WELCOME TO THE Oct. 1, 2025 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

VIRGINIA
IT AGENCY

IT Security Governance & Compliance

2025 Highlights and 2026 Plans

Amy Braden

Director of IT Security Governance and Compliance

October 1st, 2025

Agenda

- Organization Overview
- 2025 Highlights
- 2026 Plans

2025 Highlights

- Released SEC540 Data Classification and updated SEC502 IT Security Audit Standard, SEC527 Cybersecurity Awareness Training Standard, and SEC528 Prohibited Hardware, Software and Services Policy
- Supported SSA and FTI audits
- Integrated ISO Services into service delivery (SSPs)
- Increased ISO outreach programs

2026 Plans

- Provide additional guidance and clarity for key topics
- Provide customizable ISO Services engagements
- Support SSA and FTI audits
- Mature ISO outreach programs
- Update CY2025 Data points/Agency Metrics
  - New: Self Assessment (Pass/Fail) – NCSR assuming available
  - Remove: IDS Reporting
- Enforce SAT campaign requirements (e.g., naming conventions)

CISS Service Delivery

Who are we?

CISS is one of 2 security consulting services provided through VITA CSRM to assist agencies with Governance, Risk and Compliance requirements prescribed by our Commonwealth Standards.

What we do?

CISS seeks improve client organizations security cultures by providing GRC consulting services leading organizations to successful completion of security compliance activities.

- **Tri-annual BIA**
- **Annual BP reviews**
- **IT System and Data Classification**
- **System Security Plans**
- **Risk Assessments**

CISS Service Delivery

Who do we serve?

CISS is the go-to GRC-as-a-Service provider servicing COV executive branch agencies, institutions of higher learning, VITA suppliers, and expanding to partner with localities and commissions.

Current client portfolio

- 24 client organizations
- VITA supplier support

Q4-2024 to Q3 2025 Accomplishments

CISS provides GRC consulting services leading organizations to successful completion of security compliance activities.

- 58% BIA/BP reviews for 100% compliance
- 15 organizational SSP's
- 56 system specific SSP's
- 47 risk Assessments
- Intake for 50+ VITA supplier services

CISS Future State

Where are we going? Q4 2025 and beyond

Future client portfolio

- 5 potential new clients Q4 2025
- New FY-27 MOU addendums for existing clients

Project Management

- Project Charter/Plans
- AgilePlace/KSE
- ISO Service Office Hours

CISS Staffing

- 3 Approved positions
- 2 Leads
- Designated VITA/VITA supplier support team
- Leverage PM support

How to contact us

Amy Braden
Director, IT Security Governance & Compliance
amy.braden@vita.virginia.gov

Michael Vannoy
Manager, Centralized ISO Security Services
michael.vannoy@vita.virginia.gov

Thank you!
Questions?

VIRGINIA
IT AGENCY

VITA Enterprise & Security Architecture

2025 Accomplishments and 2026 Plans

Chris Williams

Director of Enterprise & Security Architecture

October 1st, 2025

Agenda

EA and SA – Our Objectives

- **Who we are**
- **What we do**
- **What we did in 2025**
- **Our plans for 2026**

Security and Enterprise Architecture – Our Objectives

Strategic Alignment and Business Value

· Align technology strategy and architecture with the Commonwealth's business goals and citizen service outcomes.

· Measure and communicate the value of IT investments in terms of efficiency, cost savings, and improved services.

Technology Standards and Interoperability

· Define and maintain technology standards, reference architectures, and integration patterns.

· Ensure interoperability across agencies by promoting shared platforms, APIs, and data exchange frameworks.

Enterprise Portfolio Management

· Maintain visibility into enterprise systems, data assets, and business processes.

· Optimize IT investments by reducing duplication and promoting reuse.

· Provide decision-makers with insights to guide system retirements, consolidations, and modernization.

Governance and Compliance (Architecture)

· Establish EA governance processes to ensure alignment with statewide standards.

· Balance centralized oversight with agency-level flexibility in the federated model.

· Ensure architectural compliance in project reviews and procurement processes.

Security and Enterprise Architecture – Our Objectives (cont'd)

Innovation and Future-State Planning

· Continuously scan for emerging technologies and assess their applicability for government services.

· Develop technology roadmaps that support digital transformation and long-term resilience.

· Pilot and scale secure, innovative solutions across agencies.

Information and Data Management

· Promote enterprise-wide data management, classification, and sharing practices.

· Enable secure, standardized data exchanges to improve decision-making and service delivery.

· Support data governance frameworks that align with security and privacy requirements.

Asset and Lifecycle Management

· Establish enterprise approaches for technology lifecycle management (from acquisition through retirement).

· Drive sustainable, cost-effective IT practices across the enterprise.

Stakeholder Collaboration and Guidance

· Act as a trusted advisor to agencies by providing reference architectures, templates, and playbooks.

· Coordinate with agency CIOs and IT leaders to harmonize enterprise standards with local needs.

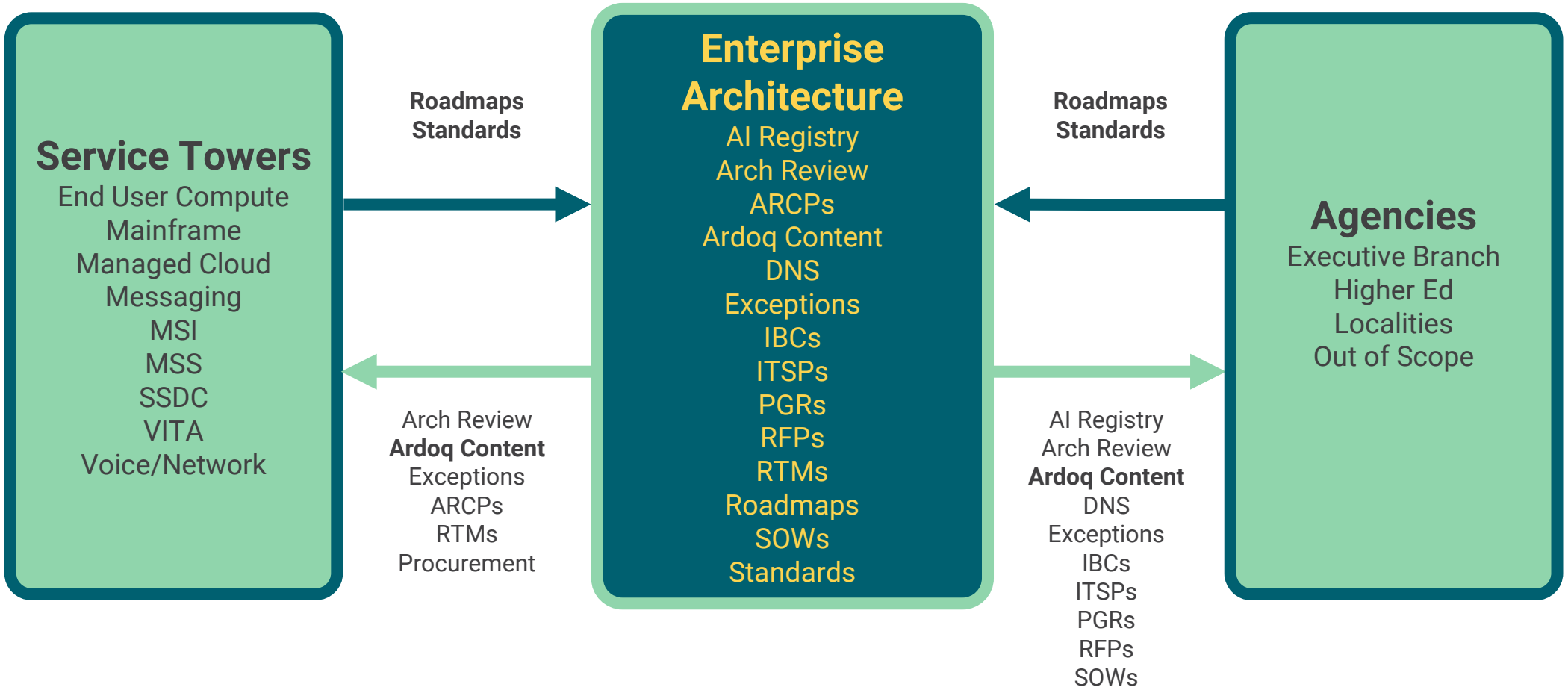
· Promote shared services and cross-agency initiatives to improve efficiency.

Workforce and Skills Development

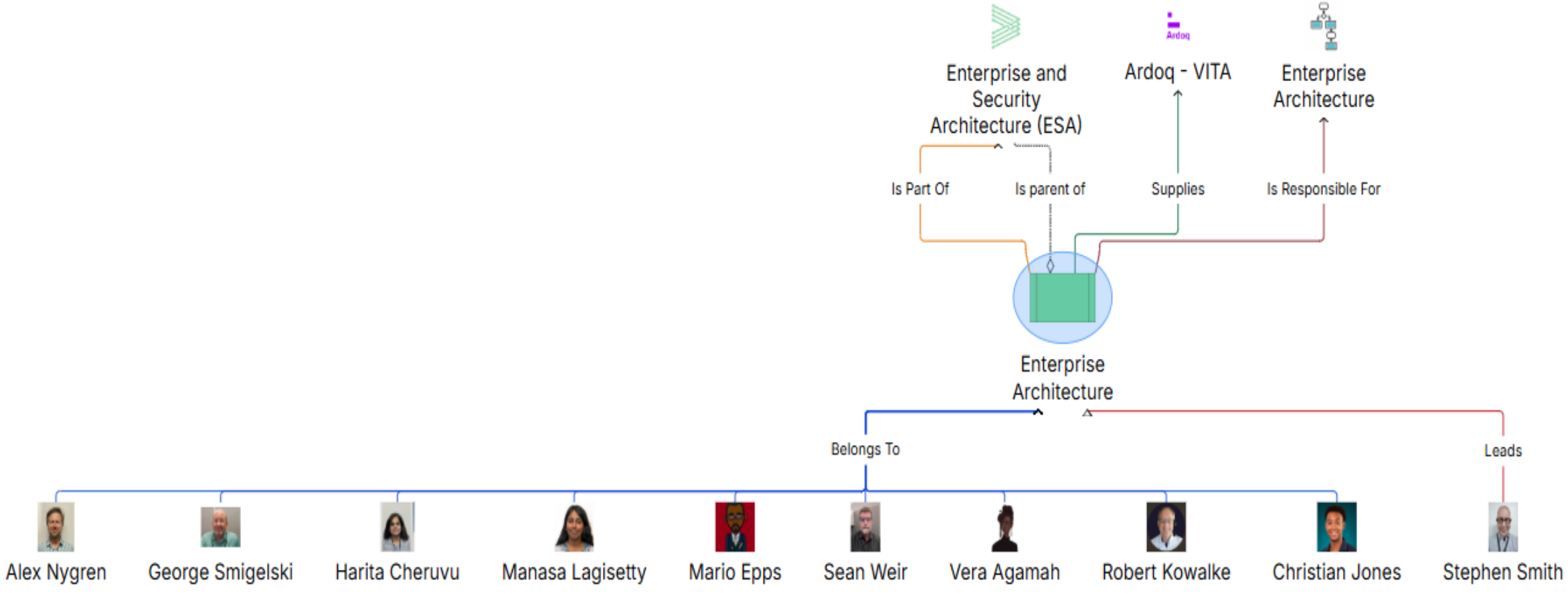
· Provide training and guidance to IT and business leaders on enterprise architecture principles.

· Build capacity for architectural thinking and system-level design across agencies.

Enterprise Architecture - What We Do



Enterprise Architecture– Who We Are



Enterprise Architecture – 2025 Accomplishments

Containerization Standard

- Created and put through ORCA and Platform for review
  - Standard created in partnership with agencies, VITA, and its suppliers
- Working on Final Approvals, to be published “soon”

Ardoq, change in scope & rollout

- Agency and VITA usage of tool
- Supplier tools

Technology roadmaps

- Updated model for roadmaps, utilizing Ardoq

Enterprise Architecture – 2025 Accomplishments (cont'd)

AI Registry & COP

- Led AI Community of Practice, held multiple AI COP meetings
- Updated AI Roadmap

Business & Technical Capability mapping

- Applied to Enterprise application portfolio

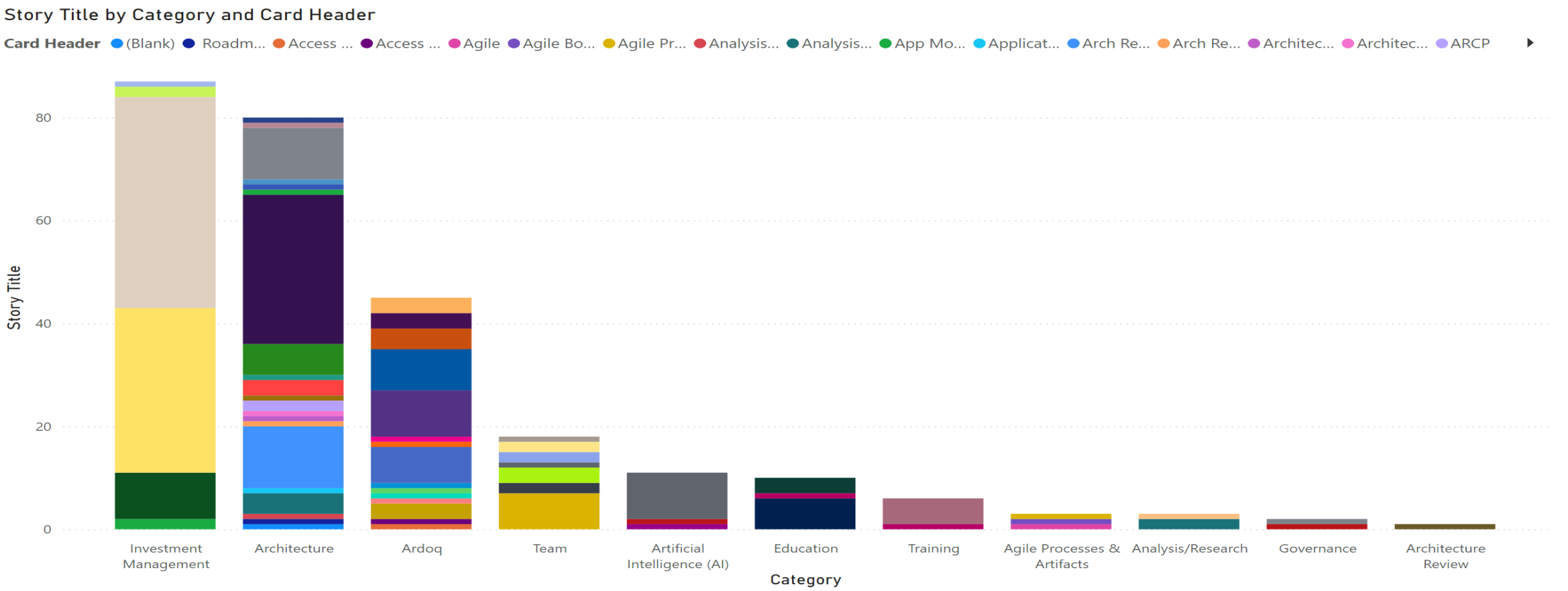
App modernization

- Enhanced agency data capture
- Took Ownership of Application Lifecycle Management

Updated EA portion of VITA website

Enterprise Architecture – Types of Work for last 3 Sprints

Smart Scapes - EA Dashboard as of 9/11



Enterprise Architecture – 2026 Priorities

Proactive

Ardoq – platform, building out content, providing additional visibility into portfolio's, providing greater insight into application portfolio

- **Growth with agencies, growth internally, adding functionality**
- **Supplier tech portfolio**
- **Patterns (AI, Cloud and other)**
- **Standards**
  - Digitizing of standards – updating process/management, draw relationships between standards and patterns and other application data.
  - Continuing to refine standards landscape
- **Additional application related data**
  - Contracts

Enterprise Architecture – 2026 Priorities (cont'd)

AI

- **Ai registry refinement**
- **AI roadmap updates**
- **AI COP**
- **AI Standard updates**
  - Agentic AI

Roadmaps

- Cloud services

AOD changes

- "Breadbasket"

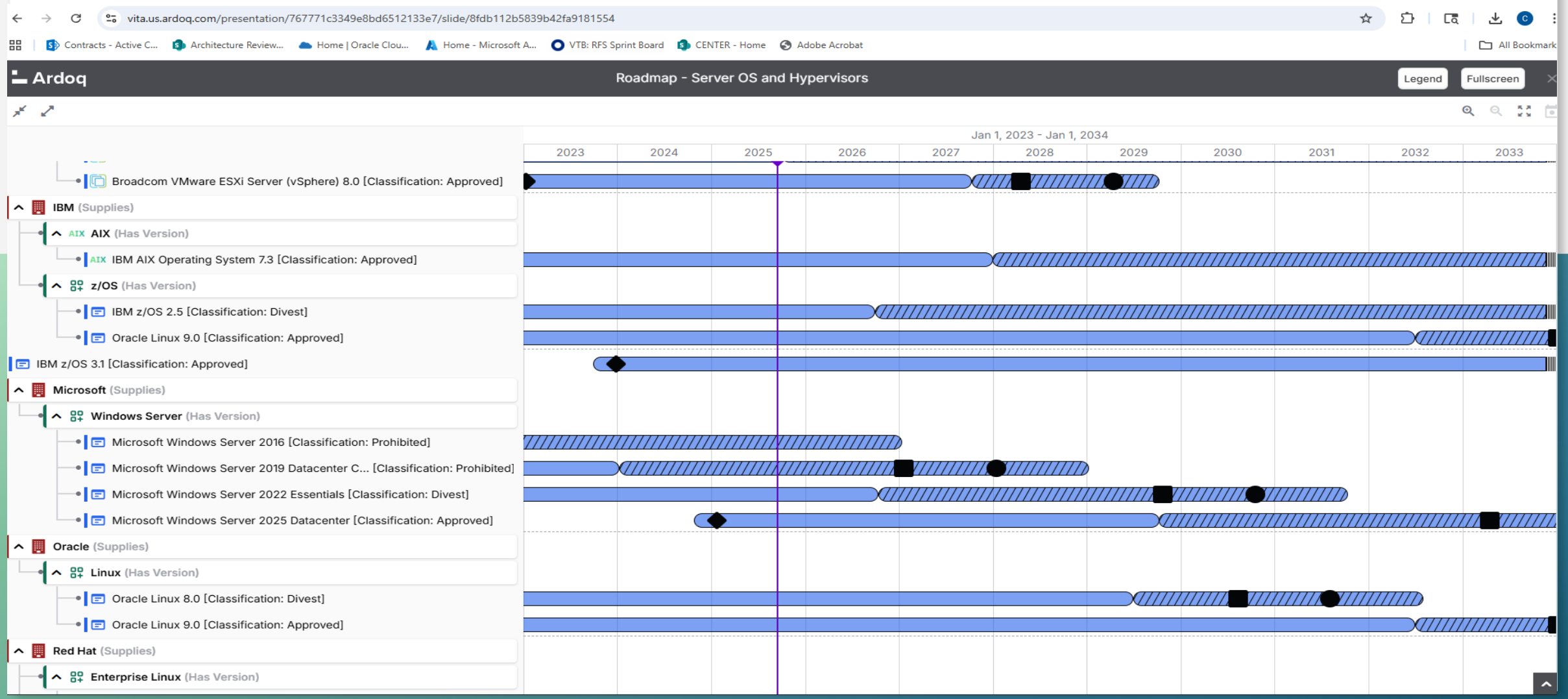
COV Ramp

- **Business and tech capability mapping**
- **Fronting the onboarding process**

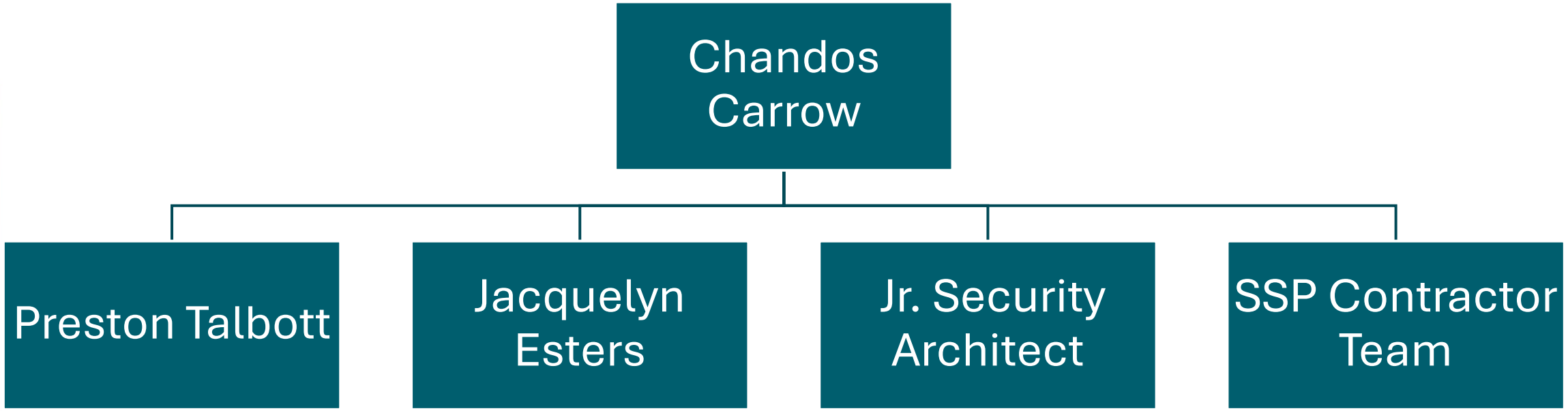
Application Lifecycle Management (formerly App Modernization)

- **Driving this process**
- **Helping agencies gain better insight into application portfolio**

Enterprise Architecture – Ardoq – roadmaps example



Security Architecture – Who We Are



Security Architecture– 2025 Accomplishments

- Over 100 security baselines reviewed
- Over 40 RITMs/INC tickets assessed
- Over 150 security exceptions assessed
- Over 350 RFS DMND requests reviewed
- Over 30 SSPs Evaluated
- Over 20 special projects completed, several more still in progress
- Involvement in 7 RFPs

Security Architecture – 2026 Priorities

Proactive / Communications / Documentation

Reoccurring Information Security Requirements for SEC530

- A document that identifies all of the events in SEC530 that a reoccurring frequency

Roles and Responsibilities Matrix for SEC530

- A document that identifies all of the events in SEC530 that a reoccurring frequency

Updates to SSP templates

Port Baseline

- Identification of the accepted and unaccepted communications ports between the zones of the Zero Trust model

Security Architecture – 2026 Priorities (cont'd)

Well Architected Cloud Framework

- A framework for all cloud service providers that identifies the network requirements to operate

Entra ID Process documentation

- Framework establishing how the various software as a services throughout the Commonwealth shall connect for identification and authorization purposes to the COV Entra ID

Control Assessment forms

- Forms to assist those with being compliant to CA-2

Baseline Instructions

- Instructions for both suppliers and the Baseline Steering Committee on how the baseline process operates and what goes into a baseline

Enterprise SSP Evaluation Instructions

- Instructions for both suppliers and the Evaluation team on how the SSP Evaluation process operates and what goes into the creation of a SSP

Questions?

VIRGINIA
IT AGENCY

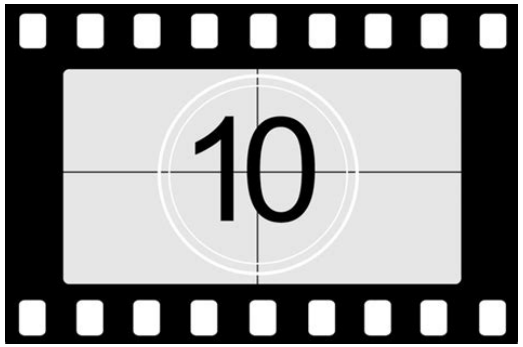
Centralized IT Security Audit Service

Mark McCreary, CISA®, CISSP®, CISM®
Director

Razaq Aweniya, CISA®
Senior IT Auditor


TOP 10 COUNTDOWN

Top Ten Audit Issues

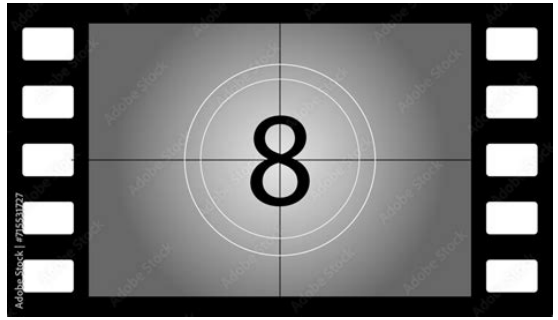


- Not documenting how the impacts resulting from a compromise of data confidentiality, integrity, or availability were determined.

Top Ten Audit Issues

- Limited review and analysis of audit logs.

Top Ten Audit Issues



- Not Disabling Inactive Application Accounts

Top Ten Audit Issues

- Agency Head not formally designating System Owners, System Owners not designating Data Owners and/or System Admins.

Top Ten Audit Issues

- Not using Two-Factor Authentication
  - When accessing sensitive systems over the Internet
  - When using a network connection to access development environments or perform administrative functions on servers or multi-user systems

Top Ten Audit Issues

- Privilege escalation using regular network accounts, for example, adding a regular network user account to a computer's Local Administrator Group or other groups used to control access to security functions.

Top Ten Audit Issues

- System Security Plans do not accurately depict "Existing" controls and/or align with Security Standards.

Top Ten Audit Issues

- Not remediating legitimate (not false-positive) vulnerabilities within required timeframes (Critical, High = 30 days, others 90 days).

Top Ten Audit Issues

- The ISO does not report directly to the Agency Head and/or is responsible for IT.

Top Ten Audit Issues

Top Ten Audit Issues

- Approved Security Exceptions are not on file for known control failures.

Top Ten Audit Issues

- No Formally Documented and Approved IT Security Policies and Procedures or Alignment with Security Standards is lacking.

What Can You Do?

Contact CSRM!

1. Become familiar with Security Standards. If you have a question about a control, the Governance team can provide clarification or an interpretation.
2. Architects can help with security exceptions and identifying mitigating controls.
3. Work with Governance to close findings when corrective actions are complete.
4. Provide quarterly finding updates to CSRM to maximize that component of the annual audit score.

Questions

Mark McCreary
Mark.McCreary@vita.virginia.gov

Razaq Aweniya
Razaq.Aweniya@vita.virginia.gov

VIRGINIA
IT AGENCY

Risk Management Update

VITA Risk Management

Jonathan Smith

Agenda

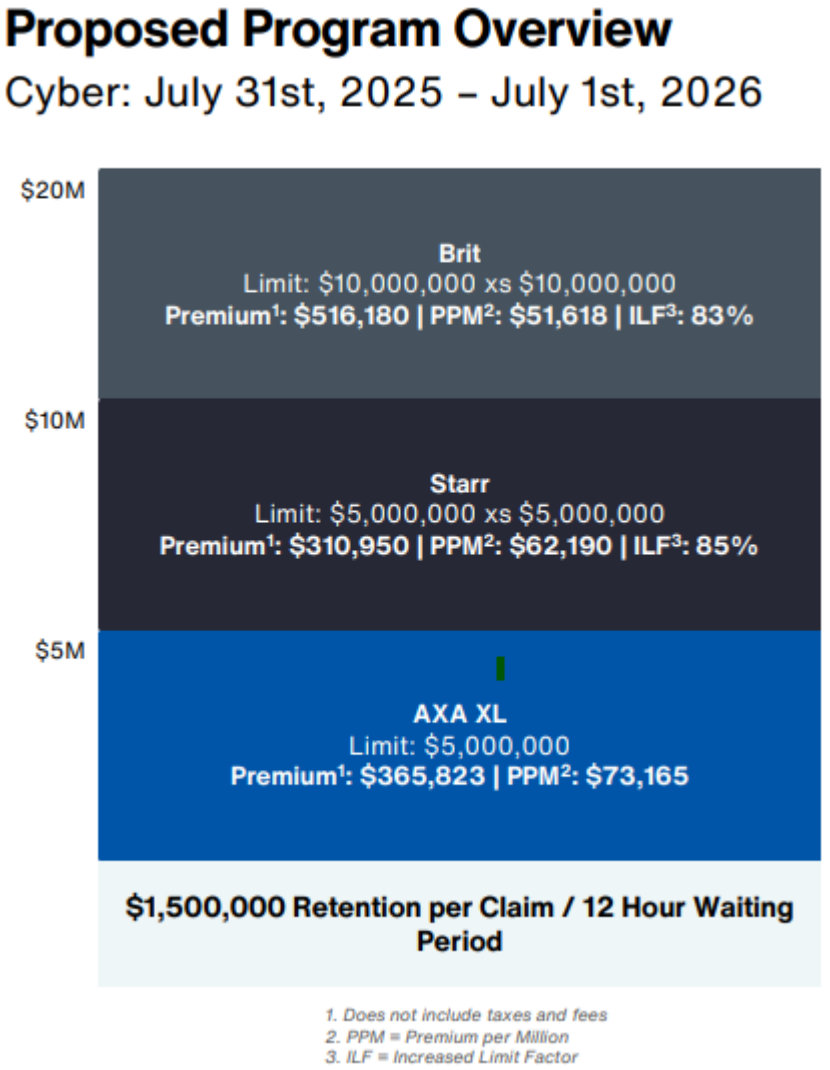
- Cyber Liability Insurance Update
- Risk Register – Purpose and Process Updates
- Team Contacts

Cyber Liability Insurance

Renewal of the Executive Branch cyber insurance policy

- Total Limit: $20,000,000

  Retention:$1,500,000
- Total Premium: $1,192,953
- Premium Savings: $376,000 reduction in annual premium costs
- Coverage Enhancements: Improved primary language and expanded coverage terms



Risk Register

Goal and Purpose

- Establish a standardized approach to agency-level risk assessments, enhance enterprise-wide reporting, and shift focus beyond compliance
- Direct agencies to conduct risk assessments based on the risks specified in the risk register
- This standardization will help agencies focus on risks CSRM has identified as important and enable CSRM and agencies to summarize system level risk to facilitate agency, secretariat, and enterprise level reporting

Risk Register

Process

- The agency risk assessment process will largely remain the same: agencies must submit Risk Assessment Plans (RAPs), conduct Risk Assessments(RAs) every three years, and report Risk Findings via Risk Treatment Plans (RTPs) to CSRM.
- The primary change is in the output: RTPs should directly reflect the assessments related to the risk register, with risk finding statements clearly mapping back to the register (e.g., “Risk of unauthorized access”)

The Risk Management Team will perform several workshops at the Risk Management Committee Meetings, and we are willing to work with agencies 1 on 1 as we get closer to the register being a requirement.

Risk Register

Process Continued- Risk Findings

- Risk Findings will tie directly to the risk register item(s) they associate to.
- Risk findings will function the same way, quarterly updates required, showing mitigation to reduce the risk to an acceptable level.
- If specific control gaps are identified as elevating risk, those controls will be documented in the risk finding mitigation plan. If the control gaps are not expected to be remediated within 90 days an exception will be required.

Access and Authorization Risks

Risk	Risk Description	Threat Agent	Vulnerability	Impact	Mitigation
Repudiation	The inability to maintain accountability (eg, asset ownership, non-repudiation of actions or inactions	Insider threats, cyber criminals, malware, software vulnerabilities	Weak Digital signatures, insufficient logging, poor time stamping, weak authentication, data integrity issues	Fraud, data manipulation; Legal disputes, operational confusion, financial loss	Digital signatures, authentication, auditing, logging services, tamper proof records
Improper Assignment of Privileged Functions	Inability to implement least privileges (eg, Role Based Access, Privileged Account Management)	Insider threats, cyber criminals, malware, software vulnerabilities, negligent administrator	Unnecessary elevated privileges, default privileged accounts, insufficient role-based access controls (RBAC), Lack of privilege reviews, insecure configurations	Fraud, data manipulation, data breach, unauthorized actions, regulatory violations, reputational damage	Least privilege, account monitoring, RBAC, automated provisioning, regular audits, approval processes, Training
Privilege Escalation	The inability to restrict access to privileged functions	Insider threats, cyber criminals, malware, social engineering, stolen credentials, misconfigurations	System misconfiguration, software vulnerabilities, weak passwords, improper access controls, kernel exploits, unsecured services, outdated software	Data breach, system disruption, lateral movement	Least privilege, Multi-Factor Authentication, Patching, Account Monitoring, Vulnerability Scanning
Unauthorized Access	The inability to restrict access to only authorized individuals, groups or services, account termination	Insider Threats, Cyber criminals, organized crime groups, nation-state actors, Third Party Contractors,	Weak passwords, lack of MFA, phishing attacks, unpatched software, misconfigurations, injection flaws, inadequate access controls, insider threat, unrevoked access, shared accounts,	Fraud; data manipulation; data exposure, budget drain, legal fallout, reputational damage	Digital signatures, authentication, auditing, logging services, access revocation, vendor vetting, endpoint security

Operational Risks

Risk	Risk Description	Threat Agent	Vulnerability	Impact	Mitigation
Mission Interruption	Interruption of COV mission critical business processes due to MEF and PBF not properly supported	Cyber attacks, natural disasters, infrastructure failures, human error, supply chain disruption, insider threats, insufficient capacity	Lack of redundancy, insufficient disaster recovery planning, poor change management, inadequate security controls, untested backups, supply chain weaknesses	Potential loss of life, negative impact to safety, disruption of critical services to citizens, reputational damage	Access Controls; IDS/IPS; Employee Training; Data Backup & Recovery; Cyber Insurance; Business Interruption Insurance; Continuous Monitoring
Business Interruption	Increased latency, or a service outage, that negatively impact business operations.	Cyber attacks, natural disasters, infrastructure failures, human error, supply chain disruption, insider threats, insufficient capacity	Lack of redundancy, insufficient disaster recovery planning, poor change management, inadequate security controls, untested backups, supply chain weaknesses	Loss of Revenue; Reputational Damage;	Access Controls; Firewalls; IDS/IPS; Employee Training; Data Backup & Recovery; Cyber Insurance; Business Interruption Insurance; Continuous Monitoring
Reduction in productivity	Diminished user productivity.	Underperforming vendor, cybercriminal, negligent contractor, Unreliable Supplier, Internal Misalignment	Third Party Downtime, Poor Integration, Inadequate Support, Over-Reliance, Lack of Training	Delayed Services, Backlogs, Staff Frustration, Financial Waste, Public Dissatisfaction	Vendor Performance Standards, Redundant Systems, Integration Testing, Responsive Support, Staff Training, Proactive Monitoring, Contingency Resources
Loss of revenue	A negative impact on the ability to generate revenue (e.g., a loss of clients or an inability to generate future revenue).	Third party vendor, cybercriminal, negligent contractor	Dependency on third parties, unsecured systems, lack of redundancy, poor contract terms, inadequate incident response	Lost Sales, customer churn, penalties and fines, reputational damage, recovery expenses	Vendor diversification, robust SLAs, Business Continuity Planning, Cybersecurity Investment, Rapid Response Protocols, Insurance, Customer Communication
Fines and judgements	Financial damages due to fines and/or judgements from statutory / regulatory / contractual non-compliance.	Third party service provider, cyber criminal, disgruntled contractor, federal/state regulator, public litigants	Lax vendor management, regulatory misalignment, unclear accountability, physical security gaps, delayed reporting	Direct Fines, court judgements, resource diversion, political fallout, service delays	Third party compliance framework, contractual safeguards, proactive audits, access restrictions, incident transparency, legal preparedness, public accountability
Reputational damage	Diminished brand value (e.g., tarnished reputation).	Incompetent vendor, cyber criminal, negligent contractor, media/activists, Disgruntled Citizens	Lack of oversight, Third-Party Misconduct, Poor Communication, Over-Dependence (third party), data exposure	Public distrust, political fallout, media scrutiny, reduced cooperation, service avoidance	Vendor vetting, Proactive Oversight, Crisis Communication, Accountability Clauses, Diversified Reliance, Public Engagement, Rapid Response

System and Data Risks

Risk	Risk Description	Threat Agent	Vulnerability	Impact	Mitigation
Data loss / corruption	The inability to maintain the confidentiality of the data (compromise) or prevent data destruction (loss).	Malicious threat actors, Non-malicious threat actors (accidental)	Human error, malware, hardware failure, network vulnerabilities, outdated software, weak authentication, phishing attacks, insider threats, power outages, natural disasters	Financial Losses (Data Recovery Costs, Downtime Costs, Productivity Losses, Regulatory Fines and Legal Fees, Compensation for Affected Individuals, Cost of Remediation); Loss of critical information; Reputational Damage	Regular Backups; Software Updates; Data Encryption; Data Validation; Invest in Reliable Hardware; Redundancy Mechanisms (Data Replication, Erasure Coding); Access Controls
Unmitigated vulnerabilities	Unmitigated technical vulnerabilities that lack compensating controls or other mitigation actions.	Hackers; Organized crime groups; Nation State Actors, Insider Threats; Third Party Vendor	Unpatched Systems; Outdated Software, Poor configurations, delayed reporting, lack of oversight	Security Breaches; Data Loss; Financial Loss; Reputational Damage; Regulatory Fines; Legal Repercussions; Operational Disruptions	Regular Vulnerability Scans; System Patches; Updating Software; Strong Access Controls; Encryption, Vendor Audits, Threat Intelligence
System compromise	A compromise of a system, application or service that affects confidentiality, integrity, availability and/or safety.	Hackers; Organized crime groups; Nation State Actors, Insider Threats (Malicious and Negligent); Script Kiddies	Unpatched Systems; Outdated Software; Weak Authentication; Weak Access Control; Cryptographic Vulnerabilities (missing data encryption, cryptographic failures, compromise of encryption keys); Human Error; Security Misconfigurations	Financial Losses (Downtime and Lost Productivity, Cost of Recovery, Legal and Regulatory Fines); Reputational Damage (Loss of customer trust, Negative Publicity); Operational Disruption (Halted Operations, Supply Chain Disruptions); Legal and Compliance Issues (Data Breach Notifications)	Strong Access Controls; Software Updates and Patches; Network Traffic Monitoring; Incident Response Plan; Encryption; Employee training
Lost, damaged or stolen assets	Lost, damaged or stolen assets.	Insider threats, cyber criminals, mishandling data storage devices, mishandling laptops and mobile devices, lack of security awareness training	Unauthorized physical access, identity theft, unencrypted hardware, lack of device tracking, lack of remote wipe capabilities	Data breaches; Financial loss (replacement costs, repair costs); Productivity loss; Operational delays; Loss of intellectual property	Physical Security (cameras, alarms, locks, badges); Asset tracking (asset tags, barcode scanners, inventory management systems); Anti-theft devices (gps tracking, laptop locks, anti-theft decals); employee training (on proper asset handling, security protocols, reporting procedures); insurance coverage (property insurance, cyber insurance, crime insurance); Policies and Procedures for asset management; Incident Response
Loss of data integrity	Unauthorized changes that corrupt the integrity of the system / application / service.	Malicious threat actors, Non-malicious threat actors (accidental)	Human error, system failures, insufficient access controls, poor data validation, outdated software, backup issues	Misguided decisions; Operational Inefficiencies; Data breach costs; Regulatory fines; Reputational damage; Inaccurate reporting; Legal liabilities	Strong Access Controls; Regular Data Validation; Data Encryption; Data Redundancy

Third Party Risks

Risk	Risk Description	Threat Agent	Vulnerability	Impact	Mitigation
Third-party cybersecurity exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from third-party cybersecurity practices, vulnerabilities and/or incidents that affects the supply chain through impacted products and/or services.	Compromised Vendor, malicious insider at third party, external hacker, nation-state actor	Misconfigurations; Weak Access Control; Unpatched Software; Outdated Software; Lack of Security training; Weak Authentication; Lack of Visibility into Vendor Security; Exploitation of Vendor Networks; Vulnerabilities in Third-Party Applications; unsecured data sharing	Data Breaches and Information Exposure; Financial Losses; Reputational Damage; Operational Disruptions; Regulatory and Legal Consequences	Due Diligence (Assessing cybersecurity posture of third-party vendors before engaging them); Continuous Monitoring; Contractual Obligations; Incident Response Planning; COVRAMP/ECOS; FedRAMP
Third-party physical security exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from physical security exposure of third-party structures, facilities and/or other physical assets that affects the supply chain through impacted products and/or services.	Compromised Vendor, malicious insider at third party, compromised contractors, external criminal	Inadequate vetting, unrestricted access, poor credential management, weak perimeter controls, lack of oversight	Theft of assets, physical sabotage, data exposure, safety risks, operational downtime	Background checks, access segmentation, credential control, surveillance and logging, physical security audits, training and awareness, secure perimeters
Third-party supply chain relationships, visibility and controls	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from "downstream" third-party relationships, visibility and controls that affect the supply chain through impacted products and/or services.	Compromised Supplier, Cyber criminal, nation-state actor, negligent third party, insider threat	Limited Visibility, weak vetting, uncontrolled access, lack of standards enforcement, single source dependency	Operational downtime, security breaches, financial loss, public safety risks, reputational damage	Supply chain mapping, enhanced visibility tools, rigorous vetting, access controls, standardized requirements
Third-party compliance / legal exposure	The inability to maintain compliance due to third-party non-compliance, criminal acts, or other relevant legal action(s).	Non-compliant vendor, cyber criminal, negligent contractor, regulatory authority, litigants	Inadequate Due Diligence, Unenforced Standards, Ambiguous Contracts, Poor Oversight, Data Sharing Risks	Fines and Penalties, Lawsuits and Judgements, Operational Restrictions, Reputational Harm, Resource Drain	Comprehensive Vetting, Regulatory Alignment, Robust Contracts, Ongoing Monitoring, Secure Data Practices, Training Requirements, Legal Contingency Plans
Misuse of product / service	The misuse of the product / service in a manner that it was not designed or how it was approved for use.	Faulty Vendor, Malicious Supplier, Cyber Criminal, Negligent Contractor, End User	Substandard Quality of Services, Security Flaws, Lack of Testing, Misaligned Usage, No Usage Oversight	Service Disruption, Security Breaches, Financial Loss, Legal Exposure, Public Trust Erosion	Quality Assurance, Security Validation, Usage Restrictions, Monitoring and Audits, Vendor Accountability, Redundancy Plans, User Feedback Loops
Reliance on the third-party	The inability to continue business operations, due to the reliance on the third-party product and/or service. Lack of appropriate cyber liability insurance	Unreliable vendor, malicious actor, negligent contractor, competitor nation, regulatory body	Single point of failure, lack of alternatives, Opaque Operations (Limited visibility into third party performance), Weak Contracts, Resource Overstretch	Operational paralysis, security compromise, financial strain, public service delays, reputational damage	Diversification of vendors, contingency planning, vendor performance monitoring, strong SLAs, Capacity Building, Risk Assessments, Exit Strategies

Organizational Program Risks

Risk	Risk Description	Threat Agent	Vulnerability	Impact	Mitigation
Compliance	A lack of compliance to COV information security standards reduces an agency's ability to measure and mitigate risk.	Improper organizational reporting structure, lack of security prioritization	Hidden or Undocumented Systems; Inadequate roles/responsibilities training, lack of agency support	Undefined risk, undefined security controls,	Perform compliance documentation in accordance to SEC530 and SEC520 requirements
Compliance Reporting	Compliance reporting provides enterprise risk context and decision making	Improper organizational reporting structure, lack of security prioritization	Hidden or Undocumented Systems; Inadequate roles/responsibilities training, lack of agency support	Undefined risk, undefined security controls,	Perform compliance documentation in accordance to SEC530 and SEC520 requirements
InfoSec Structure	Information Security reporting issues, conflicts of interest, or separation of duties	Improper organizational reporting structure	Personnel constraints, lack of security knowledge from leadership	Undefined risk, undefined security controls, conflict of interests	Ensure proper reporting structure and conflict of interests
Legacy Software	The presence of legacy software or software that will become unsupported at some point	Hackers; Organized crime groups; Nation State Actors, Insider Threats; Script Kiddies; Cybercriminals	Unpatched Security Flaws, Outdated Security Measures; Lack of Vendor Support; Lack of Built-in Security Features; Lack of Modern Security Tools; Exploitation of Outdated Protocols	Incompatibility with Modern Security Tools; Incompatibility with Modern Systems; High Maintenance Costs (may require specialized knowledge and expertise and potentially lead to higher costs for spare parts and support); Difficulty/Inflexibility Adapting to change; Limited scalability (may not be able to scale to meet growing business demands hindering expansion and innovation); Inefficient Performance; Regulatory Compliance Challenges leading to fines (may struggle to meet evolving regulatory requirements); Data Privacy Concerns; Legal risks	Regular Security Audits/ Risk Assessments; Vigilant Patch Management; Network Segmentation; Dependency Management (regularly update software and frameworks to address known vulnerabilities); Robust Access Controls; Strong Identity and Access Management; Enforce Multi-Factor Authentication; Data Encryption; Data Backup and Recovery; Continuous Monitoring; IDS/IPS; SIEM; Incident Response Plan; Modernization Roadmap; Consider Modern Technologies

Contacting Us

- Jonathan Smith, CSRM Risk Manager Director- jonathan.m.smith@vita.virginia.gov
- Matt Steinbach, CSRM Risk Management Manager- matthew.steinbach@vita.virginia.gov

Risk Analysts by Secretariat

- Andrew Wirz, Andrew.Wirz@vita.virginia.gov – Commerce and Trade, Finance, Independents, Security
- Isaac Amoani, Isaac.Amoani@vita.virginia.gov – Agriculture & Forestry, Education, Labor, Natural Resources,
- John Willinger, John.Willinger@vita.virginia.gov – Administration, Authority, Public Safety, Transportation
- Marjean Adarkwa, Marjean.Adarkwa@vita.virginia.gov – Executive, Health and Human Resources

Questions?

Break

VIRGINIA
IT AGENCY

Threat Management

Dean Johnson - Director

Kathy Bortle – Threat Intelligence and Vulnerability Manager
Scott Brinkley – Incident Response Manager

October 1, 2025

Incident Response

Scott Brinkley

Incident Response Projects

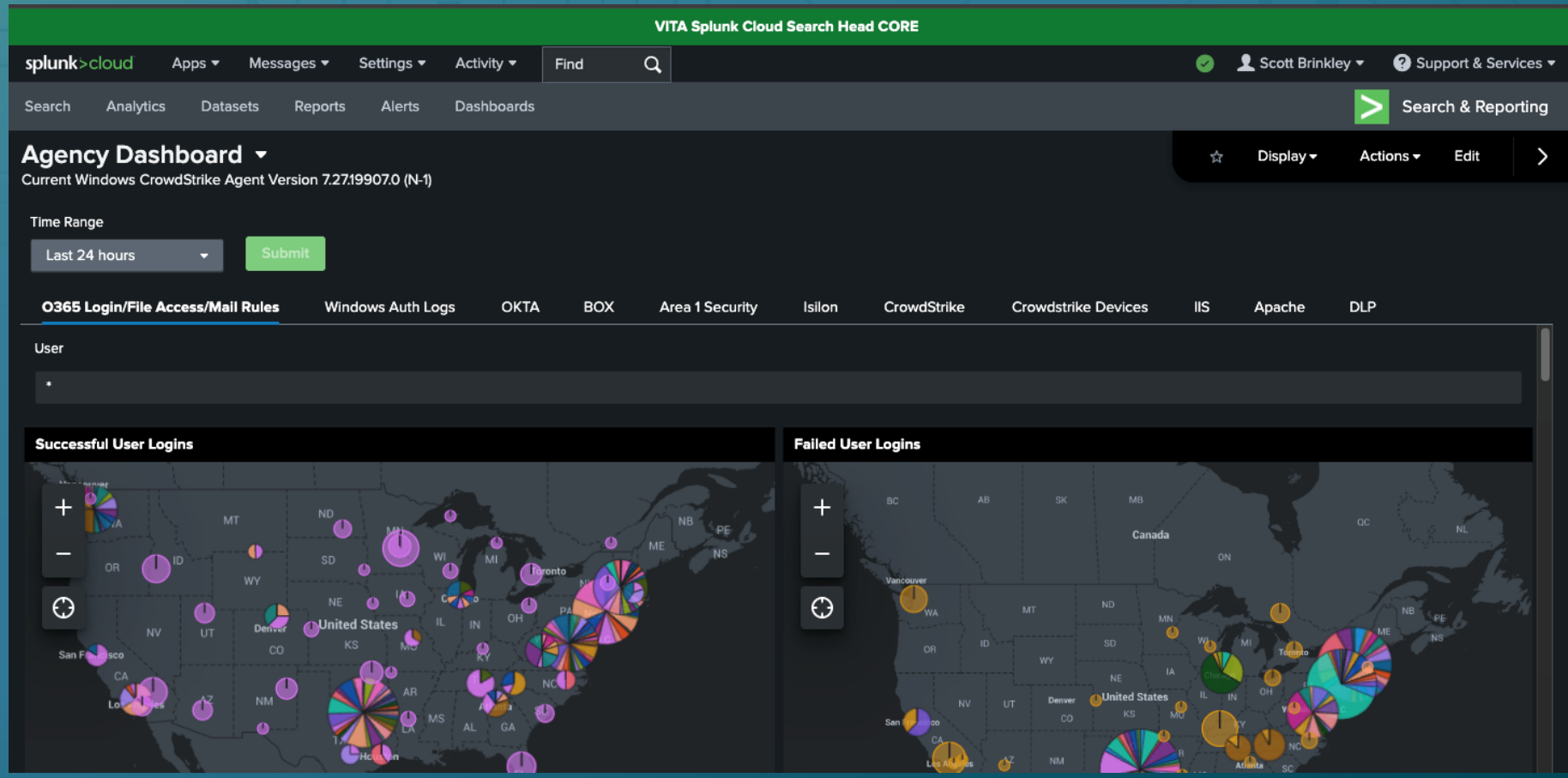
INCIDENT RESPONSE AUTOMATION INITIATIVE

Forensic Investigative Authorization Request (FIAR)

- Digital FIAR Form is alive and well
  - Forensic Investigation Authorization Request
- Do not be afraid to reach out to fiar@vita.virginia.gov if you need the link or for attachments
  - It is fed into a Microsoft List and you may see that notation at the bottom of the form
  - That Microsoft List is still only accessible by those who have been cleared

Splunk Agency Information Security Dashboard

Information Security Dashboard



VIRGINIA IT AGENCY

vita.virginia.gov

Information Security Dashboard

- O365 Login/File Access/Mail Rules
- Windows Auth Logs
- OKTA
- BOX.com
- Area1 Security
- Isilon
- Crowdstrike
- Crowdstrike Devices
- IIS
- Apache
- DLP

splunk> a CISCO company

Commonwealth of Virginia Tabletop Exercise

COV TTX

SAIC's MSI-SIRT team has been working with CSRM IR and the SOC to provide the Commonwealth Annual Tabletop Exercise

Exercise Date: October 28th (10AM-4PM)

This includes break times

After-Action Date: October 29th (11AM-12PM)

RSVP cut off is Oct 17th

msi-security-operations@saic.com

More details will be provided after October 17th to those that RSVP

Threat Intelligence and Vulnerability Management

Kathy Bortle

Threat Intelligence and Vulnerability Projects

USER-REPORTED PHISHING

KnowBe4 spun down as Phishing Alert Button

- A new phishing alert button is now live

NUCLEUS AUTOMATED TICKETING

Nucleus Security - Vulnerability Awareness

Nucleus Security

- Weekly scan calls have been discontinued
- Nucleus ticketing is being rolled out to agencies and is scheduled for completion by the end of October
- All tickets generated by Nucleus are assigned according to the ESSP
- To contact the Nucleus team, please submit a VCCC ticket for all questions and requests for assistance - This will allow the entire team visibility into the issue

Questions?

VIRGINIA IT AGENCY

VITA COV Ramp Team

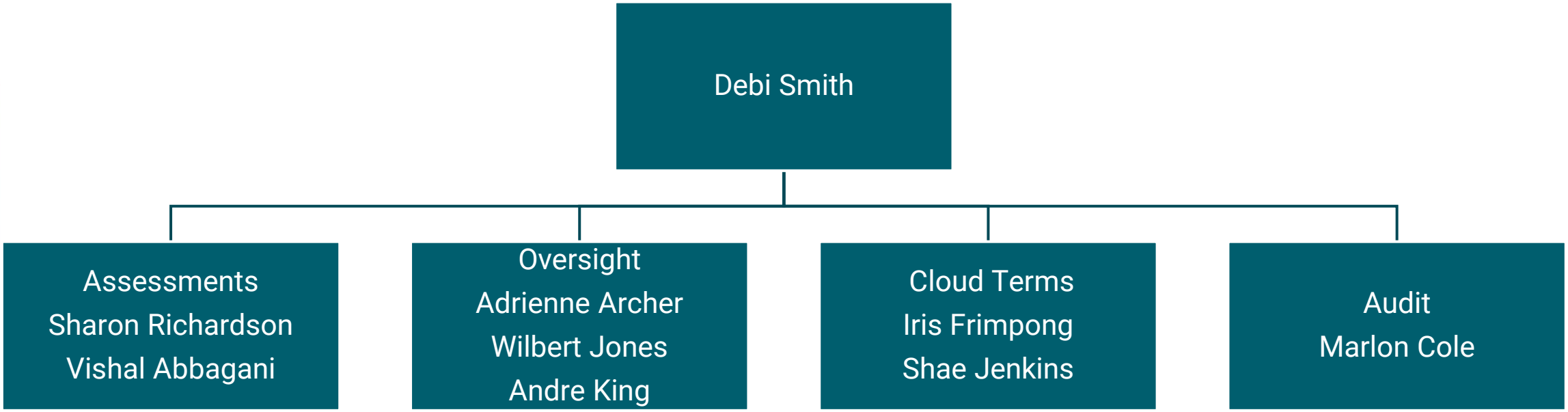
2025 Accomplishments and 2026 Plans

Debi Smith

COV Ramp Security Architect Manager

October 1st, 2025

COV Ramp Team – Who We Are



COV Ramp Team – 2025 Accomplishments

- Over 100 new security assessments completed and approved
- Over 350 security exceptions completed
- Over 100 new oversight requests received
- Over 100 security audits completed
- Over 50 new cloud terms and conditions negotiated

COV Ramp Team – 2025 Accomplishments (cont'd)

- **Updated Over 250 SEC 525 assessments to align with SEC 530**
- **Implemented and rolled out the Power BI Dashboard for Transparency**
- **Collaborated on new versions of Cloud Terms and Conditions**
  - Low Risk
  - Medium Risk
  - High Risk

COV Ramp Team – 2026 Priorities

Proactive / Communications / Documentation

Completion of Re-Reviews for SEC530

- Re-review of old SEC 525 assessments for updates to SEC 530

Roles and Responsibilities Matrix for Team

- Documentation of Team Roles and Responsibilities

Formalization of New Cloud Terms for Expedited Low Risk Solutions

- Training and Comms for the role out of the Low Risk Terms & Conditions

COV Ramp Team – 2026 Priorities (cont'd)

Proactive / Communications / Documentation

Rollout of Zen Desk

- Testing and Rollout to expedite all phases of the COV Ramp Team Tasks

Updated Training Videos

- Update Training Videos to allow for better understanding of the COV Ramp Process

Questions?

VIRGINIA
IT AGENCY

Security Products Team

Driving Innovation, Quality, and Engagement Across Our Product Portfolio

Uma Seshakrishnan

Reflecting on Success: Highlights from Last Year

The Journey Forward: Our Roadmap for Success

Main Goals: Customer Engagement and Continuous Product Evaluation

Drive **customer engagement** by leveraging direct feedback channels to optimize user activation, retention, and lifetime value. Focus on building a user-centric experience that fuels advocacy and reduces churn.

Implement **continuous product evaluation** through iterative hypothesis testing, data-driven prioritization, and backlog refinement. Ensure rapid validation to align product-market fit and accelerate value delivery.

Customer Engagement

Training & Support	Launch a series of targeted workshops to provide interactive, hands-on training sessions for users.
	Create comprehensive training videos to support smoother and faster onboarding experiences.
	Clearly communicate where users can easily locate user guides and other essential resources for self-help.
	Implement query logging system to track issues and questions efficiently

Continuous Product Evaluation

Regular user surveys to monitor product health

Define & track KPI metrics to identify gaps and measure performance

Conduct market analysis for identified gaps to ensure product-market fit

Other Important Information & Next Steps

Training Resources:

- Find user guides and onboarding videos under CSRM Connections - ISO Resources.

Share Your Feedback:

- Your input fuels continuous improvement, let us know what's working and what's not.

Get in Touch:

- Reach out at Uma.Seshakrishnan@VITA.Virginia.gov for questions, feedback, or collaboration opportunities regarding our products.

Contact Us For:

- Training support, product discovery needs, new feature requests, or pain points requiring solutions.

Questions

Richard White
Richard.White@vita.virginia.gov

Uma Seshakrishnan
Uma.Seshakrishnan@vita.virginia.gov

VIRGINIA
IT AGENCY

IS Education and Relationship Management

Kendra Burgess

Kendra.Burgess@vita.virginia.gov

Announcements

ISOAG October 2025

SPLUNK UPDATE September 2025

WE WANT YOUR LOGS:

VITA is working with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.

Top 5 Vulnerabilities

For the month of October, the Top 5 Key Vulnerabilities are:

- **PuTTY < 0.71 Multiple Vulnerabilities**
- **BeyondTrust Privilege Management for Windows < 25.2 Privilege Escalation (BT25-01)**
- **Microsoft Teams < 1.6.0.18681 RCE**
- **Citrix Workspace App for Windows Multiple Vulnerabilities (CTX691485)**
- **Microsoft Azure Data Studio < 1.48.0 Elevation of Privilege Vulnerability (CVE-2024-26203) (192147)**

NOTE Check CSRM Connections for more detailed information

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

Registration is now open!

VASCAN

October 13 – October 14, 2025

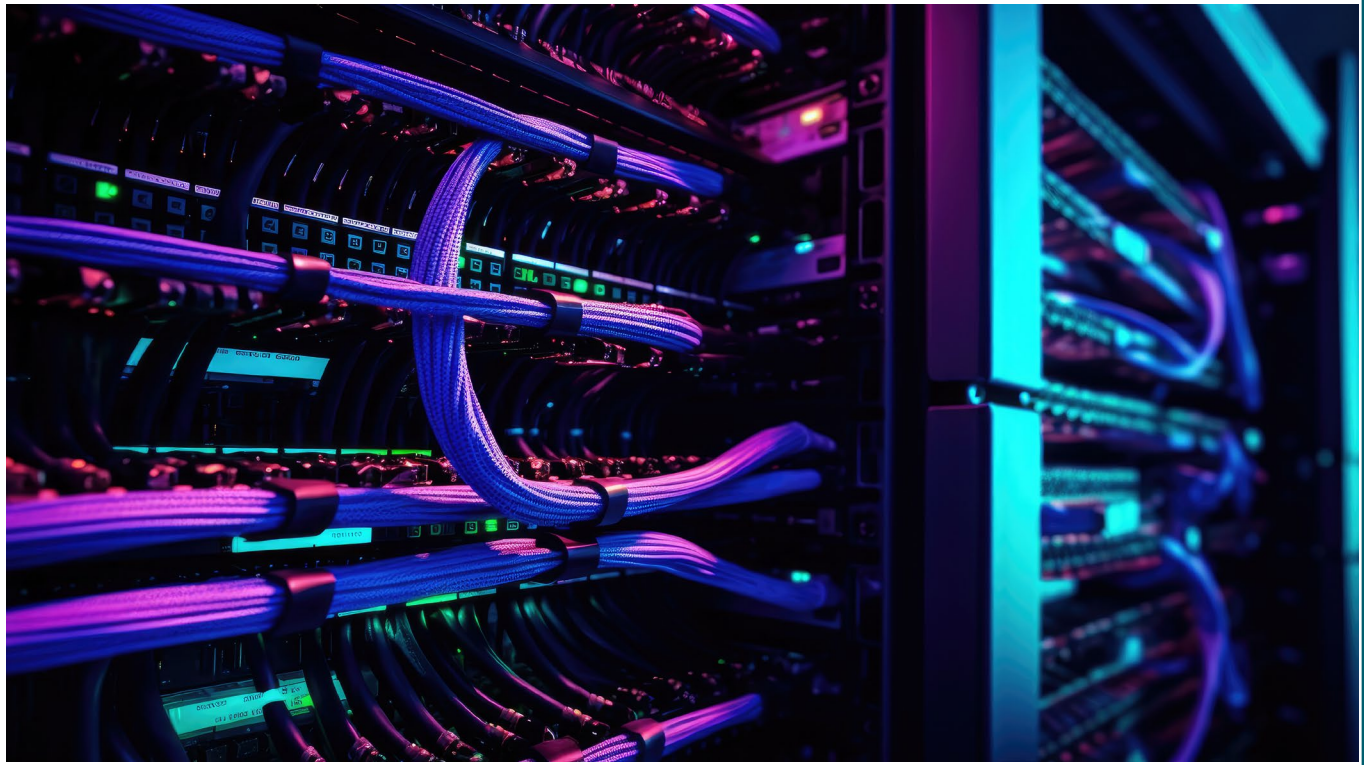
Old Dominion University
Webb University Center
1301 W 49th St, Norfolk, VA 23529

Governance Office Hours Announcement

Governance Office Hours launch recently – a dedicated space for Agency ISOs and teams to bring their questions, concerns, or ideas directly to the Governance Team.

What to Expect:

- **Open discussion place**
- **Governance Updates**
- **Q&A and support for your needs**



Next Session:
October 15th, 2025 | Microsoft Teams
[Click here to join the meeting]

Let's work together to strengthen governance across the Commonwealth!

Service Tower SOC Report Review Sessions

The upcoming SOC review session is December 11, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r4a05e20b703d317948bbc133e6645dd8

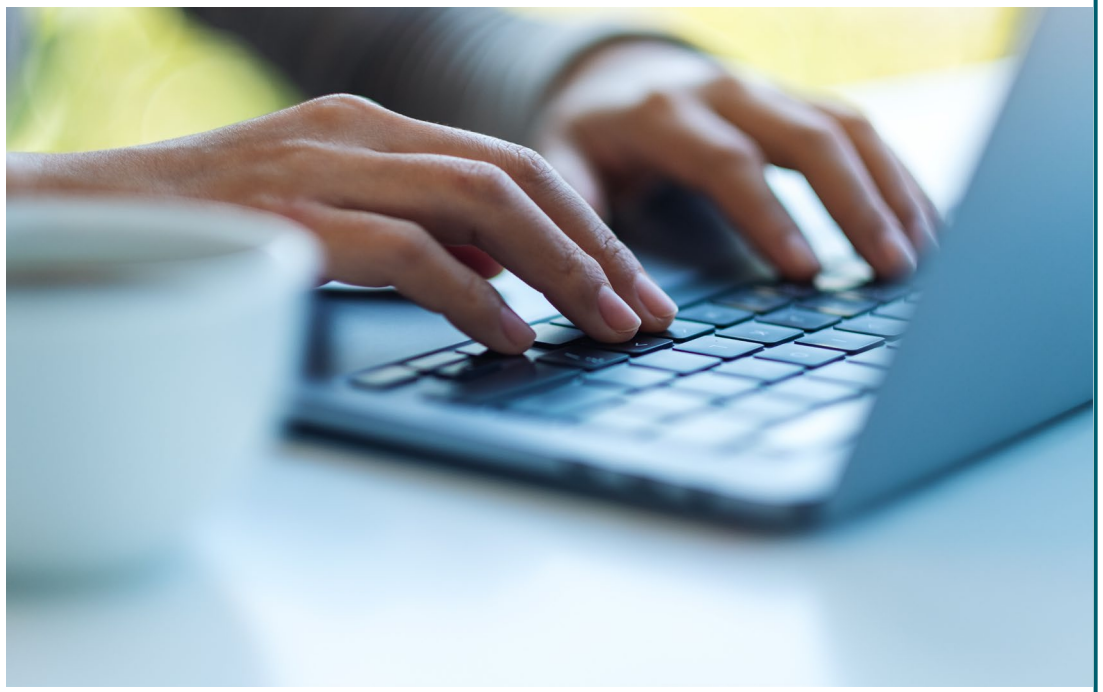
IS Orientation

The next IS Orientation is being held on December 11, 2025

- December 11, from 9am to 4pm, registration closes Dec 1st.
- It will be held in-person at the Boulders location:

  7325 Beaufont Springs Drive, Richmond, VA 23225

- Visit Commonwealth IS Orientation to register!



MEETING ADJOURNED

VIRGINIA
IT AGENCY