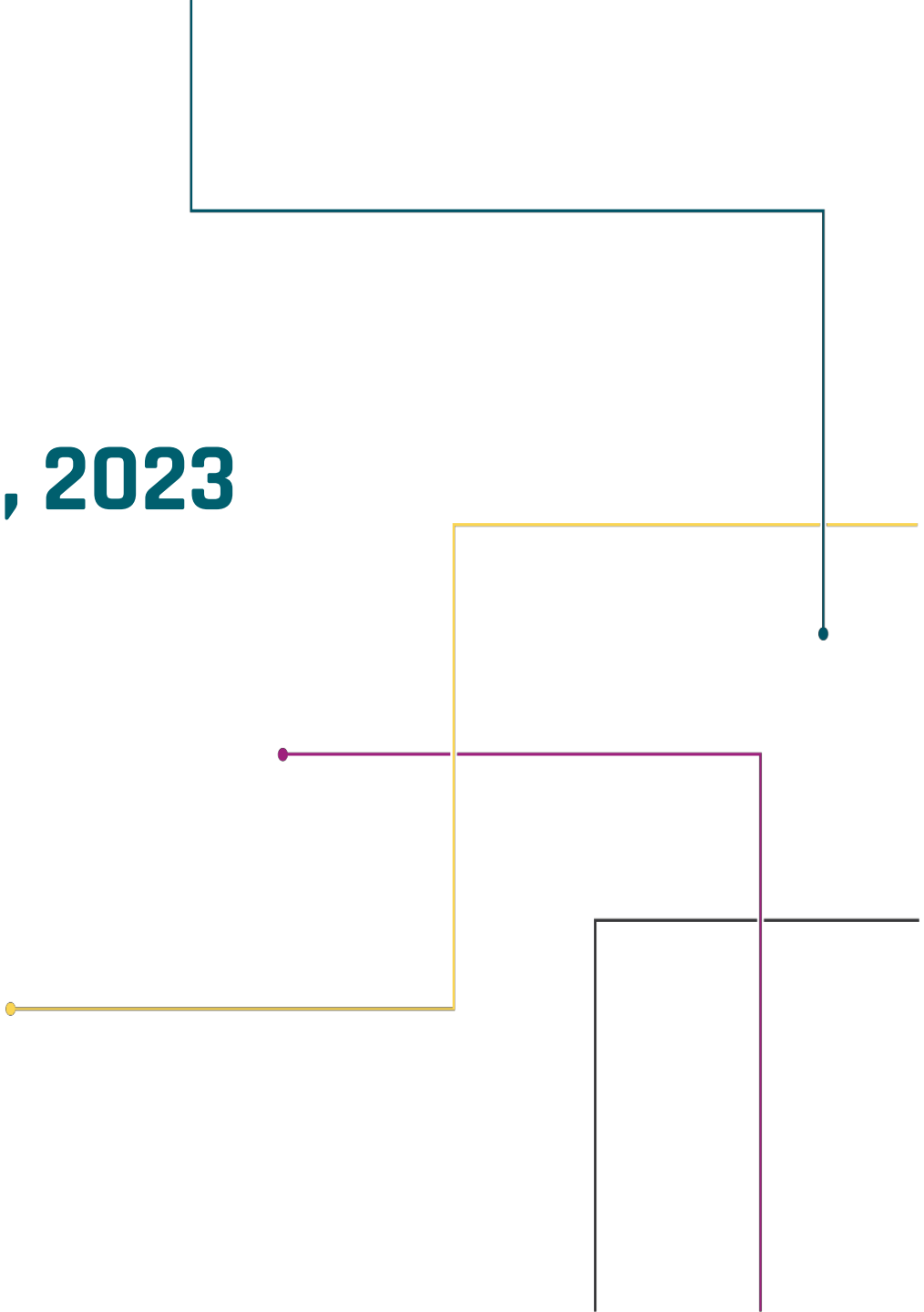
VIRGINIA
IT AGENCY

WELCOME TO THE JUNE 7, 2023

ISOAG MEETING



AGENDA	
Welcome/Opening Remarks	Tina Gaines/ VITA
Enterprise Architecture Team	Stephen Smith/VITA
Risk Assessments	Jonathan Smith/VITA
Cardinal Incident Postmortem and OKTA Updates	Dean Johnson/VITA
International Travel Q&A	Chandos Carrow & Jackie Esters/VITA
KnowBe4 Update	Tina Gaines/VITA
Upcoming Events	Tina Gaines/VITA
Adjourn	

VIRGINIA
IT AGENCY

ENTERPRISE ARCHITECTURE

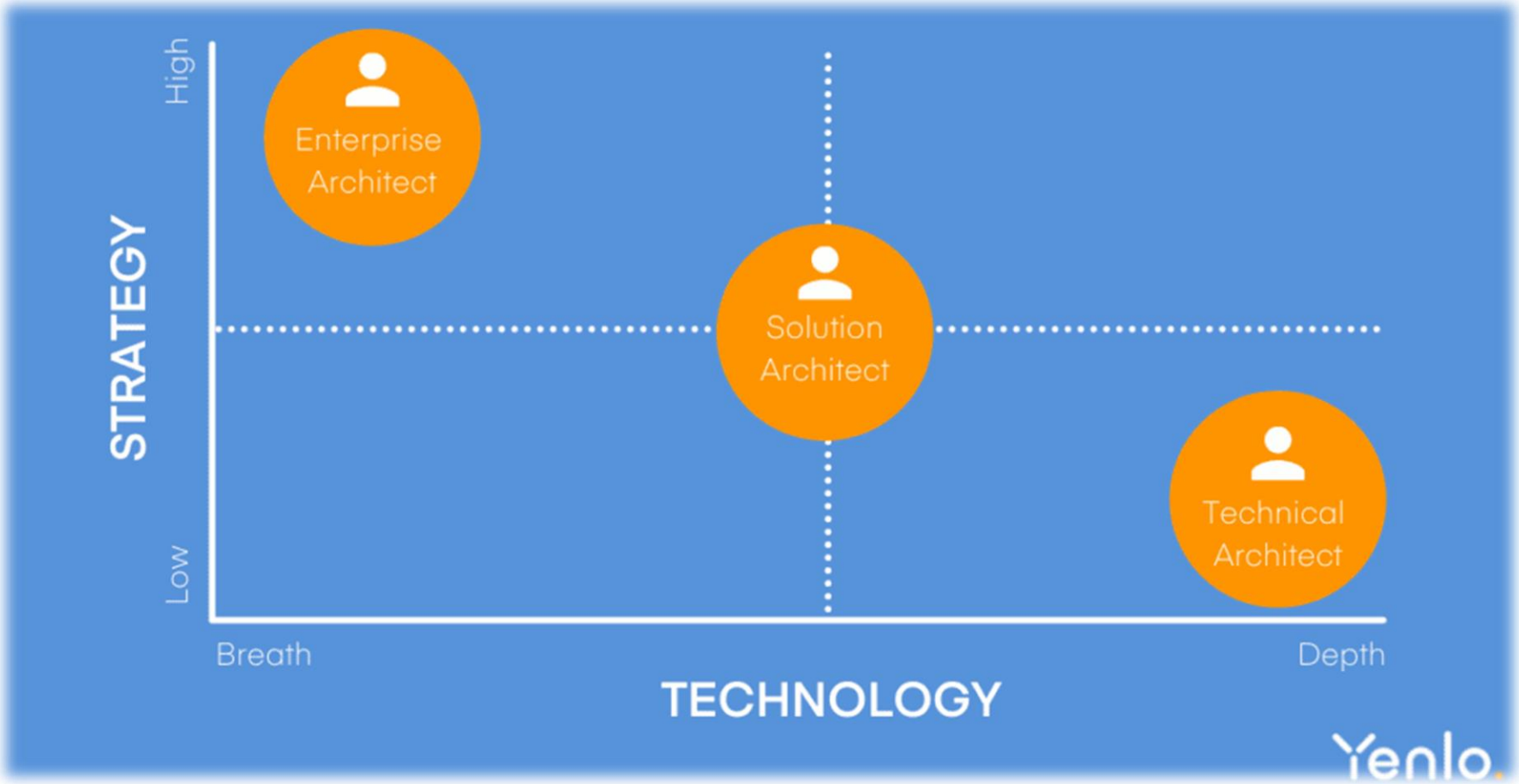
STEPHEN SMITH

Enterprise Architect Manager

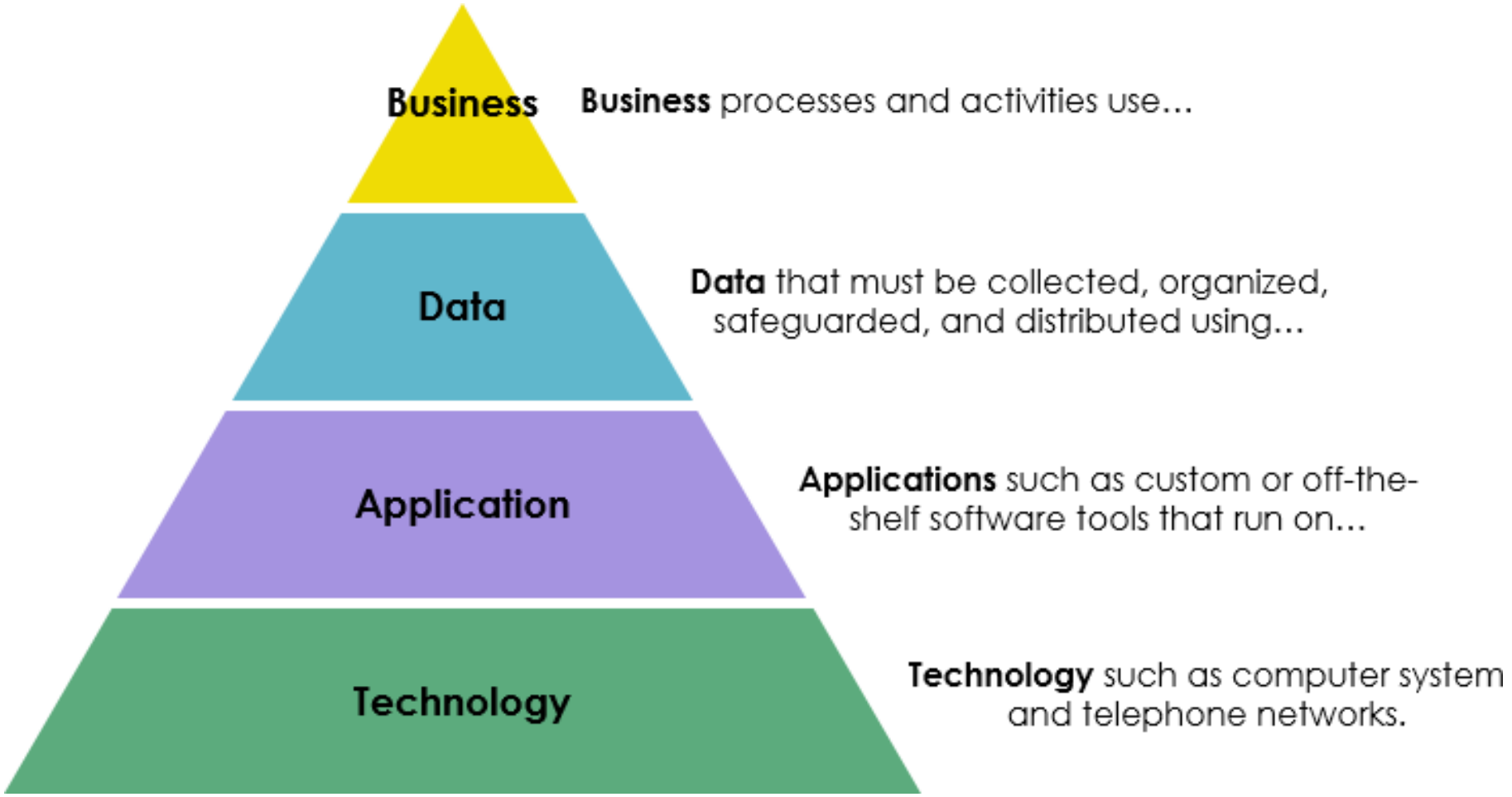
ISO ADVISORY GROUP

7 JUNE 2023

ARCHITECT SPECIES

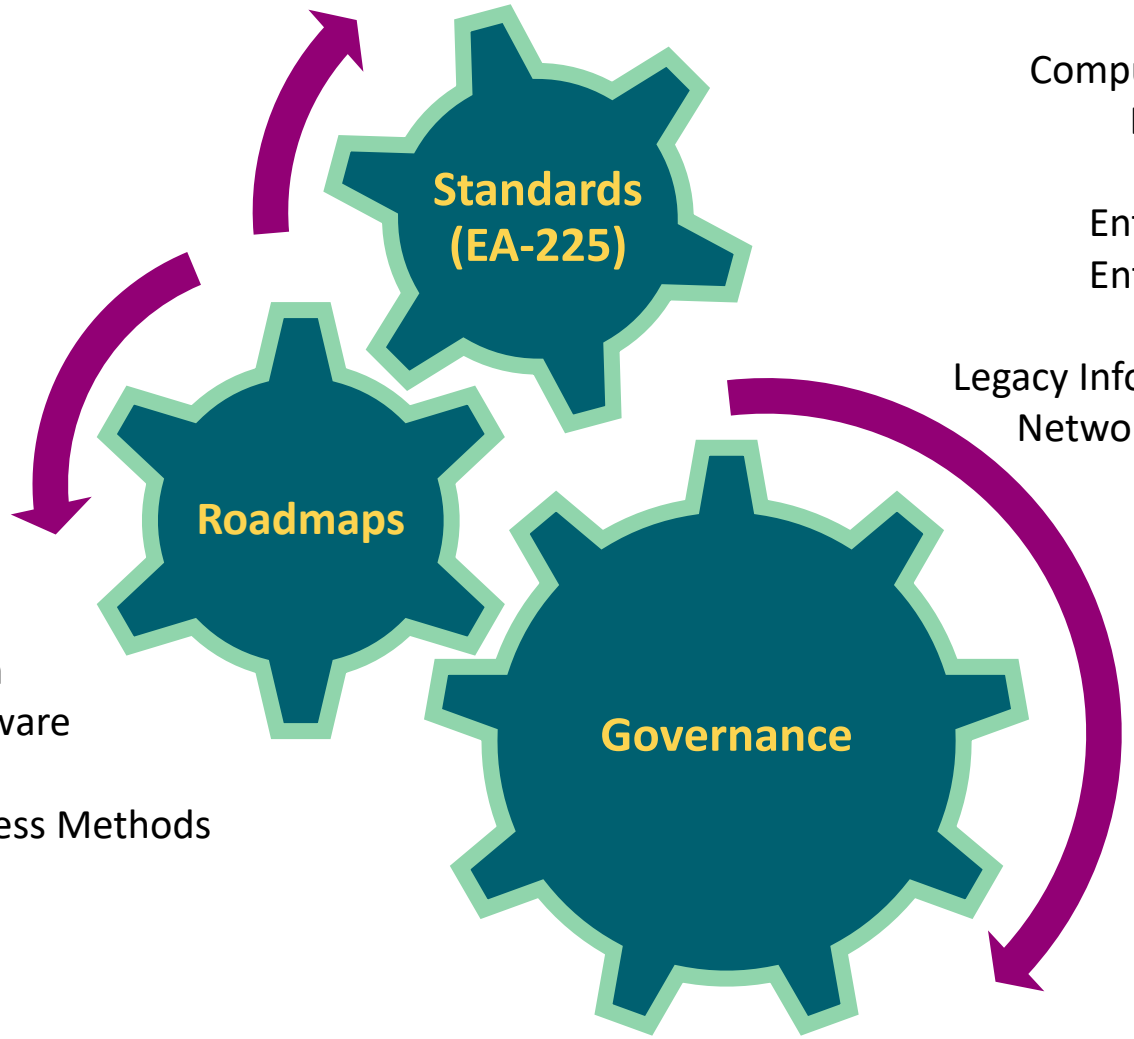


DOMAIN AREAS



WHAT EA DOES

COTS Applications
COV Search Engines
Data Management
End User Computing Operating System
End User Computing Productivity Software
End User Computing Web Browsers
Programming Languages and Data Access Methods
Server OS and Hypervisor
Web and Application Servers

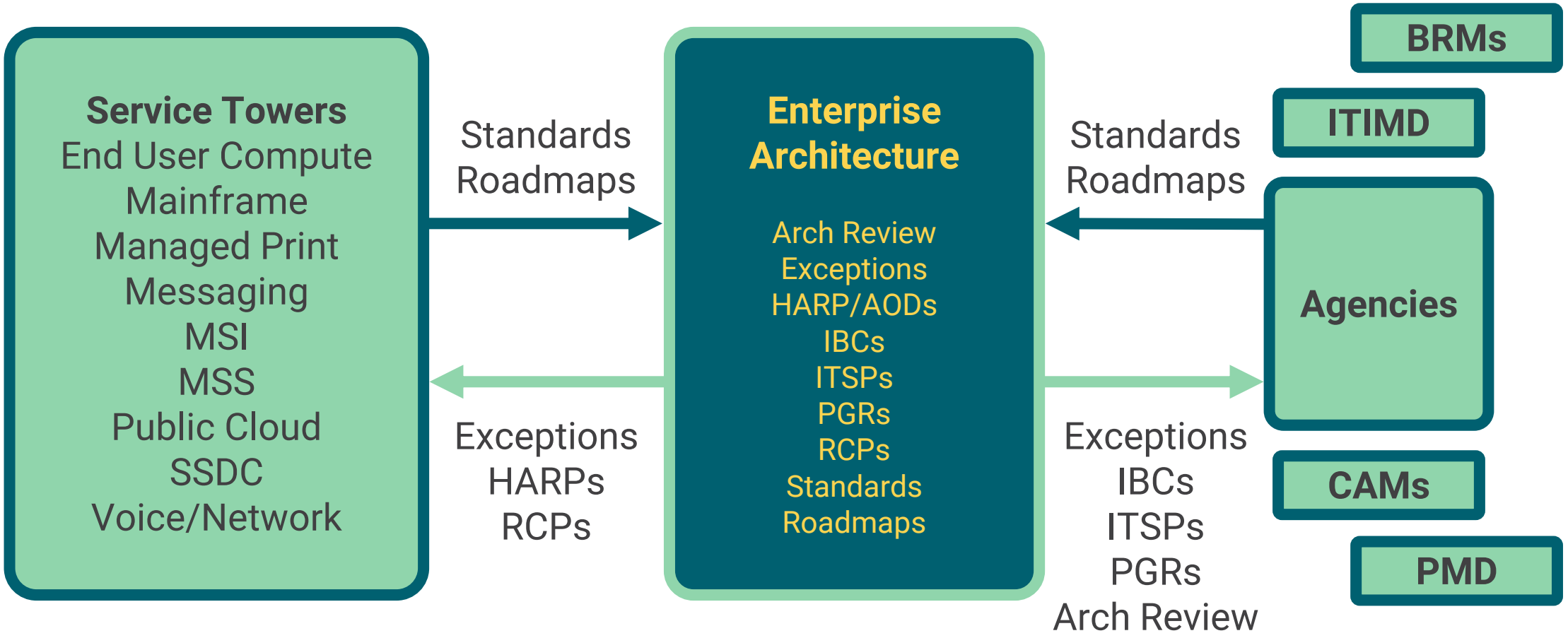


Cloud Based Hosting
Computer-based Signature Standard
Data Availability Requirements
EA Smart Device Use
Enterprise Systems Management
Enterprise Technical Architecture
Event Log Management
Legacy Information Technology Solutions
Networking and Telecommunications
SOA Integration
Smart Device Use
Social Media
Web Systems Standard
Wide Area Network

WORKFLOW PARTICIPATION

- Investment Business Cases (IBCs)
- Procurement Governance Requests (PGRs)
- IT Strategic Plans (ITSPs)
- Exceptions
- Architecture Review
- Refresh & Currency Plans

EA MODEL


Service Towers
End User Compute
Mainframe
Managed Print
Messaging
MSI
MSS
Public Cloud
SSDC
Voice/Network
Standards
Roadmaps
Exceptions
HARPs
RCPs
Enterprise Architecture
Arch Review
Exceptions
HARP/AODs
IBCs
ITSPs
PGRs
RCPs
Standards
Roadmaps
Standards
Roadmaps
Exceptions
IBCs
ITSPs
PGRs
Arch Review
BRMs
ITIMD
Agencies
CAMs
PMD

QUESTIONS

VIRGINIA IT AGENCY

IT Risk Assessments

Jonathan Smith
Director, Risk Management

June 2023 - ISOAG

Agenda

SEC 520 Risk Management Standard

- Risk assessment planning
- Performance of risk assessments
- Risk Treatment Plans
- Quarterly updates

- **Archer Risk Assessment Questionnaire**

SEC 520 Risk Management Standard

Purpose: Risk Assessment (RA) requirements delineate the steps agencies must take for each IT system classified as sensitive to: Identify potential threats to the confidentiality, integrity, and availability of an IT system and the environment in which it operates; Determine the likelihood that threats will materialize; Identify and evaluate vulnerabilities; and Determine the impact if one or more vulnerabilities are exploited by a potential threat.

SEC 520 Risk Management Standard

Risk Assessment Planning

Annually, each agency shall develop a risk assessment plan, and as necessary, update an existing one for the IT systems for which it is the System or Data Owner. The risk assessment plan shall be risk-based (to include the BIA, sensitivity classifications, etc.). Each agency head shall submit the agency risk assessment plan (or approval of the risk assessment plan) to the CISO, annually.

Agencies are required to submit their plans using the Risk Assessment Plan Template found at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/ unless an alternative is approved by the CISO

SEC 520 Risk Management Standard

Risk Assessment Plan (cont'd)

The Risk Assessment Plan Template includes the following fields:

- Agency Information
- Contact Information
- The system full name and abbreviation
- The planned assessor
- The date the last risk assessment was conducted for the system
- Scheduled risk assessment completion date

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three-year period from the submission date.

SEC 520 Risk Management Standard

Risk Assessment Plan (cont'd)

IT Risk Assessment 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 Assessor	Date Last Assessed (MM/YY)	Scheduled Assessment Completion Date(Minimum once every 3 years)			Areas for Special Emphasis and Additional RA Requirements
				20xx (MM/YY)	20xx (MM/YY)	20xx (MM/YY)	

SEC 520 Risk Management Standard

Performance of Risk Assessments

- Conduct and document a risk assessment of the IT system as needed, but not less than once every three years
- Determine and document the most appropriate methodology for assessing the controls based on agency risk and maturity
- The RA shall use, at a minimum controls from COV SEC501, COV SEC525, NIST Cybersecurity Framework as outlined in the Risk Management Standard, or CIS Critical Security Controls
- If the agency ISO completed the prior RA using a subset of the comprehensive controls, the subsequent scope shall incorporate both critical controls and those skipped in the prior year
- Conduct and document an annual assessment to determine the continued validity of the RA. Send updates to the annual assessment to CISO.

SEC 520 Risk Management Standard

Magnitude of Impact

- Determine the magnitude of impact - the level of harm that an exploited vulnerability could cause the agency or Commonwealth.

Table 1. Magnitude of Impact

Rating	Impact Definition
Critical	Direct high impact and high likelihood of occurrence.
High	Direct minimal impact and high likelihood of occurrence OR direct high impact and minimal likelihood of occurrence.
Moderate	Indirect high impact and minimal likelihood of occurrence.
Low	Indirect minimal impact and minimal likelihood of occurrence

SEC 520 Risk Management Standard

Effectiveness of Controls

- Assess the effectiveness of the controls and the vulnerabilities of the IT system

Table 2. Effectiveness of Controls

Rating	Control Impact Rating
High	Internal controls are sufficient to substantially reduce the risk to an acceptable level.
Moderate	Internal controls reduce the threat; however, additional controls should be implemented to further mitigate the risk where feasible.
Low	Few, if any, internal controls are in place to reduce the risk in any meaningful way. Additional controls should be implemented to mitigate the risk.

SEC 520 Risk Management Standard

Probability of Threat Occurrence

- Determine the probability of threat occurrence - the likelihood of a threat exploiting a vulnerability based on the effectiveness of the internal control and its expected magnitude of Impact.

Table 3. Probability of Threat Occurrence

Effectiveness of Controls	Magnitude of Impact			
	Low	Moderate	High	Critical
High	Low	Low	Moderate	High
Moderate	Low	Moderate	High	High
Low	Moderate	High	High	High

SEC 520 Risk Management Standard

Identification of risk findings

- Risks identified in the risk assessment with a residual risk rating greater than a value of low create a risk finding.
- For each risk finding, a risk treatment plan shall be created using the Risk Treatment Plan template capturing the following fields:

Agency	Magnitude of impact	Remediation status
Agency Finding reference field	Probability of occurrence	Actual remediation date
Name of the finding	Finding date	
Description of the finding	Remediation overview	
Affected applications	Initial planned due date	
Policy Section Name (control – i.e. AC-2)	Responsible Person(s)	

SEC 520 Risk Management Standard

Reporting of Risk Assessments, findings and quarterly updates

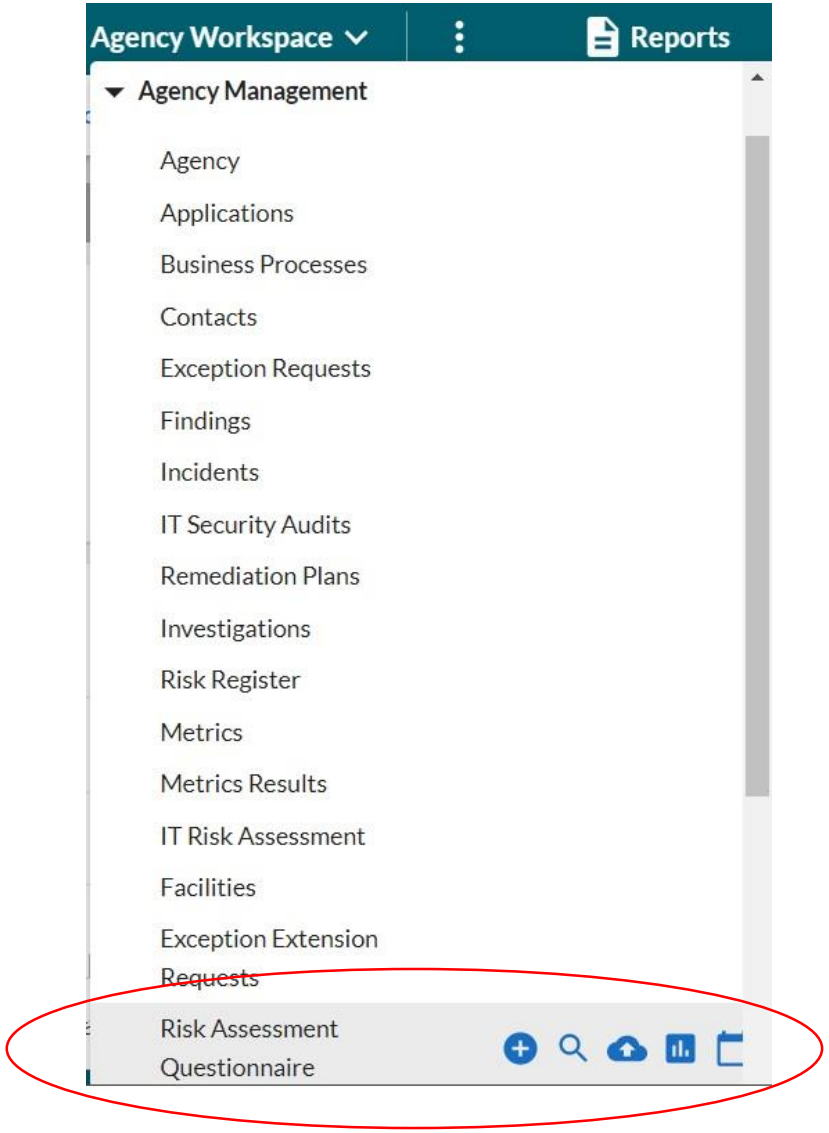
The agency head or designee shall submit to the CISO the following information:

- A record of all completed IT Risk Assessments conducted by or on behalf of the Agency.
- For each risk identified with a residual risk greater than low, a Risk Treatment Plan shall be submitted to the CISO within 30 days of the final risk assessment report
- An updated risk treatment plan must be submitted quarterly (at the end of each quarter), until all risks have been remediated
- Agencies must use the Risk Treatment Plan Template or enter the quarterly updates in the CSRM eGRC application.

Archer Risk Assessment Questionnaire

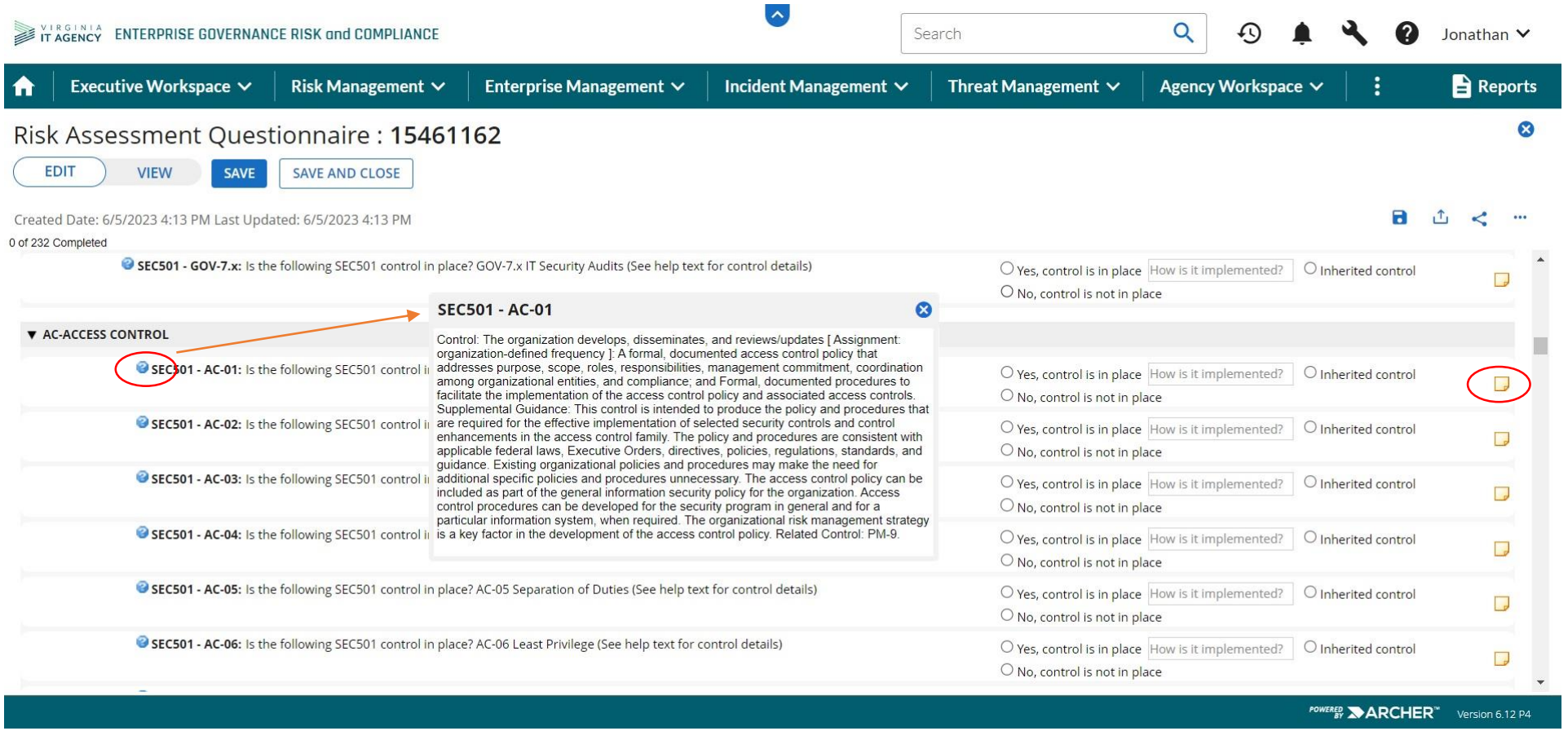
RSA Archer Risk Assessment Questionnaire:

- A control assessment that that can be used to assist with assessing IT system risk and/or system security planning
- Automatically generates Archer risk findings for controls that are not in place upon submission
- Select SEC 501 or SEC 525 control standards
- Must answer a minimum of 100 control questions to submit for completion
- Questionnaire may be saved and continued



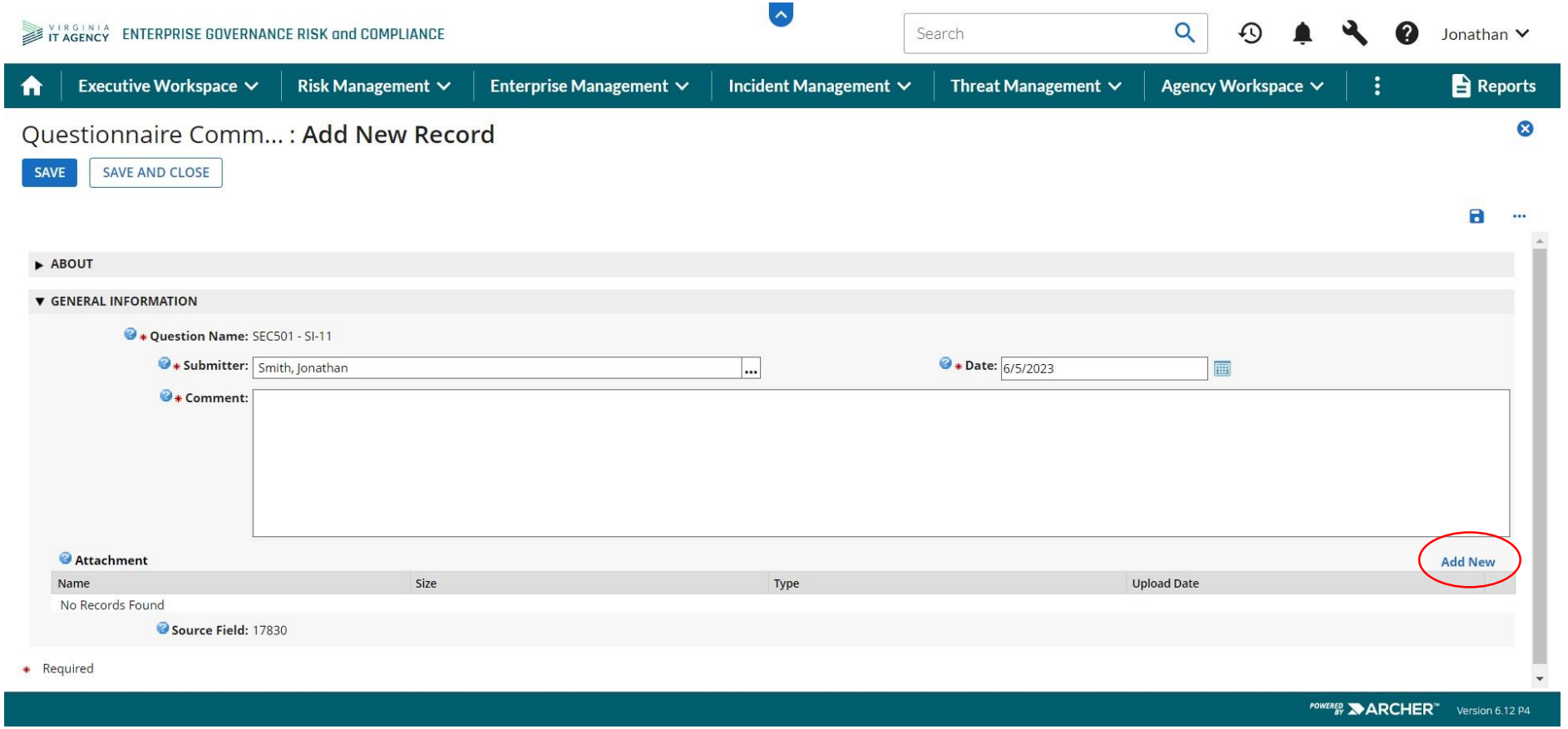
Archer Risk Assessment Questionnaire

Select the help icon to view the entire control text



Archer Risk Assessment Questionnaire

Add comments, artifacts/attachments to specific control responses



Archer Risk Assessment Questionnaire

Risk Assessment control questionnaire is not…

- Questionnaire is not a complete system risk assessment
- Questionnaire is not threat specific
- Auto-generated findings do not set the magnitude of impact or probability of occurrence
- Risk Treatment plans must still be created or added to the auto-generated findings

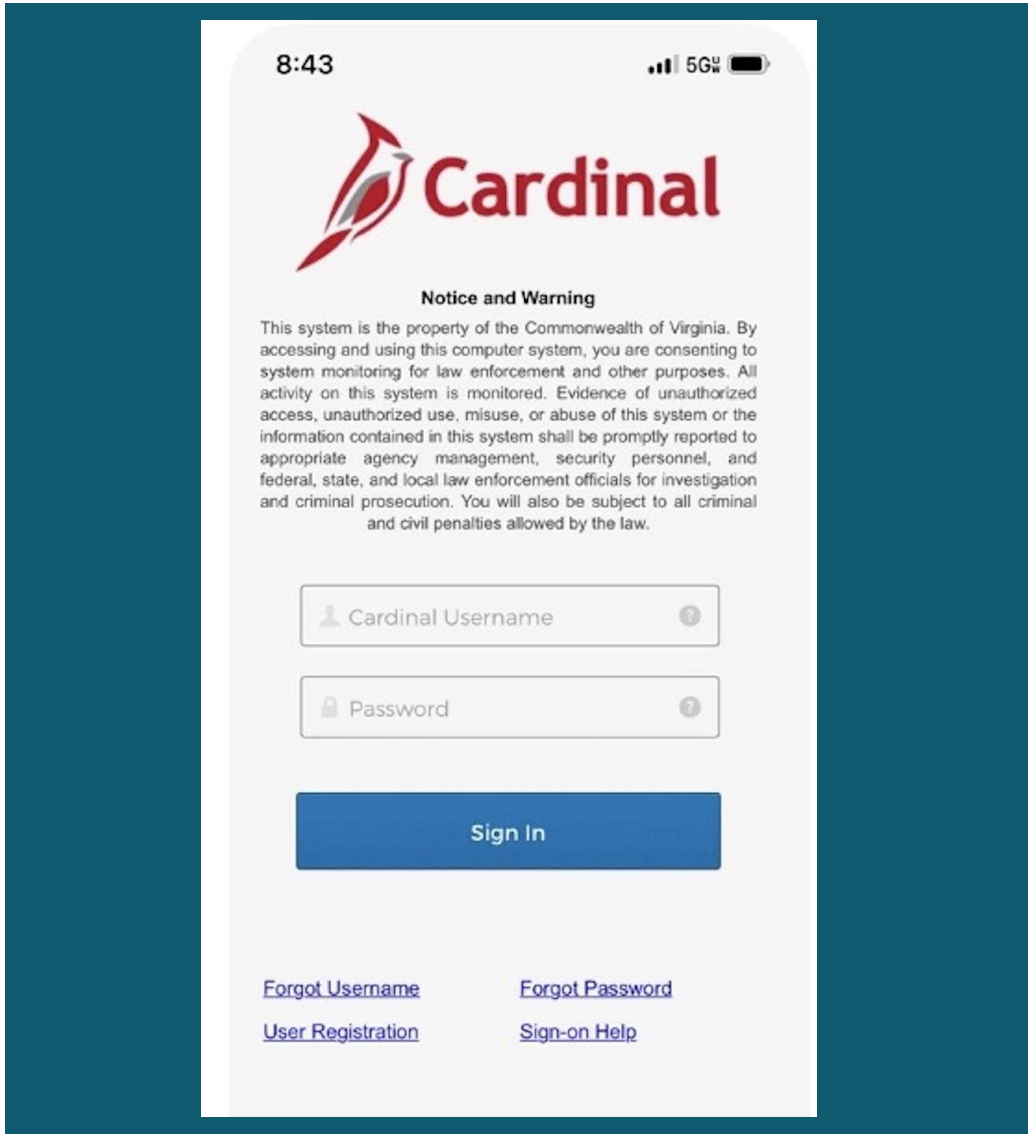
Risk Assessment control questionnaire is a work in progress

Questions?

Contact information:

Jonathan.m.smith@vita.virginia.gov

804-920-6711



VIRGINIA IT AGENCY

Cardinal incident postmortem

ISOAG June 2023

Dean Johnson
Director of Threat Management

June 2023

Cardinal incident – postmortem

Agenda

- Incident Background
- Attack Vector
- Analysis / Containment
- Eradication / Recovery
- OKTA 2FA options moving forward
- Questions

Background

Initial Incident report

- DOA reported an incident to the Virginia Fusion Center(VFC) on Apr 4, 2023 after they received a report from a DBHDS user who did not receive a paycheck via Direct Deposit as expected.
- VITA opened an incident ticket and collaborated with the Cardinal team to start triaging the incident.

Background

Triage findings

- Pivot on Direct Deposit account info
- Pivot on IP addresses that were associated
- Okta 2FA seemed to have been defeated
- 2FA commonality was SMS
- No direct correlation between any impacted users or specific device types
- Only personal user devices affected

Background

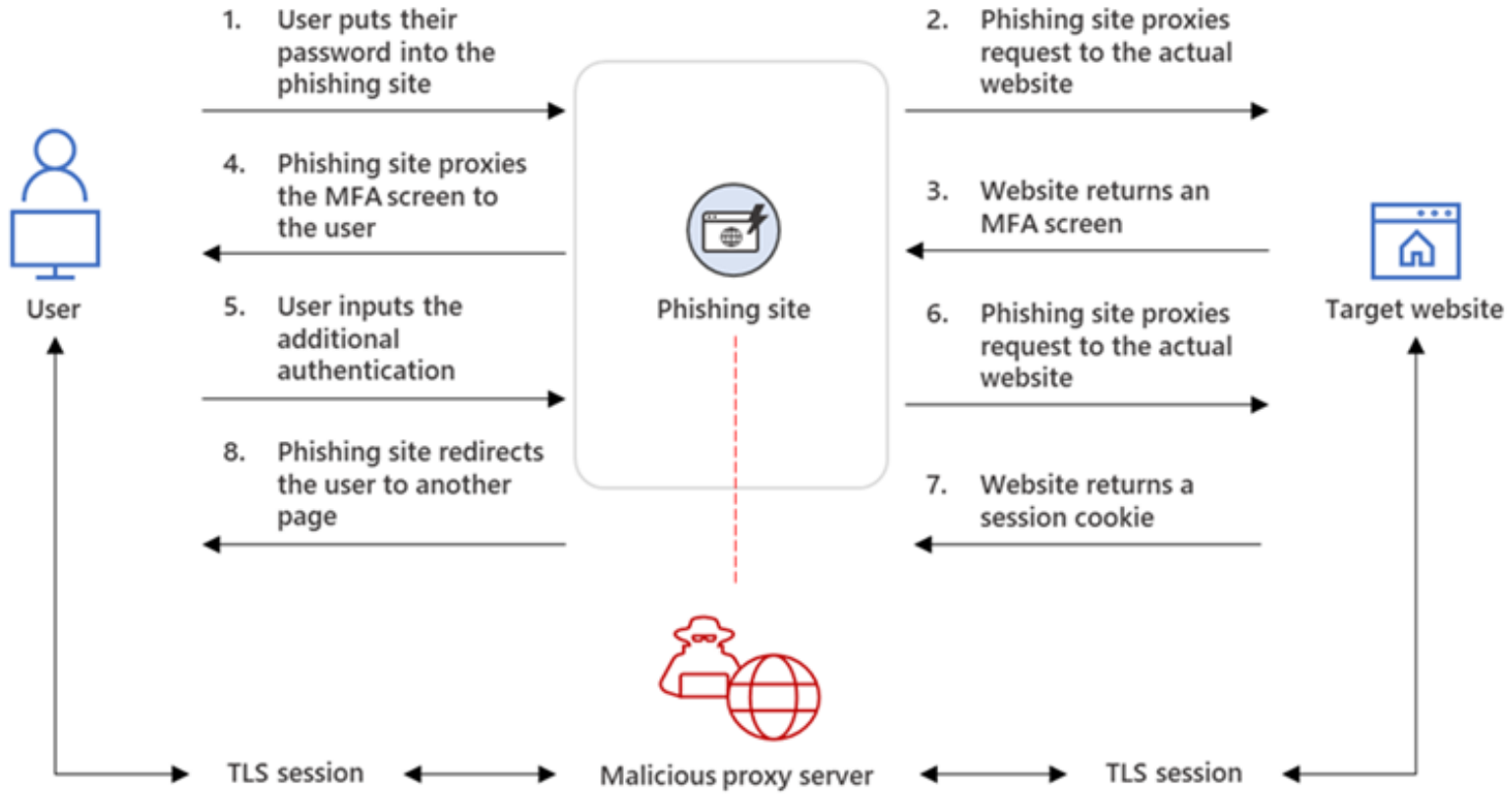
Theories on bypassing/defeating SMS 2FA

- SIM cloning
- SIM Jacking / swapping
- Infected/rooted device via malicious app
- Social Engineering
- Adversary-in-the-Middle (AitM)

Attack Vector

Adversary-in-the-Middle (AitM)

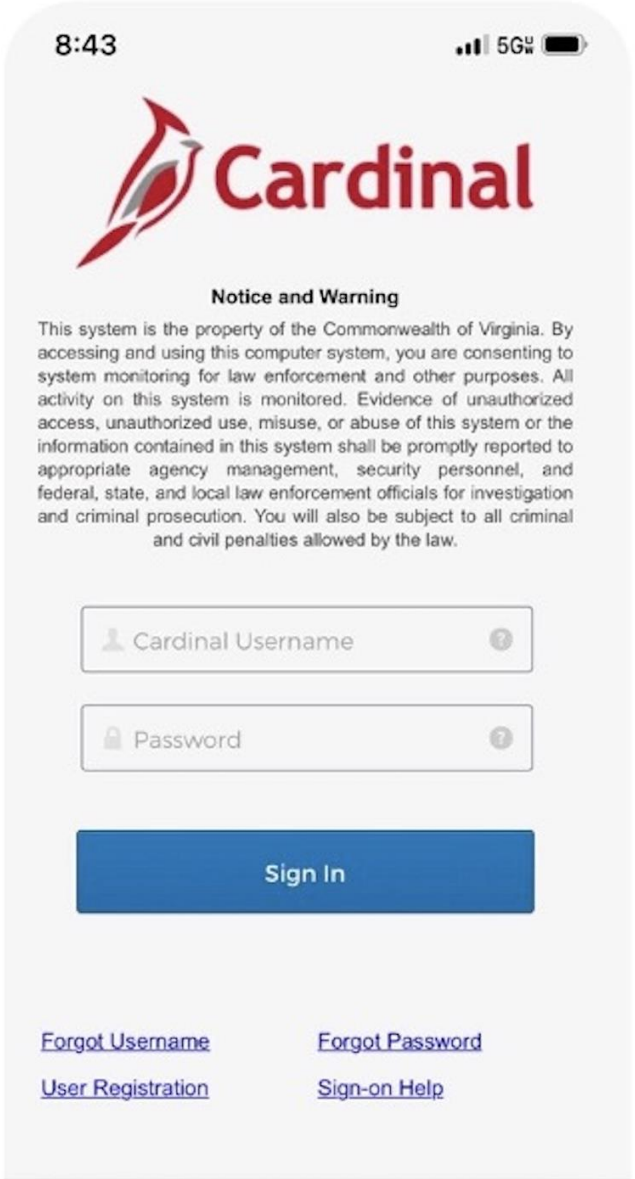
- Relatively new technique involving a proxy site that is identical to the real site.
- An adversary actively waits for user interaction with the proxy connection to obtain a valid session



Attack Vector

Adversary-in-the-Middle (AitM)

- Actual Proxy site →
- Viewed from a Mobile phone



Analysis / Containment

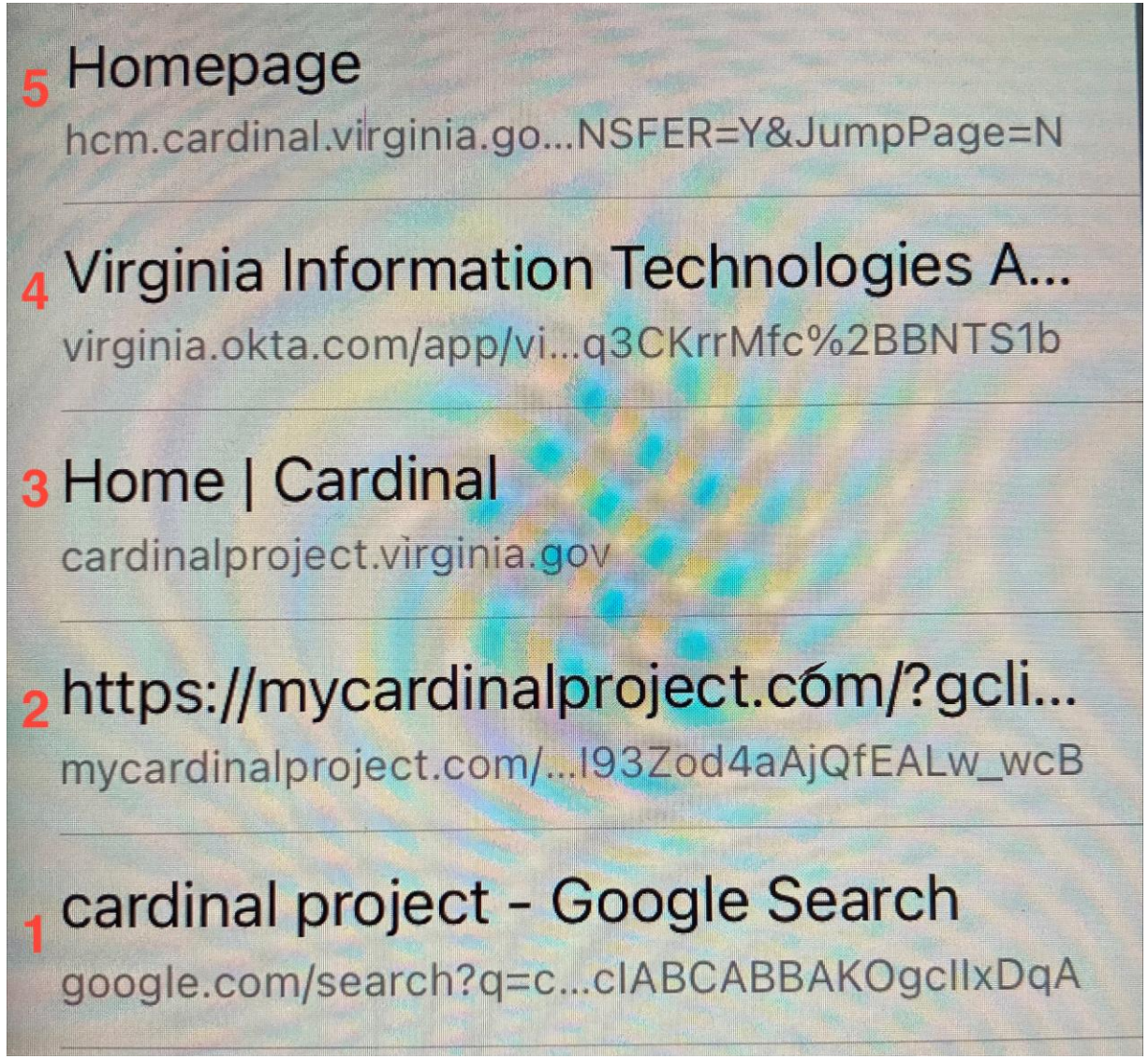
Analysis

- 2 of 28 users were open to us imaging and preforming forensics on their personal device(s)
- Mobile forensic imaging is difficult
- Android – a bit of a bust
- iPhone – worked… but no sign of the traffic shown in the logs
- Back to the logs…

Analysis / Containment

Analysis

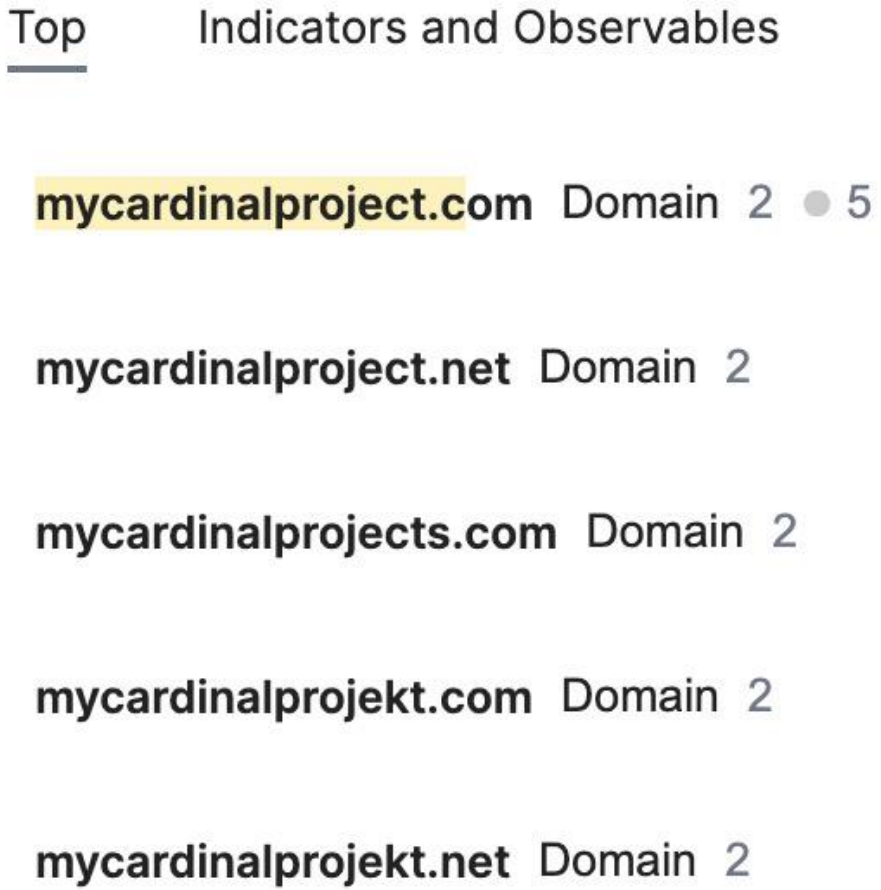
- OKTA logs showed a browser user-agent consistent with a Apple device but not an iPhone.
- The users iPad was identified and retrieved!
- VSP Hi-Tech Crimes assisted, and the puzzle came together.



Analysis / Containment

Pivoting on malicious domain in Threat intel

- Details of domains activity match incident timeline for time period of activity in late March 2023
- Domain squatting alerts for ‘mycardinal’ created.
- Domain take down process initiated and ongoing.



Eradication / Recovery

VITA

- Domain alerts and image hashes added to threat intel watch lists
- Malicious Domain monitoring rules created
- Domain takedowns issued and pending
- Investigated mitigating technologies in OKTA

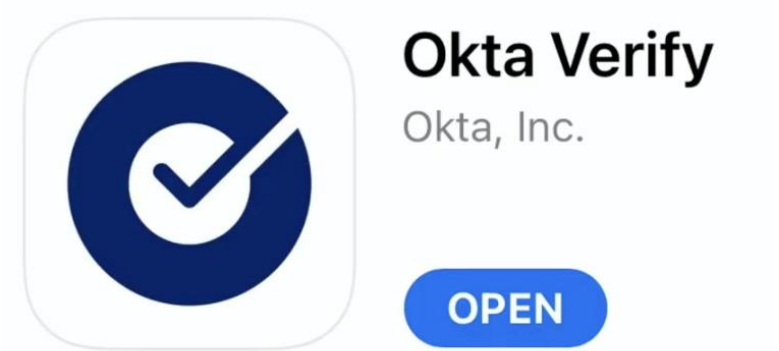
DOA

- Disabled self service Direct Deposit(DD) changes in Cardinal
- DD changes currently must go through payroll
- Email notifications now sent to users when DD changes are made

OKTA

OKTA 2FA moving forward

- Pilot Implementation of OKTA Verify app
- Pilot Implementation of Yubikey hardware authenticator
- Recommending phase out of SMS/Voice call only 2FA, especially for Admin level accounts



Cardinal incident – postmortem

Special Thanks!

- Quinton Litchford (DOA CIO), Rodgers Brewbaker (DOA Cardinal project Technical lead), Frank Pitera (DOA ISO), and the Cardinal team

- David Trent (DBHDS ISO)

- DBHDS nurse who was willing to lend her devices for analysis.

Questions?

VIRGINIA IT AGENCY

INTERNATIONAL TRAVEL Q&A

Chandos Carrow

Jackie Esters

CSRM

VIRGINIA IT AGENCY

CYBERSECURITY AWARENESS TRAINING FOR THE COMMONWEALTH KnowBe4 UPDATE

Tina Gaines

CSRM

KnowBe4 Implementation for 2023

- Knowbe4 will be rolled in three phases:

  - Phase One – Those agencies who are currently subscribed to Knowbe4. This phase took place on January 30, 2023. Phase one included over 20 state and independent agencies, two higher ed agencies, the Governor's Office, and two agencies who did not use Knowbe4. (completed)

  - Phase Two – Majority of the agencies not included in phase one. This phase is schedule to be completed by July 2023. We are currently in this phase. SANS/LITMOS subscription will expire 6/30 for agencies under the VITA subscription.

  - Phase Three – This phase will include agencies that might be a little more complex, challenging, or their subscription renewals expire later in the year or next year. This phase is scheduled for completion by December 2023.

- The Agency should:
  - Generate reports to close out their current training solution for audit purposes.
  - Start uploading your users to the KB4 platform
  - Create a preliminary test campaign
  - Create a test group to assign training to

How to Get Started with KnowBe4 Console:
https://support.knowbe4.com/hc/en-us/articles/115011714508
https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/KnowBe4-527-Crosswalk.pdf

➢ What VITA has completed:

- License Renewal Subscriptions for previous KB4 agencies/customers. Agencies should see the Diamond level and Compliance Plus subscriptions.

- KnowBe4 Training Sessions:

  Thursday, April 6
  Thursday, April 13
  Monday, April 17
  Thursday, April 27

  Wednesday, May 10
  Wednesday, May 17
  Wednesday, May 24

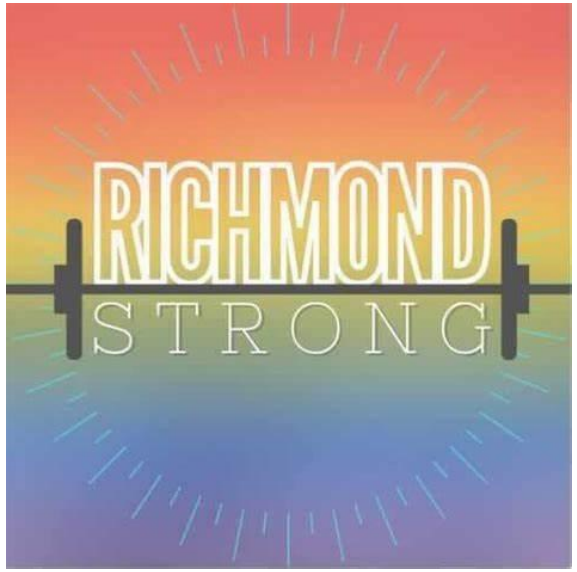
Agencies who have not reached out to VITA for training should do so as soon as possible. Individual agency sessions will be scheduled upon request.

What VITA Is Working on:

- Providing continuing KB4 support to agencies
- Working with KB4 on the issue of not being able to add non domain users
- Working with KB4 on the issue of providing training to agency localities
- Enterprise Okta integration.
  - ✓ VITA will test integration prior to roll out
  - ✓ Agencies will be notified in advance prior to final roll out

UPCOMING EVENTS

Sending our thoughts and prayers to those affected by yesterday's tragic event.



SANS ON DEMAND VOUCHERS (RETAIL = $8,275)

- On-DEMAND Vouchers are for on-line training only
- Vouchers can only be used for Long courses (5-6 days)
- Voucher expire one year from purchase date
- Discounted pricing available during SANS Buy Window (6/1/23 – 7/31/23) for $3,875 each
  - Order Directly from SANS thru 7/31/23 - Minimum ORDER or 3
  - Order through VITA/CSRM by 7/14/23 with a signed MOU – Minimum order of 1

- Note: VITA will be billing these orders during FY24. If you want it paid out of FY23, please work with your agency to reserve the FY23 funds.

ACCUNETIX 360 LICENSING - AVAILABLE IN NOV/DEC 2023

- VITA/CSRM has received some requests from agencies who are not part of the Web Application Scanning service.
- VITA can add additional licenses/agencies to their tenant at contract renewal.
- VITA is purchasing licensing in bulk at a cost of $300 per URL.
- VITA has setup an MOU for pass through purchasing for those entities that want to join VITA's tenant
  - Order Accuentix 360 licenses through VITA/CSRM with a signed MOU
  - Licenses are good for a period of 1 year and will expire as part of the VITA/Invicti contract.
  - Anyone who purchases licenses via an MOU will need to notify VITA/CSRM by 11/1 if they want to renew their licenses for the next year.

IS ORIENTATION

IS Orientation

Remote – WebEx

Date: June 28, 2023

Start time: 1:00 p.m. End time: 3:00 p.m.

Instructors: Erica Bland, Renea Dickerson and Tina Gaines

https://covaconf.webex.com/weblink/register/rbc9d847b4c8579e4428f406f6275aeb9

The next scheduled meeting for the IS Council:

July 19, 2023

12 – 1 p.m. (virtual)

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

tina.gaines@vita.virginia.gov

2023 COV SECURITY CONFERENCE - SAVE THE DATE

2023 COV SECURITY CONFERENCE - SAVE THE DATE

Save the date for the most innovative Commonwealth of Virginia Information Security conference, yet!

Date: Aug. 17, 2022
Time: 8 a.m. – 3 p.m.
Cost $125
https://www.vita.virginia.gov/information-security/security-conference/

Location: Hilton Richmond Hotel and Spa/Short Pump at 12042 West Broad Street, Richmond, VA 23233.

Join us for a day of thought - provoking discussions and networking opportunities with industry experts.

Keynotes:

Paul Chin Jr., Serverless Developer (Chat GPT)
Elham Tabassi, NIST (NIST AI Framework)

2023 COV SECURITY CONFERENCE - SAVE THE DATE

The Conference Committee is still seeking presenters.
If you are interested or know someone that would be a great presenter, contact:

isconferencecfp@vita.virginia.gov

Any conference related questions may be sent to:

covsecurityconference@vita.virginia.gov
commonwealthsecurity@vita.virginia.gov

July ISOAG MEETING

July 12, 2023

TIME 1 – 3 P.M.

SPEAKERS: TBA

MEETING ADJOURNED

VIRGINIA
IT AGENCY