



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

June 4, 2014



ISOAG June 2014 Agenda

- | | | |
|-------------|--------------------------------------|--|
| I. | Welcome & Opening Remarks | Mike Watson, VITA |
| II. | NIST Cyber Security Framework | Tom Tollerton & Ben Sady
Dixon Hughes Goodman LLP |
| III. | Cardinal Security | Julie Seitz, VDOT |
| IV. | 2014 Datapoint Requirements | Benny Ambler, VITA |
| V. | Upcoming Events | Mike Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |



discover. **develop.** **deliver.**

A Dixon Hughes Goodman Seminar

NIST CYBERSECURITY FRAMEWORK

A New Language for Cyber Risk

Ben Sady, CIA, CRISC, CISA
Director, Risk & IT Advisory Services
Dixon Hughes Goodman LLP

Tom Tollerton, CISSP, CISA, GCIH, QSA
Manager, IT Advisory Services
Dixon Hughes Goodman LLP

June 4, 2014

Presentation Agenda

- Introductions
- Presentation Objectives
- Framework Overview
- What Virginia Has Done
- “The Good and The Bad”
- How to Implement
- Q & A



Introductions

Ben Sady, CIA, CISA, CRISC

- Director, Risk & IT Advisory Services
- 10+ years experience:
 - IT Audit / Internal Audit
 - Compliance Reviews
 - Consulting



Introductions

Tom Tollerton, CISSP, CISA, GCIH

- Manager, IT Advisory Services
- 10+ years experience:
 - Cybersecurity Consulting
 - Network Assessments & Penetration Testing
 - IT Risk Management & Compliance
 - Digital Forensics & Incident Response



Presentation Objectives

- Understand the Framework
- Strengths and Pitfalls
- Road map for implementation



Framework Overview

- Presidential Executive Order 13636
 - Issued February 12, 2013
- Final revision of the Framework issued 1 year from date of EO



Framework Overview

“Provide a common language for understanding, managing, and expressing cybersecurity risk both internally and externally.”

“Identify and prioritize actions for reducing cyber security risk.”



Framework Overview

- Entirely Voluntary
- Critical Infrastructure Cyber Community (C3) Voluntary Program
 - Supporting Use
 - Outreach and Communications
 - Feedback



Framework Structure

- Three Major Components
 1. Core
 2. Tiers
 3. Profiles



Framework Structure



Core Framework

Five Functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover



Framework Structure



Identify

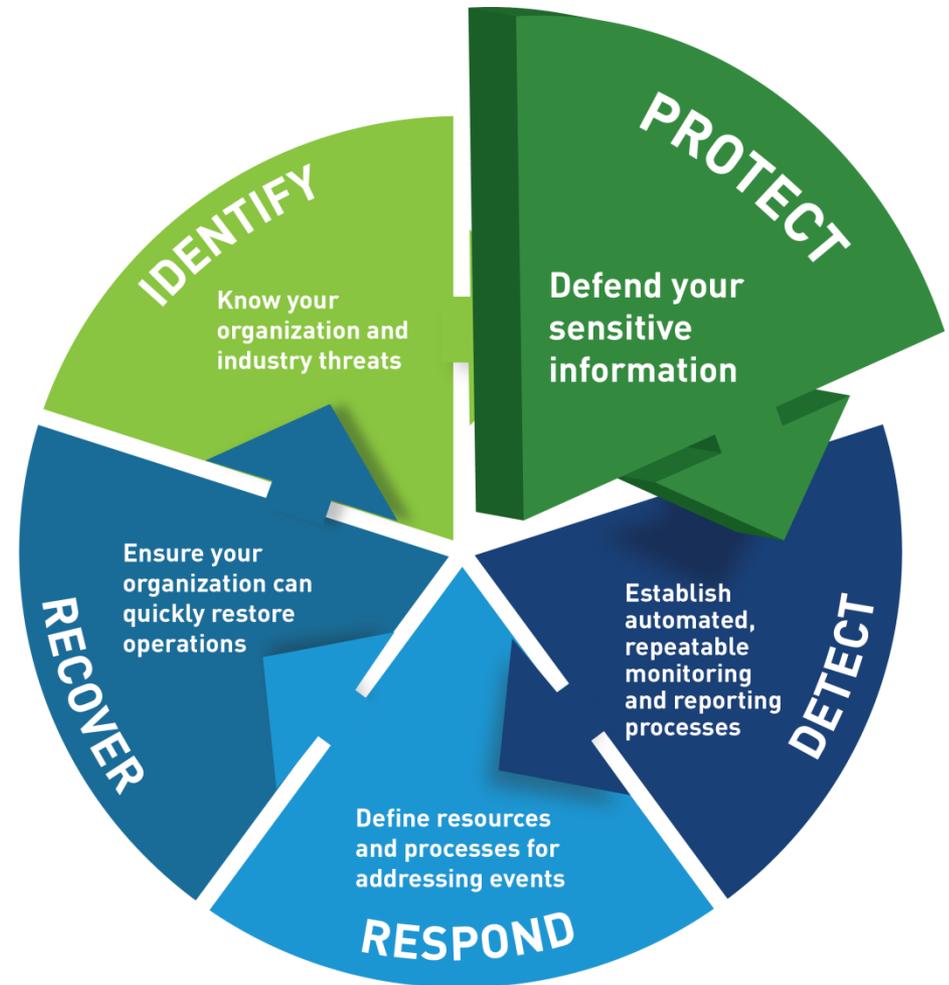
- Organizational Understanding of Cyber Risk & Business Context
- Strategic Focus & Prioritization
- Outcome Categories



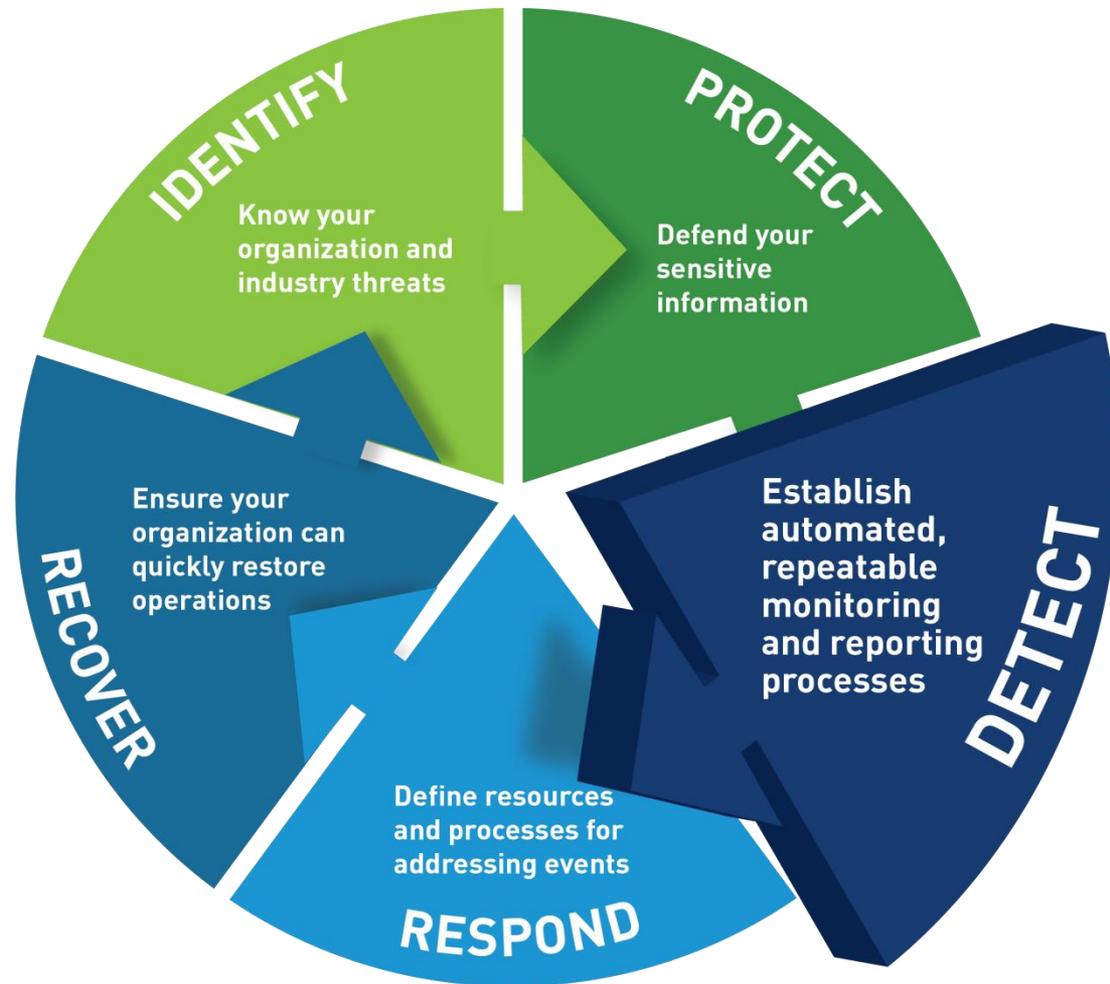
Framework Structure

Protect

- Develop & Implement Appropriate Safeguards
- Limit & Contain Impact of Cyber Events
- Outcome Categories: Physical, Technical, Administrative Security Controls



Framework Structure



Detect

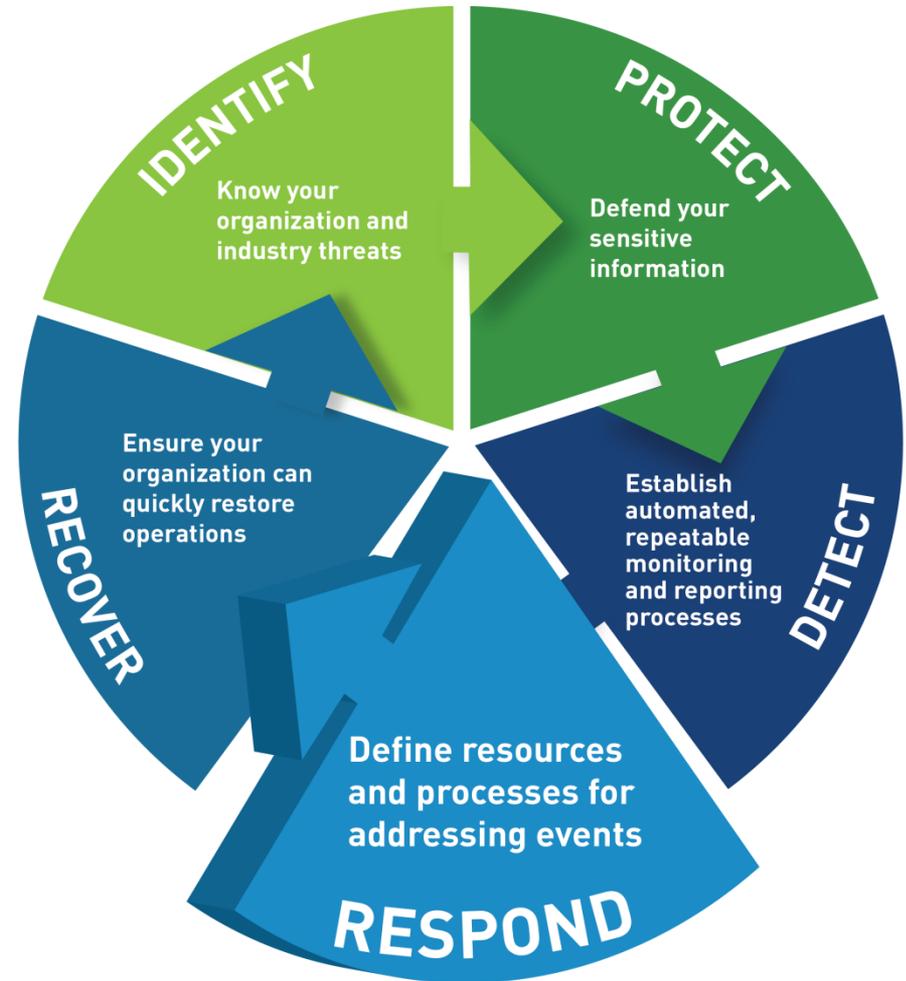
- Monitoring & Event Logging Functions
- Automated Systems Common
- Requires Customization to Limit False Positives



Framework Structure

Respond

- Strong Response Capabilities Contain Impact
- Clearly Defined Roles & Responsibilities
- Continuous Communications



Framework Structure



Recover

- Plans and Activities to Restore Business Services
- Determines an Organization's Resilience



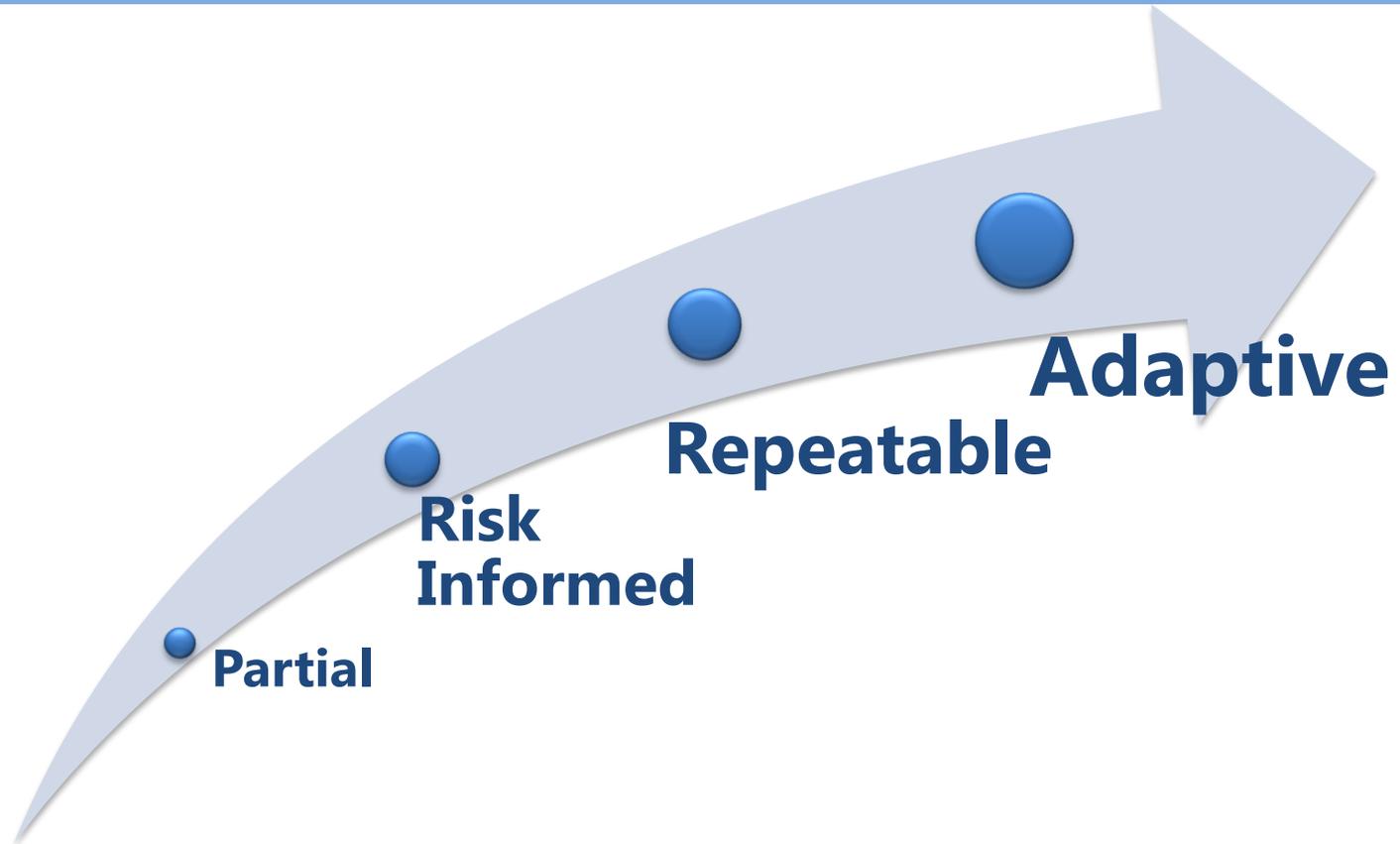
Framework Structure

Framework Core

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis



Framework Structure



Framework Tiers



Framework Structure

- Framework Profiles
 - Snapshot of current cyber security posture
 - No model for defining what a “Profile” looks like or how to develop it
 - Designed to allow implementation flexibility



Framework Structure

- A “Current Profile” is established by identifying where the organization sits with each control
- Then, a “Target Profile” is defined
- Gap assessment performed between the current and target profiles
 - Gaps are identified
 - Remediation efforts are prioritized



Framework Structure

- Unique Privacy and Civil Liberty Requirements
 - Each agency has an obligation to protect civil liberties
 - Considerations only arise when constituent personal information is collected
 - Do you understand how your agency collects, processes, maintains, or *DISCLOSES* personal information?



Framework Structure

- Unique Privacy and Civil Liberty Requirements
 - Governance
 - Identification and Authorization of Individuals with Access to Personal Information
 - Awareness & Training
 - Anomalous Activity Detection
 - Response Activities & Information Sharing Efforts



Virginia's Adoption

- Governor Terry McAuliffe announced immediate integration on Feb 12, 2014
- First annual Cyber Security Conference
- VITA has incorporated part of the Framework structure in to SEC520 - Risk Management Policy



Virginia's Adoption

- SEC520 does not address the maturity "Tiers" defined in the Framework
- Additional business requirements not in the Framework are included in SEC520
 - Business Impact Analysis
 - Vulnerability Scanning & Reporting
 - IDS Reporting



The Big Picture

- NIST Roadmap for Improving Critical Infrastructure Cybersecurity
 1. Introduction
 2. Evolution of the Cybersecurity Framework
 3. Strengthening Private Sector Involvement in Future Governance of the Framework
 4. Areas for Development, Alignment, and Collaboration
 - 4.1 Authentication
 - 4.2 Automated Indicator Sharing
 - 4.3 Conformity Assessment
 - 4.4 Cybersecurity Workforce
 - 4.5 Data Analytics
 - 4.6 Federal Agency Cybersecurity Alignment
 - 4.7 International Aspects, Impacts, and Alignment
 - 4.8 Supply Chain Risk Management
 - 4.9 Technical Privacy Standards



The Good and The Bad

- Let's start with the bad news first..
 - Too high level
 - Missing components
 - Confusion on the "Tier" concept
 - It's voluntary
 - A formal framework makes us weaker



The Good and The Bad

- Too high level
 - Framework itself is high level and the Framework Core is also tied to high level principles (COBIT, ISO/IEC, NIST 800-53)
 - Some missing mentions: system security hardening standards, employee acceptable use/misuse of computing resources, mobile device computing, patch management and user access administration



The Good and The Bad

- Too high level
 - Examples of high level controls
 - ID.GV-1: Organizational information security policy is established
 - PR.AT-1: All users are informed and trained
 - PR.PT-4: Communications and control networks are protected
 - PR.IP-3: Configuration change control processes are in place



The Good and The Bad

- Too high level
 - NEED to have a capable individual running your program, because judgment and interpretation are required.
 - Capable = relevant experience, certification, history of making sound decisions



The Good and The Bad

- Missing components
 - Does it move forward our lagging approaches to securing critical infrastructure?
 - Passwords are broken
 - Signature based protection can only do so much
 - Implement end point hardening practices / tech?
 - Implement data driven security – security based on data, analytics and employs real time prevention, detection, and remediation?



The Good and The Bad

- Missing components
 - Everything maps to COBIT, ISO, NIST, etc....

We're in a cyber war and nothing new was added. Are we going to be measurably safer? Or continue down a failing path?



The Good and The Bad

- Confusion on the “Tier” concept
 - It is not a maturity model.
 - Based on your Target Profile, you can be in Tier 1 and have successfully implemented.



The Good and The Bad

- It is Voluntary
 - No incentives to conform to the Framework.
 - Adding another compliance requirement is tedious and costly.
 - Organizations often lack the necessary resources to apply all of the outlined standards, guidelines, and practices.
 - Without executive commitment, could lead to uneven adoption across industries.



The Good and The Bad

- It is Voluntary
 - Will insurance companies incentivize?
 - Will industry organizations make it a requirement?
 - Will all state Governors do as Virginia has?



The Good and The Bad

- A formal framework makes us weaker
 - Adds another committee, set of meetings. JUST WHAT WE NEED.
 - If we focus only on conformance, we may lose sight of emerging threats. Need to stay creative, encourage R&D, and know that we won't stop everything with a framework.



The Good and The Bad

- Now, for the good...
 - Provides for a common language and model to manage cybersecurity risk.
 - Is flexible, not prescriptive (check the box).
 - Raises awareness to executive level.
 - Identifies that critical infrastructure is not a narrowly defined category.
 - Encourages information sharing to achieve a broader cybersecurity goal.



The Good and The Bad

- Provides for a common language and model to manage cybersecurity risk
 - You can discuss cybersecurity risk and response with other organizations and governmental entities and you'll be talking the same language



The Good and The Bad

- Is flexible, not prescriptive (check the box)
 - One size does not fit all, especially given 16 industries are considered Critical Infrastructure.
 - Each industry has the ability to map their standards and controls to the framework... that is powerful.



The Good and The Bad

- Raises awareness to the Executive level
 - Press and commentary has been impactful
 - Boards should be asking executives about this
 - Executives should be asking management and security leadership



The Good and The Bad

- Raises awareness to the Executive level
 - What is our biggest cyber risk and how are we addressing it?
 - Do we have a plan and policy in place?
 - What is our plan to implement and close any gaps?
 - What tier are we currently at? Are there plans to move up to a higher tier?



The Good and The Bad

- Identifies that critical infrastructure is not a narrowly defined category
 1. Chemical
 2. Commercial Facilities
 3. Communication
 4. Critical Manufacturing
 5. Dams
 6. Defense Industrial Base
 7. Emergency Services
 8. Energy
 9. Financial Services
 10. Food and Agriculture
 11. Government Facilities
 12. Healthcare and Public Health
 13. Information Technology
 14. Nuclear Reactor, Materials and Waste
 15. Transportation Systems
 16. Water and Wastewater Systems



The Good and The Bad

- Encourages information sharing to achieve a broader cybersecurity goal
 - As a community and nation, we need to do a better job of sharing information up, down, and sideways
 - RS.CO-4: Coordination with stakeholders occurs consistent with response plans
 - RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness



How to Implement

- Ok, we know everything now. Let's implement this thing...
 - Section 3 of the Framework outlines how to use the framework.
 - Let's go over an example.
 - What else should we do?



How to Implement

Section 3
Outlines How to
Use the
Framework



How to Implement

- Step 1: Prioritize and Scope

Use existing documentation to identify scope:

- Strategic plan
- Business Impact Analysis (BIA)
- System Inventory and Definition Worksheet
 - Identify Sensitive Systems

- Example: Dept XYZ has 4 sensitive systems that support MEFs.



How to Implement

- Step 2: Orient

Use existing documentation to identify threats to, and vulnerabilities of, those systems and assets:

- Risk Assessment

- Example: Complete the Risk Assessment template for the in scope systems.



How to Implement

- **Step 3: Create a Current Profile**

Develop a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.
- **Example: Add a column to the Framework Core spreadsheet to indicate the Categories and Subcategories that are currently achieved.**



How to Implement

- **Step 4: Conduct a Risk Assessment**

Analyze the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

- **Example: Use same Risk Assessment performed at Step 2.**



How to Implement

- **Step 5: Create a Target Profile**
 - Identify the Categories and Subcategories desired to be achieved. Organization is allowed to develop their own additional Categories and Subcategories to account for unique organizational risks.
- **Example: Update Framework Core spreadsheet to indicate the Categories and Subcategories that are desired.**



How to Implement

- Step 6: Determine, Analyze, and Prioritize Gaps
 - Create a prioritized action plan to address the gaps between the Current Profile and the Target Profile.
 - Determine resources necessary to address the gaps (i.e., people, time, money, technology).
- Example: Create action plan.



How to Implement

- Step 7: Implement Action Plan
 - Determine which actions to take in regards to the gaps.
- Example: Take steps to complete action plan, monitor progress, report status appropriately.



How to Implement

- COV Modified Steps
 - Prioritize and Scope
 - Orient and Conduct a Risk Assessment
 - Create Current Profile and Target Profile
 - Implement Action Plan to Address Gaps



How to Implement

- What else should we do?
 - Conformity assessment to NIST framework
 - Identify ownership of cyber risk
 - Regular communication with Executives and the BOD
 - Share information across organizations
 - Metrics and benchmarking
 - Big data analytics
 - Two factor authentication solutions
 - Don't rely on signature based solutions
 - Vendor management
 - Continue to build a cybersecurity workforce
 - Continue to build security awareness



Questions?



Contact Information

Ben Sady

- Ben.Sady@dhgllp.com
- 804.474.1267

Tom Tollerton

- Tom.Tollerton@dhgllp.com
- 704.367.7061

www.dhgllp.com

@dhg_cyber



DIXON HUGHES GOODMAN LLP



56

Links

- NIST Cybersecurity Framework
<http://www.nist.gov/cyberframework/>
- Presidential Policy Directive 21 (PPD-21)
http://www.gsa.gov/portal/mediaId/176571/fileName/ATTCH_2_-_PPD-21.action





Cardinal Security Overview

June 2014



Cardinal Project Vision & Benefits

By replacing CARS with Cardinal, the Commonwealth will be able to take advantage of proven enterprise resource planning (ERP) software (PeopleSoft).

- Reduce risks associated with our aging financial systems
- Provide standard, proven government business processes
- Meet the majority of Commonwealth financial management business requirements
- Allow for configuration and limited software customizations to meet critical business requirements
- Provide an enterprise (i.e., statewide) focus
- Leverage vendor supplied upgrades to commercial-off-the-shelf (COTS) software for functional and technical improvements
- Provide robust reporting tools and capabilities
- Provide flexible Chart of Accounts structure that will facilitate consistent financial reporting across agencies



Cardinal Project Parts

- ✓ Part 1: Replacement and rollout of a new financial management system at VDOT
 - Functional areas in scope included General Ledger, Accounts Payable, Accounts Receivable/Billing, Project Accounting, Purchasing, and Time and Attendance (and Labor Distribution)
 - A new Commonwealth Chart of Accounts structure was established for use by all state agencies

- ✓ Part 2: Establishment of the “Base” Financial System at DOA
 - Functional areas in scope include General Ledger, Accounts Payable, and Accounts Receivable-Funds Receipts

- Part 3: Statewide Rollout of “Base” Financial System and Replacement of CARS (Statewide Rollout)
 - Functional areas in scope include General Ledger, Accounts Payable, and Accounts Receivable-Funds Receipts



Part 3 Scope

- All state agencies currently using CARS will use Cardinal
- Agencies will use Cardinal similarly to how they use CARS
 - CARS online agencies will be Cardinal online agencies
 - Agencies with their own financial management systems that currently interface those systems with CARS will be Cardinal interfacing agencies
- At the end of Part 3, CARS will be retired and Cardinal will become the Commonwealth's new financial management system of record



Part 3 Statewide Rollout Strategy

- Cardinal will be deployed to the remaining state agencies in two “waves.” A wave is a full deployment cycle (e.g., Design, Build, Test) with its own go-live date. All agencies have been assigned to transition to Cardinal with either Wave 1 or Wave 2.
 - **Wave 1:** The system will be rolled out to agencies that primarily process transactions online. This wave will also serve as a pilot for interfacing agencies by rolling the system out to a small subset of these agencies. Go-live for Wave 1 projected for October 1, 2014.
 - **Wave 2:** The system will be rolled out to the remaining agencies. This will include the majority of the interfacing agencies that process some or all transaction types via a direct system interface. In addition, this wave may also include some online agencies that are logically grouped with an interfacing agency because of their joint fiscal operations relationship. Go-live for Wave 2 projected for February 1, 2016.



Access and Authentication

Cardinal is NOT public facing via internet. Users are required to be authenticated prior to accessing the system.

– COV (VITA/NG Partnership supported) Agencies

- All agency workstations connected to the Commonwealth's MPLS network will have direct HTTPS access to Cardinal's load balanced URL.
- Users will be authenticated in Cardinal with existing COV Active Directory (AD) credentials.
- Once authenticated to Cardinal, the access to different pages/data is dictated by roles assigned within PeopleSoft security

– Non-COV Agencies

- External users will have a two-step login process utilizing a clientless SSL VPN solution (Cisco SWAP) to access Cardinal.
- The Cisco SWAP (Secure Web Application Portal) will authenticate users with existing AUTH Active Directory (AD) credentials. These same credentials are then used to access Cardinal
- Once authenticated to Cardinal, the access to different pages/data is dictated by roles assigned within PeopleSoft security



CARS vs. Cardinal : Key Security Access Differences

CARS

- General user access is granted with three roles (i.e., View, Enter, Release) across all transaction types
- Users can either Enter transactions or Release them; they cannot do both
- Transactions are released (approved) at a batch level

Cardinal

- Access is granted in a “cafeteria style” by transaction types and business functions with up to 30 “base system” agency roles available to select
- Any given user may have the ability to enter transactions for one transaction type and approve for another transaction type (journal entries are an exception and controls must be handled through process/procedure)
- Approval is completed at the individual transaction level
- Users will have the ability to run reports and queries across all base system modules



How Security Works in Cardinal

**Cardinal /
PeopleSoft v9.1**

User

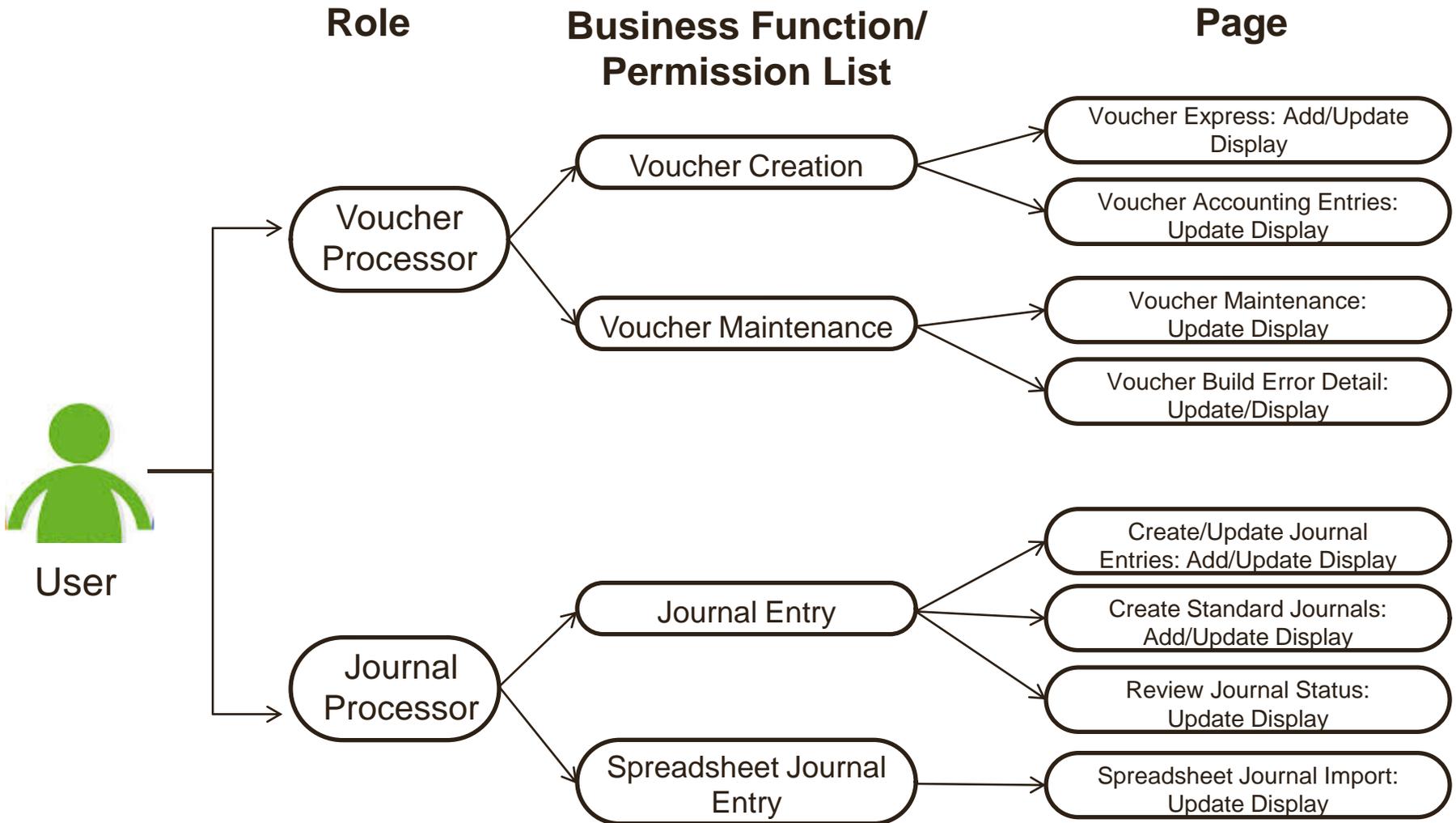
Role

Pages

- Cardinal security links users to roles
- Each user can be assigned multiple roles
- Each role determines what pages the user can access to view, edit, enter and/or approve transactions



Cardinal Security Profile Building Blocks





Row Level Security in Cardinal

- Below the page level, additional select security (row level) can be invoked to restrict access
- Each user in Cardinal is assigned a Row Level Security Permission List
- A user can only view, enter, or process transactions for Business Units included in their Row Level Security permission list
- An agency with controlling access or responsibility for other agencies may choose to grant all of its users access to the Business Units under their control, or restrict access to a smaller group of users
- Some reports may not be restricted by Business Unit



Cardinal Security – General User Roles

All users are given the Cardinal Reporter, Cardinal Viewer and Cardinal PeopleSoft User roles:

- **Cardinal Reporter**
 - Access to run non-sensitive reports

- **Cardinal Viewer**
 - View-only access to transaction pages
 - View-only access to vendor records (excluding TIN, banking information)

- **Cardinal PeopleSoft User**
 - Grants access to general PeopleSoft pages
 - Process Monitor, Report Manager, Report Books
 - Access to run public queries



Role Mapping

Role mapping is the process by which agencies assign specific roles to their Cardinal users. Cardinal roles define the end users' access, the functions they can perform in Cardinal, and the screens and data that are available when working in Cardinal, including:

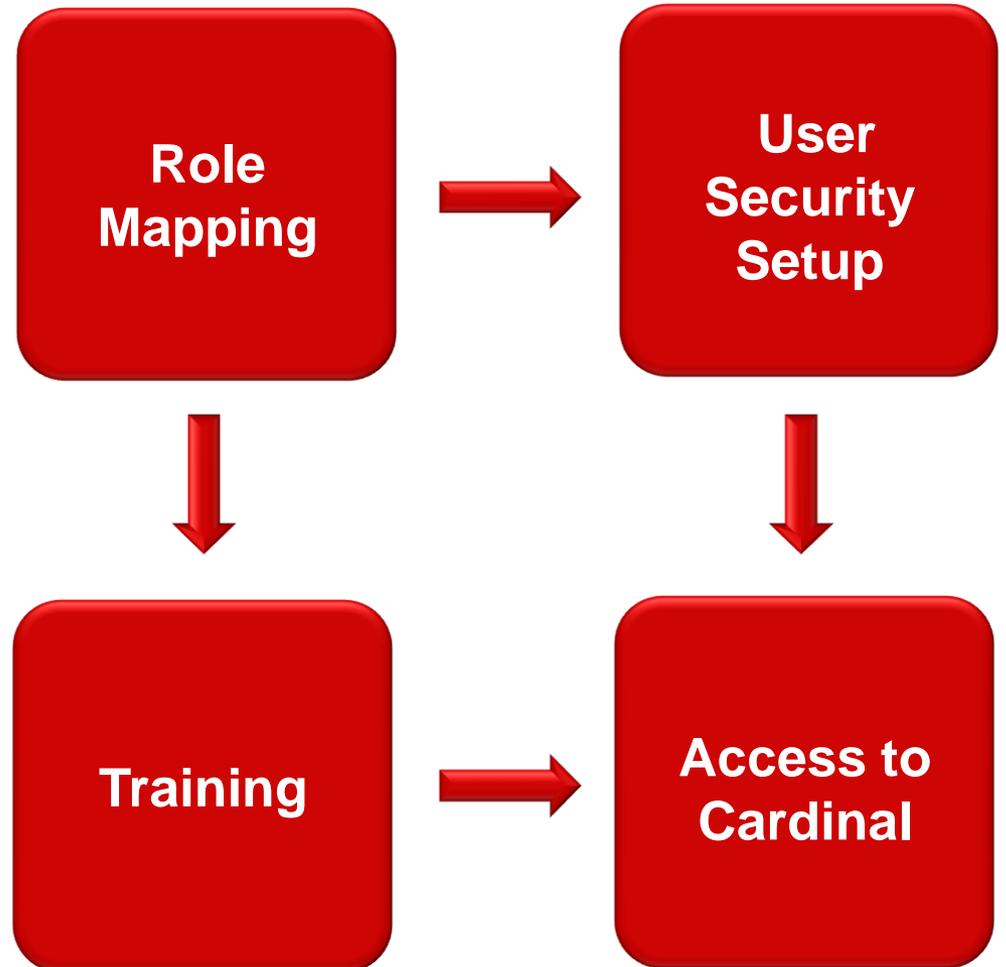
- View, enter and/or process transactions in Cardinal
- Approve transactions in Cardinal (e.g., journals, vouchers, expense reports)



Why Role Mapping Matters

Role mapping results will be used to:

- Configure security for all users
- Determine training courses each Cardinal user will need to complete
- Provide users access to Cardinal





Assigning Users to Cardinal Roles

Users need to be accurately mapped to Cardinal roles based on their responsibilities. Roles are assigned based on the users' responsibilities in Cardinal.

Cardinal roles are outlined by:

- Descriptive Role Name
- Role Description
- Separation of Duties
- Other Role Considerations

AP User Roles & Descriptions Table

Descriptive Role Name	Role Description	Separation of Duties	Other Role Considerations
Vendor Conversation Processor	This role is for users routinely involved in the Vendor Procure to Pay process who have a need to interact with vendors. This role has access to: <ul style="list-style-type: none">• Record Vendor Conversations	N/A	N/A
Voucher Processor	This role has access to: <ul style="list-style-type: none">• Enter and maintain vouchers• Review voucher accounting entries• Delete vouchers	Should not be given to a user with the Voucher Approver or Final Voucher Approver roles.	N/A



Interfacing Partners

- All Cardinal interface files will be collected and distributed via a centralized file management solution
 - Built around industry leading Ipswitch MOVEit DMZ and MOVEit Central software
 - Supports both SFTP and FTPS transfers
 - Interfacing agencies will be provided credentials to transfer files using these protocols
 - Data is fully encrypted while in flight and at rest



Cardinal User Account Maintenance

- User security accounts are maintained by Cardinal Post Production Support (PPS) team
- After the initial setup (handled through Role Mapping process), adds/updates to accounts are made by submitting Cardinal Security Forms to PPS
- Forms require signature of employee's supervisor and the applicable agency's designated Cardinal Security Coordinator
- Select roles (as designated in the Cardinal Security Handbook) may require additional approvals
- PPS Security will check requests against rules outlined in the Handbook and ensure guidelines are followed
- An annual Cardinal Security Review /Certification process will also be performed by each agency and Cardinal PPS



2014 DataPoint Requirements

Benny Ambler
Sr. Mgr. Information Security Governance



§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



Detailed Agency Information Security - 2014 Overall Security Program Scores

Agency	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	3 Year Audit Obligation	Business Impact Analysis Status	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	IDS Report Submitted
XYZ	Incomplete	Pass	50%	50%	Fail	Pass	75%	Yes

All ISOs must be appointed by their Agency Head. Once formally assigned , ISOs must complete the ISO education requirement by taking one of the two paths described below.

Steps to obtain COV ISO Certification for those who have a professional security certification:

- Possession of recognized professional IT Security Certification CISSP, CISM, CISA, SANS (others to be determined)
- VITA Training, Attend Information Security Orientation training
- ISO Academy, Successful completion of at least one course hour in the KC ISO Academy per year.
- ISOAG attendance, Attend the mandatory October 2014 ISOAG meeting.
- Maintain compliance with the continuing educational requirements of the professional IT security certification body.

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

- VITA Training, attend Information Security Orientation training.
- ISO Academy, successful completion of at least 3 course hours per year in the KC ISO Academy.
- ISOAG attendance, attend the mandatory October 2013 ISOAG meeting.

Continuing Education Requirements in 2014 for ISOs that have already obtained the ISO Certification:

- Agree to the Commonwealth IT Security Code of Ethics
- Attend any mandatory ISOAG meetings each year
- Attend IS Orientation once every 2 years
- Obtain 20 hours of continuing education credit



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	3 Year Audit Obligation	Business Impact Analysis Status	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	IDS Report Submitted
XYZ	Incomplete	Pass	50%	50%	Fail	Pass	75%	Yes

Audit Plan Status: The Agency Head has submitted an IT Security Audit Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016)

- Current - Plan is up to date and meets the criteria
- Expired - The IT Security Audit Plan on file does is not up to date and or does not meet the criteria
- Pending - Under review
- N / C - Non Compliant

Current Percentage of Audits Received: The percentage of Audit Reports received per the IT Security Audit Plan in the current year.

- Pending - Under review
- N/A - Not Applicable

3 Year Audit Obligation: This is the percent of sensitive systems audited within the last 3 years. The sensitive system list is validated against the Commonwealth Enterprise Technology Repository (CETR). For agencies required to submit to CETR, audits are not complete unless the sensitive system subject to the audit can be identified within CETR. This datapoint is based on the IT Security Audit Standard requirement: "At a minimum, databases 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."

- Pending CETR - Values cannot be calculated until the agency reconciles their audit plan system names with the CETR database.
- Pending Review - Under review



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	3 Year Audit Obligation	Business Impact Analysis Status	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	IDS Report Submitted
XYZ	Incomplete	Pass	50%	50%	Fail	Pass	75%	Yes

Business Impact Analysis Status: The Business Impact Analysis (BIA) has been provided by the agency. [To be considered complete all applications must follow the requirements of the IT Risk Management Standard \(SEC520-00, 3.2.2\)](#)

Pass – BIA is complete

Fail – BIA has not been submitted or is incomplete

Incomplete – Agency has submitted a BIA that is currently under review or required additional information.

BIA shall, at a minimum, identify:

- Business function name and owner
- Date BIA Completed and name of person that completed the BIA
- Primary objective of the business function
- Customers of the function (internal customers, Commonwealth Agency customers, government entity customers, public customers)
- Identify whether the functions are mission essential
- Identify IT systems that the business functions rely on
- Description of the data used by the function, including the source, destination, and sensitivity
- Identify the recovery time objective (RTO)
- Identify the recovery point objective
- Rate the impact of non-performance of the function for:
 - Confidentiality – Impact on customer service, public perception/trust, impact on sensitive data
 - Integrity – Impact on finance, legality, regulation, customer service, public perception/trust
 - Availability – Impact on life, safety, customer service, public perception/trust, finance, recovery time objective, recovery point objective



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	3 Year Audit Obligation	Business Impact Analysis Status	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	IDS Report Submitted
XYZ	Incomplete	Pass	50%	50%	Fail	Pass	75%	Yes

Risk Assessment Plan Status: The Agency Head has submitted an IT Risk Assessment Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016)

- Current - Plan is up to date and meets the criteria
- Expired - The IT risk assessment plan on file does is not up to date and or does not meet the criteria
- Pending - Under review
- N / C - Non Compliant

3 Year Risk Assessment Obligation: The percentage of Risk Assessment obligation met is calculated based on the percentage of sensitive systems that have had risk assessments conducted and submitted to Commonwealth Security and Risk Management within the last three years. The risk assessment date is assigned to each sensitive system and calculated as a percentage of total sensitive systems identified within the agency. For agencies required to submit to CETR, Risk assessments are not complete unless the sensitive system subject to the assessment can be identified within CETR. The Risk Assessment information reported must follow the requirements of the IT Risk Management Standard (SEC520-00, 3.3.3).

Pending CETR - Indicates the values cannot be calculated until the agency reconciles their audit plan system names with the CETR database.

IDS Reports Submitted – Agency has submitted the required quarterly IDS/IPS reports to Commonwealth Security

Please Note: A status of “Pending Agency CETR Reconciliation” will change to “Failed” as of December 16, 2014. Again, please note that the closing date for the 2013 Commonwealth of Virginia Information Security Annual Report is **December 31, 2014.**



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings, CSRM will record this action from the audit report received. No further action will be needed.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2014



Questions ???????

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!



Upcoming Events





CSRM & Hosted Mail Archiving (HMA)

on July 1, 2014 CSRM will begin using the Hosted Mail Archiving (HMA) service. As a reminder, please do not send unprotected sensitive data via email to CSRM staff or Commonwealth Security mailbox. Starting July 1st 2014, email will be permanently archived and cannot be deleted.

Sensitive data must be encrypted otherwise it will be unencrypted in this HMA service.

Email CommonwealthSecurity@vita.virginia.gov if you have any questions.



Future ISOAG

July 9 1:00 – 4:00 pm @ VDEM EOC
Keynote: Gary T. Lupton, CCP,CBCP,MBCI
Towne Insurance Company
Topic: Continuity Planning

ISOAG meets the 1st Wednesday of each month in 2014



Future ISOAG

July 9 **1:00 – 4:00 pm @ VDEM EOC**

Keynote: Adam Crowe

VCU Emergency Coordinator

**Topic: Social Media in Emergency
Management**

ISOAG meets the 1st Wednesday of each month in 2014



IS Orientation

When: Thursday, September 4, 2014

Time: 9:00 am to 11:00 am

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>

Next IS Orientation will be held on December 4, 2014



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov