Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Nov. 6, 2019

ISOAG Nov. 6, 2019 Agenda

- Welcome and Opening Remarks - Mike Watson
- Incident Response Attack Lab - Brandon Lapetina
- Digital Transformation- Stan Lowe
- Audit Services Update - Mark McCreary
- ISO Services Update - Wes Kleene
- FY20 New and Enhanced Security Services Update - Bill Stewart, VITA and Darrel Raymond, ATOS

Virginia Information Technologies Agency

Centralized IT Security Audit Service

Mark McCreary, CISA, CISSP, CISM
Director

ISOAG
Nov. 6, 2019

Agenda

- Audit Requirements
- Centralized IT Security Audit Service
- Risk-Based Audits
- Benefits of Using the Service
- Common Issues Identified During Audits
- Memorandum of Understanding/Ordering the Service

IT security audits

IT security audit standard (SEC502) Requires:

- Annual audit plan submission for upcoming three-year period
- Audit of each sensitive system every three-years


IT'S AUDIT BUSY SEASON, SO I'M GOING TO NEED YOU
TO GO AHEAD AND COME IN ON SATURDAY

Centralized IT security audit service

- Assists with audit plan development

- Conducts risk-based sensitive system IT security audits

- Helps with management responses/corrective action plans

Risk-based audits

Focus on high-risk areas

Leverage results of other audits or reviews:

- System and organization controls (SOC) reports
- Prior audit reports

ECOS

- Emphasis placed on access controls and contingency planning (primarily areas where you have control)
- ECOS assessments/oversight

Benefits of using the service

- Familiar with Commonwealth Security Standards and VITA operations

- More cost effective than private firms

- Knowledge retention

Benefits of using the service

- Sensitive system audit compliance rose from 54% in 2017 to 92% in 2018.
- Completed IT security audits of 50 sensitive systems at 11 agencies in 2018.
- Helps to provide assurance that agencies are aware of any IT security issues related to their sensitive systems and are able to develop corrective action plans to address deficiencies.

Common issues

Common issues

- No formally documented and approved IT security policies and procedures
- ISO does not report to the agency head
- No 42-day password change frequency for:
  - Sensitive system authenticators
  - Administrative authenticators

Common issues

- Using end-of-life software
- Account management
  - Inappropriate privileges for regular COV accounts. We find many cases where regular COV accounts have been made members of administrator security groups on servers and workstations.
  - Not disabling inactive accounts
- Tier III data center requirements not met

Common issues

- Lack of two-factor authentication for:
  - Remote network connections for accessing sensitive systems
  - Network connections for accessing development environments or performing administrative functions on servers or multi-user systems. Two-factor is required for all network-based administrative access to servers and multi-use systems.
- Few security exceptions submitted

Memorandum of understanding

- Identifies the in-scope sensitive IT systems
- DPB provides funding to GF agencies
- Based on number of systems, number of internal auditors performing IT security audits

Questions/ordering the service

Contact me at:

Mark.McCreary@Vita.Virginia.Gov or
(804) 416-5174

Questions?

Email:
CommonwealthSecurity@VITA.Virginia.Gov

Centralized ISO Security Services Update

Wes Kleene, PhD, PE, CISM
Director, Centralized ISO Security Services, VITA

Work plan

Business Impact Analysis

Inventory and Classification

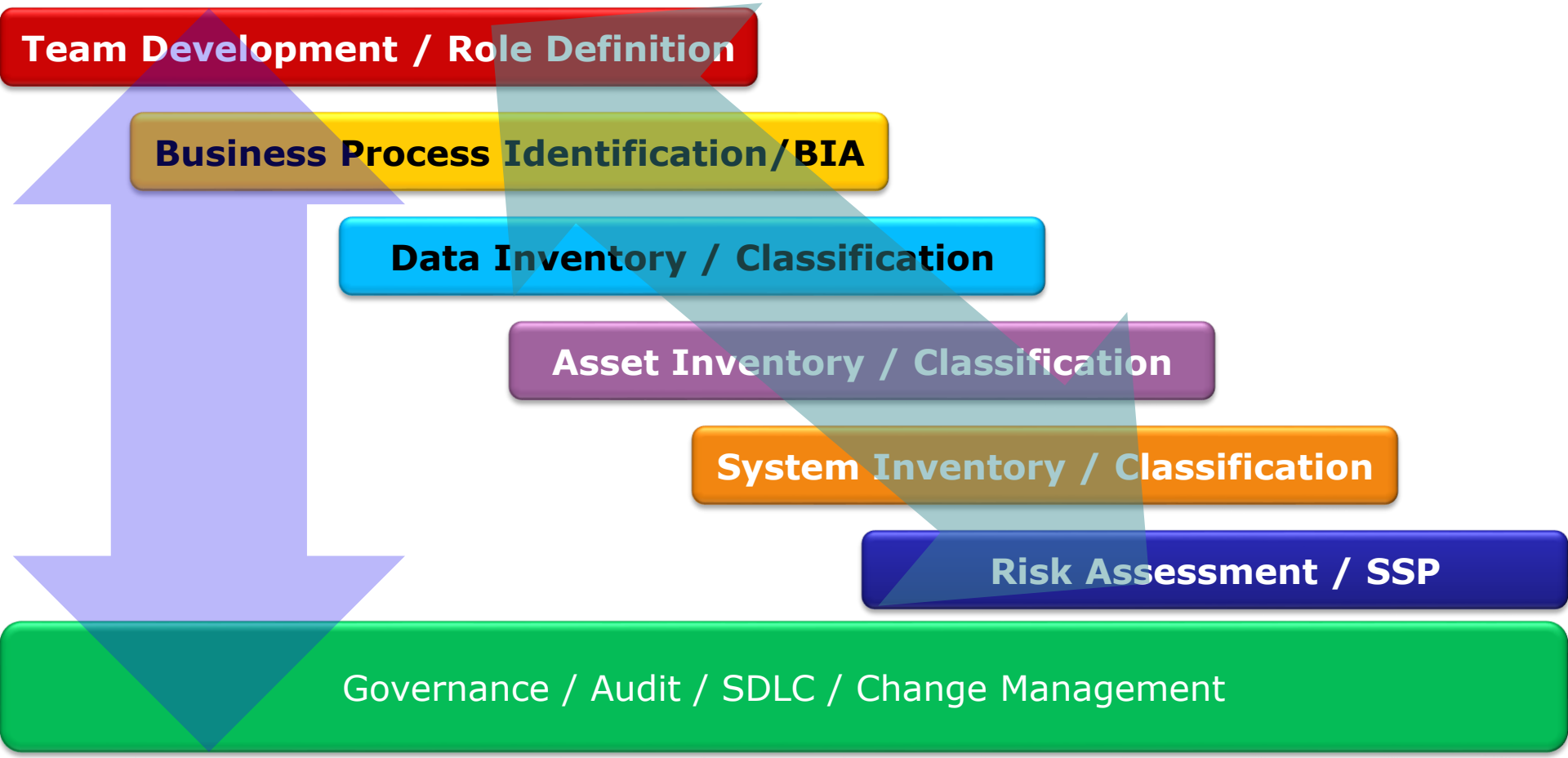
Risk Assessments

Continuous Monitoring

Business Processes

Planning

Security Program / Incident Support


Team Development / Role Definition
Business Process Identification/BIA
Data Inventory / Classification
Asset Inventory / Classification
System Inventory / Classification
Risk Assessment / SSP
Governance / Audit / SDLC / Change Management

Framework


RISK MANAGEMENT FRAMEWORK (RMF)
CATEGORIZE INFORMATION SYSTEM
SELECT SECURITY CONTROLS
IMPLEMENT SECURITY CONTROLS
ASSESS SECURITY CONTROLS
AUTHORIZE INFORMATION SYSTEM
MONITOR SECURITY CONTROLS
FEEDBACK

Program benefits / observations

- BIA / business process development for approximately 36 agencies, universities, boards, etc.
- Accomplished over 160 sensitive system risk assessments over three-year period
- Increased risk compliance from approx. 35% (2017) to approx. 98% (2019)

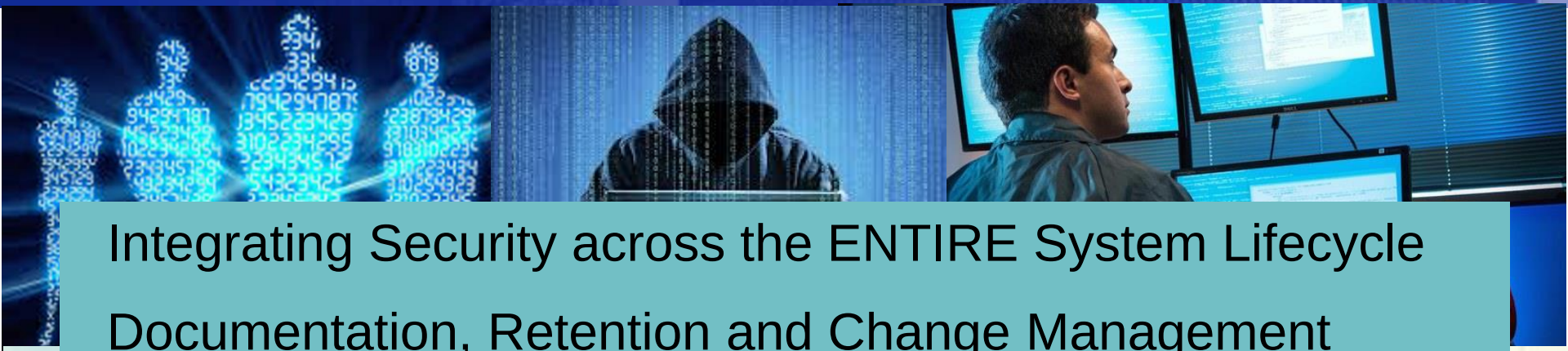
Program benefits / observations

- Security assessments included over 400 agency-specific systems (included as part of business process needs or identified as non-sensitive based on agency determinations).
- Support to agencies during high-profile events and incidents
- Where applicable, provide support for security projects (phishing, pen-test, etc.)

Who can answer the questions?

- Agency head / leadership
- Governance
- Business owner
- System owner
- Data owner
- Chief Information Officer
- Information Security Officer
- Privacy officer
- IT Project Manager
- Change Management
- System Administrator
- IT Database Administrator
- Application Administrator
- System Assessment Team
- Security Audit
- Incident Response Team
- Continuous Monitoring Team
- System Users

Observations



Integrating Security across the ENTIRE System Lifecycle

Documentation, Retention and Change Management

Continuity planning –versus- Security planning

Resources (Long-term and On-demand)

Long-Term IT and System Planning

Focus for 2020

- Agency-centric documentation to support business continuity and incident response.
- Procedural enhancements for ISO responsibilities such as:
  - Account review and approval
  - Software lifecycle planning – proactive approach
  - Risk governance, such as exception requests, system onboarding, asset inventory management
- Assessment and audit support

Focus for 2020

- Overlap between enterprise applications and agency security program needs
  - Clear definition of agency role and requirements based on specific business functions within the agency
- Communication across executive level and security team
  - Support the SEC501 Standard for ISO reporting needs

Centralized ISO security services

Security and risk management programs

- Business functions / BIA
- Inventory and asset identification
- Data classification
- System classification
- Risk assessment and remediation plans
- Vulnerability scanning
- Incident response
- Assessment and audit support

Centralized ISO Security Services

Wes Kleene, PhD, PE, CISM
Director, Centralized ISO Security Services, VITA

FY20 New and Enhanced Security Services Update ISOAG Meeting

VITA – Bill Stewart
Atos- Darrel Raymond

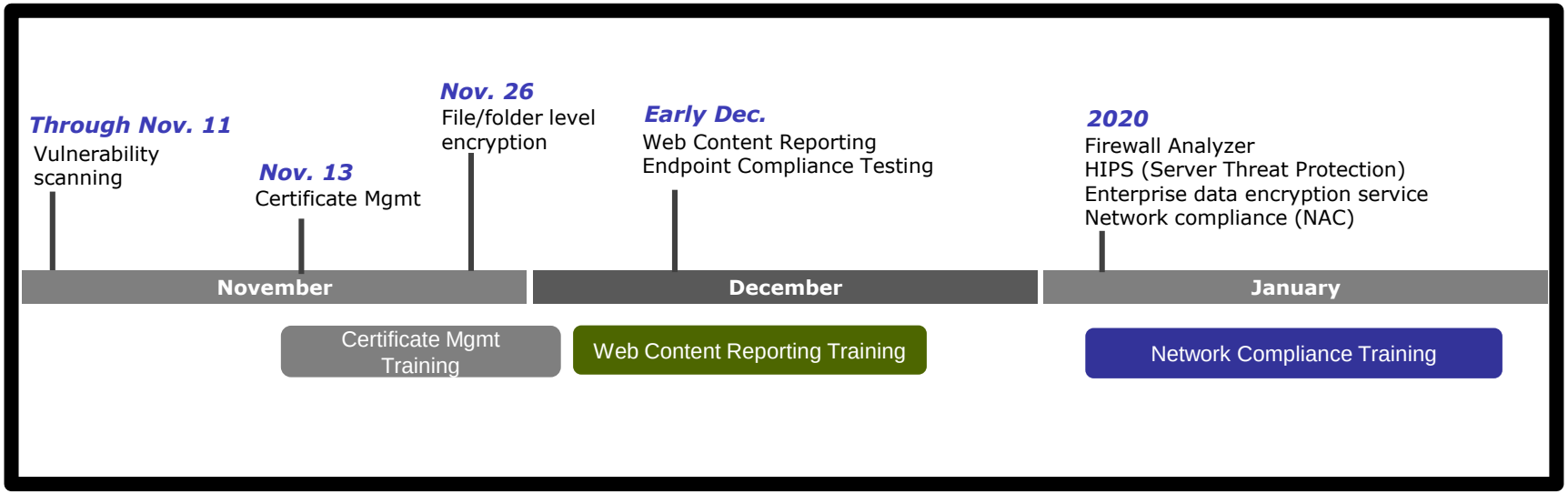
November 6, 2019

Agenda

- New and Enhanced Services Rollout Schedule Update
- Certificate Management

FY20 new and enhanced security services

VITA and it's managed security supplier, Atos, are rolling out new and enhanced security services to enhance the security of the entire COV environment and provide agencies with more choice.



*Schedule is tentative and subject to changes

FY20 new and enhanced security services

New/Enhanced Service	Catalog or Enterprise Service	Expected Launch	Training	Rollout strategy
Application and source code security	Catalog	Launched Sept. 4	Provided after purchase	Catalog addition
Vulnerability Scanning and Management	Enterprise	Agency rollouts began Oct. 14		Rolling release
Large Firewalls	Catalog	Launched Oct. 30		Catalog addition
Data Tokenization	Catalog	Launched Oct. 30	Provided after purchase	
Certificate Management	Enterprise	Nov. 13	Yes – November 19 and 21	All agencies
Endpoint file/folder level encryption service	Catalog	Nov. 26	Job aid	Catalog addition
Endpoint Compliance Testing	Enterprise	Late November		Rolling releases
Web Content Reporting	Enterprise	Early December	Yes – early December	Rolling releases
Network Compliance	Enterprise	January	Yes – January	Rolling releases
Enhanced Data Loss Prevention service	Catalog	2020		Catalog addition
Firewall Analyzer	Catalog	2020		Catalog addition
HIPS (Server Threat Protection)	Enterprise	2020		Rolling releases
Enterprise data encryption service	Catalog	2020	Provided after purchase	Catalog addition

*Schedule is tentative and subject to changes

Overview – certificate management

Provides a multi-tenant suite of certificate management for servers and end-user devices

- Helps prevent certificates from expiring
- Provides 60, 30, and 10-days notifications that prevent certificate-based outages
- New self-service portal to view all agency certificates and expiration dates
- Enforces VITA's standard certificate requirements
- Nothing is changing to the procurement process

Launches Nov. 13

Access and training

Access to self-service portal

- AITRs and ISOs will be granted access to the new tool
- Additional agency representatives can be given access through VCCC ticket

Training

- Webex training Nov. 19 and Nov. 21, 1:30–3 p.m.
- Invitations will be sent to AITRs and ISOs this week
- Additional agency representatives can be invited

Upcoming Events

IS Orientation

Dec. 10, 2019

1–3 p.m.

Room 1221

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

Future ISOAG

Dec. 4, 2019 @ CESC 1-4 p.m.

Speakers: Kathryn Rinker, NW3C

Marlon Cole, VITA

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk