



# WELCOME TO THE October 2023 ISOAG MEETING





<b>AGENDA</b>	
<b>Welcome/Opening Remarks</b>	<b>Amy Braden</b>
<b>VITA</b>	<b>Bob Osmond</b>
<b>Governance Briefing</b>	<b>Amy Braden</b>
<b>Centralized ISO Brief</b>	<b>Amy Braden</b>
<b>IT Security Audit Standard 502</b>	<b>Mark McCreary/Cory Rutledge</b>
<b>Product Demonstrations (no slides)</b>	<b>Richard White</b>
<b>Risk Management Update</b>	<b>Jonathan Smith</b>
<b>KnowBe4 Phishing Lessons Learned</b>	<b>Kathy Bortle</b>
<b>CSRM Security Architecture</b>	<b>Chandos Carrow</b>
<b>Artificial Intelligence Standard</b>	<b>Stephen Smith</b>
<b>Cybersecurity Awareness/KnowBe4</b>	<b>Bertina Gaines</b>
<b>Overview</b>	<b>Trey Stevens</b>
<b>Upcoming Events</b>	<b>Bertina Gaines</b>
<b>Adjourn</b>	



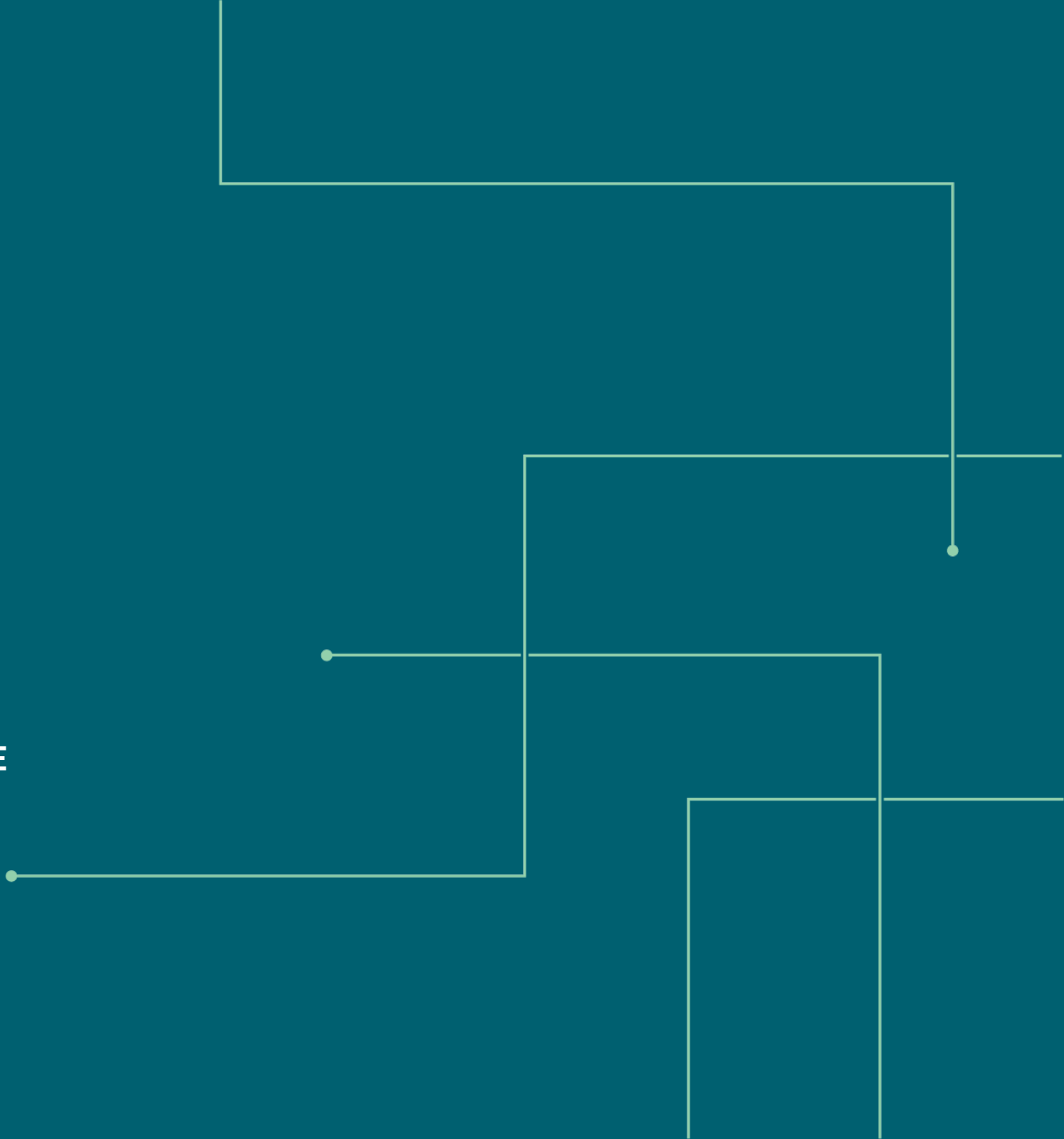
# ISOAG

**AMY BRADEN**

**DIRECTOR IT SECURITY GOVERNANCE & COMPLIANCE**

BRIEFING

10/04/2023





## AGENDA

1. Security Awareness Training Milestones
2. Policy & Standard Changes
3. Communications and Outreach

## SECURITY AWARENESS TRAINING/KNOWBE4

Milestone	Target Completion Dates	Status
Admin Training	August 2023	Complete
User Provisioning	September 25,2023	Complete
PAB Button	September 22, 2023	Complete
SAT Campaigns	September 29, 2023	In-Progress
All training complete/Reports	December 31,2023	In-Progress



## POLICY & STANDARD UPDATES & WHAT TO EXPECT

1. SEC530
2. Data Classification for Data Loss Prevention
3. Artificial Intelligence (AI)
4. Policy Template Updates



## COMMUNICATION

1. Hire Education/Relationship Specialist
2. Continue to cull and update ISO Resources
  - A. ISO Manual
  - B. ISO Training/Certification
  - C. Data Point Resource Guide
  - D. Archer Guide Update
3. Partnership with CAMs and use of standardized activity report with regular cadence

## KEY MILESTONES & DATES

1. ISO Certification – verify status before 11/1/2023
2. Ensure deliverables are submitted before **12/31/23** & metrics requirements satisfied
  - A. Missing Audit & Risk Plans align closely with grades, C or Below
3. Resources: Data Point Resource Guide, CSRM Analyst, ISO Services





## SHOUT OUT & THANK YOU TO THIS INCREDIBLE TEAM!

Chandra Barnes

Tina Gaines

Erica Bland

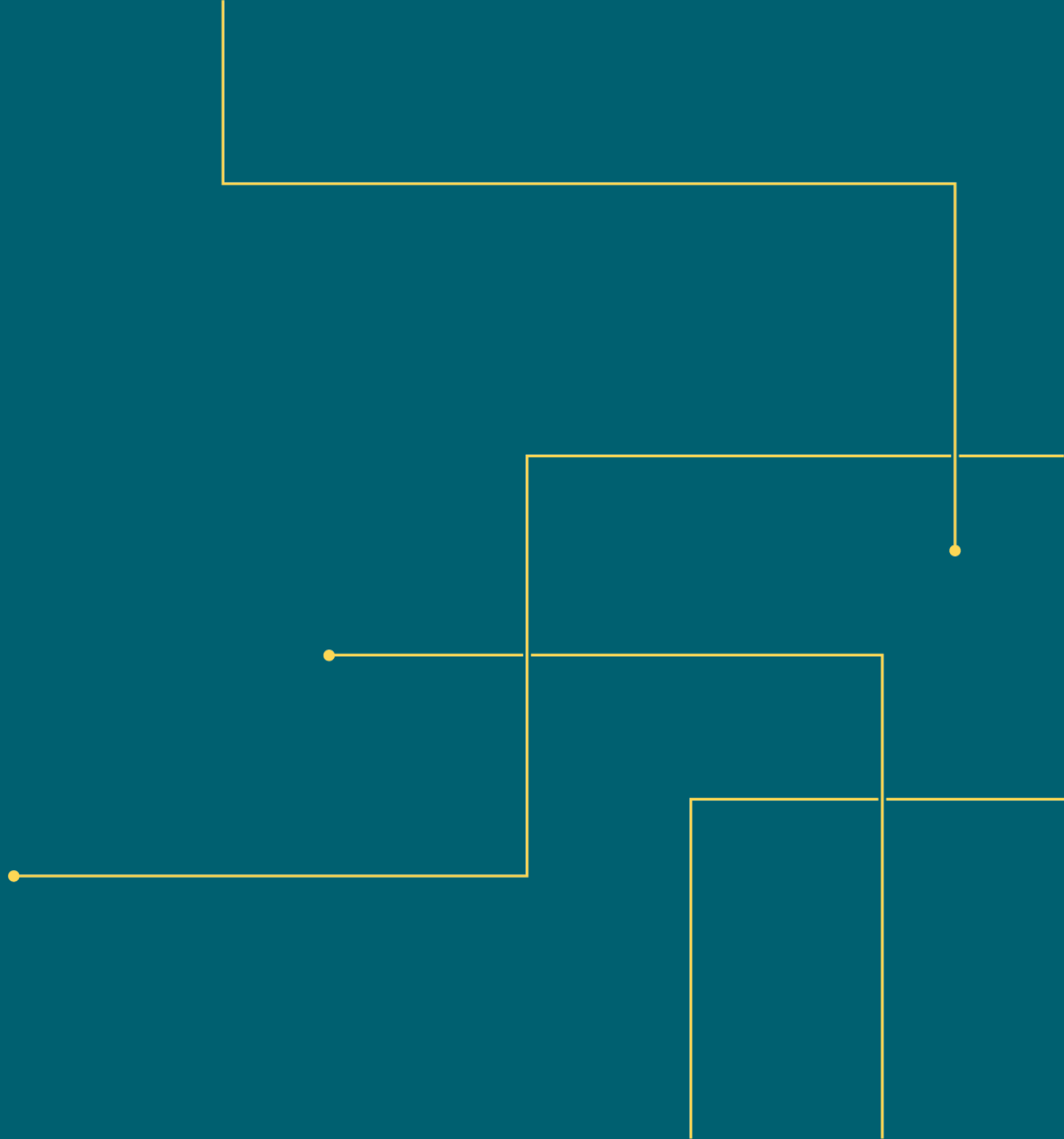
Wes Dupree

Renea Dickerson

Chris Kenyon

Johanna Opolski

**QUESTIONS?**





VIRGINIA  
IT AGENCY

## Centralized ISO Services

### ISOAG 2023 Service Delivery Brief

Michael Vannoy  
Manager, Centralized ISO Services

Oct 2023

# Service Delivery Brief

## Agenda

- Service Delivery Mission/Vision
- Program Foundations
- Key Players
- Centralized Consulting
- Current Portfolio
- Q4 Focus 52
- 2024 EPIC
- ISO Services Team
- Thank You

# Service Delivery

## Mission

- In alignment with VITA's Strategic Goal 1: Initiative 3 (Cybersecurity for VITA, VITA's customers and the whole Commonwealth), Centralized ISO Services will provide consulting services to support agency security teams in the completion of
- **Business Impact Analysis (BIA)**
- **Risk Assessments (RA) for sensitive systems**
- **System Security Plans (SSP) for sensitive systems**

## Vision

- Improve the security culture of Commonwealth agencies through increased coordination, communication, collaboration, and cooperation between VITA and agency security teams in the development and maintenance of their security programs.

# Program Foundations

## Risk Program Overview

RM Activity	SEC 519	SEC 501	SEC 525	SEC 530	SEC 520	SEC 527
Who is involved? ↓	2 (2.1) Key Security Roles	2. Information Roles and Responsibilities	2. Information Roles and Responsibilities	2. Information Roles and Responsibilities	Not defined	2. Security Awareness Training Roles and Responsibilities
Have they been Trained? ↓	2.2.7. Cybersecurity Awareness Training	AT-2 Security Awareness AT-2-COV AT-3 Role-based Security Training	AT-2 Security Awareness AT-2-COV AT-3 Role-based Security Training	AT-2 Literacy Training And Awareness AT-3 Role-based Training	Not defined	4. (C) Role Based Training
What are the Business Requirements? ↓	2.2.1 Standards	3. Business Impact Analysis	3. Business Impact Analysis	3. Business Impact Analysis	4.2 Business Impact Analysis 4.2.3 BIA / Business Process Reporting	Not defined
What are we trying to protect? ↓	2.2.1 Standards	4. IT System And Data Sensitivity Classification 5. Sensitive IT System Inventory And Definition	4. IT System And Data Sensitivity Classification 5. Sensitive IT System Inventory And Definition	4. IT System And Data Sensitivity Classification 5. Sensitive IT System Inventory And Definition	4.3 IT System Inventory and Definition 4.4 IT System and Data Sensitivity Classification	Not defined
What are our Risks? ↓	2.2.1 Standards	6. Risk Assessment	6. Risk Assessment	6. Risk Assessment	4.5 Risk Assessment (RA)	Not defined
How do we protect our data?	2.2.1 Standards	PL-2 System Security Plan PL-2-COV	PL-2 System Security Plan PL-2-COV	PL-2 System Security And Privacy Plan PL-2-COV	4.6 System Security Plan	Not defined

# Key Players

## Roles and Responsibilities / Four C's of Success



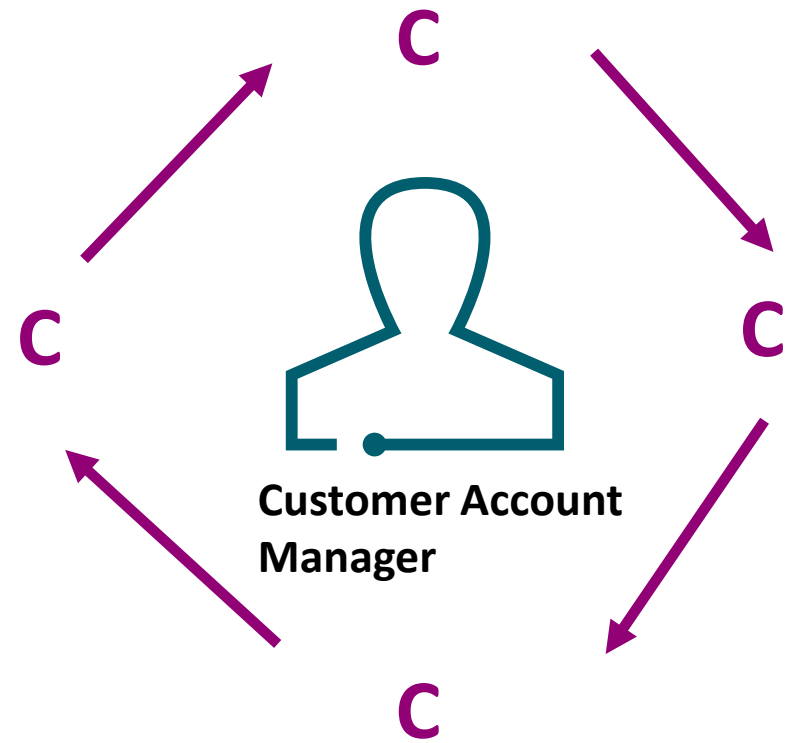
**Agency  
Head/Director**



**Information  
Security Officer**



**System Owner**



**Data Owner**



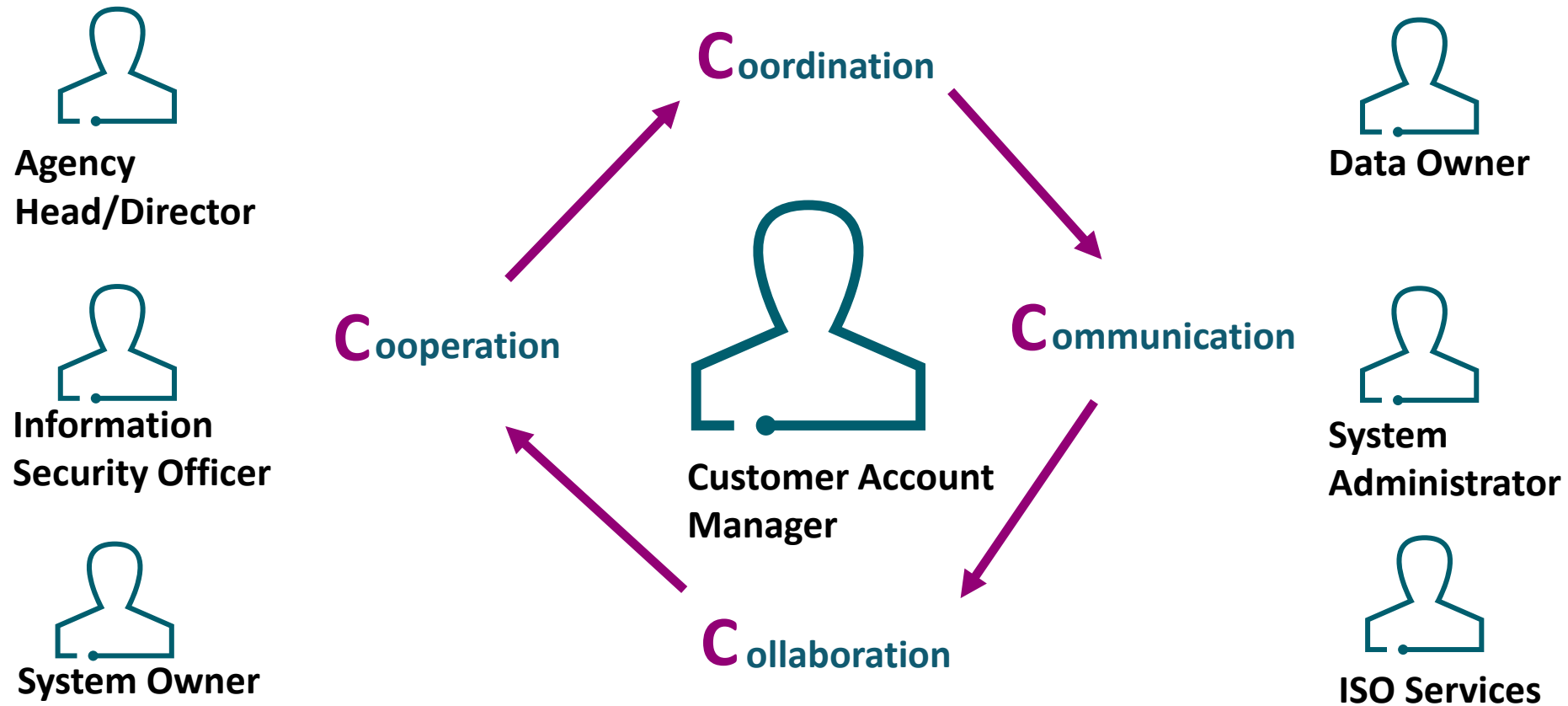
**System  
Administrator**



**ISO Services**

# Key Players

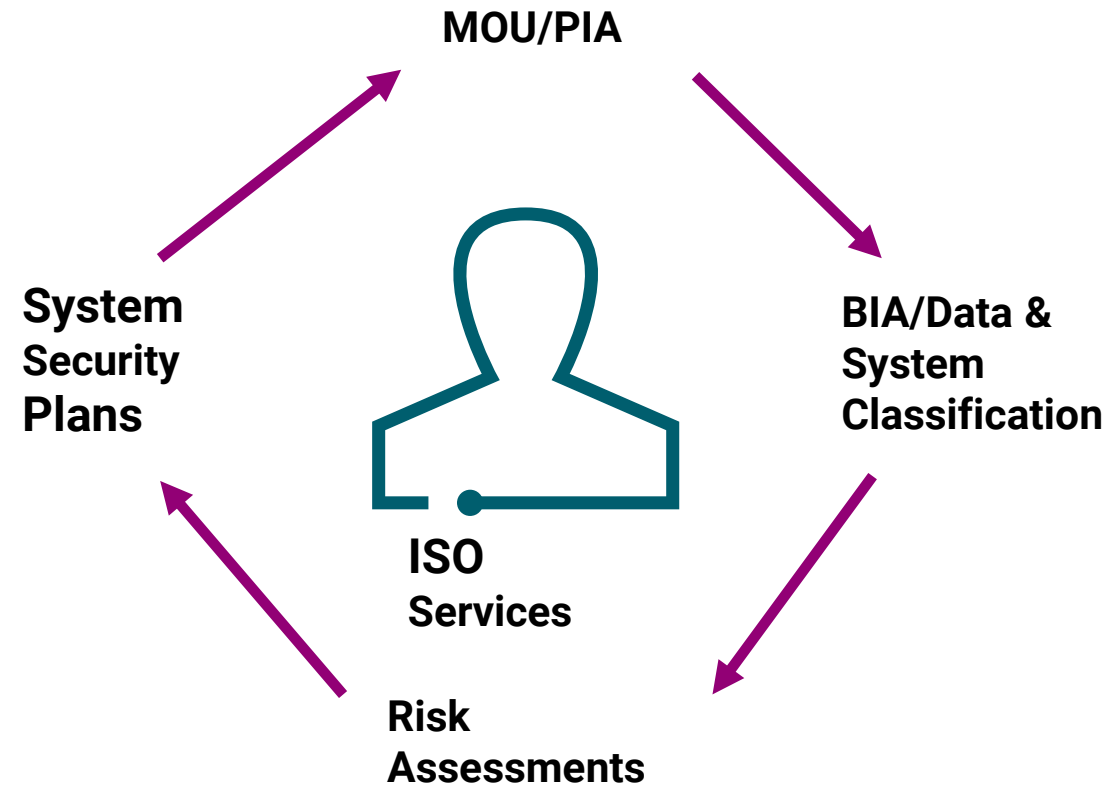
## Roles and Responsibilities / Four C's of Success



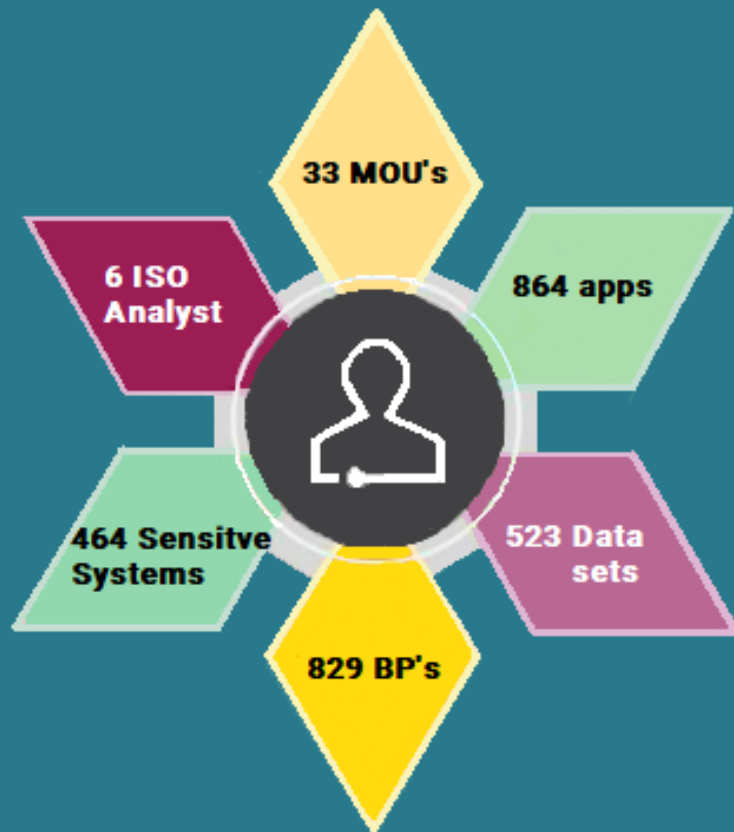


# Centralized Consulting

## Core Services



# Current Portfolio








## Current Story

- 33 Agencies enrolled
- 864 Applications
- 523 Datasets (~2.9 billion records stored)
- 829 Business Processes (351 MEF)
- 464 Sensitive Systems
- 6 ISO Analyst (~200 workdays per year)

# Q4 Focus 52

## 52 Days until the 1<sup>st</sup> week of December

 Goal	 Action Steps	 Action Officer	 Due Date	 Current Status
Update agency Business Processes	Review Archer reporting	ISO Services	10/4/2023	<b>Not Started</b>
	Provide reporting to agency for verification	ISO Services	10/5/2023	
	Review Update BIA template	Agency ISO, System Owner	10/19/2023	

## Backlog Refinement

- 165 Risk Assessments scheduled from 2021 – 2023
- 31 Sensitive Systems currently unscheduled
- 136 Risk Assessments due Q4 2023
- 553 Business processes for review (198 are MEF's)



# 2024 EPIC

## The Next 52 Weeks



## 2024 Story Splitting

Next 52 (2024)	Q1	Q2	Q3	Q4
BIA/BP Reviews	136	90	15	326
Backlog 2021&2022	99	25	6	52
Scheduled Risk Assessments	1	3	0	16
Backlog 2021&2022	*40	7	2	4
SSP Development	1	3	0	16
Backlog 2021&2022	40	7	2	4

\*Note 9 Q1 Systems schedule + 31  
Unscheduled systems

\*many of the 136 Q4 system RA's  
will be rescheduled during 2024.



- **Michael Vannoy, Manager Centralized ISO Services – [michael.vannoy@vita.virginia.gov](mailto:michael.vannoy@vita.virginia.gov)**
- **Tina Burgess, Centralized ISO Analyst – Team A**
- **Randy Jackson, Centralized ISO Analyst – Team B**
- **Emmanuel Gomez, Centralized ISO Analyst – Team C**
- **Matthew Steinbach, Centralized ISO Analyst – Team A**
- **Daniel Boakye, Centralized ISO Analyst – Team B**
- **Natthachai Chusing, Centralized ISO Analyst – Team C**

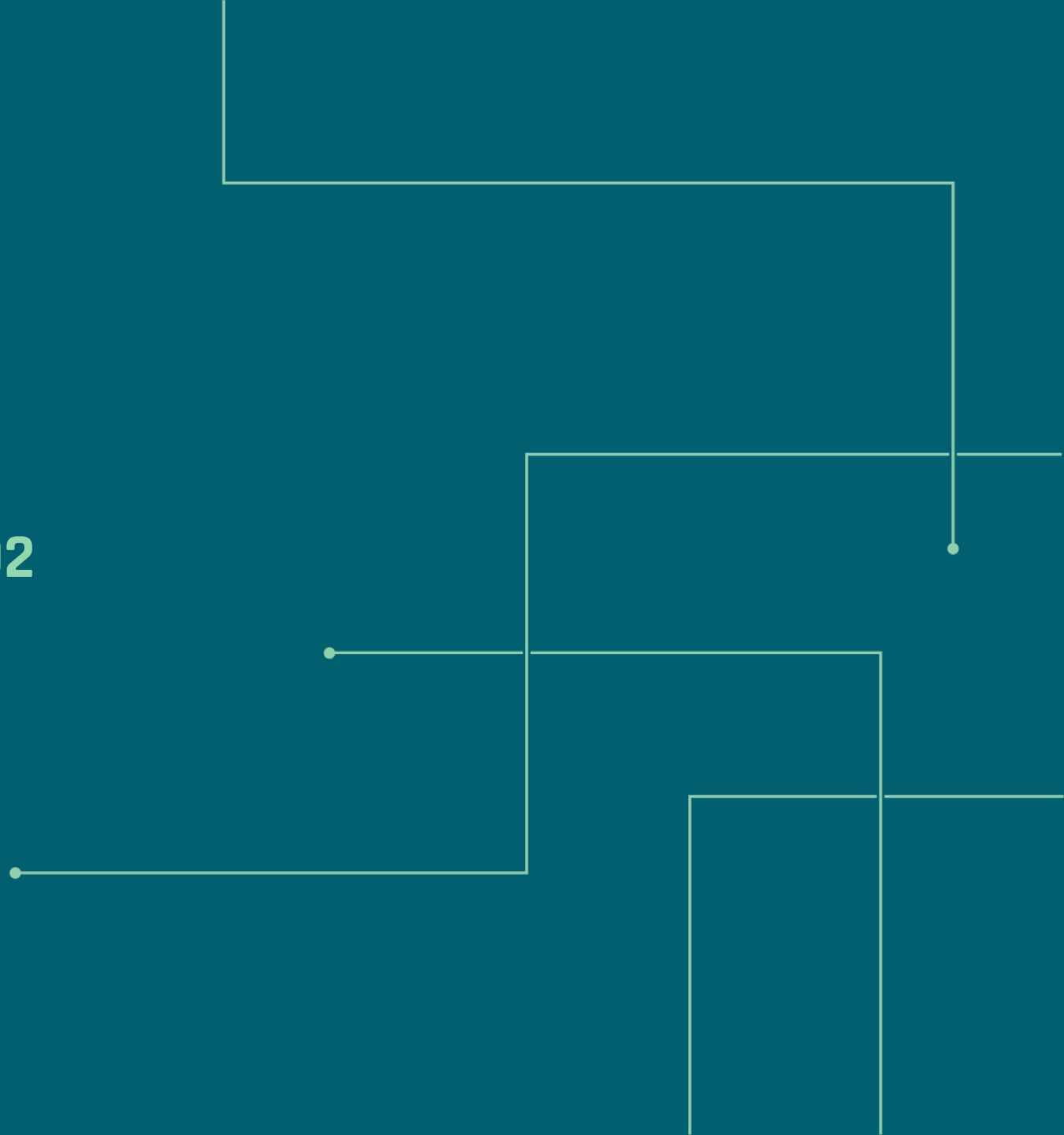




# IT SECURITY AUDIT STANDARD 502

**Mark McCreary**, CISA, CISSP, CISM  
Director, IT Security Audit Service

**Cory Rutledge**, CISA  
Manager, IT Security Audit Service



- ❖ IT Security Audit Standard Overview
- ❖ IT Security Audits
- ❖ Audit Frameworks
- ❖ Auditors
- ❖ Audit Program
- ❖ Audit Plan
- ❖ Audit Scope
- ❖ Reporting Audit Results



- Current version is 502.4

- Found on VITA's website:

<https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>

- Applies to all executive branch agencies, independent agencies and institutions of higher education that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth.

- Definition – An independent review and examination of an IT system's policies, records, and activities.



- Purpose - To assess the adequacy of IT system controls and compliance with established IT security policies and procedures.

All IT security audits must follow an established auditing framework.

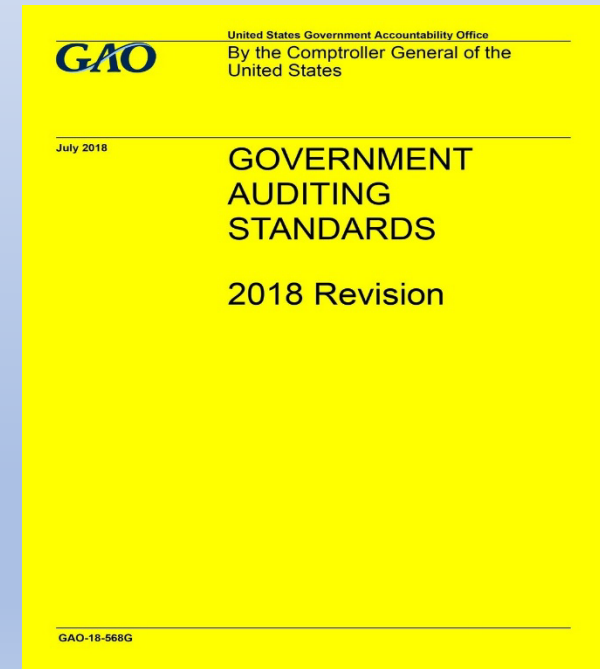
Internal auditors will follow the Institute of Internal Auditors (IIA) framework –

**Red Book**



External auditors will follow Generally Accepted Government Auditing Standards –

**Yellow Book**





**Internal Audit** departments must be recognized by the Office of State Inspector General (OSIG). OSIG helps conduct or review Peer Review results to ensure Internal Audit departments function in accordance with the Red Book.

**External Audits** are performed by an independent outside firm contracted to perform audit work. They must use an acceptable auditing framework (such as the Generally Accepted Government Auditing Standards Yellow Book; American Institute of Certified Public Accountants (AICPA) Standard for Consulting Services; or the AICPA Statement on Auditing Standards).

CSRM accepts audit reports from Auditors who provide evidence to CSRM that they have successfully passed their Peer or Quality Assurance Reviews.



When contracting for audit services, use the following language in the Evaluation and Scoring Section of your Statement of Requirements/Contract:

- ✓ *Ability to perform IT audits in accordance with the Generally Accepted Government Auditing Standards (Yellow Book) evidenced by a current, independent Quality Assurance/Peer Review report with an overall opinion of “generally conforms.” Suppliers responding to this SOR should provide this report with their SOW.*
- ✓ *An in-depth understanding of Commonwealth of Virginia (COV) Information Security Standards including IT Security Standards (SEC501/525), and IT Security Audit Standard (SEC502).*

**Note:** To maintain auditor independence, do not use a firm that has performed other IT Security work (risk assessments, business impact analysis, System Security Plans, etc.) to conduct IT Security Audits.



The audit program shall include assessing the risks associated with IT systems for which it is the System Owner and/or Data Owner.



At a minimum, IT systems that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.







### IT Security Audit Plan Template

Agency Information		Contact Information	
Agency Name		Name	
Agency Acronym		Title	
Agency Number		E-mail	
Date of submission		Phone	

IT System Acronym *	IT System Name	Planned Auditor	Date Last Audited (MM/YY)	Scheduled Audit Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional Audit Requirements
				20xx (MM/YY)	20xx (MM/YY)	20xx (MM/YY)	

*Submitting the Audit Plan annually represents 1/3 of the overall Audit Score*

Audit scope should be sufficient to assess the effectiveness of the system controls and measure compliance with the applicable COV IT Security Standards.



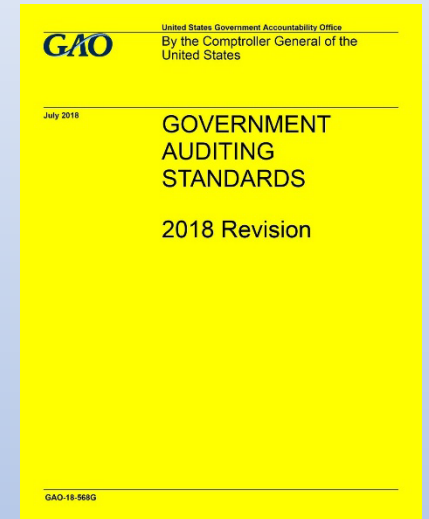
*IT Security Auditors should also use standards that measure compliance with any other applicable Federal, contractual, and COV regulations.*



**The Agency Head or designee shall submit to the CISO the following information:**

***Official Audit Reports of all completed IT Security Audits conducted by or on behalf of the Agency. IT Security Audits submitted to VITA must be reflected in the IT Security Audit Plan.***

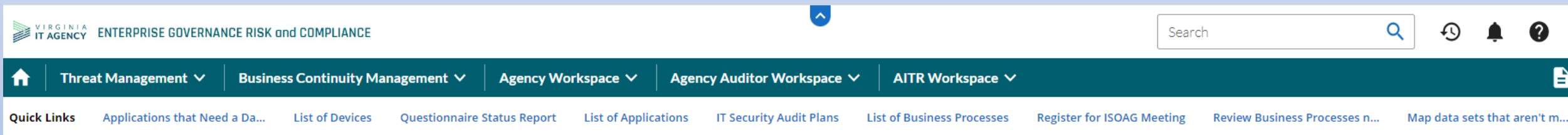
*The official audit report submitted needs to include an attestation as to the audit Standard used.*



*“We conducted the IT Security Audit in conformance with the **“International Professional Practices Framework or Generally Accepted Government Auditing Standards,”** and included an evaluation of internal controls through inquiry, inspection, analytical procedures, and confirmation as considered necessary in the circumstances.”*

In addition to the Audit Report, agencies are required to submit corrective action plans by email to CSRM using the elements from the Audit Remediation Plan template found at:

[www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs](http://www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs)



VIRGINIA IT AGENCY ENTERPRISE GOVERNANCE RISK and COMPLIANCE

Search

Threat Management Business Continuity Management Agency Workspace Agency Auditor Workspace AITR Workspace

Quick Links Applications that Need a Da... List of Devices Questionnaire Status Report List of Applications IT Security Audit Plans List of Business Processes Register for ISOAG Meeting Review Business Processes n... Map data sets that aren't m...

Quarterly Corrective Action Plan updates can be submitted to CSRM via email or by using Archer.

***Submitting 4 Quarterly Updates represents 1/3 of the overall Audit Score***

Contact information:

Email: [Mark.McCreary@vita.virginia.gov](mailto:Mark.McCreary@vita.virginia.gov)

Phone: (804) 510-7095

Email: [Cory.Rutledge@vita.virginia.gov](mailto:Cory.Rutledge@vita.virginia.gov)

Phone: (804) 510-7257





# RISK MANAGEMENT UPDATE

**JONATHAN SMITH**

Director, Risk Management

ISOAG - OCTOBER 2023

OCT 4, 2023





## AGENDA

1. Web Application Vulnerability Remediation
2. Audit and Risk Assessment Finding Remediation
3. Risk Escalation and Risk Alerts
4. Nationwide Cybersecurity Review (NCSR)
5. COV Incident Response Exercise
6. Cyber Storm IX Exercise





# VULNERABILITY REMEDIATION

Web Application Vulnerabilities (Acunetix)



## WEB APPLICATION VULNERABILITY SCAN FINDINGS MORE THAN 30 DAYS UN-REMEDIATED

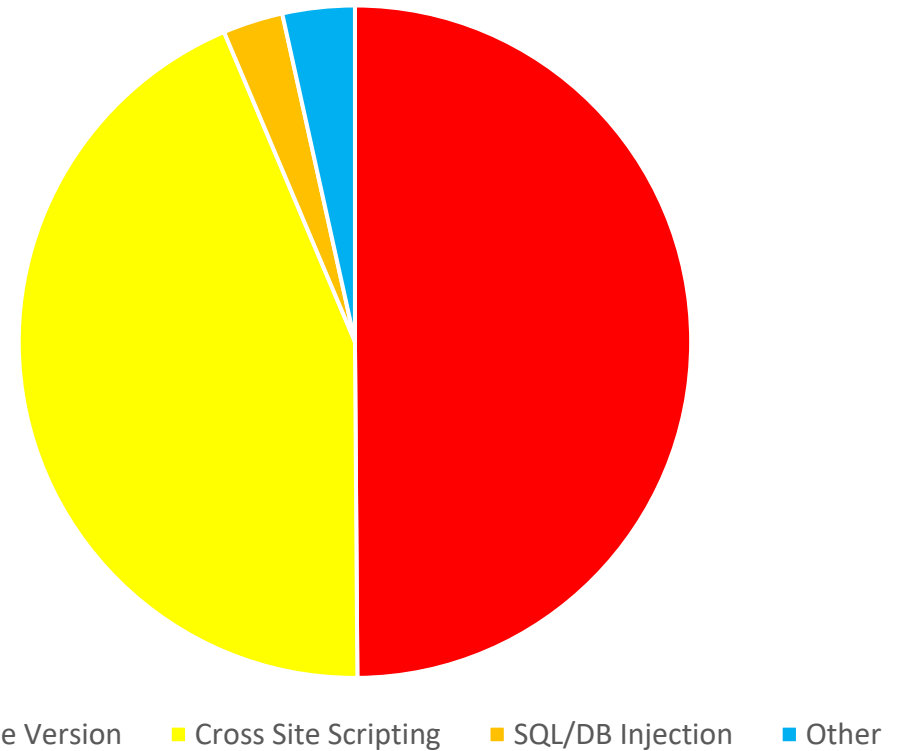
Critical Findings: 148 (from 476 July)

High: 647 (from 1567 July)

Vulnerabilities Detected:

- Out of Date Version
- Cross Site Scripting
- SQL/DB Injection
- Other

Vulnerability Detected



## REMEDATION EFFORTS

- CSRM notified agencies with critical and high vulnerabilities that have not been remediated within 30 days at the end of July, 2023. 476 critical and 1567 high vulnerabilities were identified in this effort. Agencies have made progress reducing the numbers of vulnerabilities to 148 critical and 647 high, however more work is needed!
- Agencies must log into Acunetix 360 to view their web application vulnerabilities & remediation recommendations, take actions to remediate the vulnerabilities, and perform a re-scan to ensure that the vulnerability has been remediated.
- VITA is in the process of reaching out to agencies to determine the causes for the delays in the timely remediation of the vulnerabilities and identify where VITA may be able to assist.
- Agencies with systemic issues or non-response may be issued risk alerts that may impact future IT projects.
- Progress/status is reported to and monitored by Secretary of Administration McDermid.

# FINDINGS REMEDIATIONS

Audit and Risk findings in Archer



## OPEN RISK AND AUDIT FINDINGS

### Risk Findings

- 2079 Open risk findings
  - 1738 (84%) of the open risk findings are more than 1 year old
  - 1153 (55%) of agency risk findings more than a year old with a status of "Not started"

### Audit Findings

- 1899 Open audit findings
  - 1600 (84%) open audit findings more than 1 year old
  - 838 (44%) of agency audit findings more than a year old with a status of "Not started"

## WHAT CAN WE DO?

Review and update open findings in Archer

- Verify continued validity of findings, if findings have been remediated or are no longer applicable, submit them for closure.
- Ensure finding remediation response been entered into Archer.
- Ensure status for the finding is accurate (not started, underway, awaiting review, etc).
- Ensure that quarterly updates are being submitted and updated in Archer.

Having difficulties within Archer? Contact you CSRМ analyst or [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

# RISK ESCALATION & RISK ALERTS



## OVERVIEW

VITA and CSRM are implementing new and improved tools for agencies and CSRM to better assess vulnerabilities, issues and risks within the Commonwealth enterprise.

- Agencies can expect an increase in risk notifications, escalations, and alerts from CSRM
- Some examples of issues that may warrant risk notification, escalations, or alerts are:
  - Security and risk program systemic issues (annual program scores/grades)
  - Findings remediation
  - Vulnerability scan remediation
  - Security incidents and remediation
  - Identity and access management



# NATIONWIDE CYBERSECURITY REVIEW

October 1, 2023 - February 28, 2024



## OVERVIEW

The NCSR is a no-cost, anonymous, maturity based, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Score	Maturity Level <i>The recommended minimum maturity level is set at a score of 5 and higher</i>
7	<b>Optimized:</b> Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	<b>Tested and Verified:</b> Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	<b>Implementation in Process:</b> Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	<b>Risk Formally Accepted:</b> Your organization has chosen not to implement based on a risk assessment.
4	<b>Partially Documented Standards and/or Procedures:</b> Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	<b>Documented Policy:</b> Your organization has a formal policy in place.
2	<b>Informally Performed:</b> Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	<b>Not Performed:</b> Activities, processes and technologies are not in place to achieve the referenced objective.

## BENEFITS

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers.
- Attain reporting and resources that can help you prioritize next steps towards desired cybersecurity improvement. For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool.
- Gain access to a repository of informative references, such as NIST 800-53, COBIT, and the CIS Controls that can assist in managing cybersecurity risk.
- Fulfill the NCSR assessment requirement for the Homeland Security Grant Program (HSGP). Additional information located here: <https://www.fema.gov/homeland-security-grant-program>.

## REGISTRATION

- CSRM is working with CIS to enroll Commonwealth Executive Branch and Independent agencies
- You should be receiving registration confirmation emails
- Login URL: <https://cis.my.logicmanager.com/login>
- New users will be need to select “Reset Password” to complete the registration process

# COV INCIDENT RESPONSE EXERCISE

Tabletop Exercise - October 26, 2023



## OVERVIEW

The COV Annual Incident Response (IR) Tabletop Exercise is an unclassified, adaptable exercise developed by the MSI/MSS for the Commonwealth of Virginia. The main purpose is to evaluate performance of the multisupplier model, promote dialogue around opportunities for continuous improvement, and identify recommendations for improvement for the COV Cybersecurity Incident Response process and test agency incident response plans and playbooks.

## OBJECTIVES

The main objective for this exercise is to uncover strengths and weaknesses within the integrated IR process:

- Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic cybersecurity events
- Evaluate Service Delivery communication and responsiveness
- Run the event through the Service Delivery and State Agency Incident Response plans, identify opportunities for alignment, and any gaps in Service Delivery execution
- Test agency incident response plans and playbooks
- Provide recommendations for corrective action to VITA-CSR

## EXPECTED OUTCOMES

Conduct a tabletop event where coordination of multiple Suppliers and Service Delivery ensures COV information systems will successfully operate in support of the exercise scenario, and when the managed environment is under attack.

- Demonstrate successful coordination of Multiple Supplier Service Delivery
- Enhance awareness, readiness and coordination within the integrated environment
- Test capability to determine operational impacts of a cyberattack
- Test and exercise participant's incident response playbooks, incident analysis, incident response plans and incident reporting procedures
- Demonstrate compliance with MSI Security Incident Management Process and VITA Incident Response Playbooks
- Identify Enterprise-wide opportunities for improvement
- Further integration of multi sourcing program between MSI, VITA-CSR, Service Towers, and the Agencies

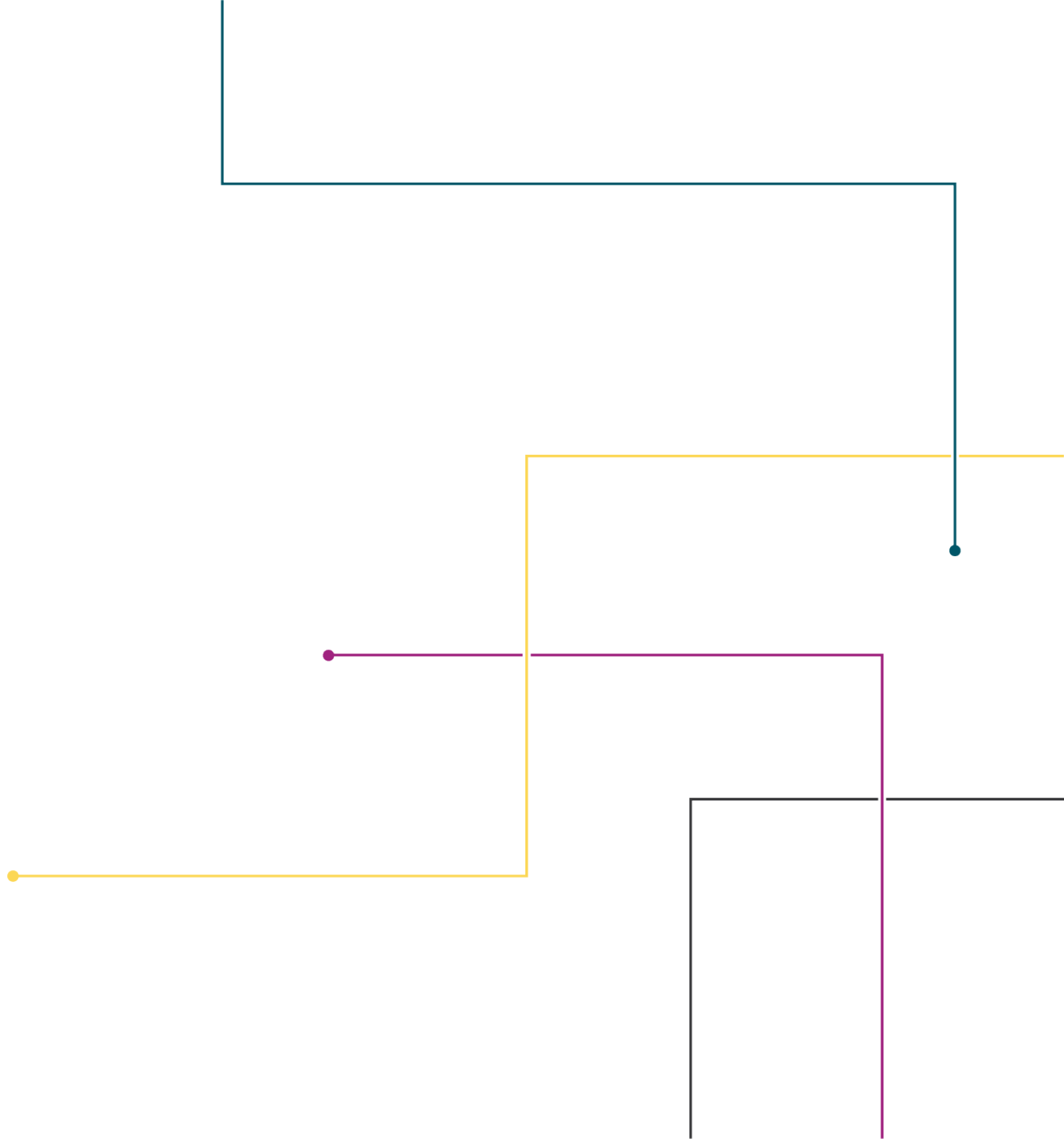


## EVENT INFORMATION

- When:
  - Exercise: Thursday, October 26th, 2023, from 8am-2pm
  - Hotwash: Friday, October 27th, 2023, from 11am-12pm
- Who:
  - Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
  - Participants include representatives from each participating agency and service tower
- Where:
  - Zoom Meeting will be hosted for coordination
  - Participation from your usual workspaces
- Questions: [MSI-Security-Operations@saic.com](mailto:MSI-Security-Operations@saic.com)

# CYBER STORM IX

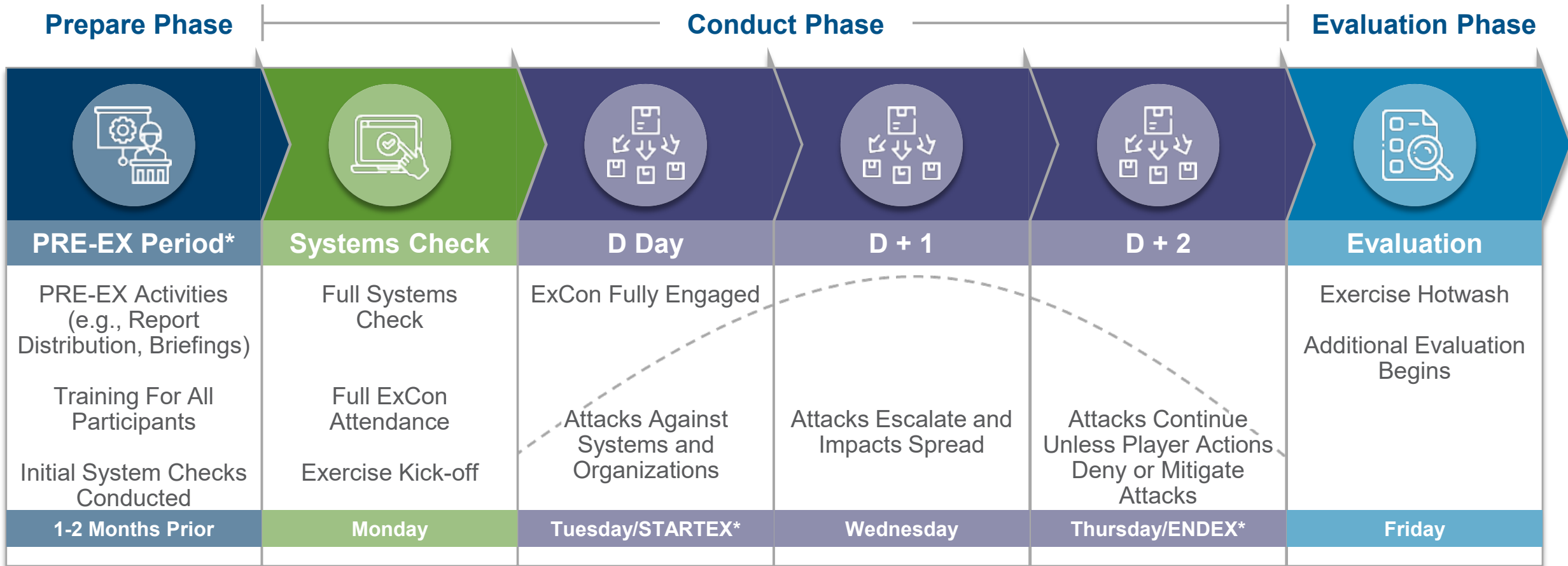
TBA March/April, 2024



## WHAT IS CYBER STORM IX

- It is the National Cybersecurity Exercise, focused on policy, information sharing, coordination, and decision-making.
- It provides a venue to simulate discovery of and response to a large-scale, coordinated cyber incident impacting the nation's critical infrastructure.
- Players participate from their work locations and receive “injects” that describe impacts to their organization and respond according to policy and procedure.

## CS IX INITIAL EXECUTION TIMELINE



\*PRE-EX (Pre-Exercise); STARTEX (Start of the Exercise); and ENDEX (End of the Exercise)

## ADDITIONAL INFORMATION

Cyber Storm IX was presented to the ISOAG in July 2023. If you would like a copy of the redacted slides from that presentation or your agency is interested in participating, please email [Jonathan.m.smith@vita.virginia.gov](mailto:Jonathan.m.smith@vita.virginia.gov) or [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

## QUESTIONS?

*Please reach out to the Risk Management Team if you have any additional questions:*

Jonathan Smith, Dir Risk Management – [jonathan.m.smith@vita.virginia.gov](mailto:jonathan.m.smith@vita.virginia.gov)

John Willinger, Sr. Risk Analyst – [john.willinger@vita.virginia.gov](mailto:john.willinger@vita.virginia.gov)

Marjean Adarkwa, Sr. Risk Analyst - [marjean.adarkwa@vita.virginia.gov](mailto:marjean.adarkwa@vita.virginia.gov)

Isaac Amoani, Sr. Risk Analyst - [Isaac.Amoani@vita.virginia.gov](mailto:Isaac.Amoani@vita.virginia.gov) (currently on military leave)

Andrew Wirz, Archer Sys Admin - [andrew.wirz@vita.virginia.gov](mailto:andrew.wirz@vita.virginia.gov)

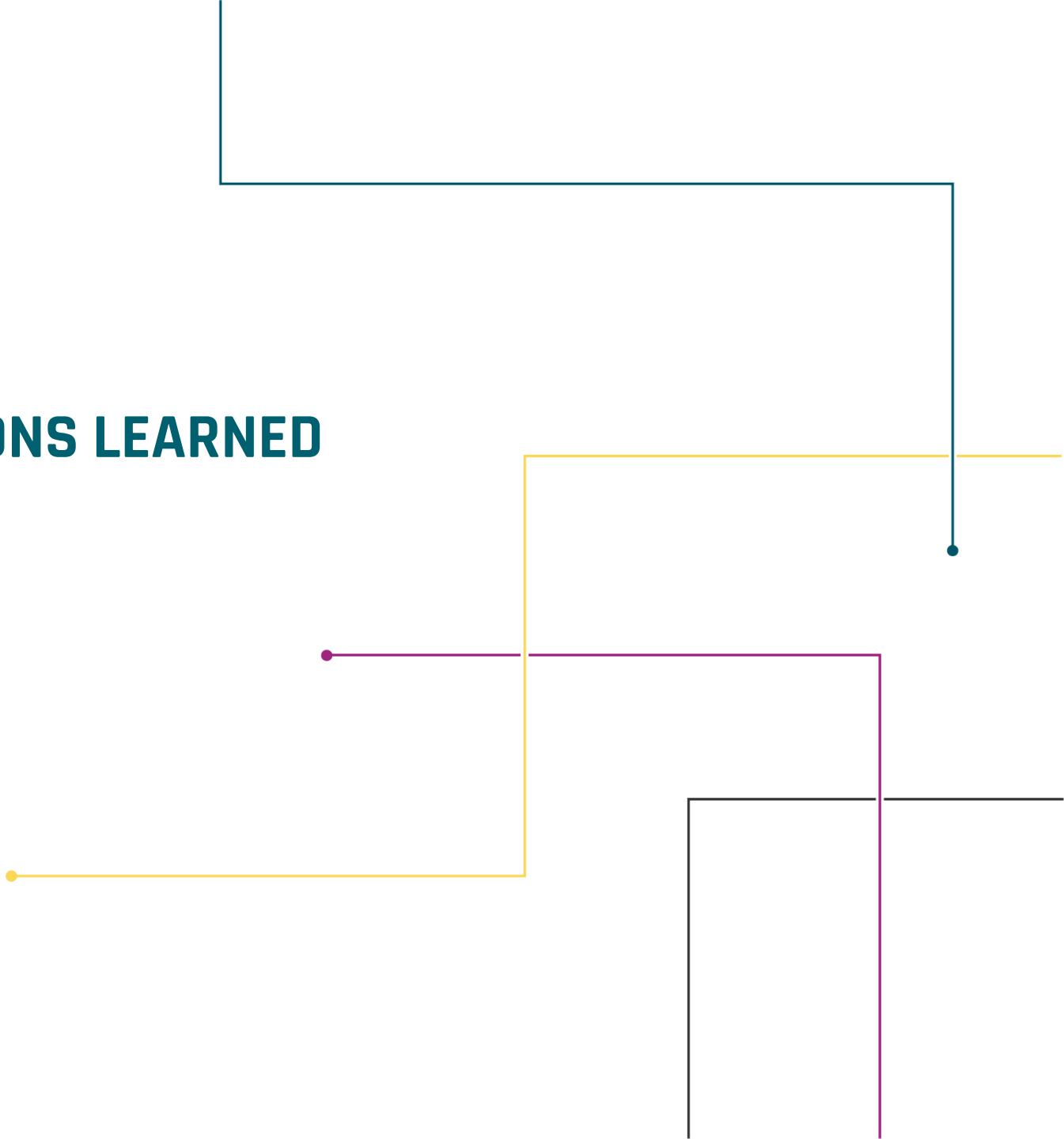
# KNOWBE4 PHISHING LESSONS LEARNED

**KATHY BORTLE**

Incident Response Specialist

ISOAG MEETING

OCT 4TH, 2023





## User Provisioning:

- All Executive Branch agencies were updated using a one-time ADI-Sync the week of 9/25. This was completed to facilitate the COV 2023 3<sup>rd</sup> Qtr. Phishing Campaigns.
- Agencies requesting to use ADI-Sync have been setup. If other agencies want to use ADI-Sync, please reach out for assistance.

## Okta - Single Sign On

- Agencies wanting to use Okta for Single Sign-On should have a tile that is associated with their Okta-KnowBe4 group in Active Directory.
- If any agency wants to use Okta, but is missing the tile, please let us know
- Remember, Okta will log you into KnowBe4 with your AD credentials. Please do not try to use a different account/email for login as it will fail.



- PAB Button Not Available - Okta supports embedded AD groups but Microsoft does not. To allow the button to be distributed to agencies, the Messaging Team created a group for each domain name and associated the PAB button with each group based on the button name. After learning that several agencies had been missed, Messaging corrected the issue. All agencies should have received the PAB button by 9/28/23. If the PAB button is not available, please report it to Commonwealth Security so it can be addressed.
- PAB Button Location differs by client – The location of the PAB button is dependent on the version of the client being used. In the full desktop client, the PAB button resides on the ribbon bar. The web and mobile clients do not have it in the same location. These clients require the user to open the message and click on the 3 dots to the right of the sender's name to bring up a menu that contains the button. The user must scroll down the menu to find it as it is located near the bottom. Job aid have been created to assist users with finding it.
- PAB Button Spam Submissions – Messages reported as spam will be sent to Area1 spam queue and to the CSRM incident mailbox. The user will receive an automated response thanking them for the report and providing the instructions for blocking it in their mailbox.
- PAB Button Phishing Submissions – These will be sent to the VCCC and the Area1 phishing queue. The submission will automatically include all the information needed (headers, subject and copy of the message) to investigate the report. When the VCCC receives it, Service Now will automatically generate the ticket and route it to the SOC for investigation.

## Phishing Campaign

- Phishing Beta – Opting into this module prevents an account from participating in a non-beta campaign.
- False Positives - false positives are triggered when the message and/or its links are scanning. Domains must be whitelisted everywhere that the message can be scanned.
- Random Domain selection for sender, links and landing pages – KnowBe4 will pick any domain that is available in the console. If a domain has not been whitelisted, it needs to be hidden. Any domain that is not hidden can be used by this feature. If the domains in the list are not whitelisted, it can trigger a false positive for clicks.
- Downloading Pictures in messages – the Outlook client is configured to prevent the automatic downloading of pictures in the emails. This affects KnowBe4's ability to track whether the message has been opened. The only opened stats that are reliable are for those messages where the user clicked the link, opened an attachment or submitted data. When the user takes one of these actions, the system automatically marks the message as opened. Therefore, opened should not be included in any phishing test reports.



## **False Positives have returned -**

While false positives were resolved the end of August it appears that they have returned. We have seen some data where the user clicked on the message before they opened it. As a result, we cannot consider any 2023 Q3 Failures as valid. We are working with messaging to find out what changed in our environment to cause the issue to re-surface.

## **Phishing Activity Report (single agency) -**

While some of the reports will allow combined results, the Phishing Activity Report does not. It can only provide data on one account at a time. This means that we will have to develop COV wide stats instead of having them provided for us. We are currently working on a way to automate this process.

## **Exporting Phishing Active Report Data (single agency) -**

PDF format – only provides charts. It does not include any user data.

CSV format - only provides individual user records.

The total bar show on the phishing campaign results page (# delivered, # clicked, # opened, etc.) is not provided in either format. These numbers can be attained by counting the occurrences in the raw user data (csv format).



## Phishing Campaigns -

- Do not consider any failures from the 2023 Q3 COV-wide campaign to be valid
- Report suspected false positives with user details so they can be investigated.
- Let us know if you are willing to participate in testing for false positives.
- Hold off on launching any phishing campaigns until the false positive issue is resolved.
- Please provide suggestions for what data you would like to see in the COV-wide statistics.

# QUESTIONS?

---





# CSRM SECURITY ARCHITECTURE TEAM

**CHANDOS CARROW**

Acting Security Architecture Manager

INFORMATION SECURITY OFFICER ADVISORY GROUP (ISOAG)

OCTOBER 4, 2023

# AGENDA

- Who we are?
- What we do?
- What happened in 2023?
- Where are we going for 2024?
- Questions?







# WHO WE ARE?

- Preston Talbott – Security Architect
- Jacquelyn (Jackie) Esters – Security Architect
- Chandos Carrow – Acting Security Architecture Manager



# WHAT DO WE DO?

- SEC501/SEC530 Security Exceptions
- Review Enterprise Tools/Services Baselines
- Review Enterprise Tools/Services SSPs
- Security SMEs or CSRMs Voting Members on RFPs
- Provide Technical Interpretations of the Security Standards
- Write/Review/Update Security Standards
- CSRMs Representatives during the SPLM and RFS Processes





## WHAT HAPPENED IN 2023?

- International Travel KBA and KSE Request Form
- CSRM Involvement in new RFS Sprint Process
- SEC501 Security Exception Cleanup Effort
- SSP and Baseline Process Adjustments
- Start of SSP and Baseline Delta Project
- Increased CSRM Involvement in SPLM Process
- And....
- A new security standard or something like that

## WHERE ARE WE GOING IN 2024?

- Finishing the SSP and Baseline Delta Project
- Improving the availability of the Enterprise Services security documentation to the agencies
- SEC530 Security Documentation Update Project
- Start the first revision review process on SEC530
- Finishing the SEC501 security exception cleanup effort
- More trainings, more knowledge transfers, more clarity, more communications, more involvement, and more assistance with/for the agencies







# QUESTIONS?



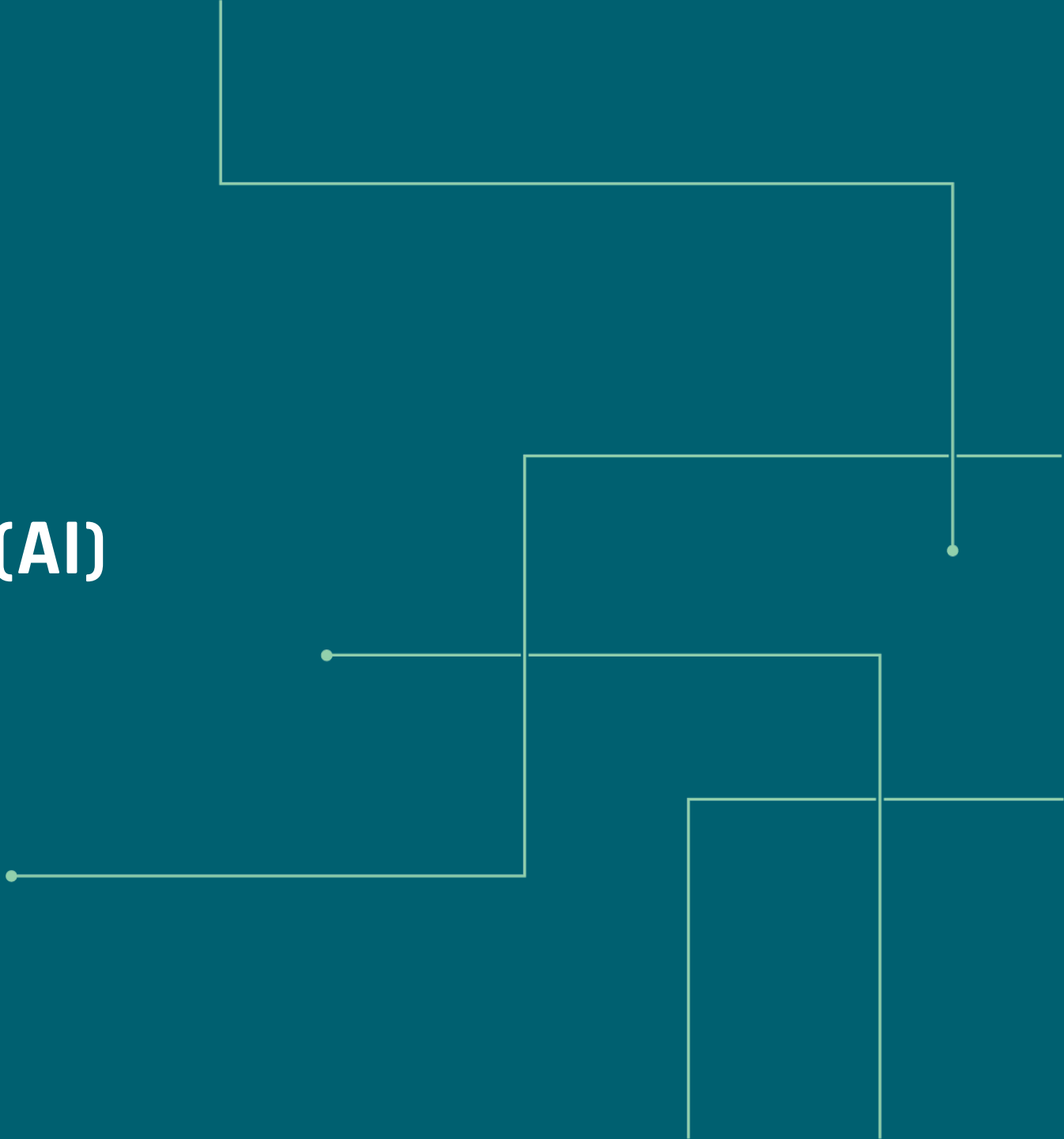
# ARTIFICIAL INTELLIGENCE (AI)

**STEPHEN SMITH**

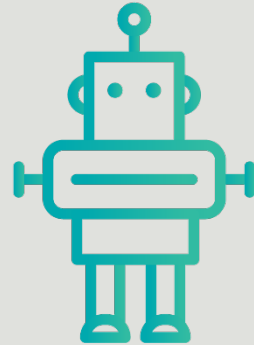
**Enterprise Architecture Manager**

INFORMATION SECURITY OFFICER ADVISORY GROUP (ISOAG)

OCTOBER 4, 2023

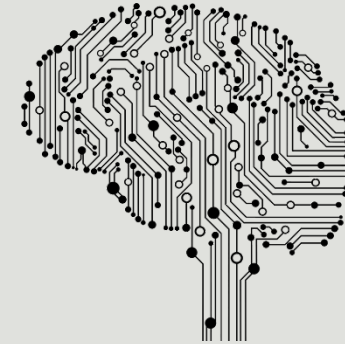


That Commonwealth of Virginia (COV) agencies and workers shall be able to leverage the creative and insightful capabilities of Artificial Intelligence (AI) while ensuring that the use of such AI does no harm to citizens of the Commonwealth, its guests, the business of the Commonwealth, any known business interest, or the environment.



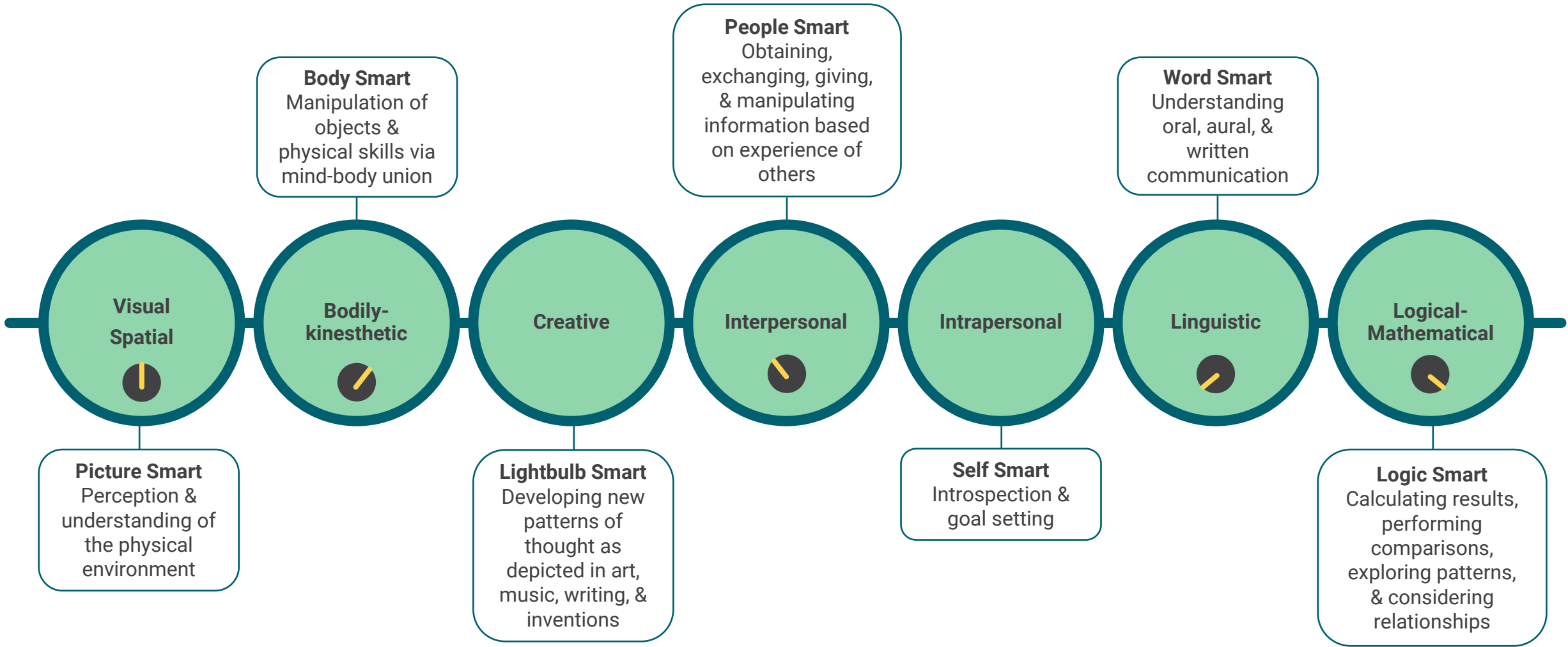
## Robotic Process Automation (RPA)

- Simulates human **behavior**
- **Process** driven

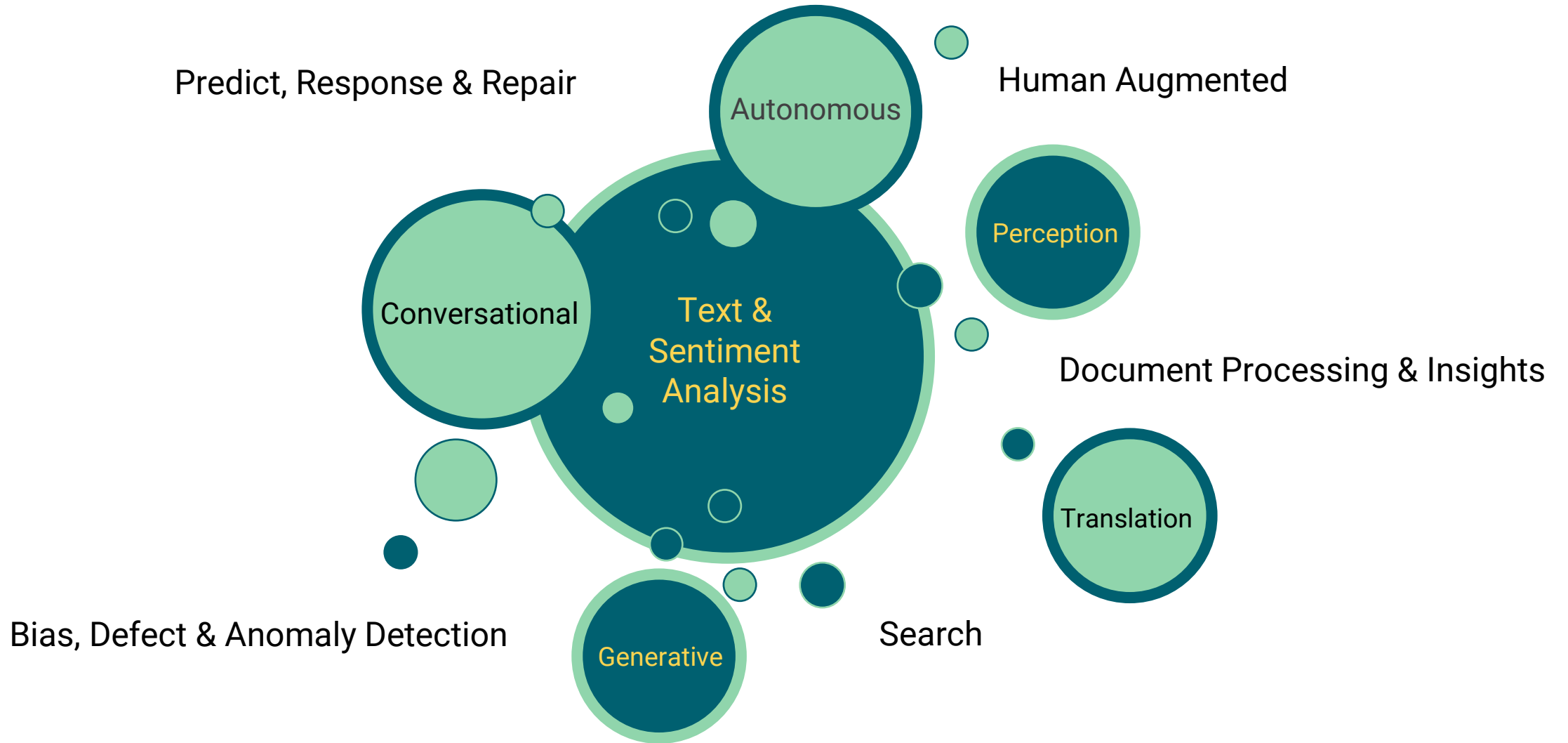


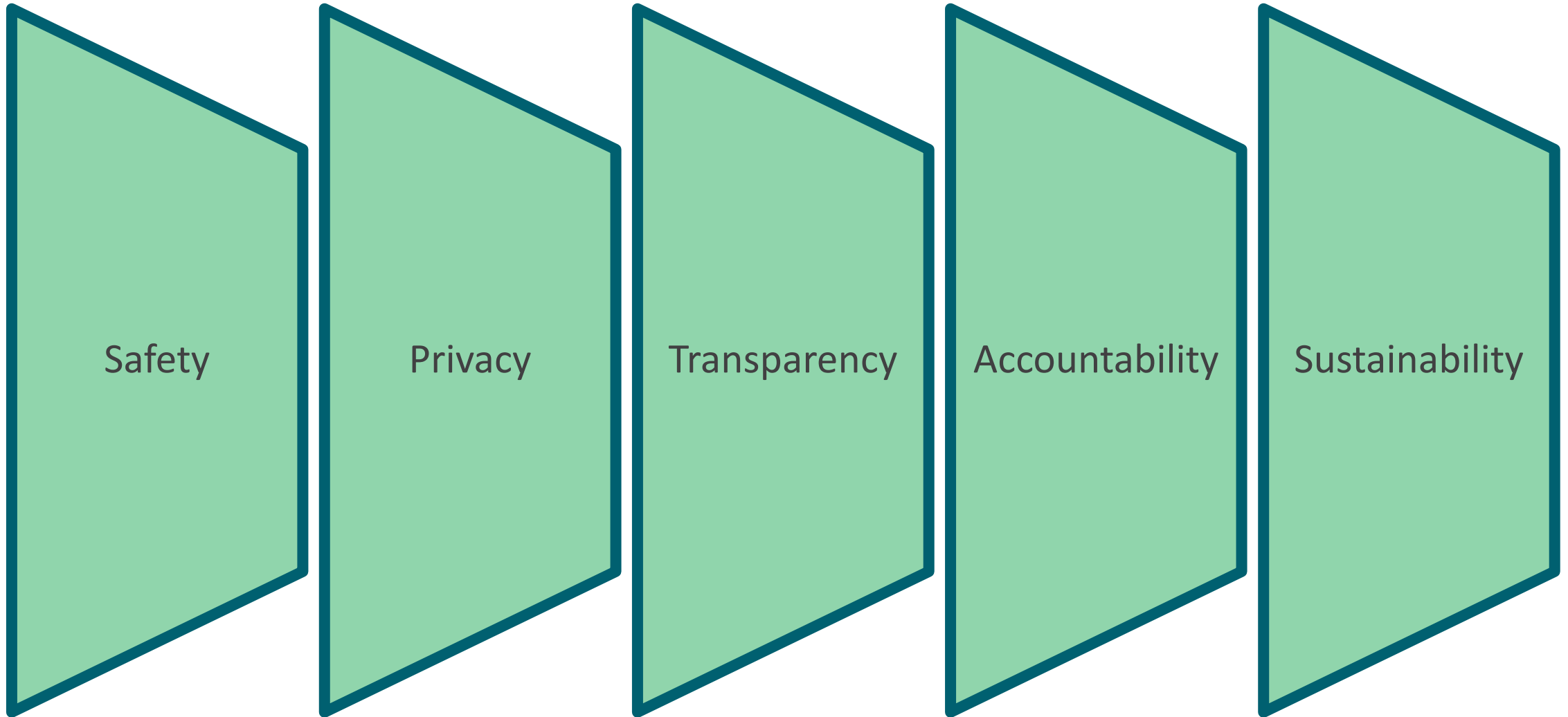
## Artificial Intelligence (AI)

- Simulates human **intelligence**
- **Data** driven







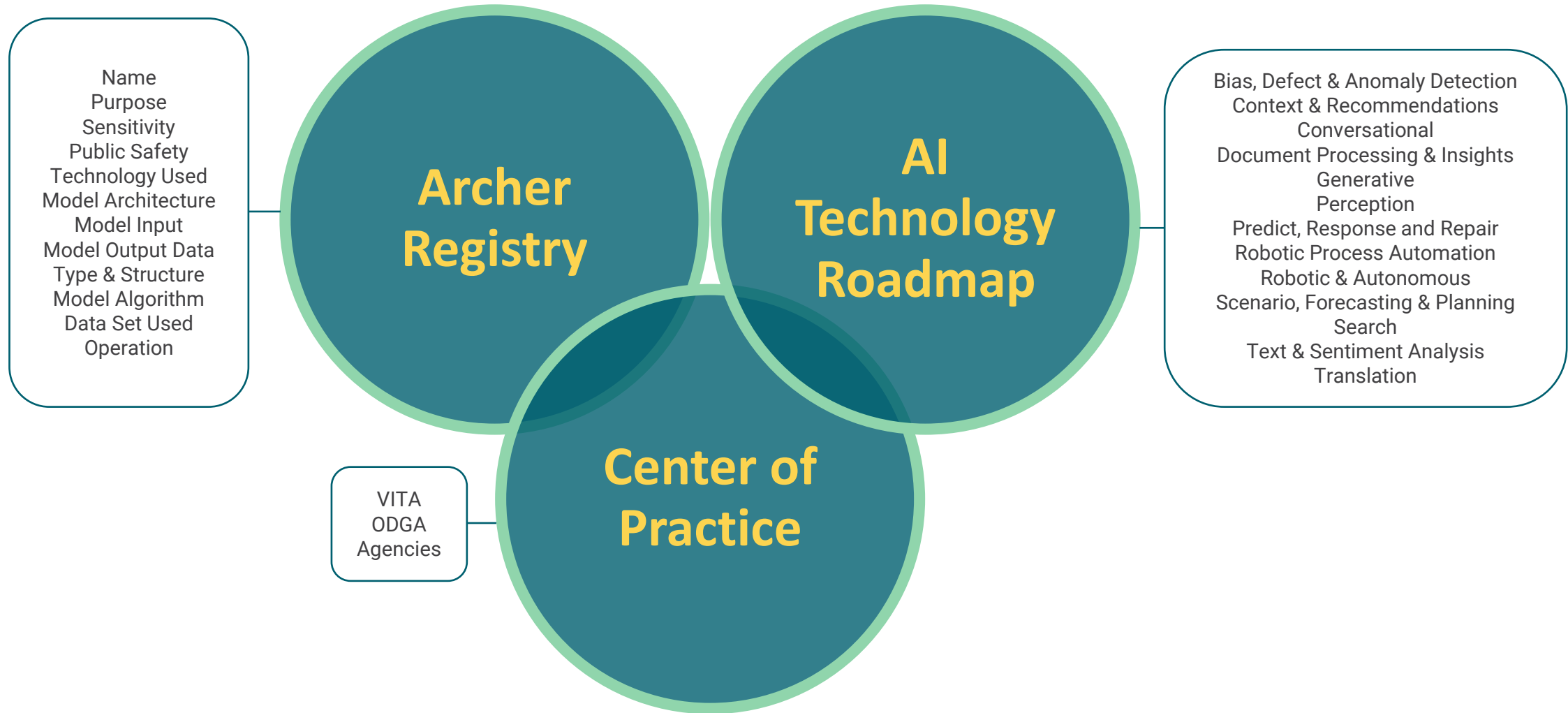


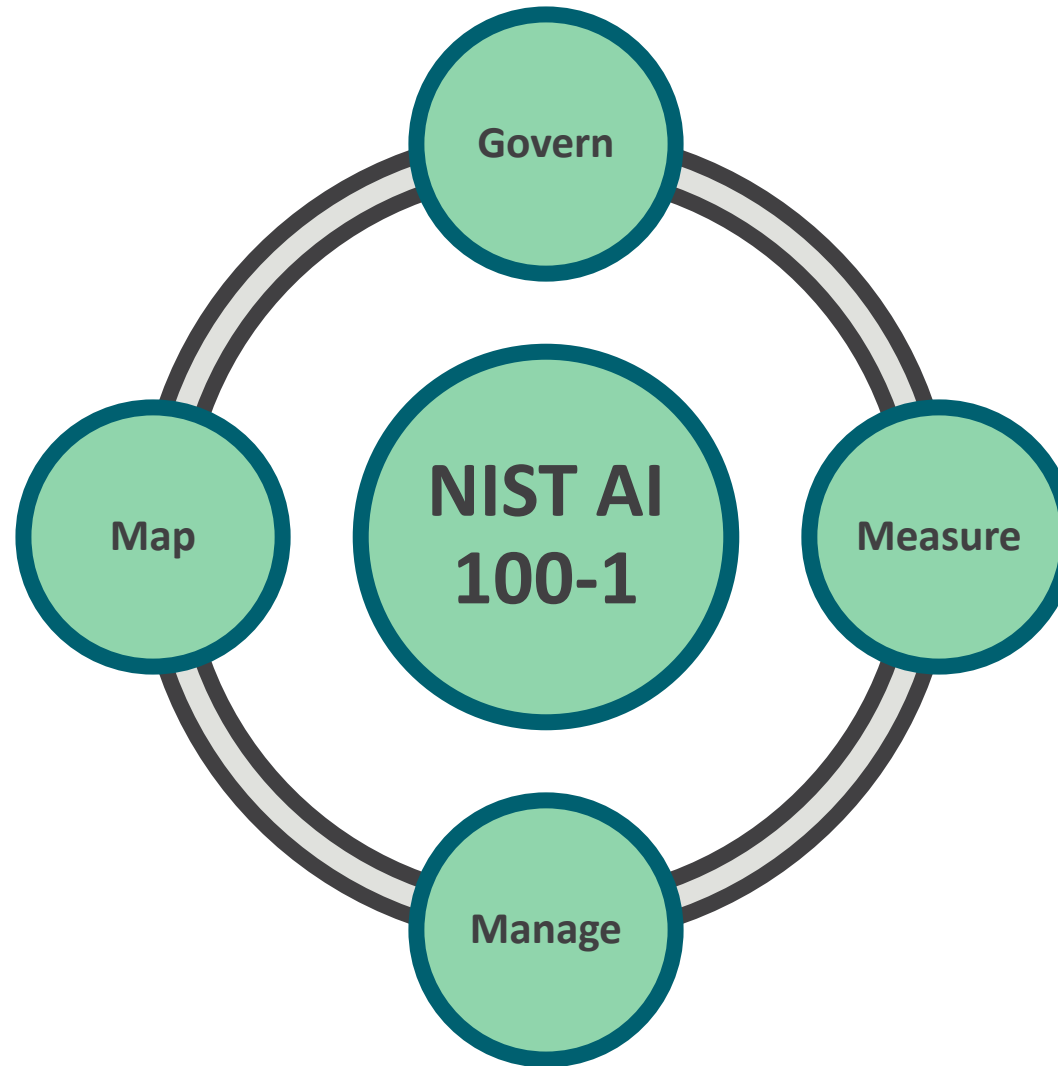


Mission Essential



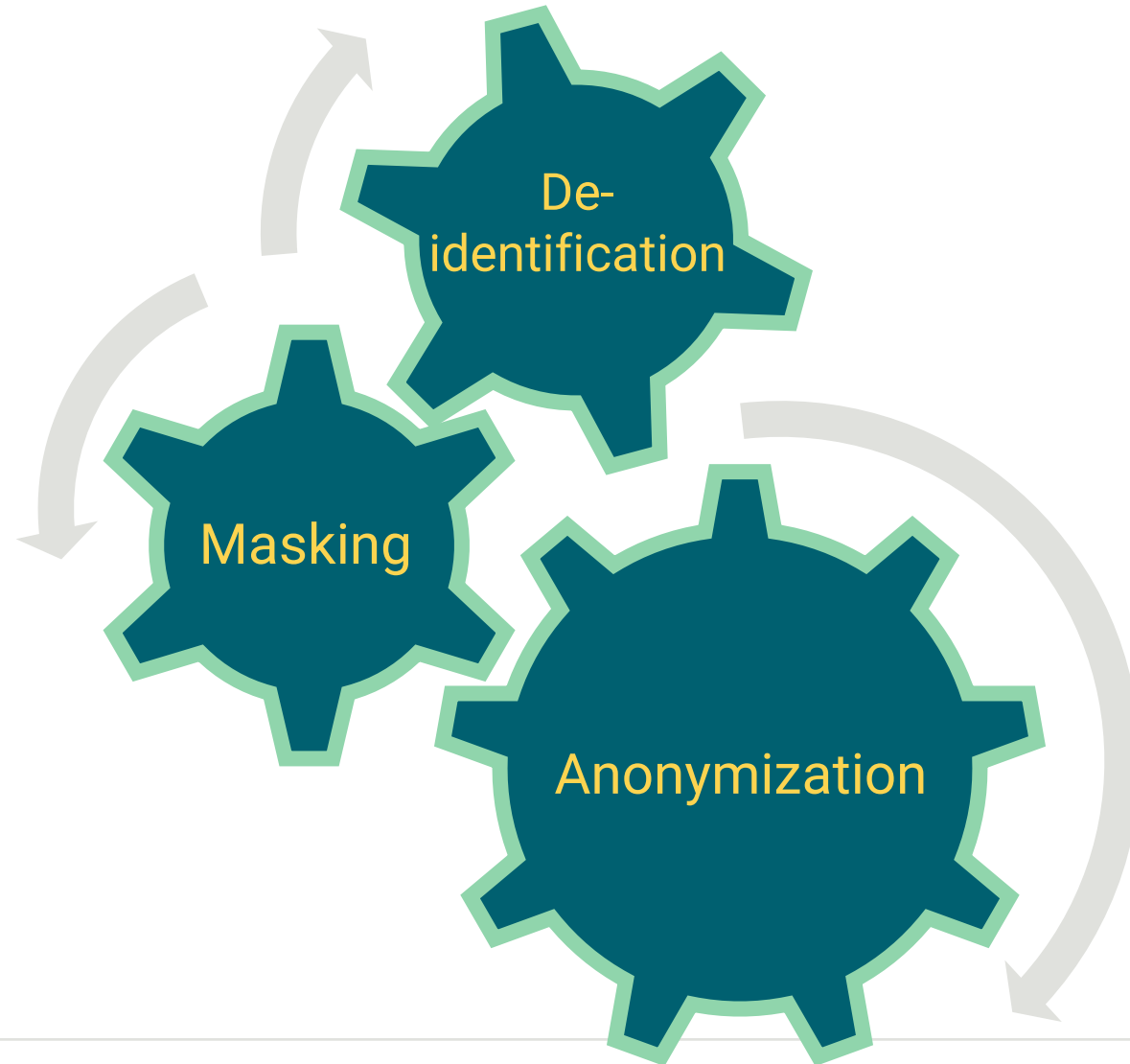
Business Critical



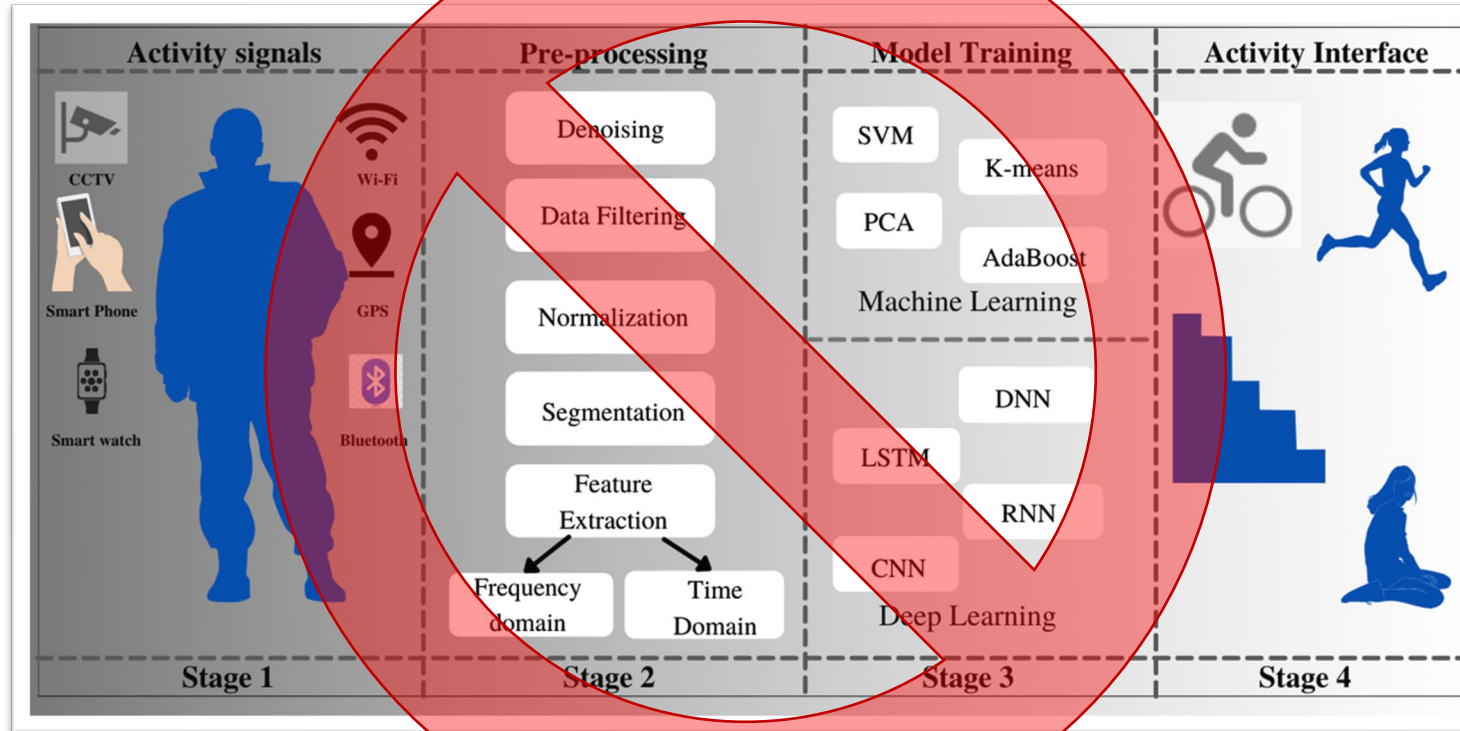


- Valid & Reliable
- Safe
- Secure & Resilient
- Accountable & Transparent
- Explainable & Interpretable
- Privacy Enhanced
- Fair with Harmful Bias Managed









(Source: Human activity recognition in artificial intelligence framework: a narrative review 1/18/2022)



Algorithm  
Extent  
Value Provided





Ethics  
Bias  
Privacy  
Accountability  
Security



**AI Training**



**New Skills Development**

AI design  
System validation  
Integration testing  
Regulatory compliance  
Bias mitigation  
Algorithm risk analysis  
Model calibration  
Incident detection

# Questions

???





**October is  
Cybersecurity  
Awareness Month**

# Theme



SECURE.  
OUR **WORLD**



# Overall Campaign



## Goal

- Take actionable steps to stay safe online

## Tone

- Positive
- Approachable
- Simple
- Back to basics

# Feelings Toward Cybersecurity

- **78%** of people consider staying secure online a priority
- **34%** noted they often feel overwhelmed by information and, as a result, minimize their online actions
- **46%** felt frustrated while staying secure online
- **39%** of users trying to keep safe felt information on how to stay secure online is confusing

Findings from [Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022](#)



# Our Online Behaviors

- **Only 33% of individuals create unique passwords for all accounts**
  - Only 18% of individuals have downloaded a password manager
- **43% of respondents have never heard of multifactor authentication (MFA)**
  - Out of the 57% of the participants who had heard about it:
    - 79% applied it at least once and 94% of them reporting that they were still using MFA
- **92% of respondents took action after a security training**
  - 58% say they are better at recognizing phishing
  - 45% started using strong and unique passwords
  - 40% started using MFA
  - 40% started regularly installing software updates

# 4 Easy Ways to Stay Safe Online

**Use Strong Passwords and a Password Manager**

**Turn on Multifactor Authentication**

**Recognize and Report Phishing Attacks**

**Update Your Software**



# Recognize and Report Phishing

## PHISHING RED FLAGS:



- **A tone that's urgent or makes you scared**  
*"Click this link immediately or your account will be closed"*
- **Bad spellings, bad grammar**
- **Requests to send personal info**
- **Sender email address doesn't match the company it's coming from**  
Ex: Amazon.com vs. Amaz0n.com
- **An email you weren't expecting**

# Recognize and Report Phishing

## WHAT TO DO

### Do NOT

- Don't click any links
- Don't click any attachments
- Don't send personal info



### Do

- Verify
- Contact that person directly if it's someone you know
- Report it to your IT department or email/phone provider
- DELETE IT

# Ways to Get Involved

## AT WORK

- Publicize resources and activities
  - Intranet
  - Website
  - Emails to employees/customers
- Promotions
  - Discounts
  - Giveaways
- Hold a contest
  - Phishing simulation
  - Poster contest

## AT HOME

- Share helpful tips and resources
  - Kids
  - Parents
  - Friends
- Hold a family “tech talk”
  - Discuss how each family member can protect their devices, accounts, and personal information.
- Create a culture of security in your family



# Ways to Get Involved Cont.

## IN YOUR COMMUNITY

- Volunteer to teach others in your community
- Reach out to
  - Your kid's school
  - A library/community center
  - Senior center
  - Place of worship

## ONLINE

- Join on the conversation on social media using
  - [#CybersecurityAwarenessMonth](#)
  - [#SecureOurWorld](#)

# Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online and learn about risks** like phishing and business email compromise.

# Additional Resources

## CISA

- [Report a Cyber Issue](#)
- [Secure by Design](#)
- [Cross-Sector Cybersecurity Performance Goals](#)
- [Cyber Resource Hub](#)
- [Cybersecurity Training & Exercises](#)
- [CISA YouTube Channel](#)

## NCA

- [Resources and Guides](#)
- [Videos and On-Demand Webinars](#)





# Get in Touch

## **CISA**

- [cisa.gov/cybersecurity-awareness-month](https://cisa.gov/cybersecurity-awareness-month)
- [AwarenessCampaigns@cisa.dhs.gov](mailto:AwarenessCampaigns@cisa.dhs.gov)

## **NCA**

- [staysafeonline.org](https://staysafeonline.org)
- [info@staysafeonline.org](mailto:info@staysafeonline.org)

# KnowBe4 Updated Content

Tina Gaines

CSRM



# KnowBe4 New Content

October is Cybersecurity Awareness Month, and KB4 wants to help you run an engaging security awareness training campaign this month and beyond!

They have put together a set of resources you can use to help your users keep up their cybersecurity defenses. You also get access to a **user guide and weekly planner to make it easy to launch your training campaign.**

Access the kit on the web page linked below and via the ModStore. Courses and content will be available across all subscription levels and can be saved to your library to use in your training campaigns through October 31.

**Access your resource kit:**

<https://info.knowbe4.com/cybersecurity-awareness-month-resource-kit>

**Attention Diamond customers! We have a kit specially crafted for you. Check it out:**

<https://info.knowbe4.com/cybersecurity-awareness-month-resource-kit-diamond>

## **NEW!** Callback Phishing

Callback phishing isn't your typical email scam. Threat actors set up a multi-layered trap using some smooth-talking tactics to get you to dial a fake number and spill your sensitive information. The good news is you can run simulated callback phishing campaigns in your KnowBe4 console to see if your users will call an unknown phone number in an email and share sensitive information.

### **How does it work?**

An email lands in your users' inbox with a phone number and a callback code. If they dial the number, they'll be asked for the callback code. Your users face two challenges. First, they fail if they dial the number and enter the code from the email. Second, they fail if they provide any personal information, like Social Security or credit card numbers. You can use premade templates, including email and audio, create custom templates using text-to-speech, or by uploading audio files. Callback Phishing is available to customers with a Diamond-level subscription. To learn more on how to create callback phishing campaigns in your KnowBe4 console, check out the Knowledge Base article:

<https://support.knowbe4.com/hc/en-us/articles/18223402626323-How-to-Create-and-Manage-Callback-Phishing-Campaigns>



## KnowBe4 Quarterly Product Update Video

Here at KnowBe4, we're always adding new features and improving our products. Watch the latest Quarterly Product Update to catch up on all the fresh content and new features that we've added to your KnowBe4 platform over the last quarter.

**Here's the direct link to the KnowBe4 platform support article and video:**

<https://support.knowbe4.com/hc/en-us/articles/360015575313>



## The Security Awareness Company – Top 5 Phishing Fundamentals

Phishing continues to be one of the most common and effective cyber attacks that target organizations and individuals alike. This short Mobile-First module reviews the five fundamentals of phishing attacks to reinforce what phishing is, why it's dangerous and how to avoid falling for common scams.

*Eighteen new pieces of training content added this month. Training content from the Security Awareness Company, including Top 5 Phishing Fundamentals, is available at the Diamond subscription level.*



## Popcorn Training – World Wild Web: Acceptable Use of Devices

Countless threats are trying to find new ways of compromising your devices. That is why your organization has such strict policies in place about what work devices can and cannot be used for. In this training module, you will learn how to browse the internet safely and protect yourself against cybercrime.

*Twenty-four new pieces of training content added this month. Training content from Popcorn Training, including World Wild Web: Acceptable Use of Devices, is available at the Diamond subscription level.*



## **El Pescador** – How To Behave: Protecting Sensitive Information

This Mobile-First module is key for improving security practices in your organization. Your users will learn about the various types of sensitive data and how to keep them secure. At the end, your users will be better equipped to protect sensitive information, reduce risk and prevent cybersecurity breaches.

*One new piece of training content added this month. Training content from El Pescador, including How To Behave: Protecting Sensitive Information, is available at the Diamond subscription level.*





- **KnowBe4 – 2024 Common Threats**

- In this training module, you will learn some of the latest ways that cybercriminals are targeting you and your organization using social engineering. Kevin Mitnick demonstrates a new spin on a common email trick to show how cybercriminals get information from you and then access your computer and the organization's network.

- Fifteen new pieces of training content added this month. 2024 Common Threats is available across Gold, Platinum and Diamond subscription levels.



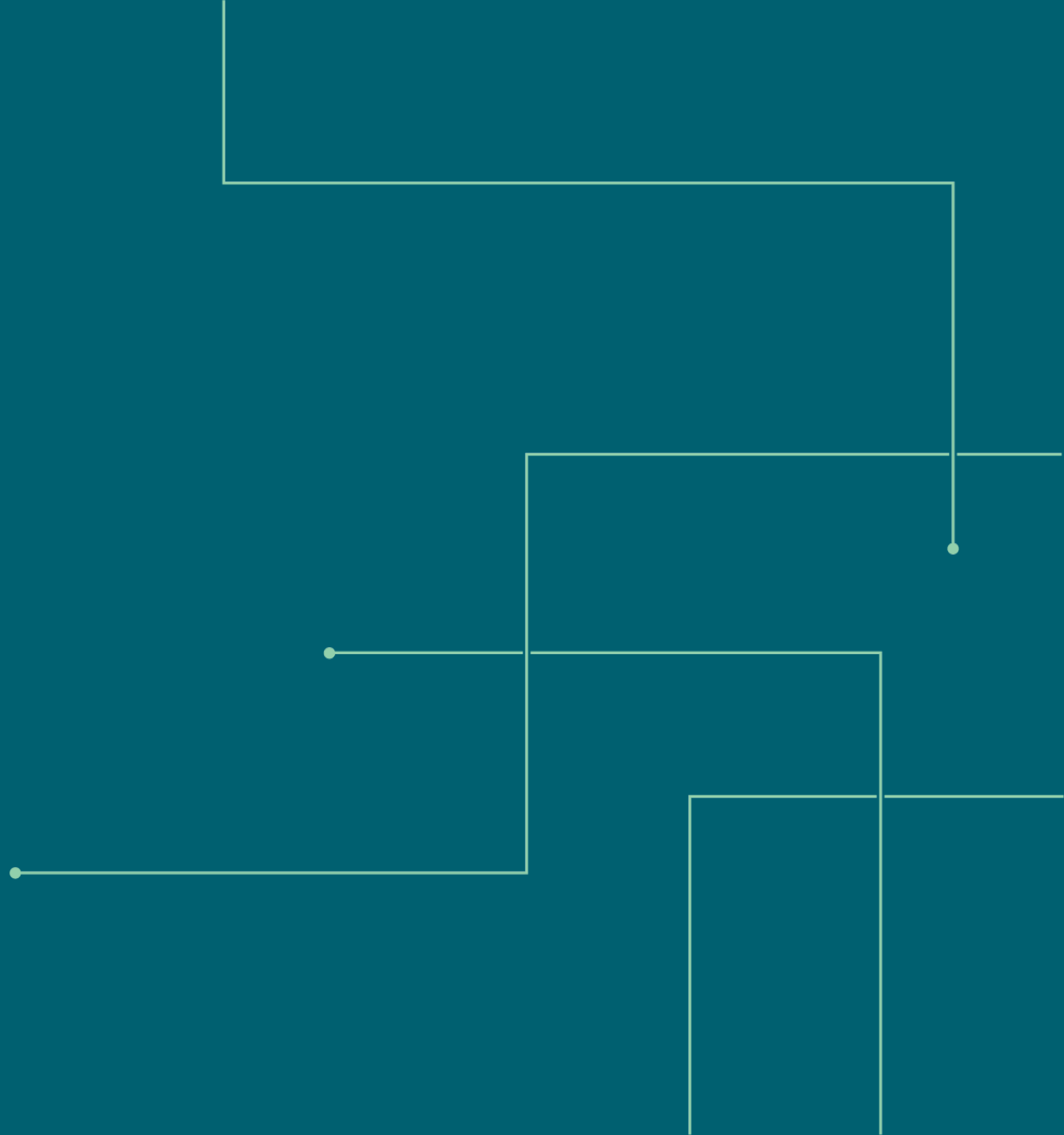
# OVERVIEW/RECAP

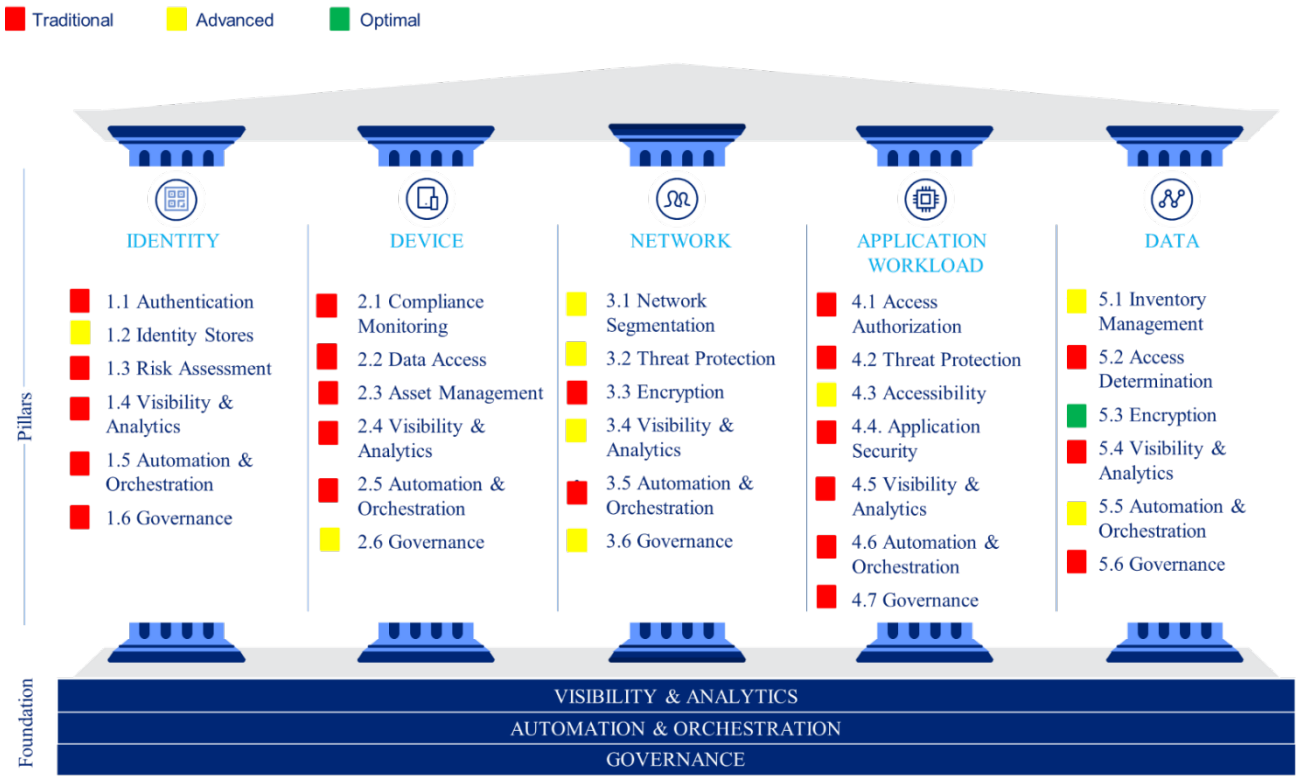
TREY STEVENS

Deputy CISO

INFORMATION SECURITY OFFICER ADVISORY GROUP (ISOAG)

OCTOBER 4, 2023





There were 31 functions evaluated as part of this assessment. There were twenty-one (21) capabilities found to be operating at the Traditional level, or 68%. There were nine (9) capabilities found to be operating at the Advanced level, or 29%. There was one (1) capability found to be operating at the Optimal level, or 3%.



## Phase 1

Focus has been on identity, visibility and analytics. Investments have also been made in automation and orchestration.

- Splunk Cloud
  - Splunk SOAR and UBA
  - Nucleus (for vulnerability management)
  - Axonius (for asset management)
  - Improvements to web scanning by moving to 360 product
  - Sailpoint upgrade
- 
- New standard underway to define data classification groups at the Commonwealth level
  - MDM security baseline
  - Researching WAF alternatives to Silverline



## Phase 2 (Q1 2024)

- Data classification – starting with products available via G5 license. Will look at third party products if necessary
- Multi factor for all users
- Microsegmentation – both on prem and cloud networks; start with preventing lateral movement within enclaves but continuing to realize investment in hardware based firewalls for other segmentation
- Evaluate tools to further secure mobile devices (ie MDR/antiphishing) – currently leveraging a team a Virginia Tech to evaluate options and present recommendations
- Determine best solution to perform posture assessment against non-COV devices
- Start implementing self service provisioning for Sailpoint
- Start implementing conditional access to data
- Splunk SOAR/UBA

- We have a new standard SEC530!
  - Meant to solve confusion over which standard to follow 501 or 525
  - Based on rev 5 of NIST 800-53
    - COV did not adopt two new families; third party risk and privacy
  - **Published last week but compliance will start on March 31, 2024**
- Executive directive 5 was released in September related to the use of artificial intelligence
  - AI standard has been released by EA
  - Additional guidance will be forthcoming from the Office of Regulatory Management
  - <https://www.governor.virginia.gov/media/governorvirginiagov/governor-of-virginia/pdf/ed/Executive-Directive-No.-5---Recognizing-the-Risks-and-Seizing-the-Opportunities-of-Artificial-Intelligence.pdf>
- Vulnerability remediation continues to be monitored and reported to SoA.
  - New tools have been purchased to assist in getting information into your hands faster and in prioritization
- If you haven't started your agency wide security awareness training, what are you waiting for? 😊



# UPCOMING EVENTS

The logo for VASCAN features the word "VASCAN" in a bold, black, sans-serif font. The letter "A" is stylized with two light blue triangles pointing upwards and downwards. The text is set against a dark blue background with a circuit board pattern. A thin grey horizontal line is positioned below the letters.

**October 17 – October 18, 2023**

**University of Virginia – Darden School of Business**

100 Darden Blvd, Charlottesville, VA 22903

Link to Register: **October 17 – October 18, 2023**

**University of Virginia – Darden School of Business**

100 Darden Blvd, Charlottesville, VA 22903

Link to Register: [VASCAN 2023 Conference – VASCAN](#)



# Cyber sweep competition

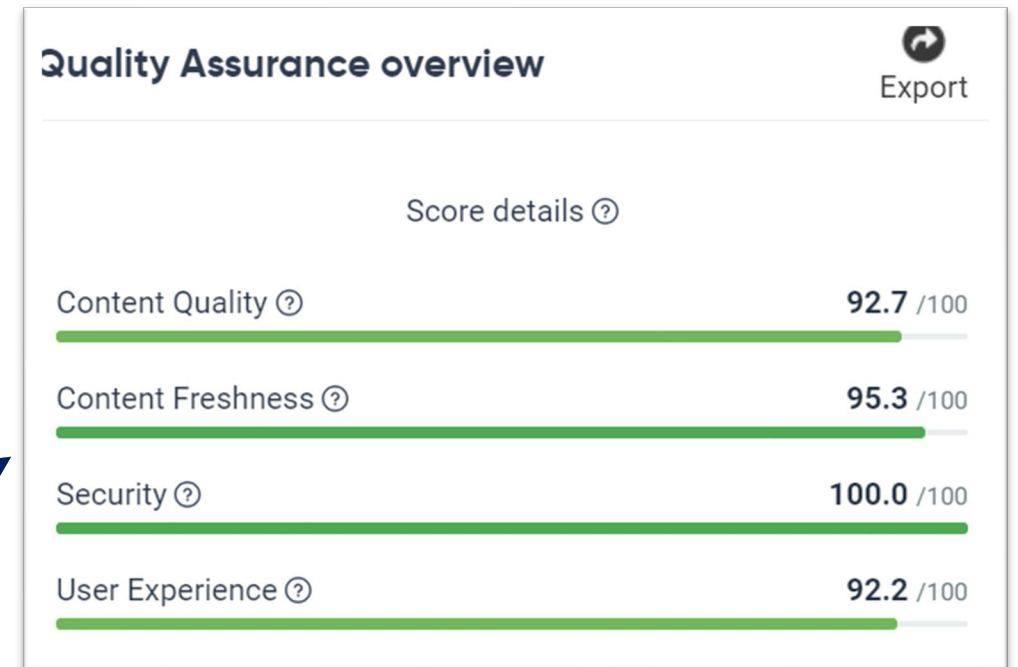
clean out the cobwebs

*In observance of Cybersecurity Awareness Month, and in tandem with the website modernization initiative, we challenge you to "clean out the cobwebs" of your agency's websites!*

Auditing, reviewing and refreshing the content on your sites will improve user experience and engagement. The focus of the competition is website quality assurance as measured by Siteimprove.

On Oct. 31, final scores will be tabulated.

Winners will be named in two categories: 1) highest overall score and 2) the largest average increase in score across four elements of quality assurance.



Feel free to contact VITA's website modernization team with any questions at [webmod@vita.virginia.gov](mailto:webmod@vita.virginia.gov)

# Annual COV Tabletop Exercise 2023

The COV Annual Incident Response Tabletop Exercise will be conducted October 26<sup>th</sup>, 2023. It is an unclassified, adaptable exercise developed for the Platform, and the Commonwealth of Virginia agencies to help evaluate the performance of the Multi-supplier Model and promote dialogue to identify opportunities for continuous improvement. Participation will add realism to the exercise and contribute greatly to successfully accomplishing the goals.

The organized security event will be held:

Thursday, October 26<sup>th</sup>, 2023 from 8AM-2PM EST via ZOOM conference call.

The after action/hot wash will be held:

Friday, October 27<sup>th</sup>, 2023 from 11AM-12PM EST via ZOOM conference call.

Any questions can be directed to: [MSI-Security-Operations@saic.com](mailto:MSI-Security-Operations@saic.com).

The next scheduled IS Orientation:

October 19, 2023

12 p.m. - 1 p.m. (virtual)

Presenters: Erica Bland  
Renea Dickerson  
Tina Gaines

<https://covaconf.webex.com/weblink/register/r4ed41f5d2193c51251a3fac9d04b42c7>

## **rvatech/Women in Technology**

Wed, Oct 25 at 9:00 AM – 4:30 PM

Dominion Energy Center

600 East Grace Street

Richmond, VA

Registration Link: [2023 rvatech/Women in Technology Conference / rvatech](#)

rvatech/Women in Technology is a technical conference for all technologists + business professionals, curated and presented by our rvatech/Women in Technology committee. Aimed at bringing together professionals on a wide range of relevant topics to learn, engage, and collaborate, this event will feature a robust panel of keynote speakers, fascinating breakout sessions, and ample opportunities for networking.



# November ISOAG MEETING

November 1, 2023

TIME 1 P.M. - 3 P.M.

SPEAKERS: TBA



The next scheduled meeting for the IS Council:

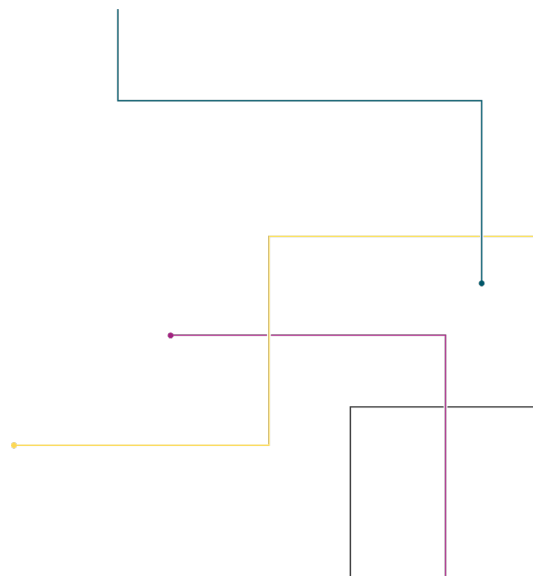
November 15, 2023

12 p.m. - 1 p.m. (virtual)

If you would like an invite to the meeting, contact:

[Commonwealthsecurity@vita.virginia.gov](mailto:Commonwealthsecurity@vita.virginia.gov)

**MEETING  
ADJOURNED**



**VIRGINIA  
IT AGENCY**