WELCOME TO THE May 1, 2024 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

May 1, 2024

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Erica Bland/ VITA
Centralized ISO BIA	Matthew Steinbach/ VITA
SSP Templates/Process	Jacquelyn Esters/ VITA
Upcoming Table-Top Exercise 2024	Zachary Wilton/ SAIC
Announcements	Erica Bland/VITA
Upcoming Events	Erica Bland/ VITA
Adjourn	

VIRGINIA IT AGENCY

Business Impact Analysis (BIA)

Centralized ISO Services

Matt Steinbach

About Me

- Member of the VITA CSRM team since 2018
- Prior Experience:
  - VITA –Information Security Auditor
  - Newberry Group – Supported federal agencies in NIST Compliance Authorizations, IT Help Desk for private businesses
- Current Role:
  - ISO analyst for the Centralized Information Security Officer Services (CISS)
  - The Centralized ISO team supports various Commonwealth agencies in the development and maintenance of their information security program

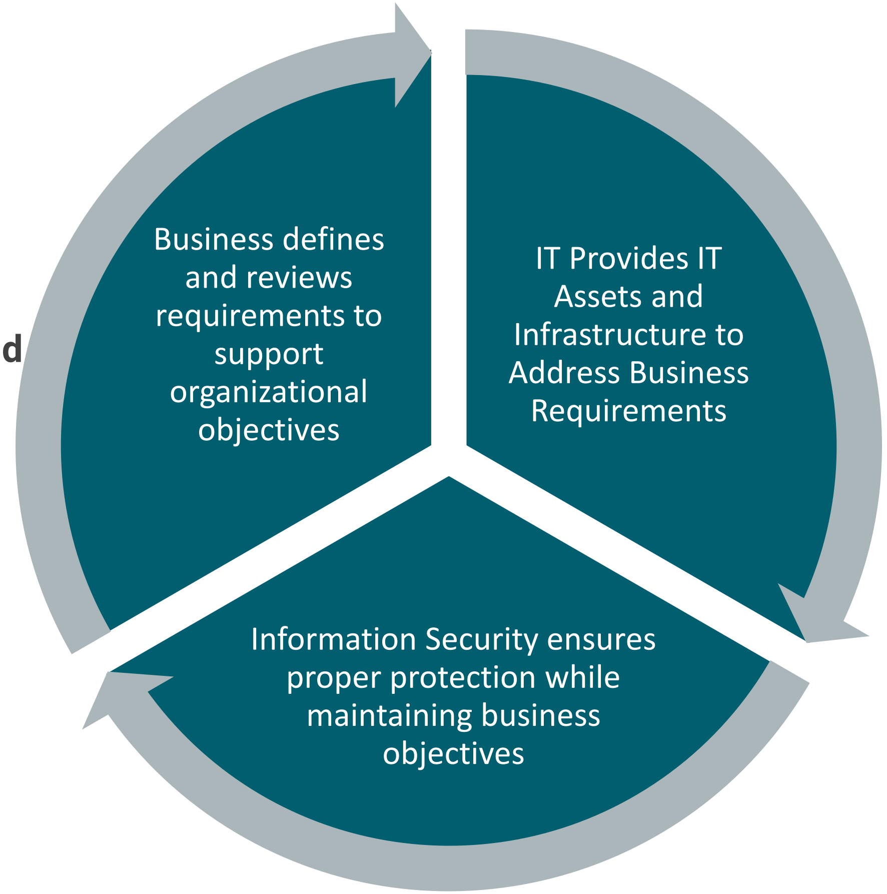
Fostering Collaboration Across the Business, Information Technology, and Information Security

Business Units determine IT and InfoSec functions

- Align IT and InfoSec requirements with the overall business objectives
- Identify critical systems and data that support business functions
- Prioritize IT and InfoSec requirements based on the criticality of systems and potential risks

The BIA provides an opportunity for the business to define what is required by IT and InfoSec

- Demonstrates to IT and InfoSec the repercussions the organization faces if a process stops
- Identify gaps where technology is needed to support lines of business
- Allows the business unit to set recovery objectives needed to maintain their business within acceptable operating levels


Business defines and reviews requirements to support organizational objectives
IT Provides IT Assets and Infrastructure to Address Business Requirements
Information Security ensures proper protection while maintaining business objectives

BIA completion requires input and collaboration from business and IT departments

What is a BIA?

- Systematic method of identifying and documenting all elements of essential, non-essential, and supporting functions and impacts to the organization if those functions were to fail
- Helps predict the consequences of disruption of business processes
- Helps ensure the right people, equipment, capabilities, records, and supplies are identified and available in the event of the disruption of normal operations
- Ensures that essential and supporting functions can be resumed quickly and performed as required

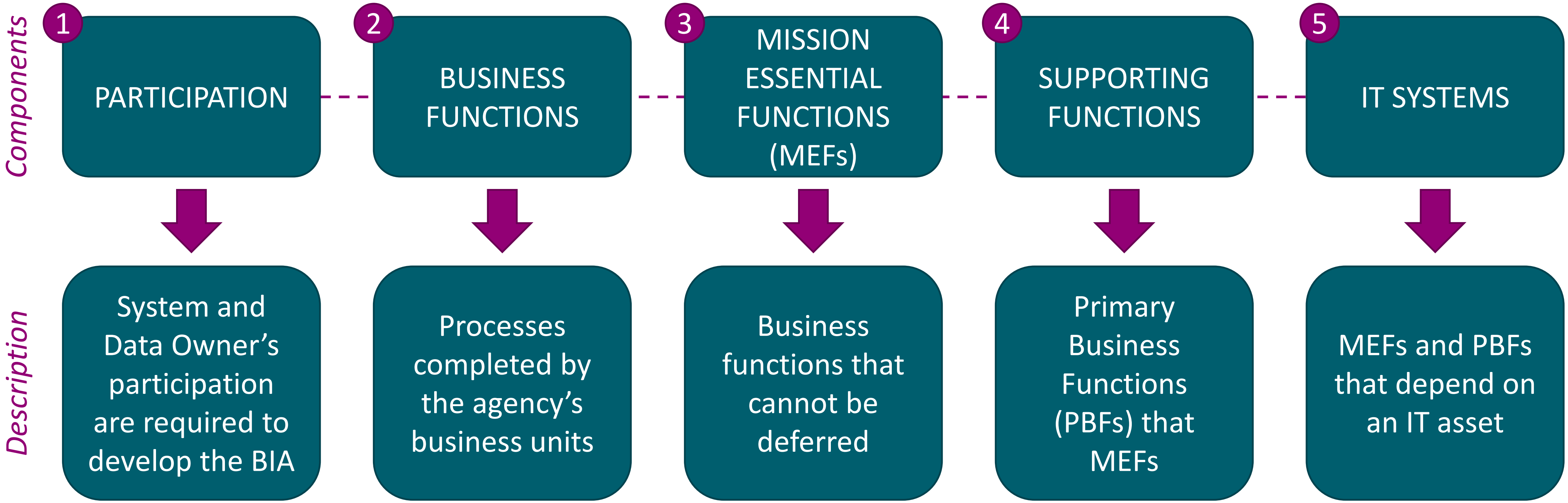
Why is a BIA Important?

- Integral part of business continuity program
- Identifies legal and regulatory impacts to the business
- Uncovers application dependencies
- Prioritizes needs and allocation of resources
- Calculates threshold of acceptable downtime for systems and data

Negative Impacts of Incomplete or Incorrect BIA:

- ➢ *Wasted resources protecting non-critical processes*
- ➢ *Leaving critical operations unidentified*
- ➢ *Unprotected Assets*
- ➢ *Faulty Recovery Plans*
- ➢ *Increased or unidentified risks*

Requirements of a Business Impact Analysis



Components

1 PARTICIPATION

2 BUSINESS FUNCTIONS

3 MISSION ESSENTIAL FUNCTIONS (MEFs)

4 SUPPORTING FUNCTIONS

5 IT SYSTEMS

Description

System and Data Owner's participation are required to develop the BIA

Processes completed by the agency's business units

Business functions that cannot be deferred

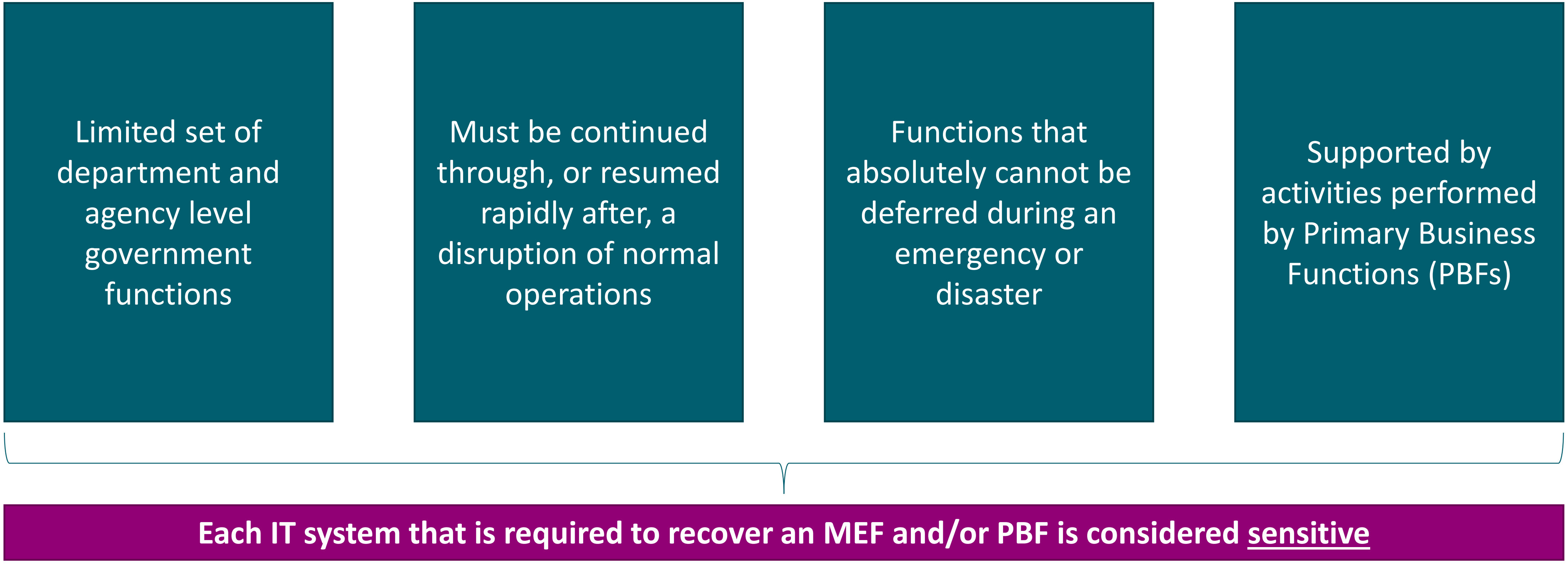
Primary Business Functions (PBFs) that MEFs

MEFs and PBFs that depend on an IT asset

BIAs should be reviewed on an annual basis, and fully revised every three (3) years.

SEC530-01.0 , 3.1

What are Mission Essential Functions?



Limited set of department and agency level government functions

Must be continued through, or resumed rapidly after, a disruption of normal operations

Functions that absolutely cannot be deferred during an emergency or disaster

Supported by activities performed by Primary Business Functions (PBFs)

Each IT system that is required to recover an MEF and/or PBF is considered sensitive

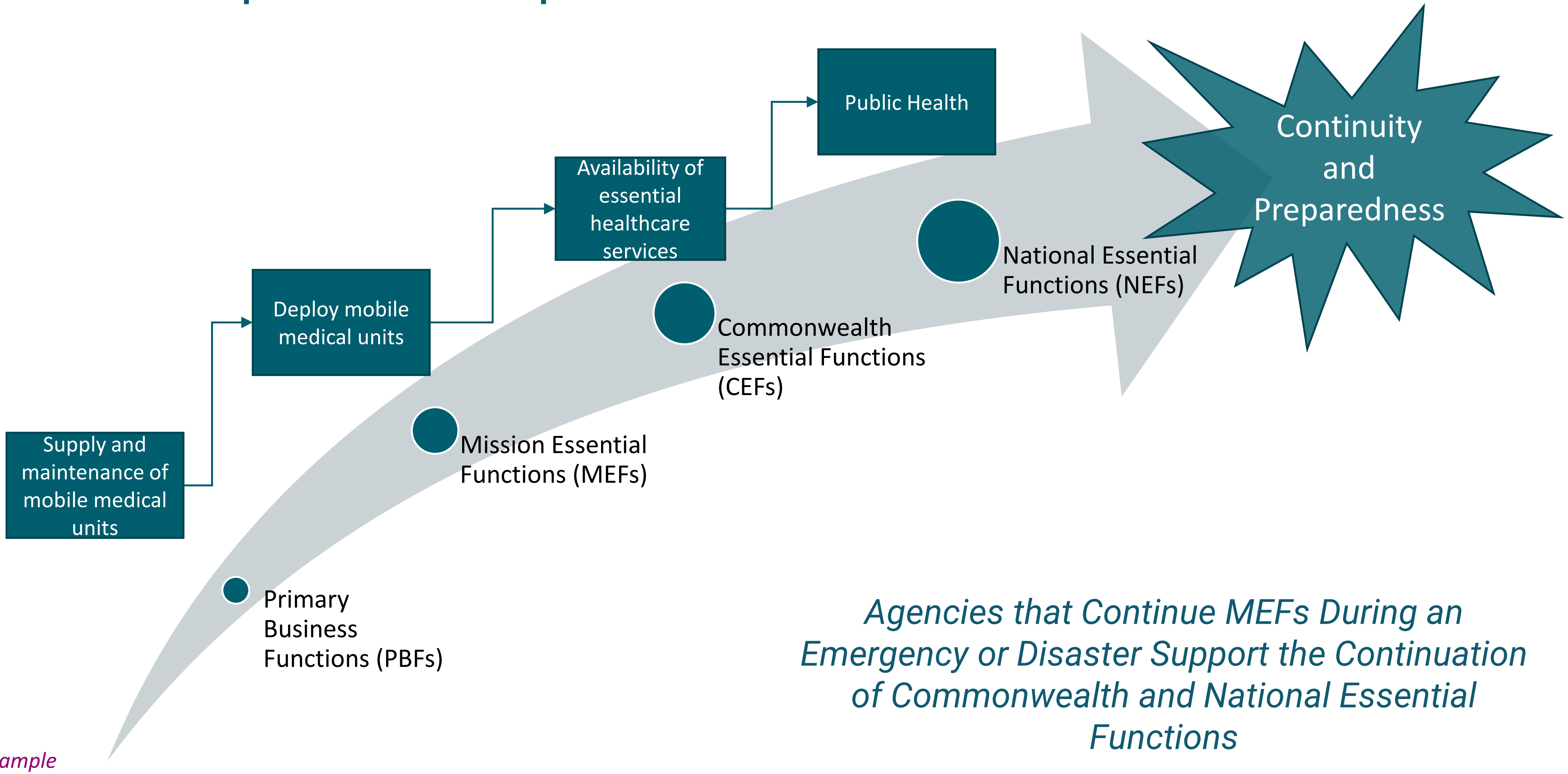
Examples of Essential and Non-Essential Functions

Function	Essential	Deferrable (Non-Essential)
Mission	Mission Essential Functions (MEF) • Coordinating the Commonwealth's response to emergencies and disasters • Maintaining transportation infrastructure • Providing safe water supply	Deferrable Mission Functions • Providing instruction to first time home buyers • Archaeological Collections Management • Providing public education/communication
Non-Mission	Essential Supporting Activities • Providing communication support for responders • Maintaining vehicle fleet • Maintenance of water treatment facilities	Deferrable Support Activities • Recruiting and hiring of staff • Training staff • Selling merchandise

Essential functions cannot be deferred during an emergency

Non-essential functions will be deferred during an emergency

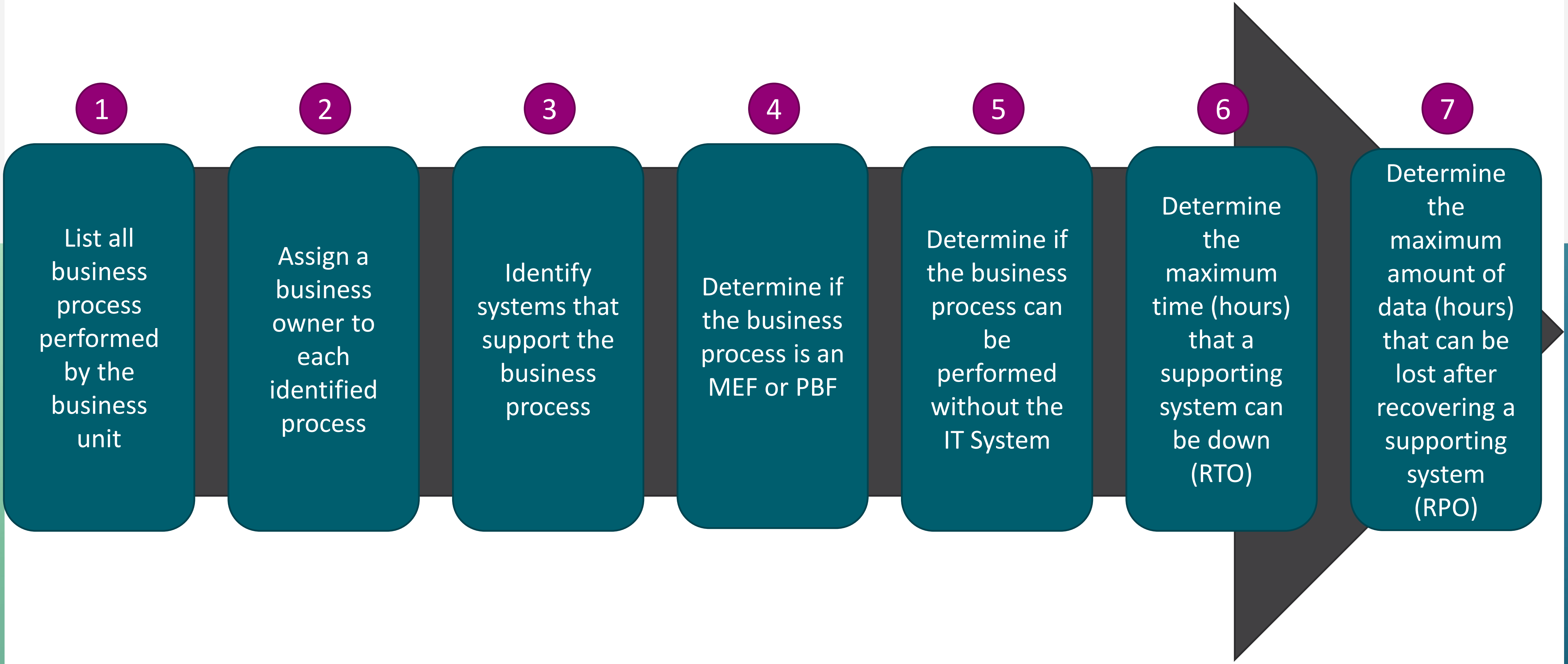
Mission Essential Functions can directly impact Commonwealth and National Essential Functions to Support Disaster Preparedness and Response


Supply and maintenance of mobile medical units
Deploy mobile medical units
Availability of essential healthcare services
Public Health
Continuity and Preparedness
Primary Business Functions (PBFs)
Mission Essential Functions (MEFs)
Commonwealth Essential Functions (CEFs)
National Essential Functions (NEFs)

Agencies that Continue MEFs During an Emergency or Disaster Support the Continuation of Commonwealth and National Essential Functions

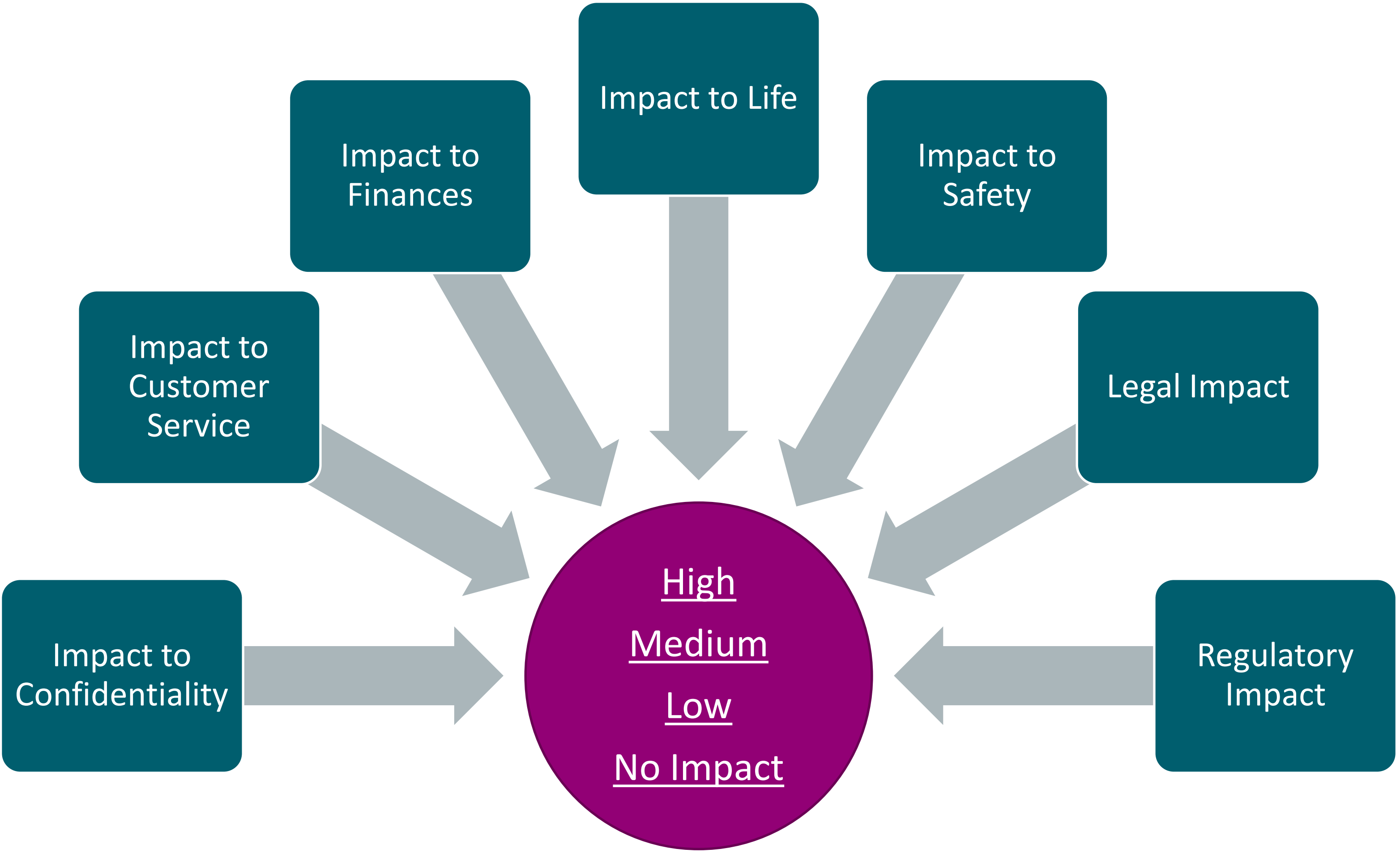
Illustrative Example

Steps of Completing a Business Impact Analysis



1. List all business process performed by the business unit
2. Assign a business owner to each identified process
3. Identify systems that support the business process
4. Determine if the business process is an MEF or PBF
5. Determine if the business process can be performed without the IT System
6. Determine the maximum time (hours) that a supporting system can be down (RTO)
7. Determine the maximum amount of data (hours) that can be lost after recovering a supporting system (RPO)

Business Process Assessment Identifies Organizational Impact Across Critical Domains



- Impact to Confidentiality determine the BP's Confidentiality designation
- Impacts to Finance, Customer Service, Regulatory, and Legal determine the BP's Integrity Designation
- Impacts to Finance, Customer Service, Life, and Safety determine the BP's Availability designation
- Life and safety are weighted

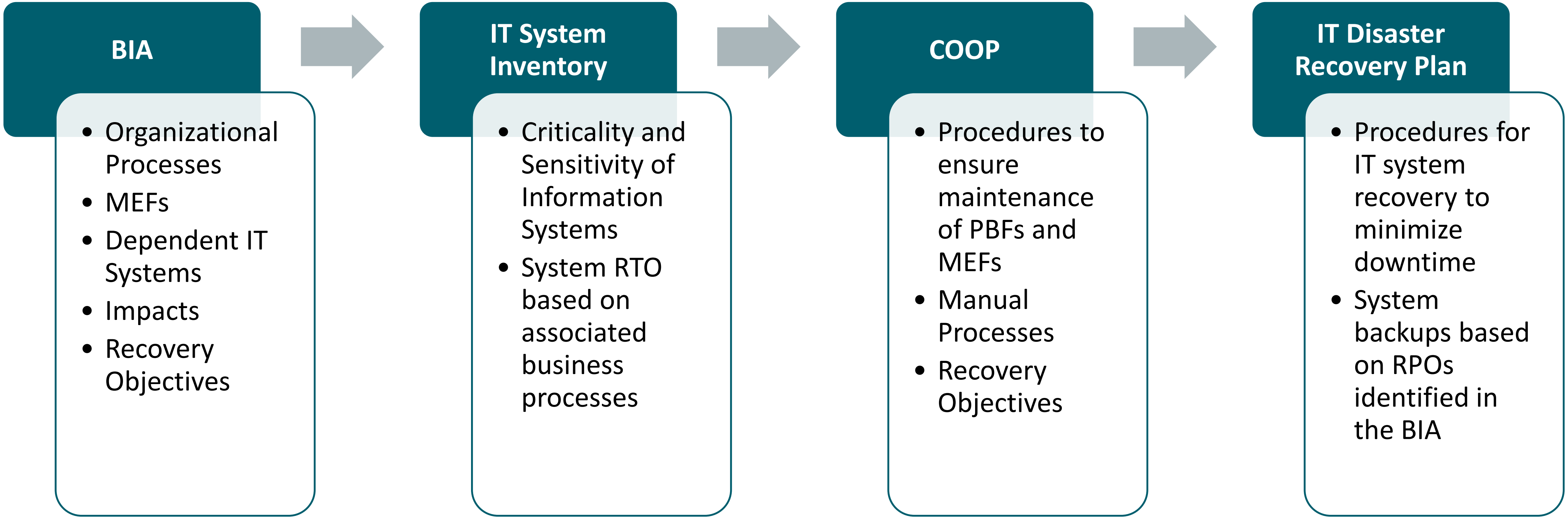
The BIA Can Impact System Sensitivity in Several Ways

Process Name	Criticality Rating	Confidentiality	Integrity	Availability
Process A	High	High	Medium	High
Process B	High	Low	High	Medium
Process C	Low	Low	No Impact	Low

Data Set Name	Sensitive to Confidentiality?	Sensitivity to Integrity?	Sensitive to Availability?
Dataset A	Yes: Contains SSNs	No	No
Dataset B	No	Yes: Contains Financial Data	No
Dataset C	No	No	Yes: Data must be accessible

- ➢ An application will determine overall system sensitivity based on the highest designation for associated business processes and data sets.
- ➢ An application will also pull the lowest value RTO and RPO and assign it to that application.
- ➢ Any Process identified as an MEF will be sensitive to availability

The BIA Informs Other Critical InfoSec and Contingency Planning Documents



BIA

- Organizational Processes
- MEFs
- Dependent IT Systems
- Impacts
- Recovery Objectives

IT System Inventory

- Criticality and Sensitivity of Information Systems
- System RTO based on associated business processes

COOP

- Procedures to ensure maintenance of PBFs and MEFs
- Manual Processes
- Recovery Objectives

IT Disaster Recovery Plan

- Procedures for IT system recovery to minimize downtime
- System backups based on RPOs identified in the BIA

Recap

- Organizational Business Units Drive IT and Information Security
- BIA is a comprehensive list of processes performed by an organization
- Mission Essential Functions are processes that cannot be deferred during an emergency
- Mission Essential Functions can directly impact Commonwealth and National Essential Functions to Support Disaster Preparedness and Response
- BIA Drives an Agency's Continuity of Operations and Disaster Recovery
- Negative Impacts of Incomplete or Incorrect BIA:
  - Wasted resources protecting non-critical processes
  - Leaving critical operations unidentified
  - Unprotected Assets
  - Faulty Recovery Plans
  - Increased or unidentified risks

Questions?

- Matt Steinbach- matthew.steinbach@vita.virginia.gov
- Mike Vannoy, Centralized ISO Services Manager- michael.vannoy@vita.virginia.gov
- VITA CSRM Mailbox- CSRM@vita.virginia.gov

VIRGINIA
IT AGENCY

Security Architecture- CSRM

New SSP Templates/ Process

Jacquelyn Esters- Security Architect

May 1, 2024

Overview

- What has changed
- Examples
- Updates to the process
- Updates to the templates
- Types of SSPs
- How to fill out a SSP
- Implementation status
- Questions

What changes have happened?

- Previously we suggested suppliers/ agencies complete a System Security Plan (SSP) for their entire environment. These SSP's covered all controls found within the standard

- Based on the NIST control summaries we broke down the SSP into multiple templates to provide suppliers and agencies an opportunity to document these specific controls for various scenarios

Examples:

Previously:

If a supplier submitted a SSP that covered all controls- they were lumping all their systems into one document. The level of detail needed to ensure that the service was compliant, was missing.

Example:

- **Supplier A states they have implemented Access Control (AC-3- Access enforcement) on 5 of the systems within their purview. Unfortunately, this blanket statement does not outline:**
  - The Role-based access control (RBAC) needs for each system
  - Level of Restriction access to data repositories containing organization-defined information types recognizing that systems can host many applications and services
  - Are the systems sensitive or non sensitive

Examples (Cont):

Example:

- **Agency B states they have implemented information flow (AC-4 Information Flow Enforcement) on 3 of the systems within their purview. Unfortunately, this blanket statement does not outline:**
  - Does the system enforce approved authorizations for controlling the flow of information within the system and between connected systems based on the appropriate organization-defined information flow control policies
  - How the information travels within a system and between systems
  - Rules set for established configuration settings that restrict system services
  - What architecture is in place to control information flow- API gateways, Content filtering web proxies, host-based firewalls, network segmentation, web access control, etc.

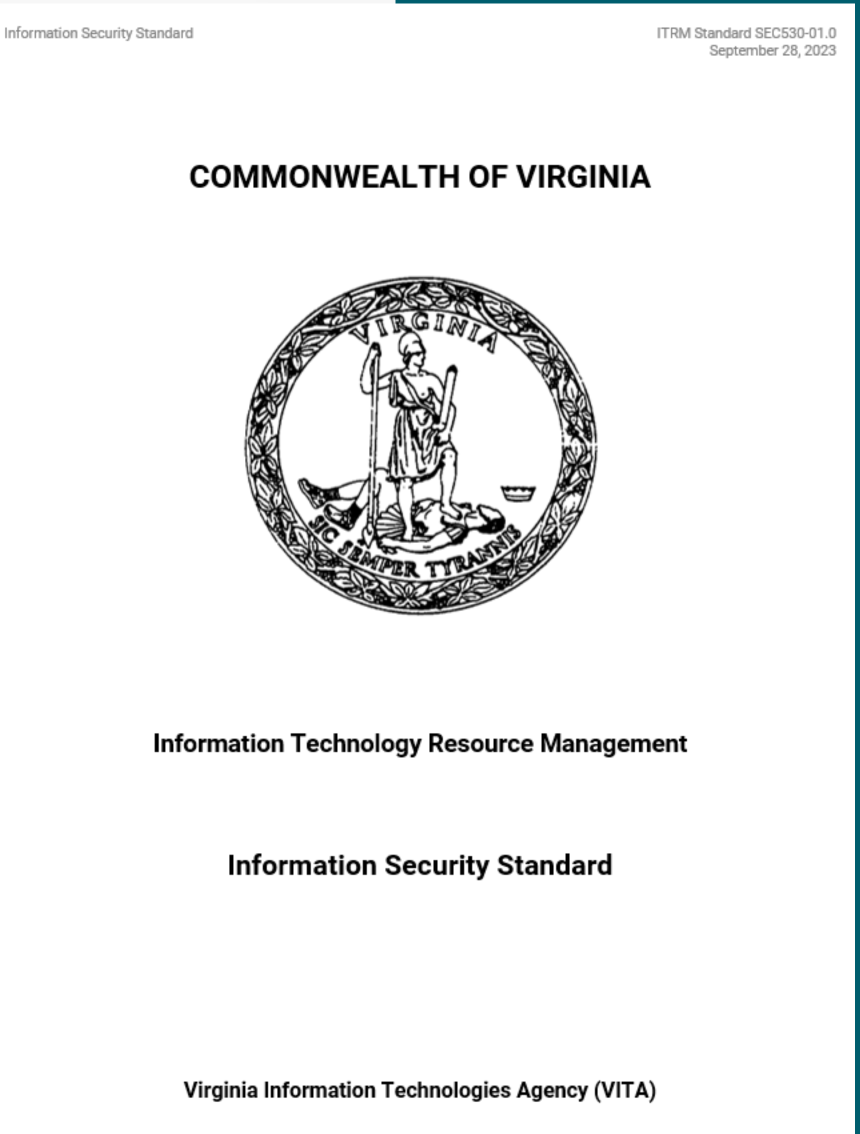
Updates to the process

- With the roll out of SEC530, we recognized this gap and provided the opportunity to follow an Organization / System Specific defined approach

- The new security requirements compliance date was March 31, 2024. The standard can be found on the VITA website under Policies, Standards, and Guidelines.

Updates to the Templates

- We have now broken out the templates in 4 areas to better align as we realize IT security is not a one size fit all.
    - SEC530 SSP (All controls)
    - SEC530 SSP (Non-Sensitive System Specific)
    - SEC530 SSP (Sensitive System Specific)
    - SEC530 SSP (Organization Controls)



Information Security Standard

ITRM Standard SEC530-01.0
September 28, 2023

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Standard

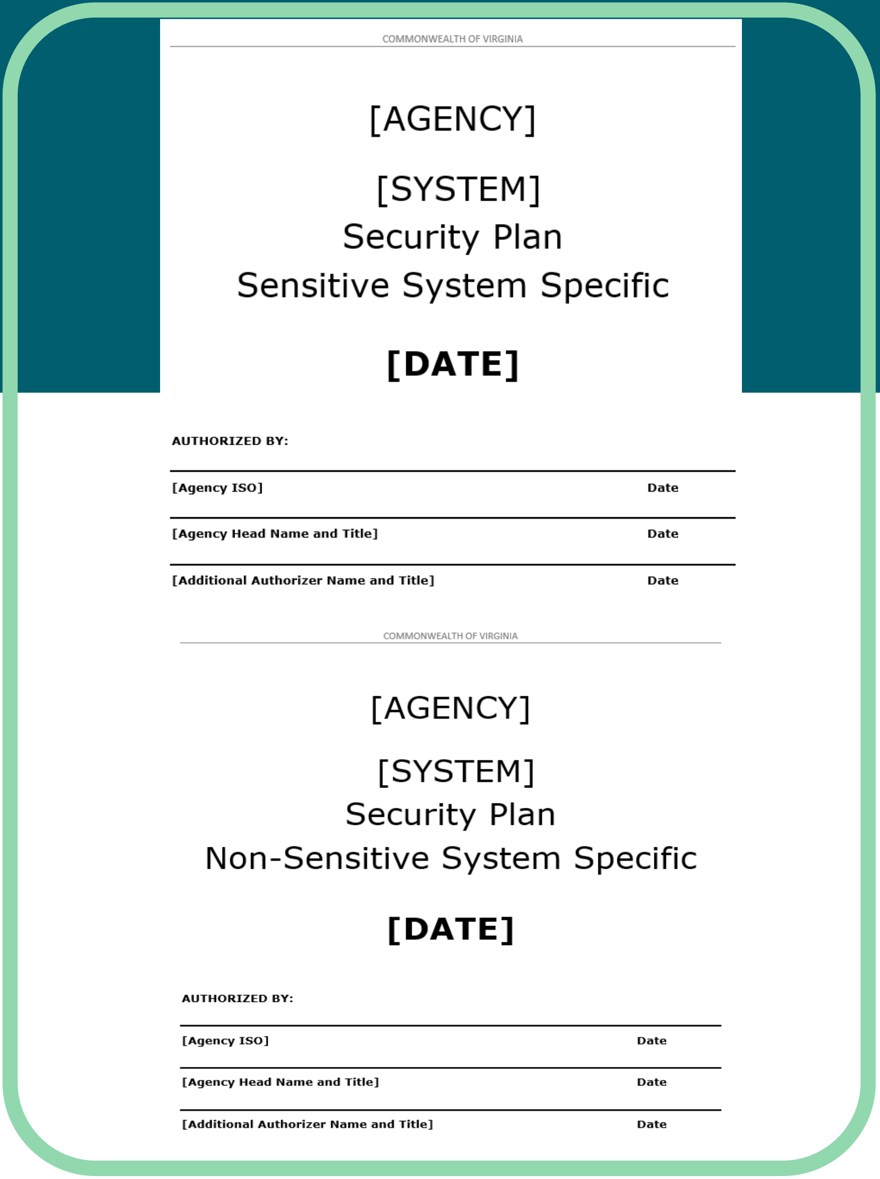
Virginia Information Technologies Agency (VITA)

System Specific Security Plans

- The System Specific SSP templates are scoped to the system and system components within a defined authorization boundary. These SSPs contain an overview of the security requirements for the system and the controls necessary to satisfy the requirements

- These System Specific SSPs are broken up into two Categories:
  - Sensitive System Specific
  - Non-Sensitive System Specific

- These plans should still be reviewed at least on an annual basis and following an environmental change



COMMONWEALTH OF VIRGINIA

[AGENCY]

[SYSTEM]
Security Plan
Sensitive System Specific

[DATE]

AUTHORIZED BY:

[Agency ISO]	**Date**
[Agency Head Name and Title]	**Date**
[Additional Authorizer Name and Title]	**Date**

COMMONWEALTH OF VIRGINIA

[AGENCY]

[SYSTEM]
Security Plan
Non-Sensitive System Specific

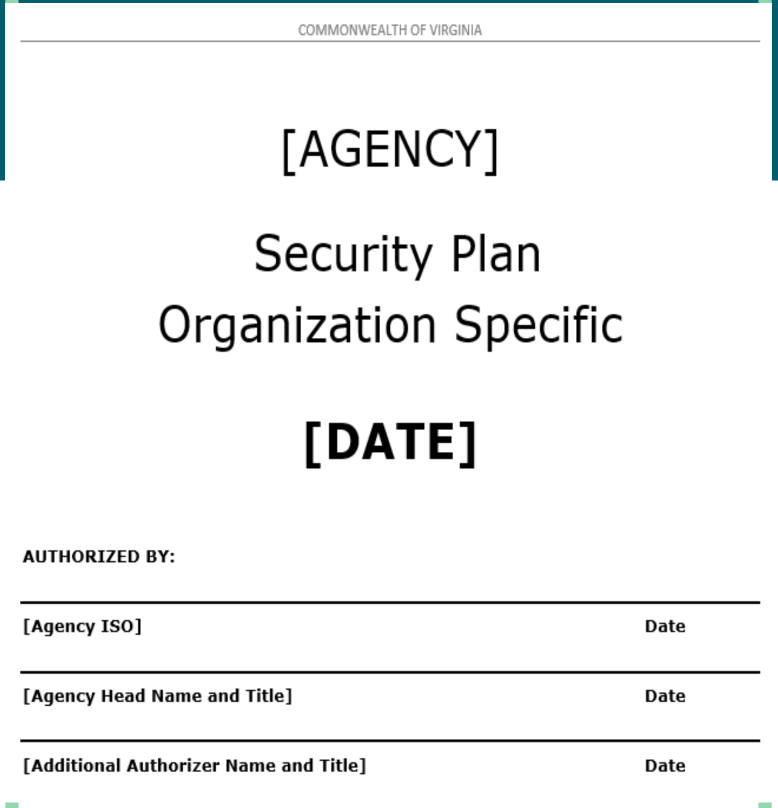
[DATE]

AUTHORIZED BY:

[Agency ISO]	**Date**
[Agency Head Name and Title]	**Date**
[Additional Authorizer Name and Title]	**Date**

Organization Specific Security Plans

- The Organization Specific SSP templates is scoped to the organization and organizational practices. This SSP contains an overview of the security requirements for the organization and the controls necessary to satisfy the requirements



COMMONWEALTH OF VIRGINIA

[AGENCY]

Security Plan

Organization Specific

[DATE]

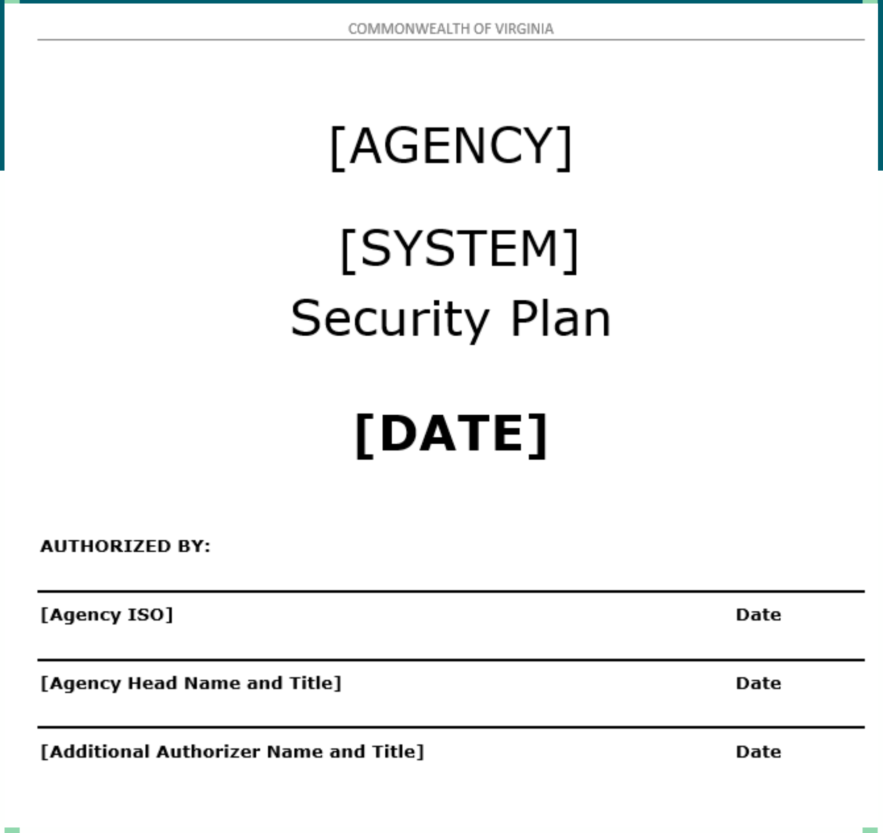
AUTHORIZED BY:

[Agency ISO]	**Date**
[Agency Head Name and Title]	**Date**
[Additional Authorizer Name and Title]	**Date**

All Controls Security Plans

- This is the traditional SSP that requires all controls to be answered

- Examples of when to use this SSP template version:
    - Supplier C only offers a singular service to the Commonwealth
    - Agency B only has a single system that they operate
    - If you are an Agency or supplier that wishes to combine all your systems/services into one SSP where all controls/control enhancements are answered for each system/service as well as organization to the level of detail necessary to show compliance



COMMONWEALTH OF VIRGINIA

[AGENCY]

[SYSTEM]
Security Plan

[DATE]

AUTHORIZED BY:

[Agency ISO]	**Date**
[Agency Head Name and Title]	**Date**
[Additional Authorizer Name and Title]	**Date**

How to fill out a SSP

How to fill out an Organizational Specific SSP Example

AU-4 AUDIT LOG STORAGE CAPACITY

Control: Allocate audit log storage capacity to accommodate the retention requirements identified in the Enterprise Architecture Standard: Enterprise Technical Architecture: Event Log Management.

When answering this control, the scope should be from the Organization perspective. How does the organization allocate audit log storage capacity? It is important to have an organization allocate sufficient audit storage to reduce the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability

Control Enhancements:

(1)AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Transfer audit logs at least once every 30-days to a different system, system component, or media other than the system or system component conducting the logging.

The scope for this control enhancement should identify the defined process the organization has in place to off load audit records every 30 days. This is opposite of if the system has the ability to do so, but rather is there a process in place to ensure it gets done, by whom, at what interval, and etc.

Tips for Organizational control responses

Scope

Respond to the control from the organization as a whole

Policy

What policies does the organization have in place outlining the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Also, that is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

Procedure

Procedures that can be established for security programs or business processes, that can be directed to the individual or role

Implementation

Think of how the control is implemented by the organization (i.e., by an individual through nontechnical means)

How to fill out a System Specific SSP

AC-12 SESSION TERMINATION

Control: Automatically terminate a user session after 24 hours of inactivity.

When responding to this control, the scope should be from the system perspective. Does the system have the capability to terminate a user sessions after 24 hours of inactivity? The system must show it is configured in a manner that ends all processes automatically that are associated with a user's logical session at the defined time frame as shown in the standard.

Control Enhancements:

(1) SESSION TERMINATION | USER-INITIATED LOGOUTS

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources.

Does the system have a logout capability for users? 24 hours would be the maximum threshold a session on the system is configured for. There should be an option to log out before then. The response should show the system has that capability.

(2) SESSION TERMINATION | TERMINATION MESSAGE

Display an explicit logout message to users indicating the termination of authenticated communications sessions.

Does the system have the capability to display a logout messages for web access after authenticated sessions have been terminated. This is separate from the organizational scope that has policies outlining the message contents, but rather the technical configurations within the system.

Tips for System Specific control responses

Scope

Respond to the control from the system level- Does the system have the ability to execute the task outlined

Procedure

Is there a team in place that can monitor the system to ensure that functions are working as intended

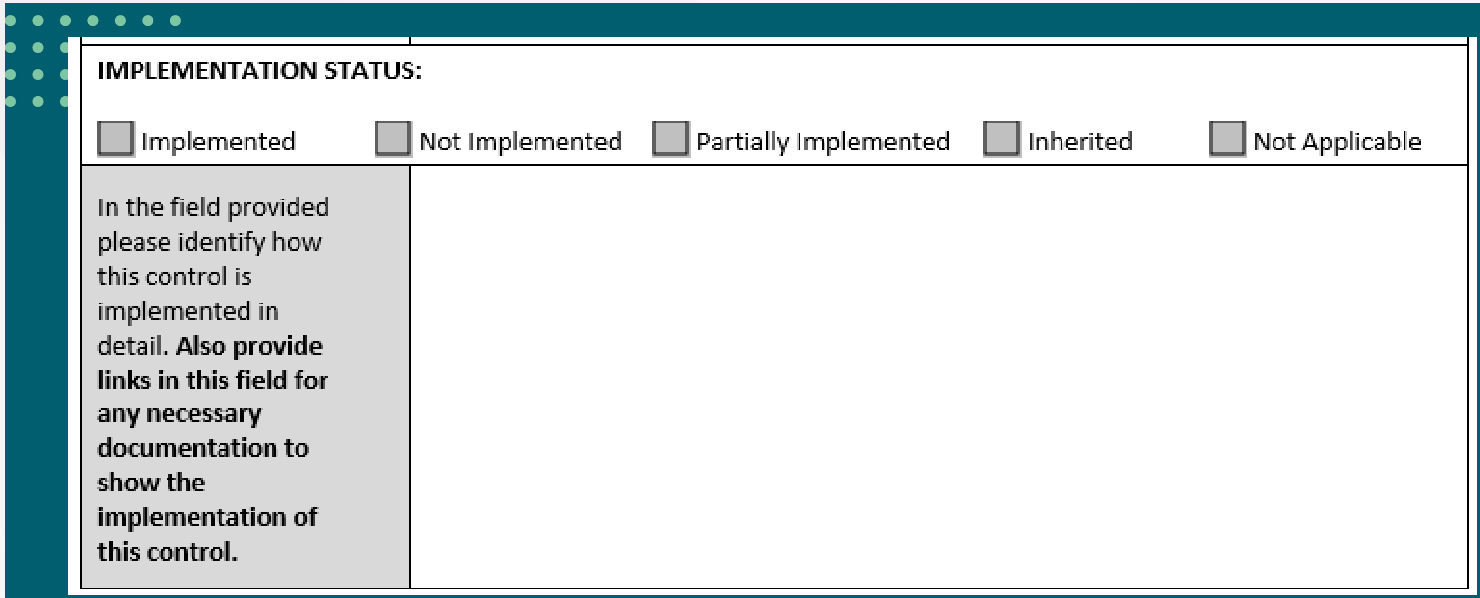
Execute

Does the system automatically handle the function or can be configured in a way to meet the control limiting the risk

Implementation

Think of how the control is implemented by an information system through technical means

Implementation Status



IMPLEMENTATION STATUS:

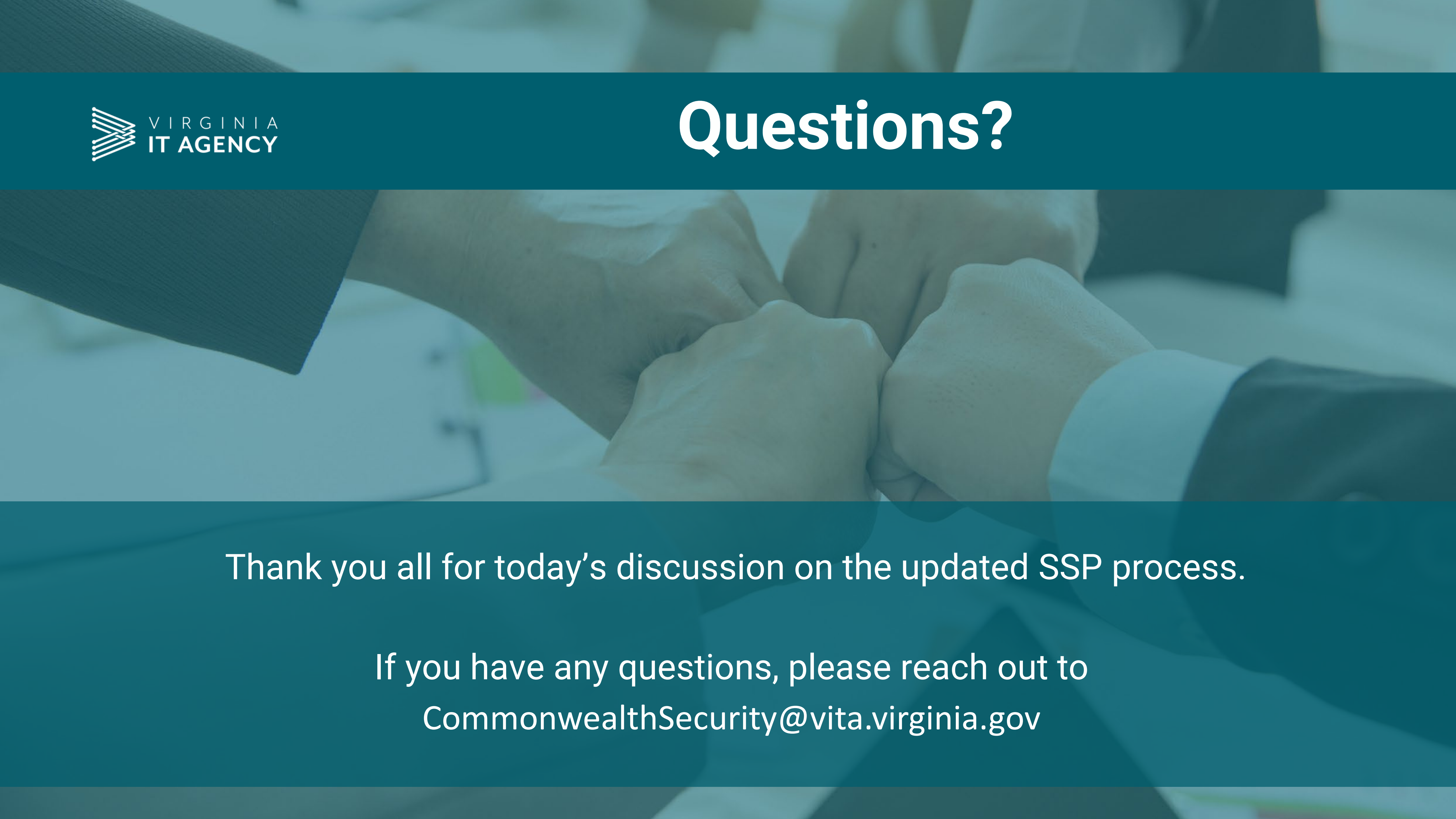
□ Implemented □ Not Implemented □ Partially Implemented □ Inherited □ Not Applicable

In the field provided please identify how this control is implemented in detail. **Also provide links in this field for any necessary documentation to show the implementation of this control.**	

Regardless of what template is used, the implementation status must be checked. There can only be one status, so it is important to understand their meanings:

- **Implemented:** The organization or system meets the control and is responded to
- **Not implemented:** The organization or system does not meet the control. This would result in a risk finding tracked via a POAM
- **Partially implemented:** The organization or system has some part of the control met but other areas have a planned future date. This would also need to be added to a POAM
- **Inherited**- The organization or system meets this control from another service supplier and here is how. Note: A system specific SSP would rarely use this status since the control has to be answered from that specific systems perspective and utilizing a feature from a different system (e.g. SSO from OKTA) is not considered inherited.
- **N/A-** The organization or system has effectively shown how the control is not appliable to their environment

Questions?



Thank you all for today’s discussion on the updated SSP process.

If you have any questions, please reach out to
CommonwealthSecurity@vita.virginia.gov

COV Tabletop Exercise 2024

Zachary D. Wilton
SAIC MSI Security Incident Response

Redefining Ingenuity

Agenda

- Overview
- Objectives
- Expected Outcomes
- Event Information

Overview

The COV Annual 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.

Objectives

- The main objective for this exercise is to uncover strengths within the COV IR process:
  - Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic 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
  - Provide recommendations for corrective action to VITA-CSRM

Expected Outcomes

- Expected outcome from this event is to 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
  - Ensure COV information systems will successfully operate in support of the exercise scenario
  - Enhance awareness, readiness and coordination
  - Test capability to determine operational impacts of a cyberattack
  - Test participant’s exercise playbooks, incident analysis, incident response plans and procedures, and incident reporting
  - Demonstrate compliance with MSI Security Incident Management Process SMM 4.1.5.7 and VITA Playbooks
  - Identify Enterprise-wide opportunities for improvement
  - Further integration of multi sourcing program between MSI, VITA-CSRM, Service Towers, and the Agencies

Event Information

- When:
  - Exercise is TBD (Targeting sometime in mid/late August)
  - Hotwash is TBD
- Who:
  - Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
  - Participants include representatives from each agency and service tower (Last year had over 50)
- Where:
  - Virtual only event - A link will be provided at a later date!

Event Information

- How to join:
  - You are always welcome to send an email to MSI-Security-Operations@saic.com stating that your agency/tower would like to participate in this year's event!
  - A weekly email will be sent to all ISO's requesting a response to sign-up, if your agency/tower has not done so already.
    - If you have replied to the invitation, you will stop receiving the weekly emails!
  - The full meeting invite for the event will be sent out closer to the event time, once we gather participation
  - RSVP Cut-off: TBD

Please direct all questions about the exercise to MSI-Security-Operations@saic.com

Announcements

ISOAG May 1, 2024

FYSA

Staff Changes

- Todd Kissam has retired from his role of Enterprise and Security Architecture Director. We wish him a very happy retirement!
- Stephen Smith will step forward as the acting Enterprise and Security Architecture Director!
- We have a new CSRM Governance Analyst. We are so pleased to have Amira Yagoub joining Governance.

GovTec’s National “Top 25 Doers, Dreamers and Drivers”

Michael Watson has been named one of Government Technology's Top 25 Doers, Dreamers, and Drivers for 2024.

Mike has been recognized for his work as Virginia CISO for the past 12 years, Mike has experienced and led programmatic growth, industry changes and incredible work to keep Virginia's information and IT systems secure.

[Top 25 Doers, Dreamers & Drivers (govtech.com)]

KnowBe4 Fresh New Content

KnowBe4 has added 33 new pieces of training content in April.

1. Handling Sensitive Information with Care in the U.S.
2. Cyber World Cup Data Privacy Game
3. IT Security in the Workplace 2024
4. The Inside Man New Recruits Game

More information can be found by clicking the link below:

[Your KnowBe4 Fresh Content Updates from April 2024]

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

The RVASec Conference is being held June 4-5, 2024

The Marriott Richmond: 500 East Broad Street, Richmond, VA 23219.

There will be a CTF event at the conference.

Register - RVAsec

- **The June ISOAG has been changed to June 12, 2024**

The Laws of Physics are irrefutable, one object can not be in two places at the same time..

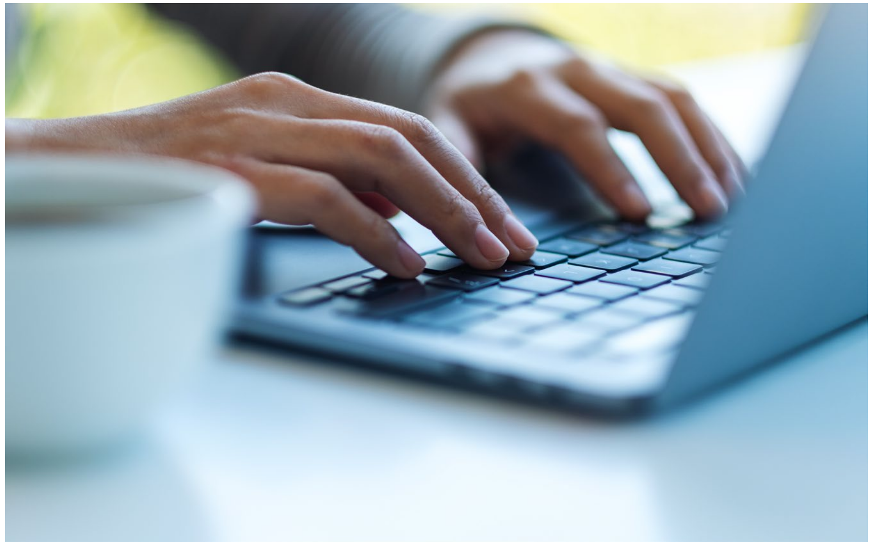
- As many both within VITA and at the various agencies will be attending the RVASec conference June 4-5, 2024. We are moving the ISOAG meeting to the following Wednesday! It will cover the same time frame from 1-3pm, and still be held via WebEx.

IS Orientation

The next IS Orientation is being held on June 26, 2024

- It will be held virtually via WebEx from 1pm-3pm
- Please register at the link below:

  https://covaconf.webex.com/weblink/register/r85904edc047089bb5c65f3261a80bd46



Commonwealth of Virginia Information Security Conference 2024

Join us for the COV IS Conference 2024

Titled: “The Art of Cyber War”

August 15, 2024, at the Hilton Richmond Hotel and Spa located at Short Pump:

12042 West Broad Street,
Richmond, VA 23233

Register at: https://www.vita.virginia.gov/information-security/security-conference/

MEETING ADJOURNED

VIRGINIA
IT AGENCY