/A

Emerging Risks, Security Challenges

- Business/IT units using agile development methodologies are delivering rapid results, but not compliant with state and federal system documentation standards.
- Local DSS using unsecured, unmanaged mobile devices to process client data
- PowerBI, new Data Warehouse and Operational Reporting tool being deployed without adequate governance:
  - No Security Model or Framework
  - No Data Model
- Security – Identity and Access Management (IaM) not cloud ready
  - SAMS was built to pre-cloud requirements
  - No clear VITA model for cloud based IaM
  - Solution will need to account for legacy IaM requirements

Questions and Answers

Thank You!

Questions and Answers

Thank You!

XEROX

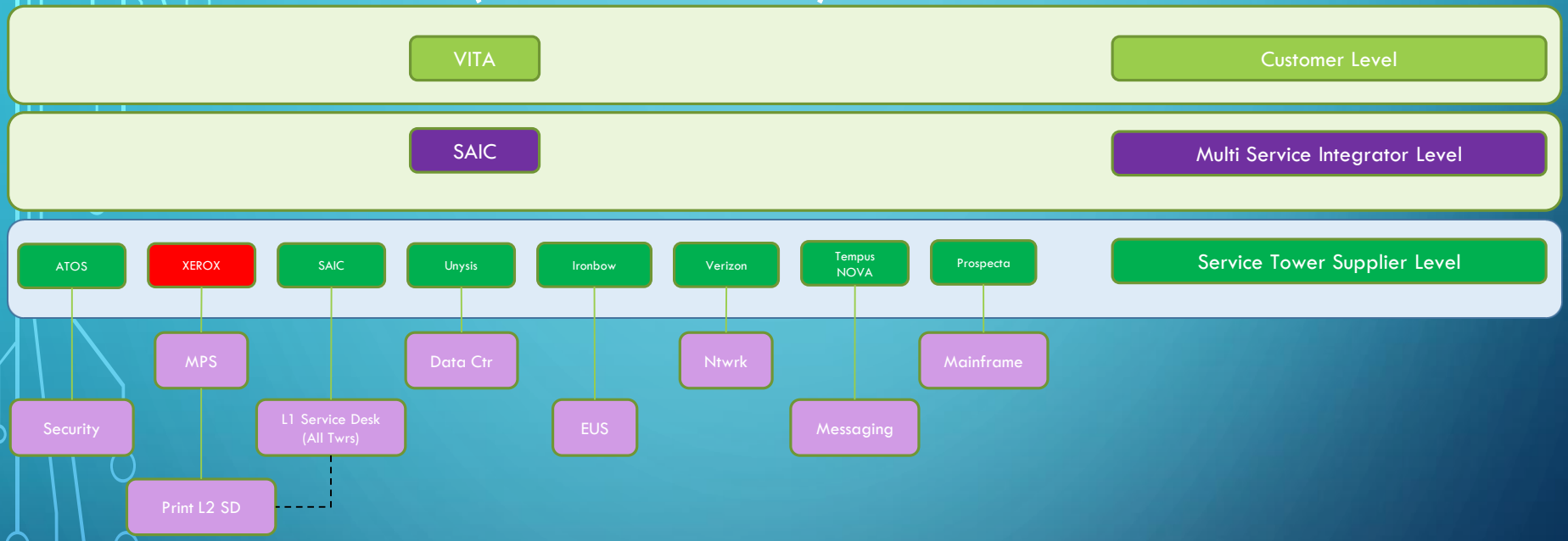
NOT YOUR MOTHER'S PRINTING!

AGENDA

- Account Structure (How we fit in)
- Team Structure
- Day to Day Operations
- Account Overview (it's what we do)
- Devices we SECURE!
- Questions?

xerox

Account Structure (How we fit in)



8 TEAM STRUCTURE

Operations

- Account Executive — Joe Chambers
- Account Manager — Rickey Wood
- BRM — Tyrone Rucker
- Security Manager — Sean Lucas
- Project Manager — Russell Smith
- Security Analyst — Emmett Blapooh
- Service Del Coordinator — Terence Starckey
- Security Analyst — Dominique Woods

xerox

DAY TO DAY OPERATIONS

01

Remediate security vulnerabilities provided by VITA CSRM

02

Update Emerging Threats of security vulnerabilities for XEROX devices.

03

Update the Change management team weekly of possible upgrades or modifications to the VITA environment and other agencies.

04

Conduct weekly Security Team meetings to gain knowledge of any security violations, breaches or incidents.

05

Update and scan for all possible threats to XEROX devices.

IT'S WHAT WE DO

24x7x365 Help Desk

Local, dedicated 8 member team

- Dedicated security team

Management of all **in-scope**, networked print devices

- IMAC
- Break-fix - Service tiers (4 levels)
- Supplies included (Xerox and non-Xerox)
- Asset Management (CMDB, XSM) (~4,000 devices)
- Security Monitoring via Security Center and XDM (Xerox Device Manager)

Management of Xerox activity in KeyStone Edge (KSE)

- Services Catalog orders
- Incident and Request management

Reporting & Analytics

IT'S WHAT WE DO (CONT.)

- Service Incidents, Requests, Events, Problems, etc. originate in MSI instance of ServiceNow (Key Stone Edge – KSE)
- Xerox L1 will monitor alerts from XSM
- XSM will be bi-directionally E-Bonded with KSE
- XDM will pull data from all connected devices for security and billing purposes.
- The configurations for devices maintained in XDM will be used to assist remediation
- Security Center (Tenable.SC) is used in tangent with XDM for device vulnerabilities
- Provide security solutions such as firmware updates or security patches via the Change Management team to be implemented.

DEVICES WE SECURE

- Single function printers and MFDs
- Desktop & workgroup
- Black & white and color models
- Multi-brand
- AltaLink have McAfee EPO Capabilities to assist with vulnerabilities.

Product List

Copier Category 1
Copier Category 1A - Copier Volume
Copier Category 2
Copier Category 2A - Copier Volume
Copier Category 3
Copier Category 3A - Copier Volume
Copier Category 4
Copier Category 4A - Copier Volume
Copier Category 4B - Copier Volume
Copier Category 5
Copier Category 5A - Copier Volume
Copier Category 5B - Copier Volume
Copier Category 6
Copier Category 6A - Copier Volume
Copier Category 6B - Copier Volume

Network Attached Printer - Category 1
Network Attached Printer - Category 2
Network Attached Printer - Category 3
Network Attached Printer - Category 4

QUESTIONS?

Virginia Information Technologies Agency

Enterprise Cloud Oversight Services: Made Easy

Debi Smith
Cloud Security Architect

ISOAG
Aug. 7, 2019

ECOS – Enterprise Cloud Oversight Services

- ECOS is a service **specifically** created for third-party suppliers offering SaaS applications
- **What is SaaS?**
  - Capability provided to the consumer to use the provider's applications running on a cloud infrastructure
  - Applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
  - Consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities; with the possible exception of limited user specific application configuration settings

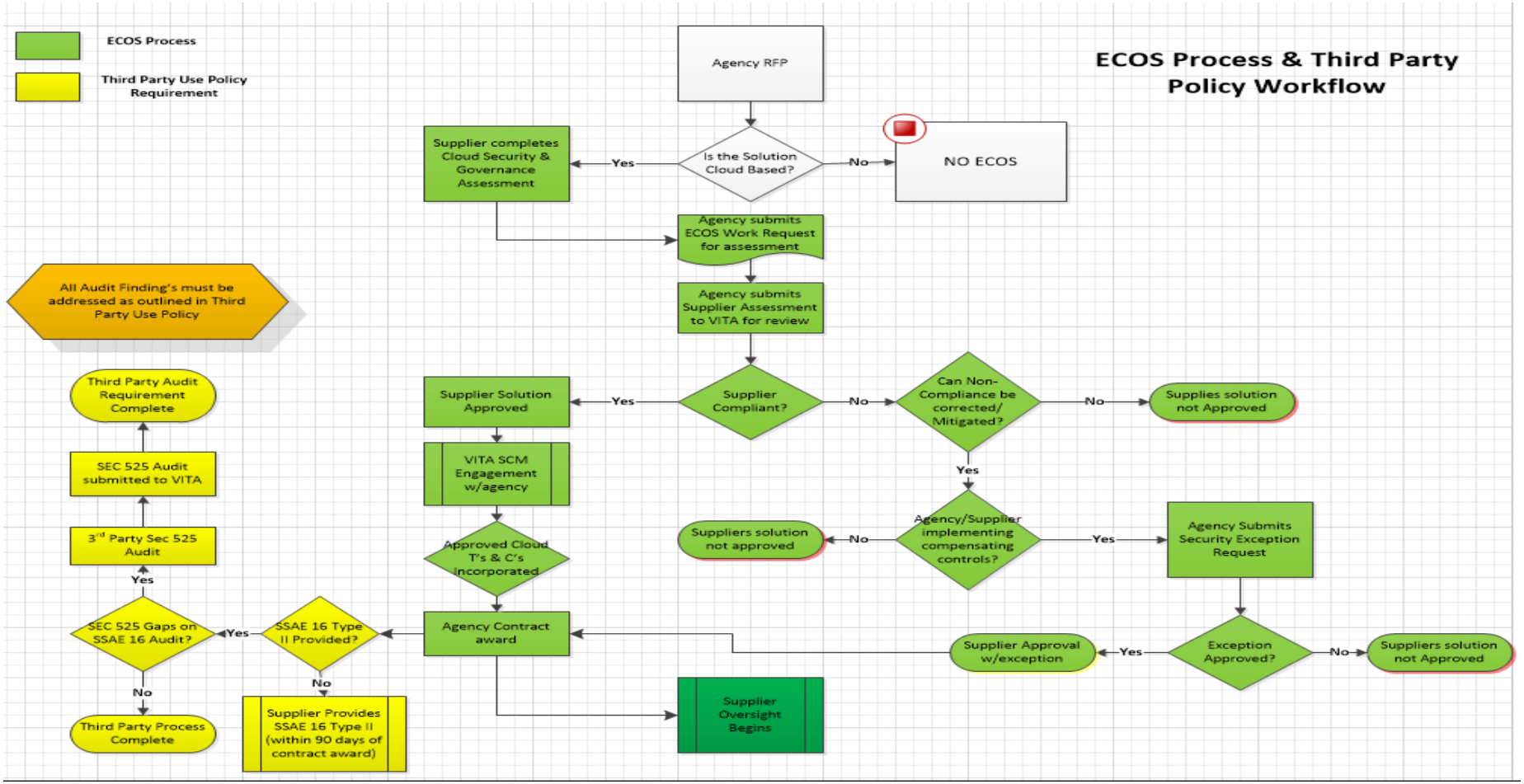
ECOS – SaaS characteristics

- **SaaS characteristics**
  - Network-based access to and management of commercially available software
  - Supplier-provided services accessed through an internet connection to a third-party hosted facility
  - Service delivery typically a one-to-many model (single instance, multi-tenant architecture); generally includes common architecture for all tenants, usage based pricing and scalable management
  - Third party supplies management of the service, including functions such as patching, upgrades, platform management, etc.
  - Multi-tenant architecture, all users and applications share a single, common infrastructure and code base that is centrally maintained
  - Subscriber/user manages access controls for the application
  - Provider is *data custodian and server administrator*

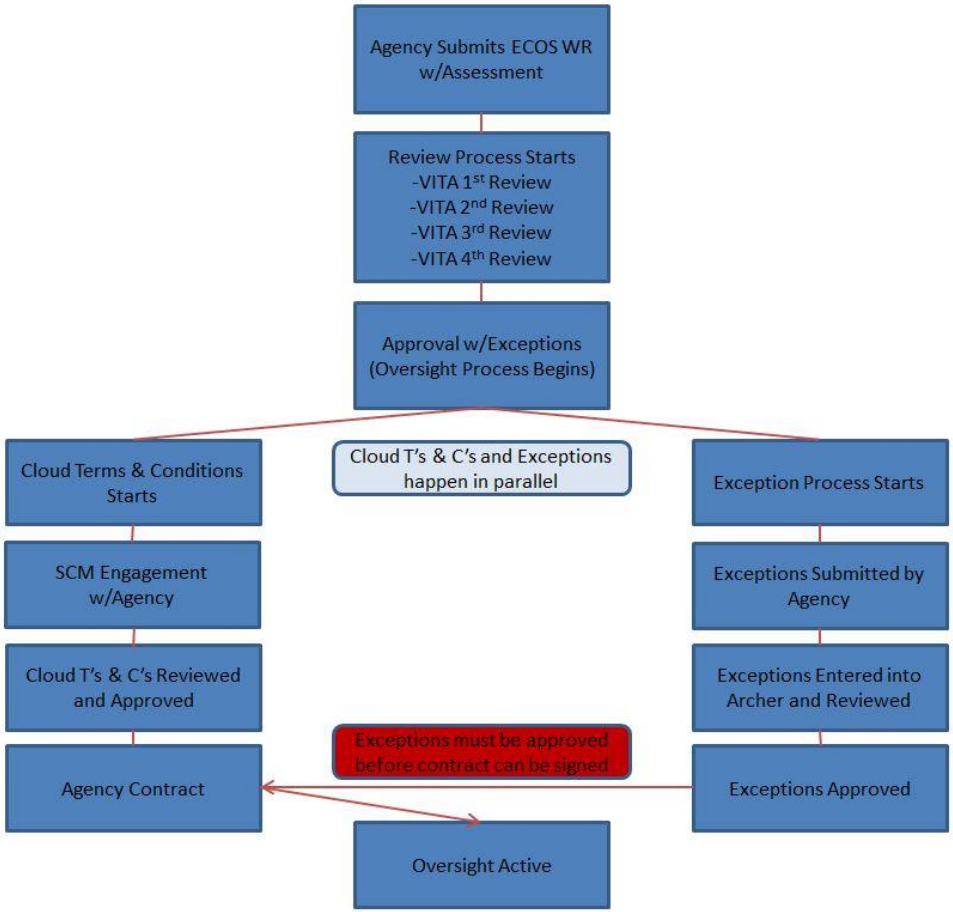
ECOS – Applies when

- **ECOS applies when**
  - Services being procured meet the above definition and/or characteristics of a software as a service (SaaS) provider
  - ECOS does not cover PaaS requests as part of the current service. PaaS solutions are available through the eGov contracts or through a hosting exception request.
  - When an agency is requesting the provider act on behalf of a Commonwealth entity and/or is accepting commonwealth data, serving as the *data custodian and/or system administrator* of that data for purposes of making it available back to the Commonwealth via an interface for fee.

ECOS – The Process



ECOS – The Process – Made Easy



ECOS – Made Easy

- **Step 1 – Complete Assessment**
  - Determine your Vendor/Supplier
  - Have the Vendor/Supplier complete the assessment
  - **Review** their responses
  - Submit your request to Keystone Edge

  - **Helpful Hints:**
    - Check your Vendor/Supplier – look at their website and terms
    - Check to see if the Vendor is already approved
    - Ensure the Vendor has filled out the form completely – not simply Yes/No responses
    - If they say they have documentation – request it – this speeds up the process
    - Ensure ALL documents are attached and the assessment is in EXCEL format

ECOS – Made Easy

- **Step 2 - VITA first review**
  - VITA will review vendor/supplier's responses
  - VITA may ask for more detail and supporting documentation
  - VITA will return the assessment for you to work with vendor

  - **Helpful Hints:**
    - VITA may contact you if items or incomplete or missing – respond promptly
    - VITA will require supporting documentation – the more provided, the quicker the review
    - VITA will return the assessment after the review – review and submit to vendor
    - If you have questions, please call or email

ECOS – Made Easy

- **Step 3 – Reviewing VITA comments**
  - Review VITA comments on assessment
  - Send to Vendor and request any relevant documentation
  - Obtain response and review to ensure you have responses and documents
  - Send to VITA for second review

  - **Helpful Hints:**
    - Review VITA comments on assessment – look for areas of concern or questions to agency
    - If the review asked for documents, ensure the vendor supplies them
    - Submit all relevant documents for review

ECOS – Made Easy

- **Step 4 – VITA second review**
  - VITA will review vendor responses and supporting documents
  - VITA will ask any final questions
  - VITA will return the assessment to you for submission to vendor

  - **Helpful Hints:**
    - VITA may have additional questions based on responses – those questions will be outlined in the assessment
    - VITA will return the assessment after the review – review and submit to vendor

ECOS – Made Easy

- **Step 5 – Reviewing VITA comments**
  - Review VITA comments on assessment
  - Send to vendor and request any final information
  - Obtain response and review to ensure you have responses and documents
  - Send to VITA for third review

  - **Helpful Hints:**
    - Review VITA comments on assessment – look for areas of concern
    - Request a teleconference for faster completion
    - At this point there should only be a few outstanding questions – let's wrap it up

ECOS – Made Easy

- **Step 6 – The Approval**
  - VITA will issue a "conditional" approval
    - Listing any "exceptions" and/or "contractual requirements"
  - Agency submits security exceptions
  - Agency submits oversight request
  - Cloud T's & C's begin

  - **Helpful Hints:**
    - Submit exceptions as quickly as possible – contract cannot be signed without exceptions
    - Work with CRM on Cloud T's and C's
    - Never hesitate to ask for assistance

ECOS – Made Easy

- **Requirements for faster processing**
  - Review vendor responses
  - Ensure all questions are complete w/explanation
  - Obtain relevant documentation (i.e., SOC 2, FedRamp Cert, Access Control Policies, Security Policies, Risk Assessment Procedures, etc.)
  - Obtain good contact information from the vendor for both technical and business related questions

ECOS – Made Easy

- **Areas of concern**
  - Hosting provider – geographic region
  - Integration capabilities – can the vendor support OKTA
  - Incident Response – timeline MUST be 24 hours
  - Scanning – frequency
  - Patching – time frames
  - Keys – who holds the keys
  - Third party attestation – for both the hosting provider and application

ECOS – Made Easy

- **Exceptions**
  - Common
    - AC-7(a) and (b) – (unsuccessful logon attempts)
    - AU-6(1) - (audit review, analysis, and reporting – process integration)
    - IA-5(1) – (password complexity)
    - SC-12-COV(3) – (keys remain in exclusive control of the commonwealth)
  - Uncommon
    - IA-2-COV - (two-factor authentication for all network-based administrative access)
    - SI-2-COV(b) – (applies security updates, not to exceed 30 days)
    - RA-5 – (scans for vulnerabilities at least once every 30 days)
  - Rare
    - IR-6-COV – (within 24 hours – see Code of Virginia 2.2-603(g))
    - MA-5-COV – (all maintenance performed by US Citizens or those authorized to work in the US)
    - PE-18-COV – (all information system components and services remain with the continental United States)

ECOS – Final Thought

- **Exception Notes:**
  - Agency or supplier must provide documentation of implemented controls to address risk posed by failure to meet security requirements
  - Exceptions are granted to allow agency or supplier time to correct deficiency (not to exceed 12 months)

ECOS – Final Thought

- **Remember**
  - The "agency" is responsible for the data !!!

Questions

Contact: Debi Smith
Debi.Smith@vita.virginia.gov

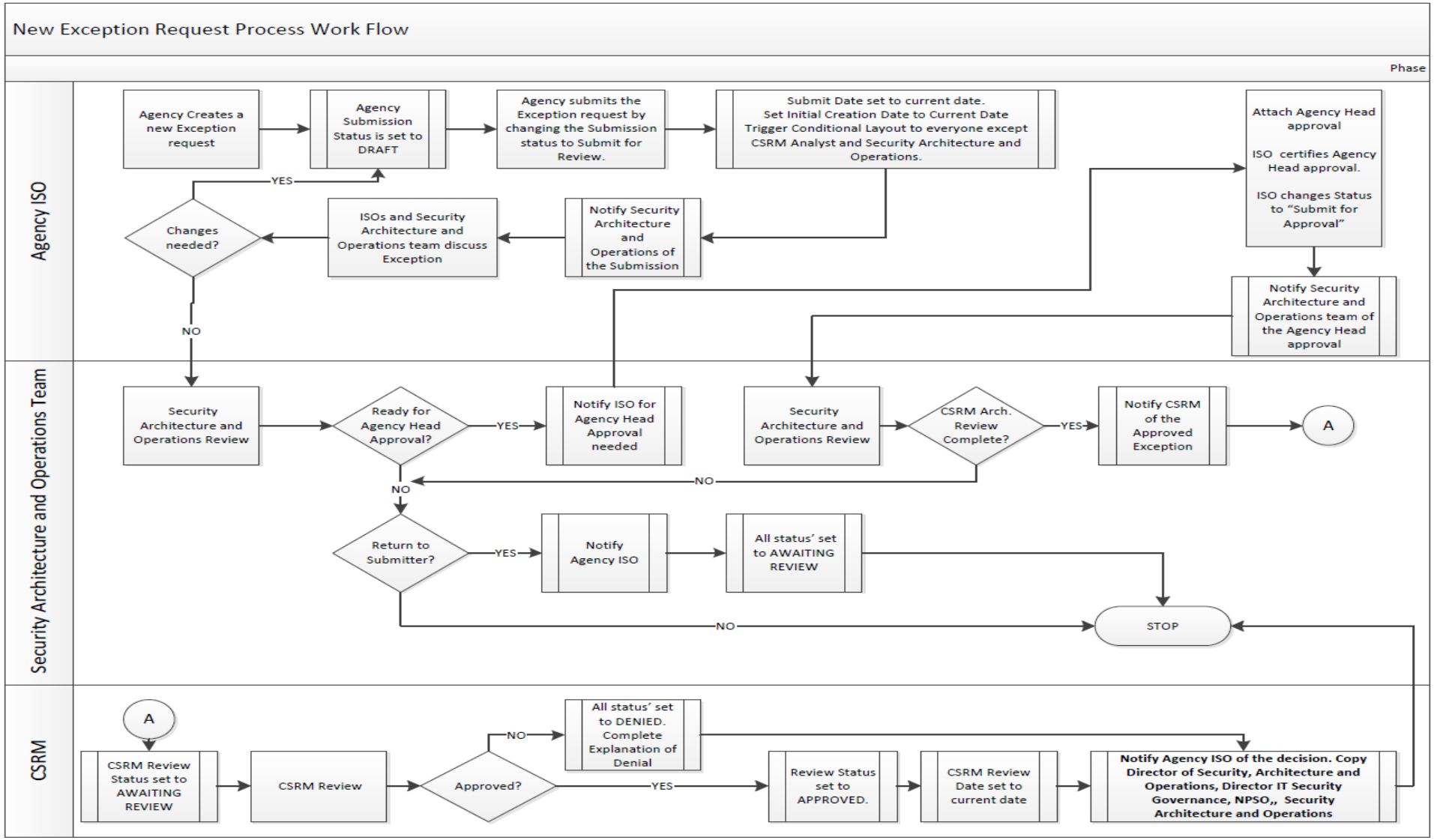
Virginia Information Technologies Agency

ARCHER SECURITY EXCEPTION

Lourdes Lunsford
Security Architect
Lourdes.Lunsford@vita.virginia.gov

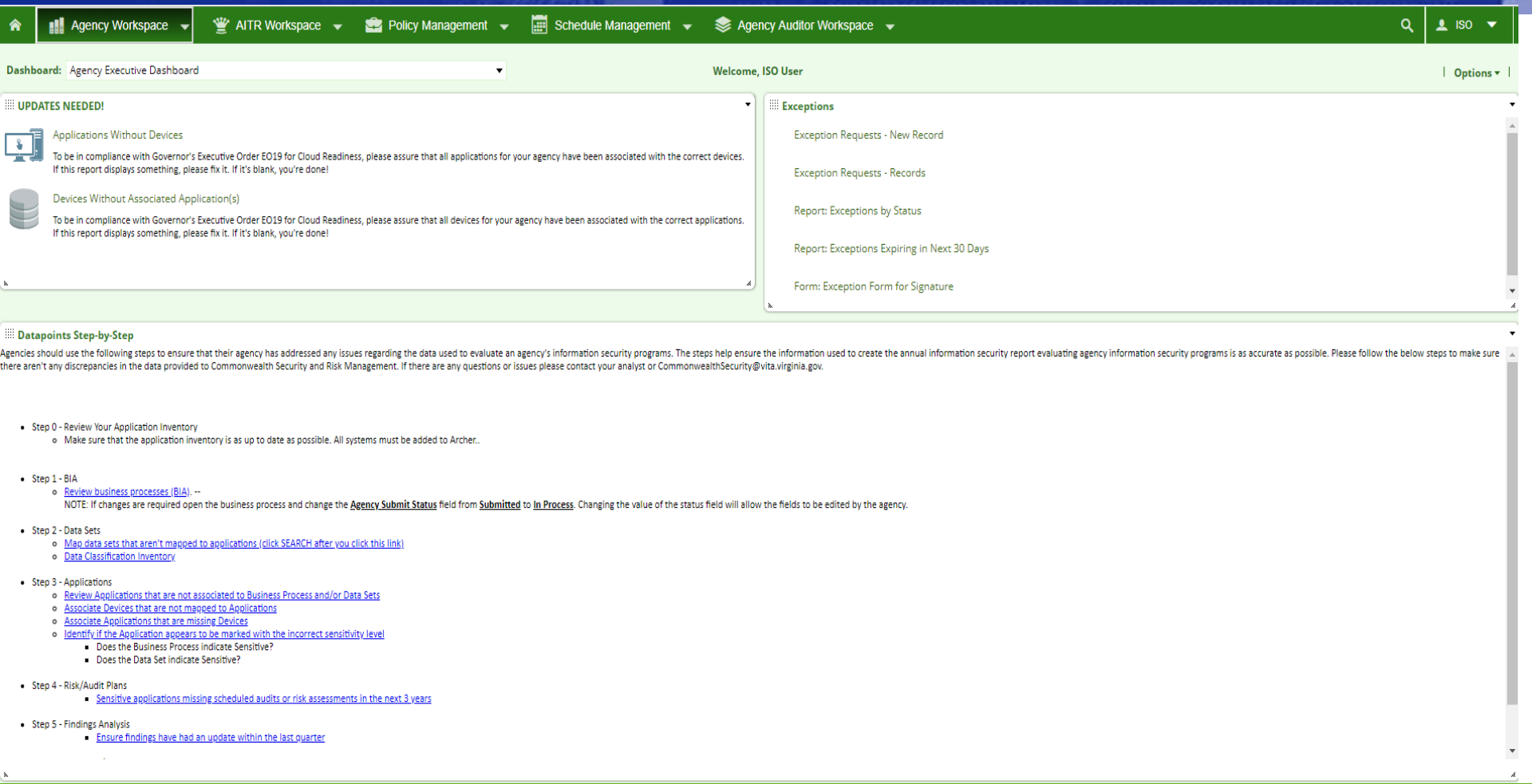
Overview

- Security exception request workflow
- Security exception review
- Security exception live demo

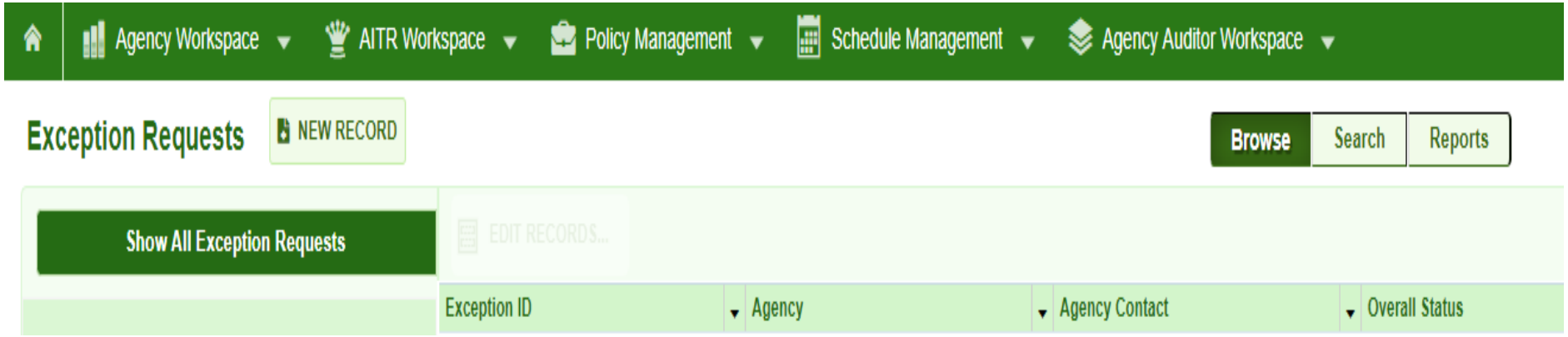

New Exception Request Process Work Flow
Phase
Agency ISO
Agency Creates a new Exception request
Agency Submission Status is set to DRAFT
Agency submits the Exception request by changing the Submission status to Submit for Review.
Submit Date set to current date.
Set Initial Creation Date to Current Date
Trigger Conditional Layout to everyone except CSRM Analyst and Security Architecture and Operations.
Attach Agency Head approval
ISO certifies Agency Head approval.
ISO changes Status to "Submit for Approval"
Notify Security Architecture and Operations team of the Agency Head approval
Notify Security Architecture and Operations of the Submission
ISOs and Security Architecture and Operations team discuss Exception
Changes needed?
YES
NO
Security Architecture and Operations Team
Security Architecture and Operations Review
Ready for Agency Head Approval?
YES
Notify ISO for Agency Head Approval needed
Security Architecture and Operations Review
CSRM Arch. Review Complete?
YES
Notify CSRM of the Approved Exception
A
NO
NO
Return to Submitter?
YES
Notify Agency ISO
All status' set to AWAITING REVIEW
NO
STOP
CSRM
A
CSRM Review Status set to AWAITING REVIEW
CSRM Review
Approved?
NO
All status' set to DENIED. Complete Explanation of Denial
YES
Review Status set to APPROVED.
CSRM Review Date set to current date
Notify Agency ISO of the decision. Copy Director of Security, Architecture and Operations, Director IT Security Governance, NPSO,, Security Architecture and Operations

Virginia Information Technologies Agency

Navigate to the exception request

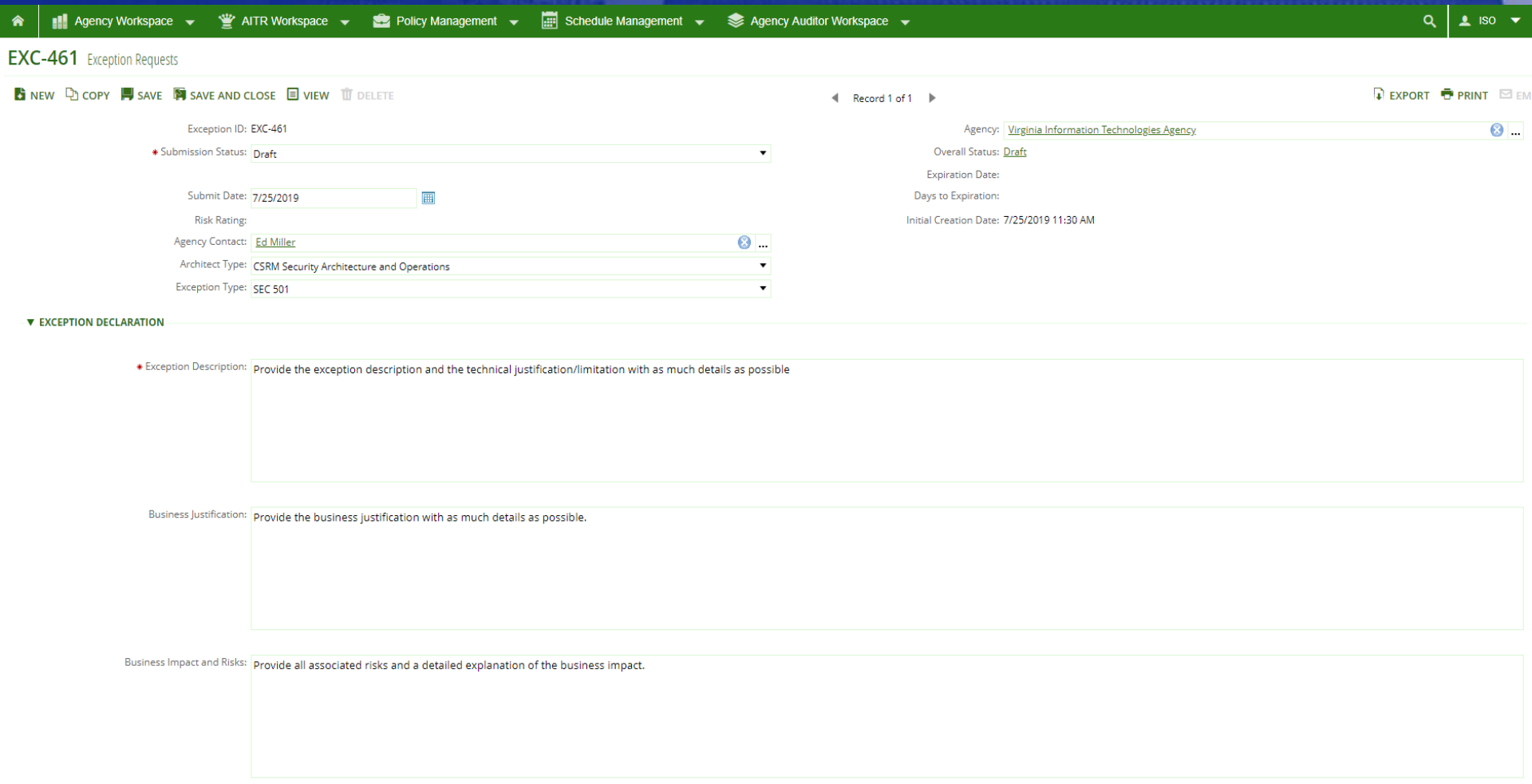


Create a new record



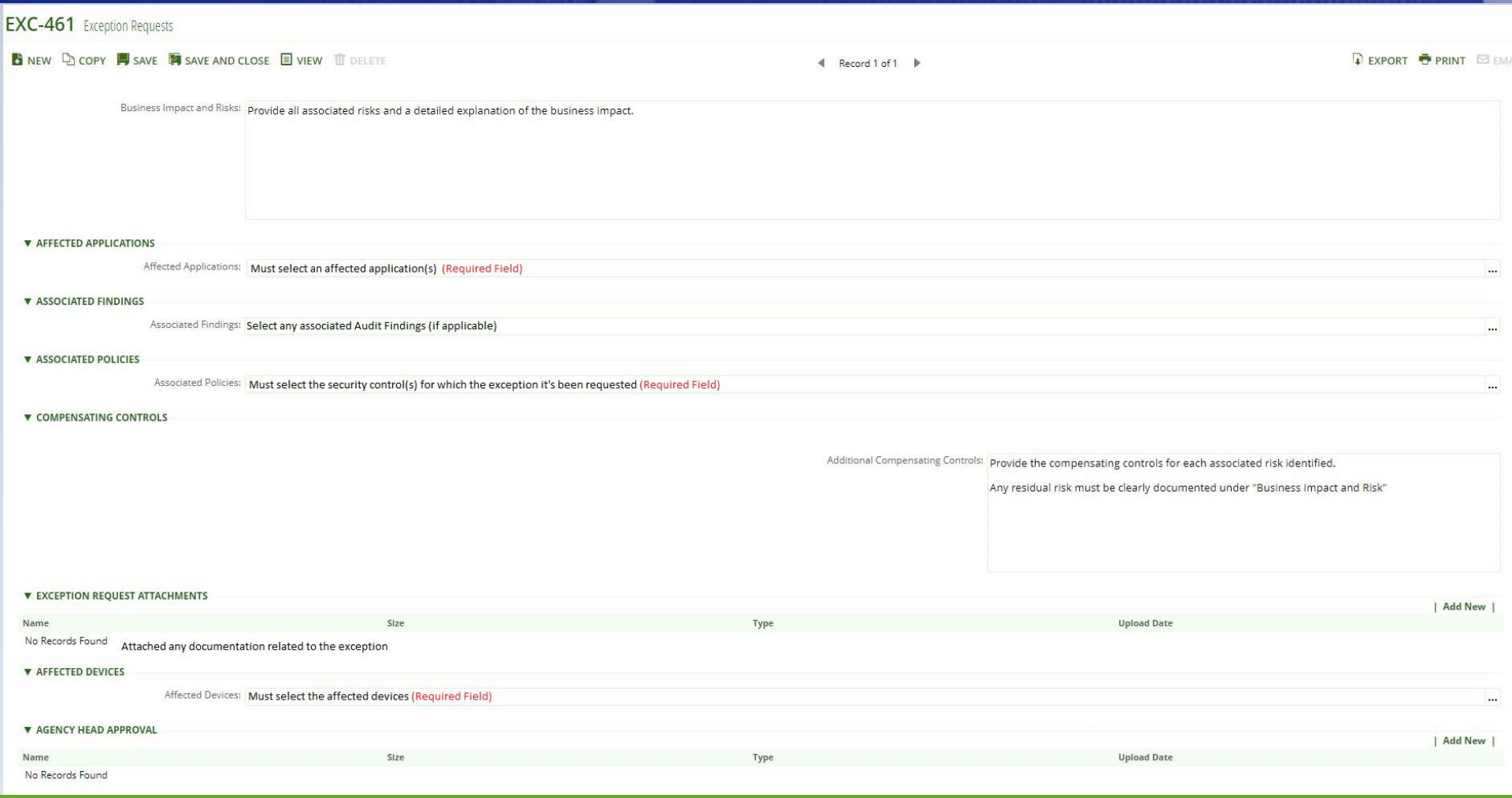
Virginia Information Technologies Agency

Enter the new record information



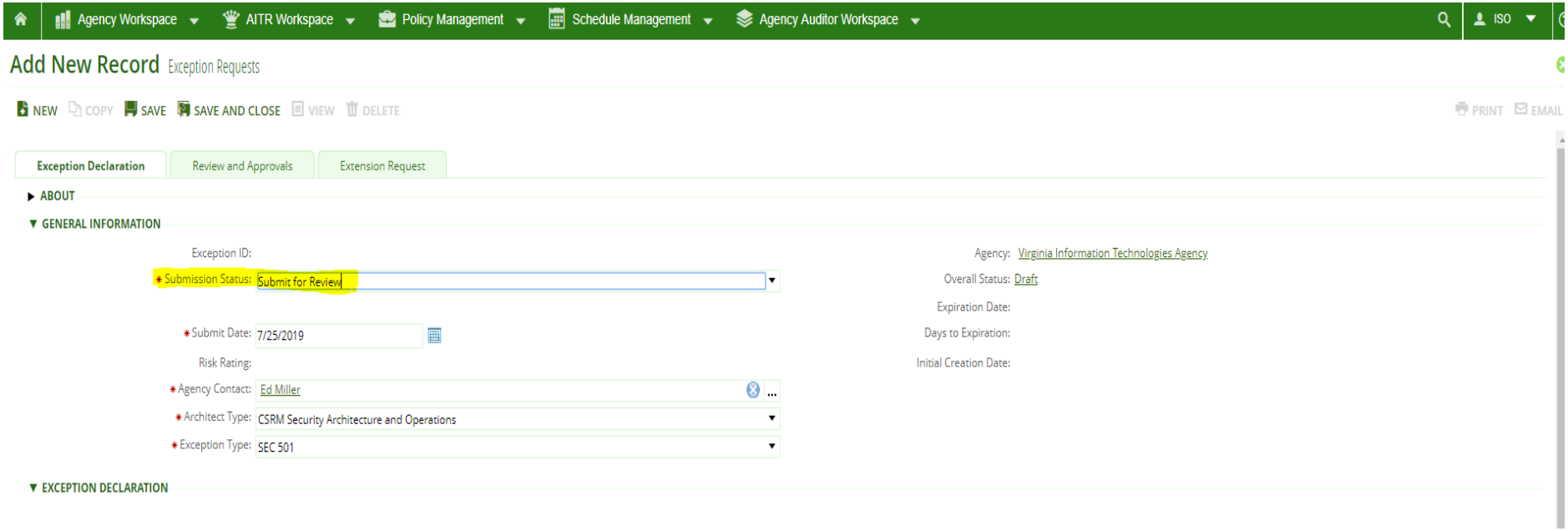
Virginia Information Technologies Agency

Enter the new record information



Change submission status

When the new record is completed and ready for Architectural review change the Submission Status to “Submit for Review” and SAVE.



An email is sent to the Architectural team. The Overall Status will update to

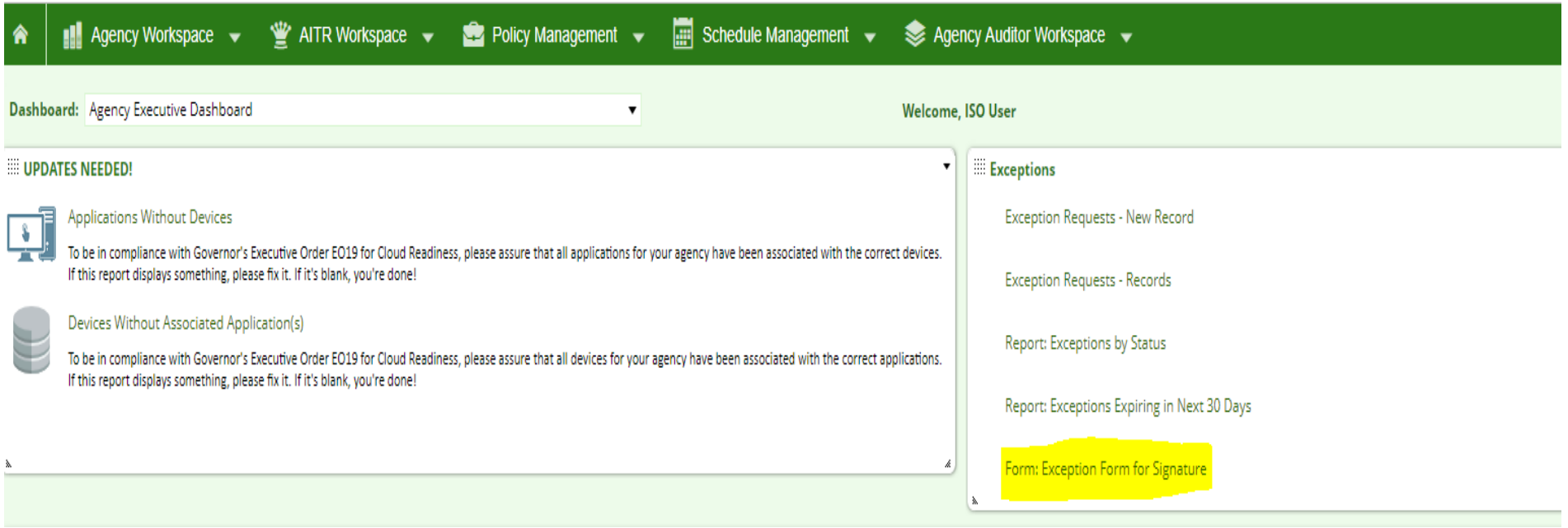
Overall Status: In Architecture Review

Architectural review

- During the architectural review the security architecture team, operations team and ISOs will discuss the exception and finalize the exception for agency Head approval.
- The exception status will be changed to architect review complete and the agency ISO will receive a notification email to obtain agency head approval.

Agency head approval

- ISO can print the "exception form for signature" located at the agency workspace. Submit to agency head for signature.



Agency head approval

- Agency head approval can also be obtained by emailing the agency head. The email must include the following exception information:

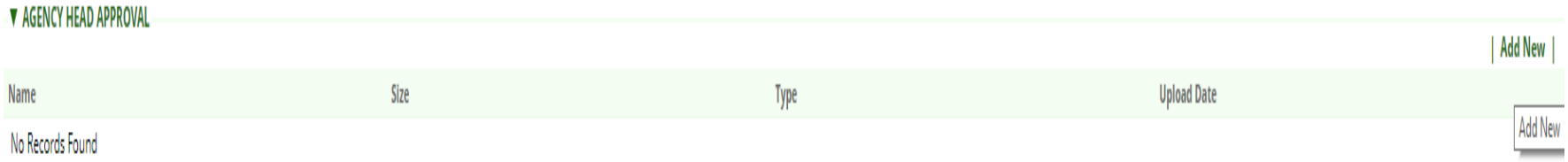
✓ Agency	✓ Associated Policies
✓ Submit Date	✓ Exception Description
✓ Agency Contact	✓ Business Justification
✓ Exception Type	✓ Business Impact and Risks

- Agency head will email back approval to ISO, acknowledging and accepting all the risks.

Remember emails must be encrypted!!!!

ISO update exception

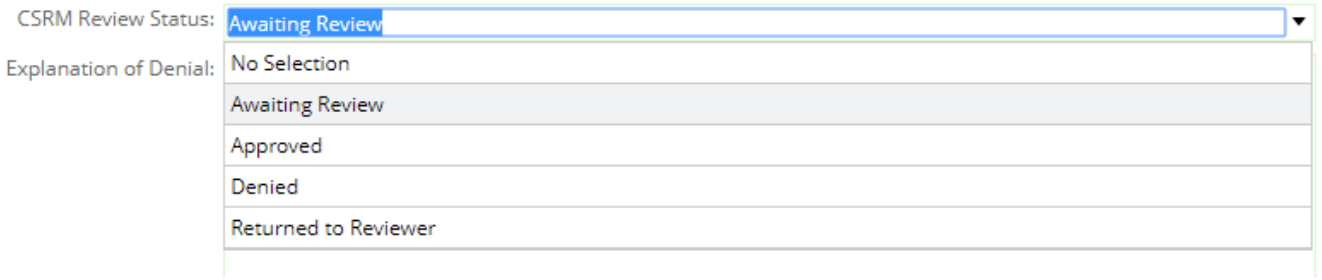
- Updates exception record by attaching the agency head approval (signed form or email)



- Changes submission status to "submit for approval"

CSRM review

- Architectural team is notified by email and the exception is routed for CSRM review
- CSRM completes review and CSRM review status is updated to either approved or denied



- Agency head and ISO receive an email notification with either approval or denial.

LIVE DEMO

https://test.itgrcs.vita.virginia.gov/default.aspx?manuallogin=true

Questions?

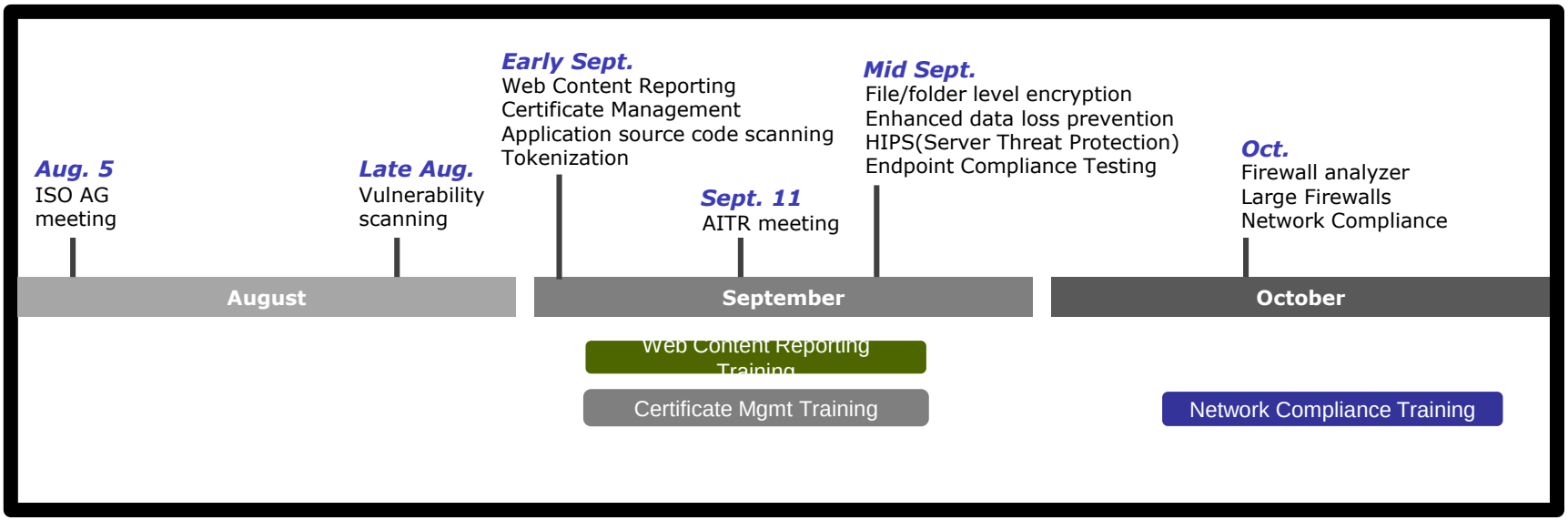
THANK YOU!

FY20 New and Enhanced Security Services
ISO AG Meeting

Aug. 7, 2019

FY20 enhanced security services

VITA and its managed security supplier, Atos, are rolling out new and enhanced security services over the next 4 mo. to enhance the security of the entire COV environment and provide agencies with more choice.



FY20 enhanced security services

New/Enhanced Service	Catalog or Enterprise Service	Expected Launch	Training?	Rollout strategy
Vulnerability Scanning and Management	Enterprise	Late August		All agencies
Web Content Reporting	Enterprise	Early September	Yes	All agencies
Certificate Management	Enterprise	Early September	Yes	All agencies
Application security / source code scanning service	Catalog	Early September	Provided after purchase	Catalog addition
Enterprise data encryption service (Tokenization)	Catalog	Early September	Provided after purchase	Catalog addition
HIPS (Server Threat Protection)	Enterprise	Mid September		Rolling releases
Endpoint Compliance Testing	Enterprise	Mid September		Rolling releases
Endpoint file/folder level encryption service	Catalog	Mid September	Job aid	Catalog addition
Enhanced Data Loss Prevention service	Catalog	Mid September		Catalog addition
Network Compliance	Enterprise	October	Yes	Rolling releases
Firewall Analyzer	Catalog	October		Catalog addition
Large Firewalls	Catalog	October		Catalog addition

Communication and training

You will receive regular communications and training (if applicable) for each new service

- Targeted audience
  - AITRs
  - ISOs
  - Agency IT staff (if requested)

70

Vulnerability scanning and management

The new Nessus agent is a lightweight agent designed to go on endpoints in cloud, mobile or on premise environments. Designed to have minimal impact on the network and the systems that they are installed on so that we may have direct access without disrupting regular operations.

- The new Nessus agent will be installed on the agency's workstations and servers
- VITA will complete pilot testing in early Aug.
- Installation will correlate directly with the agency regular patching window to not disrupt normal operations
- Atos will provide the agency with an asset list for validation

71

Vulnerability scanning and management

Installation

- Nessus Agents will be installed using VITA's software management system
- First installed under the local SYSTEM account in Windows or root on Unix-based operating systems
- Agent then inherit the permissions of the account used for installation so they can perform credentialed scans, even if the credentials on the system change

72

Vulnerability scanning and management

Benefits

- Extend scan coverage to laptops and other transient devices.
- Remove credential headaches – once deployed, agents no longer require host credentials to run future scans
- Reduce network scan performance overhead
- Easy to deploy and can be installed anywhere
- Highly secure – including leveraging encryption to protect your data
- Scan quickly – perform rapid scans on demand with little network impact

73

Upcoming Events

2019 COV ISO Certification

In order to maintain your status as a Commonwealth Certified ISO in each year after you have

initially received the certification, you need to meet 4 basic conditions:

1. **Agree to the Commonwealth IT Security Code of Ethics**
2. **Attend any mandatory ISOAG meetings each year**
3. **Attend IS Orientation once every 2 years**
4. **Obtain 20 hours of continuing education credit per year**

Steps to obtain COV ISO Certification for those who already have a professional security certification:	
Possession of recognized professional IT Security Certification	CISSP, CISM, CISA, SANS (others to be determined)
VITA Training	Attend Information Security Orientation training every 2 years
ISO Academy	Successful completion of at least one course in the KC ISO Academy per year
ISOAG attendance	Attend the mandatory October ISOAG meeting
Annual Continuing Education (only required after COV ISO Certification has been obtained)	Maintain compliance with the continuing educational requirements of the professional IT security certification body

Steps to obtain COV ISO Certification for those who do not have a professional security certification:	
VITA Training	Attend Information Security Orientation training every 2 years
ISO Academy	Successful completion of at least 3 courses per year in the KC ISO Academy
ISOAG attendance	Attend the mandatory October ISOAG meeting
Annual Continuing Education (only required after COV ISO Certification has been obtained)	Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)

Contacts

Ed Miller
Edward.Miller@vita.virginia.gov
804-416-6027

Tina Harris-Cunningham
Tina.Harris-Cunningham@vita.virginia.gov
804-416-6033

IS Orientation

Sept. 26, 2019
1–3 p.m.
Room 1221

Dec. 10, 2019
1–3 p.m.
Room 1221

Register at:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Virginia Information Technologies Agency

RVA Tenable Users Group

- **DATE: Thursday, Aug. 22, 2019**
- **TIME: 3-4:30 p.m.**
- **LOCATION: Virginia 529**
- **ADDRESS: 9001 Arboretum Parkway North Chesterfield, VA 23236**

Sign up: "Meetup"

https://www.meetup.com/RVA-Tenable-Users-Group/events/263371535/

AGENDA:

- **Open networking time**
- **Intros of all the group members**
- **Planning for next Meeting:**
  - **Topics**
  - **Speakers**
  - **Location**
- **What's new with Tenable?**
- **Demo (Technology Solution – TBD)**
- **Door Prize Raffle (Item – TBD)**

Upcoming Events

(ISC)2 Richmond Chapter Meeting

Date: Aug. 29, 2019
Time: 6-8 p.m.
Venue: Tech for Troops
4840 Waller Rd, Richmond, VA 23230

https://www.isc2rva.com/events

ISOAG meets the first Wednesday of each month in 2019

Future ISOAG

No meeting Sept. 4, this meeting is the second Wednesday of the month.

Sept. 11, 2019 @ CESC 1-4 p.m.

Speakers: Tony Fountain, Red Hat

Tanya Nacey, SAIC

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk