VIRGINIA IT AGENCY

JUNE ISOAG MEETING

VIRGINIA
IT AGENCY

AGENDA

- PATRICK ROBINSON &
  BINDU SANDARESAN, ATT
- TONY ENCINIAS, DELL
- MARK MARTENS & JON SMITH, VITA
- UPCOMING EVENTS
- ADJOURN

Top of Mind

Seven Cyber Topics that are Top of Mind to CIO's and CISO's

Commonwealth of Virginia
VITA
ISOAG Meeting
June 2021

AT&T Proprietary (Internal Use Only) - Not for use or disclosure outside the AT&T companies except under written agreement

AT&T Business

Agenda

Introductions

Setting the Cyber Scene:
What's Top of Mind

Patrick Robinson

Associate Director,

AT&T Cybersecurity – Public Sector

Bindu Sundaresan

Director,

AT&T Cybersecurity Consulting

2021 Cyber Scene

2021 Top of Mind Security Initiatives

Risk based Vulnerability Management

Managed Vulnerability Program (MVP)
- IT/OT/On Prem/Cloud, Container security, Applications

Sustaining Compliance & Risk Management
- Enterprise Risk Assessments
- Annual Compliance Health checks
- CMMC Compliance Readiness Assessment

Supply Chain Risk Assessment & Management
- Automated Third-Party Risk Management (TPRM one time) Continuous Monitoring as a service

Next-gen Network & Security Transformation
- SASE, SOAR, ZTNA
- Zero Trust Workshop
- Zero Trust Readiness Assessment
- Zero Trust Design and Implementation

Breach Readiness and Response
- Malware Readiness
- Incident Response (IR)
- Compromise Assessment/Threat Hunt

Secure Remote Workforce, Resilience
- Safe Return Cybersecurity Best Practices

Cloud Transformation
- Security Architecture, Visibility and Monitoring
- Cloud Security Alignment-Compliance
- Cloud Misconfiguration Scanning

patrick.robinson@att.com

bindu.sundaresan@att.com

PRESENTATION:
TONY ENCINIAS, DELL
(NO SLIDES)

VIRGINIA IT AGENCY

RISK ASSESSMENTS VIA ARCHER QUESTIONNAIRE

MARK MARTENS

Risk Analyst

JUNE ISOAG MEETING

JUNE 2

WHY A RISK QUESTIONNAIRE WITHIN ARCHER AND WHY THE UPDATE?

- Agencies requested a questionnaire to satisfy the risk assessment requirements
- Our initial attempt did not include all control questions.
    - The latest version covers every control.
- The previous questionnaire did not provide guidance from SEC520

- Performance of risk assessments
  - For each IT system classified as sensitive, the data-owning agency shall:
    - a. Conduct and document a risk assessment (RA) 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.

PERFORMANCE OF RISK ASSESSMENTS

- The RA shall use, at a minimum controls from COV SEC501, COV SEC525, NIST Cybersecurity Framework as outlined in IT Risk Management Standard SEC520, or CIS Top 20 Critical Security Controls. Examples of risk assessment control questions provided in Appendix A. The agency ISO is responsible for documenting the methodology, assessment, results and corrective actions (risk treatment) to the CISO using the risk assessment/risk treatment template. (https://www.vita.virginia.gov/it-governance/itrm-policiesstandards/).

COVERING THE CONTROLS

- b. 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 UPDATES ANNUALLY

- Conduct and document an annual assessment to determine the continued validity of the RA. Send updates to the annual assessment to CISO.

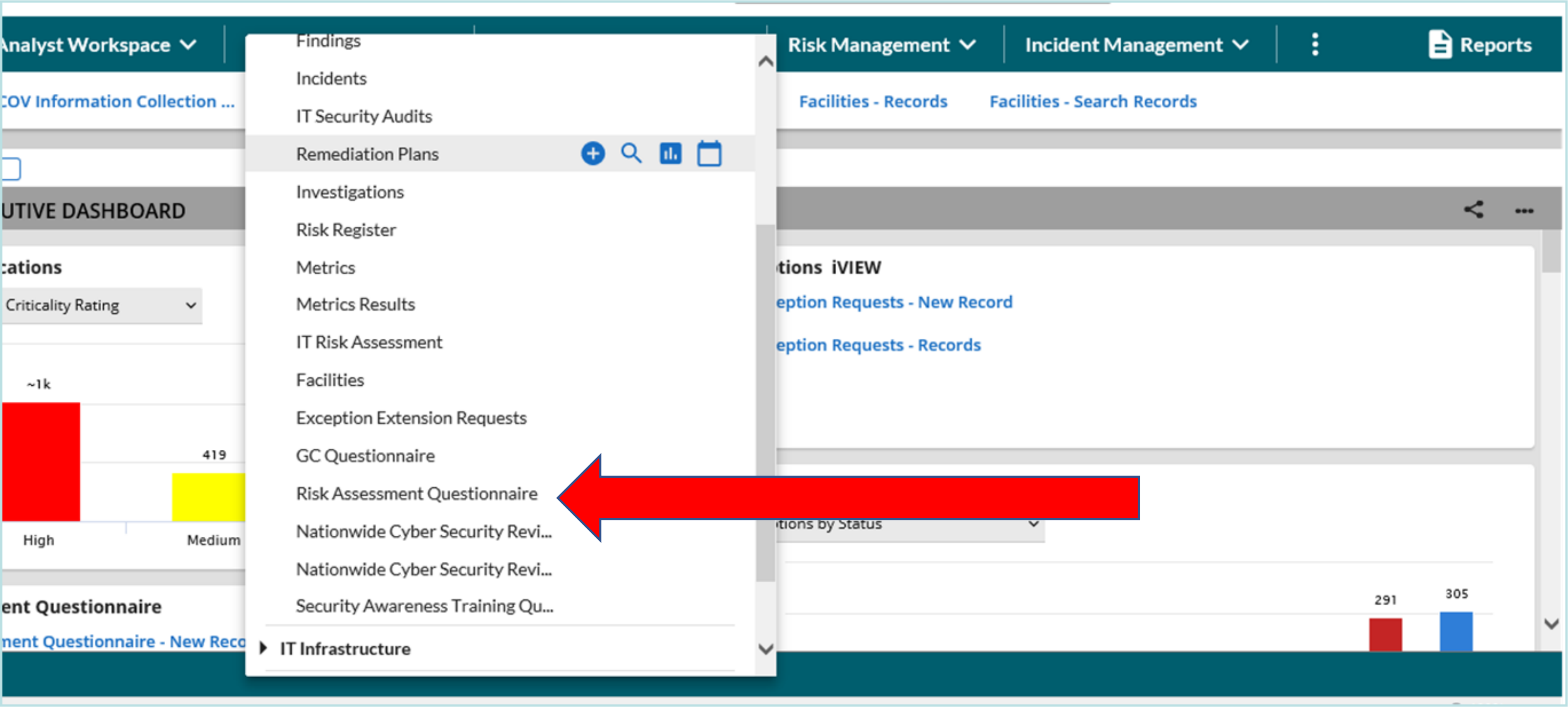
SEND CSRM YOUR FINDINGS

- Risks identified in the risk assessment with a residual risk rating greater than a value of low create a risk finding. **Note: Residual risks are calculated based on the data from the risk assessment.*
- e. For each risk finding, a risk treatment plan shall be created using the Risk Treatment Plan template. (https://www.vita.virginia.gov/it-governance/itrmpolicies-standards/)

SUBMIT QUESTIONNAIRE VIA ARCHER

- This is an option
- Not a requirement

NAVIGATE TO "RISK ASSESSMENT QUESTIONNAIRE"



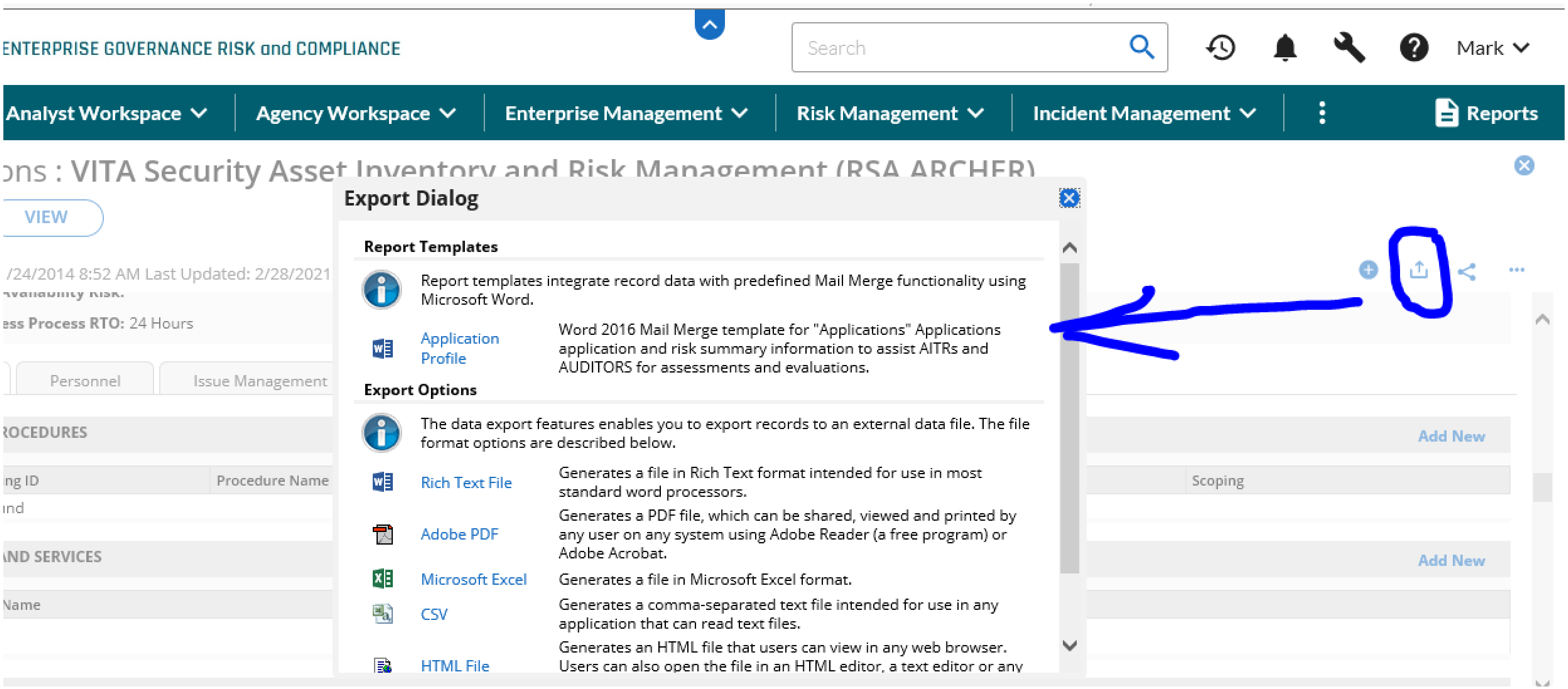
HOW TO START A QUESTIONNAIRE

- Find the "…" in the top right corner
- Select "New Record"
- Select the application to assess
- Read the Instructions at the top
- Select your Agency

INSTRUCTIONS: STEP ONE

1. Review the Application Profile for systems being assessed. For your convenience we created a report template that enables you to export information that will inform you of what laws, regulations, and known vulnerabilities exist for your application(s). Look for the export icon on the upper right hand side of the application layout and in the export dialog, select "Application Profile."

GO TO THE APPLICATION YOU ARE ASSESSING



ons : VITA Security Asset Inventory and Risk Management (RSA ARCHER)

/24/2014 8:52 AM Last Updated: 2/28/2021

Availability Risk:

ess Process RTO: 24 Hours

ROCEDURES

ng ID	Procedure Name	Scoping
ınd		

AND SERVICES

Name

Export Dialog

Report Templates

Report templates integrate record data with predefined Mail Merge functionality using Microsoft Word.

Application Profile	Word 2016 Mail Merge template for "Applications" Applications application and risk summary information to assist AITRs and AUDITORS for assessments and evaluations.

Export Options

The data export features enables you to export records to an external data file. The file format options are described below.

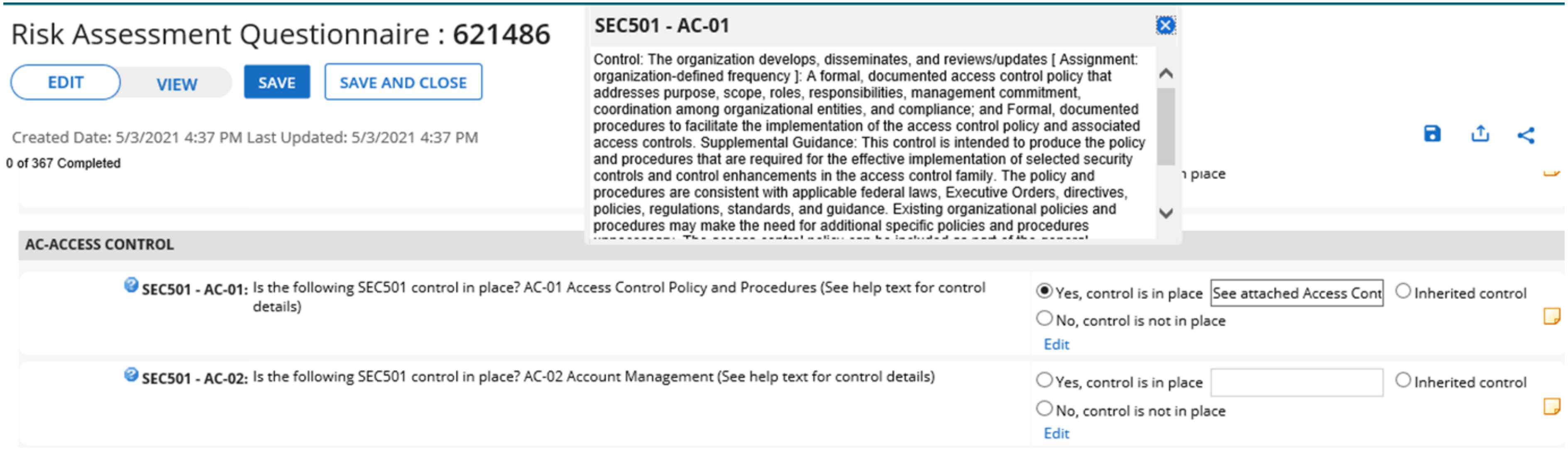
Rich Text File	Generates a file in Rich Text format intended for use in most standard word processors.
Adobe PDF	Generates a PDF file, which can be shared, viewed and printed by any user on any system using Adobe Reader (a free program) or Adobe Acrobat.
Microsoft Excel	Generates a file in Microsoft Excel format.
CSV	Generates a comma-separated text file intended for use in any application that can read text files.
HTML File	Generates an HTML file that users can view in any web browser. Users can also open the file in an HTML editor, a text editor or any

APPLICATION PROFILE

- Word Document with a description of the application, associated devices, business processes, data sets, findings, $ baseline risk, residual risk, business owner, sensitivity ratings for business processes and summary of data types associated.
- Example: Contains PCI, Contains PII, Contains FTI, etc.

2. Answer questions. Answer a minimum of 100 questions. You may skip over questions that are not appropriate to the application you are assessing. Question specific help text may be available via the icon.

EXAMPLE QUESTION



Risk Assessment Questionnaire : **621486**

Created Date: 5/3/2021 4:37 PM Last Updated: 5/3/2021 4:37 PM

0 of 367 Completed

SEC501 - AC-01

Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures

AC-ACCESS CONTROL

SEC501 - AC-01: Is the following SEC501 control in place? AC-01 Access Control Policy and Procedures (See help text for control details)

● Yes, control is in place See attached Access Cont ○ Inherited control
○ No, control is not in place
Edit

SEC501 - AC-02: Is the following SEC501 control in place? AC-02 Account Management (See help text for control details)

○ Yes, control is in place ○ Inherited control
○ No, control is not in place
Edit

INSTRUCTIONS: STEP THREE

3. Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added. This information will be passed along to the "remediation overview" field, should your answer result in a finding.

INSTRUCTIONS: STEP FOUR

4. Change the Status. You may keep the questionnaire "In Process" until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that a minimum of 100 questions must be answered before submitting the questionnaire.

5. Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire.

Four options:

- Complete the questionnaire
- Save your work and close the questionnaire
- Save your work and remain in the questionnaire
- Close the questionnaire without saving your work

6. SEC501. These questions were taken directly from language in SEC501. Please consult the security standard for additional details and context. https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

FINDINGS WARNING

- Please note: Once the status is changed to "submit," your assessment is locked. Findings will be generated upon approval of your assessment by VITA security.
- The job for the findings runs every hour on the hour.
- Give some time to copy over the details.

SEND US YOUR RISK TREATMENT PLAN

- Please export the associated findings into the Risk Treatment Plan template found here: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/
- Email your risk treatment plan, including your remediation overview, to commonwealthsecurity@vita.virginia.gov.

QUESTIONS?

UPCOMING EVENTS

2021 Virtual Commonwealth of Virginia Information Security Conference

The theme of the conference is “2021 Cybersecurity Reboot: Tools for building cyber resilience.” In addition to break-out presentations, the conference program will feature two keynote addresses.

Conference details:

Date: June 24

Location: Virtual! Event will be hosted by the College of William & Mary.

Registration cost: $25 for conference

Conference website: https://www.vita.virginia.gov/information-security/security-conference/

Questions: covsecurityconference@vita.virginia.gov

We encourage you to register early – we have almost reached maximum capacity!

IS ORIENTATION

DATE: June 30, 2021

TIME: 1 p.m.

REGISTRATION LINK:
https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e36fecc7d3d8344a0b0944dfa8f891bcc

PRESENTER: Marlon Cole (marlon.cole@vita.virginia.gov)

JULY ISOAG MEETING DETAILS

Date: July 14, 2021
Time: 1- 4 p.m. WebEx

Agenda
Mach 37/VA Cybersecurity Partnership

Krishna Marella, Xerox

Prashant Dixit, VITA

VIRGINIA IT AGENCY

THANK YOU FOR ATTENDING!