



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

April 2, 2014



# ISOAG April 2014 Agenda

- |  |   |
|--|---|
| <b>I. Welcome &amp; Opening Remarks</b>                                  | <b>Mike Watson, VITA</b>                        |
| <b>II. Changing Lens of Info Protection</b>                              | <b>Brian Geffert, KPMG LLP</b>                  |
| <b>III. SEC520 – Getting to Know the<br/>IT Risk Management Standard</b> | <b>Jonathan Smith, VITA</b>                     |
| <b>IV. ISO Manual</b>  | <b>Bob Auton, VITA</b>                          |
| <b>V. Archer GRC in the COV</b>  | <b>Benny Ambler, VITA</b>                       |
| <b>VI. Upcoming Events</b>   | <b>Mike Watson, VITA</b>                        |
| <b>VII. Partnership Update</b>   | <b>Bob Baskette, VITA<br/>Michael Clark, NG</b> |



*cutting through complexity*

# Changing Lens of Information Protection

***Brian Geffert***

*Principal, Information Protection  
and Business Resiliency*

April 2, 2014





Virginia Department of Motor Vehicles

## Renew Your DRIVER'S LICENSE Today

It's time to renew your DRIVER'S LICENSE. Your DRIVER'S LICENSE will expire on Tuesday, June 3, 2014.

Save \$5 and renew your DRIVER'S LICENSE at [www.dmvNOW.com/online](http://www.dmvNOW.com/online). Renew at least 15 days before it expires.

Whether you renew online or in person, you will receive a temporary driving permit to carry with your old license. You will also receive a temporary permit issued in DMV customer service centers. If your license was suspended, revoked or cancelled after this notice was generated, you must see [www.dmvNOW.com/eligibility](http://www.dmvNOW.com/eligibility).

Renew by Tuesday, June 3, 2014. After expiration Virginia law requires you to visit your local DMV office and present proof of acceptable documents or information on obtaining your DRIVER'S LICENSE, visit [www.dmvNOW.com/documents](http://www.dmvNOW.com/documents).

To [opt out](#) of receiving e-notices, update your myDMV Account.

You have received this notification because you have signed up for DMV notifications or updated your DMV contact information.

This is an automated notice. Please do not reply. For more information, read the [FAQs](#) or [contact us](#).

# Shifting Focus – It's All About the Data!

## Traditional View



- Technology = Tool
- Typically, data internal use only
- Security = perimeter network & infrastructure focus



## Current View



- Technology = Business Enabler
- Data used internally and with business partners/third parties
- Security = Data focus

**Moving beyond the traditional view of security at the perimeter level toward a more strategic focus on protection at the data level**

# The New View of Information Protection

Due to increasing pressure to significantly reduce costs and improve performance, to adhere to increasing regulations, and to respond to rapidly changing needs, information protection is on the cusp of an evolutionary era that has the potential to redefine the culture, strategy, and function of IT within an organization.

The quality and integrity of information is vital to an organization's success. If the information is lost or stolen, or its integrity is compromised in any way, the damage to the organization's reputation and revenue stream could be irreparable.

Information protection is moving beyond the traditional view of security at the perimeter level—where barriers, such as firewalls and antivirus software, aim to surround and protect the network—toward a more strategic focus on protection at the data level.

# Mobile Devices Growing and Clouds are Forming!

Number of different devices, functionality and access brings new opportunities to connect with citizens for them access data



Risk of data compromises, protection of citizen information, and secure access to programs

**With new opportunities = new, but manageable risks!**

# Technology as an Enabler

Organizations need to enable programs with technology that improves operational functionality and data availability and optimizes performance while safeguarding the information and reducing costs.

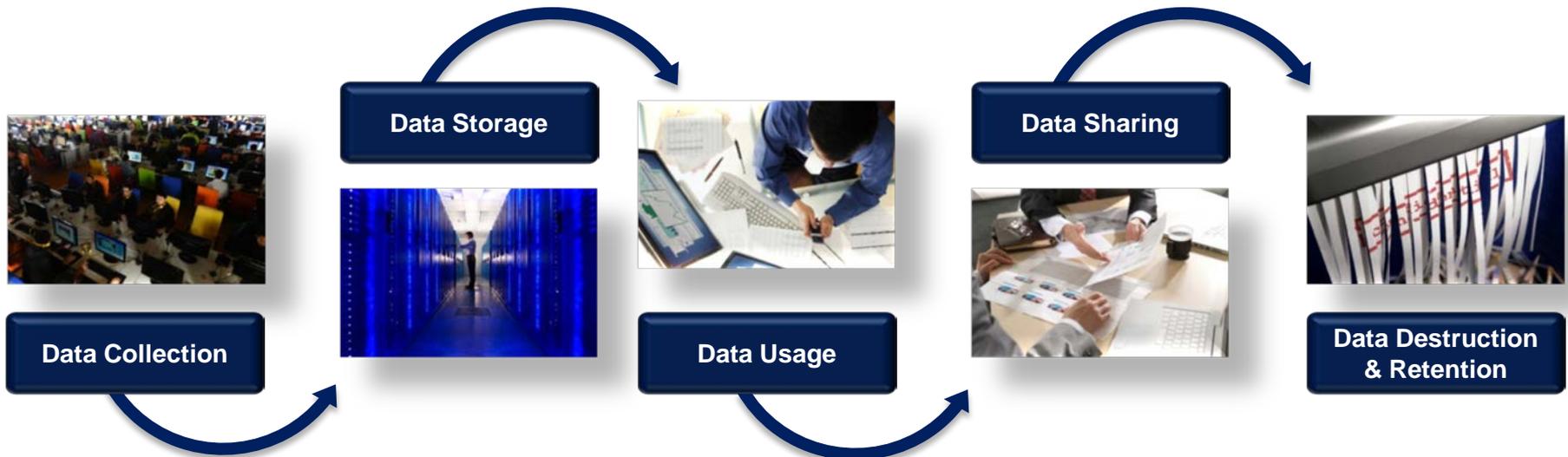
An information security strategy must support strategic goals and be as dynamic as the needs it to be, while adequately protecting the information.

The future-forward focus relies on more of an information-centric security model, in which users do not need to access data, rather the data reaches the user.

Today's security organization should abandon the worst-case scenario approach that led to an inflexible architecture and should adopt a risk-appropriate scenario approach that provides for exceptions and contingency plans. (e.g., Information sharing or aggregation)

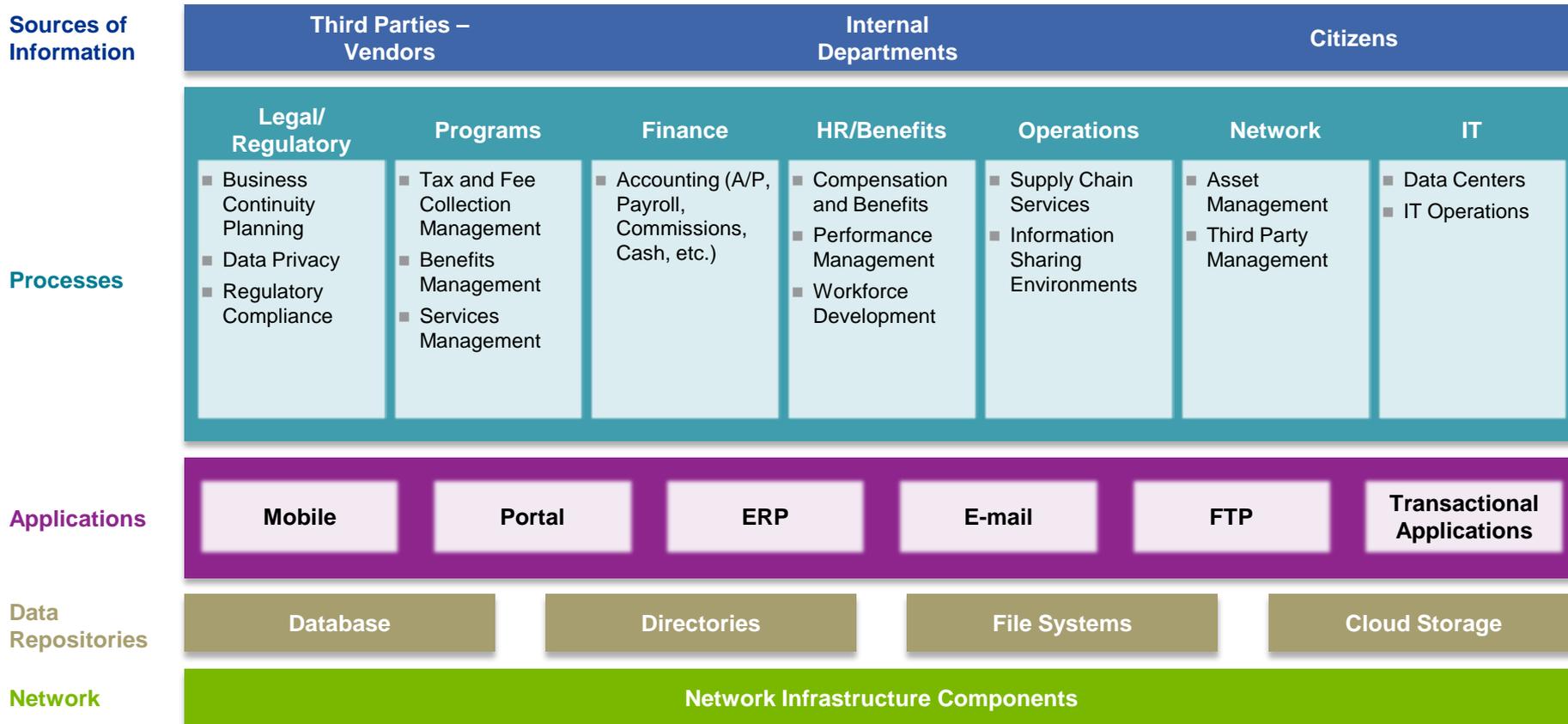
# Following the Data has Become Key Risk Mitigation Approach

Organizations transmit “Sensitive Data” through disparate forms of data transfer with multiple stakeholders using the data for different purposes.



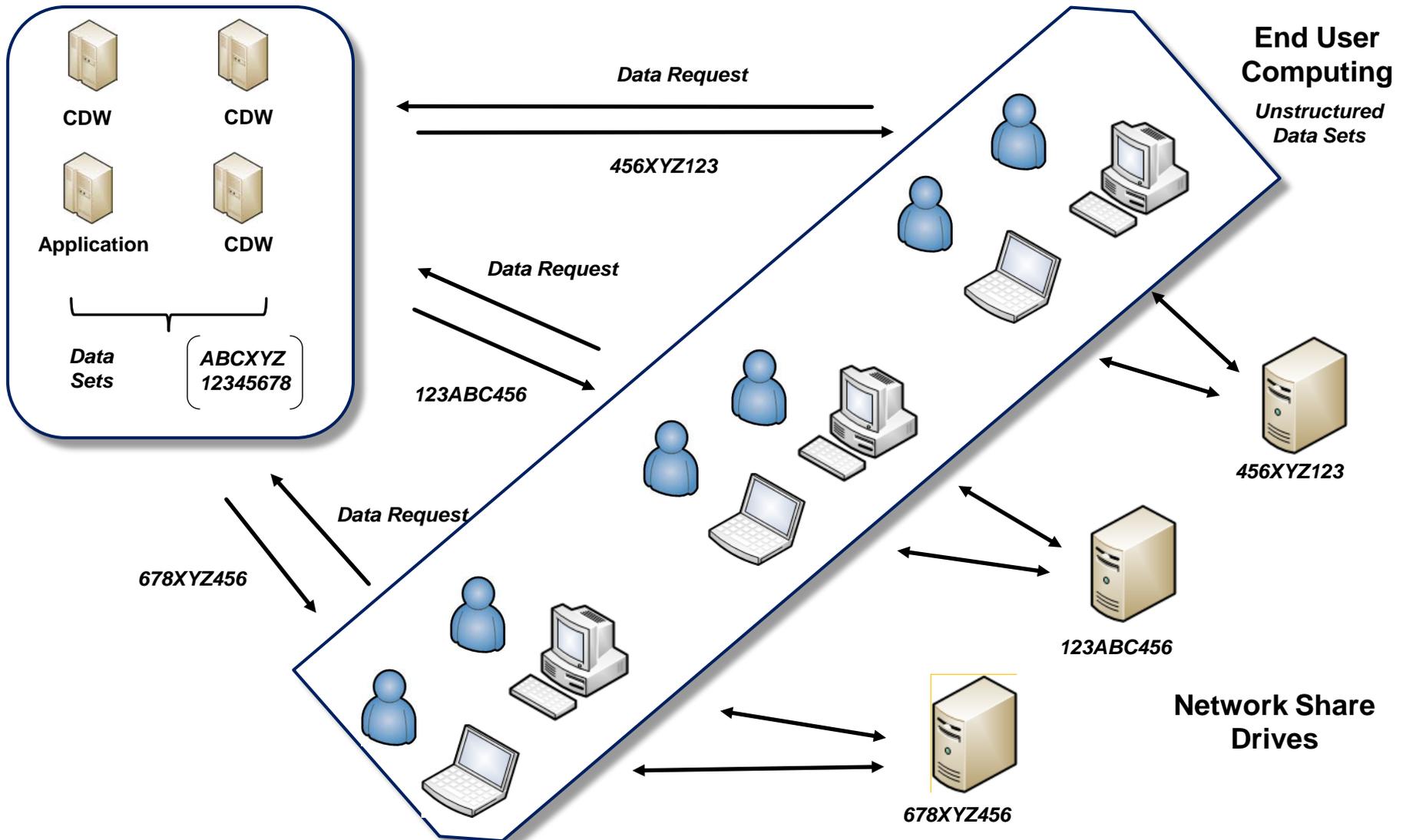
**Organizations need to understand where sensitive data is being handled by the organization throughout the data lifecycle including both process and IT related controls/safeguards which requires a joint effort with programs and IT.**

# Where is the Data Being Stored?



Understanding the key data stores for “Sensitive Data” becomes the other key component in the risk based data security equation to help uncover areas of “Shadow IT”

# Addressing the Challenge End User Computing

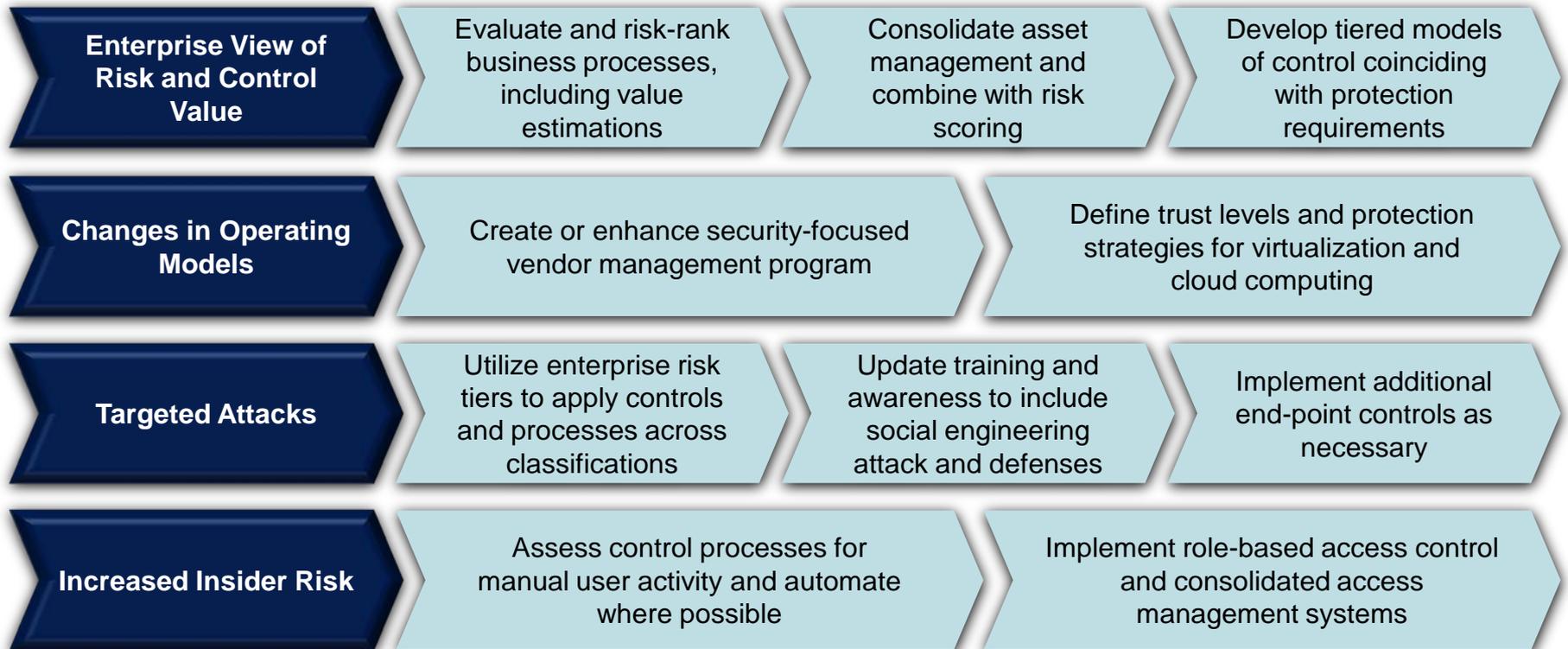


# Taking Key Data Risk into Consideration

Key risks	Significance to organization
<b>Outsourcing to Third Parties</b>	Organizations continue to outsource business processes, including associated customer data, to third parties and many organizations struggle to appropriately include third parties in their information security and privacy assessments
<b>Compliance</b>	The multitude of privacy and security regulations that must be complied with can be daunting to even the most mature organization
<b>Securing at the “Speed of Thought”</b>	Organizations are continuously offering new services, and securing the supporting data must be done in lock-step
<b>Lack of Information Governance and Ownership</b>	Several business units may be utilizing shared data stores, and the lack of a formal ownership structure may lead to the unintended leakage of sensitive data
<b>Resilience &amp; Integrity</b>	Information moves throughout the organization sometimes outside the infrastructure created to maintain the data integrity
<b>Availability</b>	Organizations need to balance the demand for data availability on multiple platforms (e.g., mobile devices, cloud) against the organization’s capabilities to secure and protect the data within the particular environment

# Leading Practices in Information Protection

As government undergo sweeping changes, new control models and risk management mechanisms will be required to preserve and create value through strong information protection models, right-sized to fit emerging processes.





*cutting through complexity*

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.



# SEC 520 - Getting to know the IT Risk Management Standard

**Jonathan Smith**  
Sr. Risk Manager



## Authority

*Code of Virginia, §2.2-2009*

*(Additional Powers of the CIO relating to security): ...*

*H. the CIO shall also develop policies, procedures, and standards that shall address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO. Such cooperation includes, but is not limited to, (I) providing the CIO with information required to create and implement a Commonwealth risk management program; (ii) creating an agency risk management program; and (iii) complying with all other risk management activities.*



## Introduction

- The intent of this *Information Risk Management Standard* is to establish a risk management framework, setting a baseline for information risk management activities for agencies across the Commonwealth of Virginia (COV).
- These risk management activities will provide identification of sensitive system risks, their associated business impact, and a remediation/recommendation strategy that will help mitigate risks to agency information systems and data.



# Risk Management Program

## Contents:

- Risk Management Framework
- Business Impact Analysis (BIA)
- Sensitive System Inventory and Definition
- Risk Assessment (RA)
- Vulnerability Scanning
- Intrusion Detection System (IDS) Reporting



# Risk Management Framework

- Feb 12, 2014 – Governor McAuliffe announced that Virginia adopted the National Cybersecurity Framework
- Risk Management Framework aligns with NIST Framework for Improving Critical Infrastructure Cybersecurity (aka Cybersecurity Framework)



# Risk Management Framework

Risk Management Framework provides a common method to:

- Describe current risk management posture;
- Describe target risk management state;
- Identify and prioritize opportunities for improvement within information security and risk management programs;
- Assess progress toward the target risk state;
- Report risk management postures and activities.



## Framework Core

The Risk Management Framework Core consists of four elements:

- Functions
- Categories
- Subcategories
- Informative References



## Framework Core - Functions

The Risk Management Framework Core utilizes a methodology in which risk management activities comprise of five primary functions:

- Identify – Understand your organizations IT environment and the business functions supported
- Protect – Implement safeguards
- Detect – Identify information security events
- Respond – Take action regarding detected security events
- Recover – Restoration of services impaired by a security event



## Framework Core - Categories

- Categories are subdivisions of the five primary functions
- Similar to SEC 501/NIST 800-53 Control Families
- Categories may apply to more than one function

### Function

Identify

Protect

Detect

Respond

Recover

### Example Categories

Asset Management, Risk Assessment

Access Control, Awareness and Training

Detection Processes, Security Monitoring

Response Planning, Communications

Recovery Planning, Communications



## Framework Core - Subcategories

- Subcategories consist of high level goals
- Subcategories are subdivisions of categories
- Similar to SEC 501/NIST 800-53 controls

### Category

Asset Management

Access Control

### Subcategory

Physical devices and systems within the organization are inventoried

Identities and credentials are managed for authorized devices and users



## Informative References

- Specific controls or sections from standards, guidelines, and procedures
- References may include controls from numerous sources, such as:
  - SEC 501
  - NIST 800-53
  - Top 20 Critical Controls
  - COBIT
- COV risk management framework core is focused initially on the Top 20 Critical Controls



## Risk Maturity

- Measurement of current risk management program in relation to the desired implementation of risk management processes
- CSRM will include risk maturity results in the annual report on information security
- Risk maturity ratings are based on the implementations of information security standards



# Business Impact Analysis

## Reporting requirements:

Each agency ISO shall submit the results of the periodic review and revision of the agency BIA annually.

- An online template will be provided to capture the required information.
- Identify business functions utilizing IT
- Identify whether functions are mission essential (MEFs)
- Identify Recovery Time Objectives (RTO) for each function
- Identify Recovery Point Objectives (RPO) – New 2014
- Identify the IT systems that business functions rely on
- Identify the data processed by the functions (is data sensitive?)
- Provide impact ratings for functions in the event of a disruption



# Risk Assessment Planning

- Annually, each Agency shall develop a risk assessment plan or review and as necessary, update an existing one for the IT systems for which it is the data owner
- Risk assessment plans are similar to IT security audit plans
- Agencies are required, unless otherwise approved by the CISO, to use the Risk Assessment Plan Template found at:  
<http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs>



# Risk Assessment

## Reporting Requirements:

*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
- Agencies are required to use the risk assessment templates
- Risks identified with a residual risk greater than 'low' create a risk finding
- Each risk finding shall have a risk treatment plan to implement compensating controls to reduce the residual risk to low
- Risk treatment plan is similar to a corrective action plan (audit)
- Risk treatment plans shall be submitted to the CISO
- Provide quarterly updates on open risk findings



## CETR

- Commonwealth Enterprise Technology Repository (CETR) is the system of record for agency system names.
- IT system names must be consistent across agency IT security, risk management and security audit programs
  - CETR
  - Business impact analysis
  - Risk assessment
  - IT security audit plan
  - IT security audit reports and corrective action plans



## Sensitive System List

- Agency sensitive system list is based on the IT security audit plan
- Sensitive system designation in CETR does not impact the sensitive system list
- Coordination is required between agency ISO, AITR, and audit



# Vulnerability Scanning

**Requirements:** For each IT system classified as sensitive, the data owning agency shall:

- Conduct a vulnerability scan of the **information system** and **hosted applications** at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported
- Document and report vulnerabilities identified and related remedial actions to CSRM once every 90-days

\*Note: If VITA is performing the information system scans and/or hosted applications scans, results will be submitted to the CISO on the agency's behalf, unless otherwise instructed



# Vulnerability Scanning

## Vulnerability scan reporting template fields:

- Date of Scan
- Host Name
- IP or DNS Entry
- Vulnerability description
- Severity level/Risk Rating (high, medium, low)
- Common Vulnerability and Exposure (CVE) reference
- Remediation action (e.g. what's needed ... disable port, etc.)
- Results of follow-up scan after remediation action is taken



# Intrusion Detection Systems

- Intrusion detection systems (IDS) are used to monitor incoming and outgoing network traffic for signs of attacks. These systems can provide valuable intelligence on:
  - Severity of the attacks
  - Type of attacks
  - Origin of the attacks
  - Protocols/services and ports being attacked
- Agencies shall provide IDS reports at the end of each quarter.



# Intrusion Detection System

## Quarterly IDS Reporting Requirements:

- Name of Agency
- Date Range for the Report
- Total number of attacks per month
- Total number of high attacks per month
- Total number of medium attacks per month
- Total number of low attacks per month
- Top 10 high attacks & number of attacks seen
- Top 10 Source IPs
- Top 10 Destination IPs
- Top 10 Countries of Origin of Attacks with percentages per month
- Top 10 types of attacks
- Top 10 inbound attacks by protocol/service/port
- Top 10 outbound attacks by protocol/service/port



# Intrusion Detection System

- Analysis of IDS reports provides insight to common attacks across the Commonwealth
- If VITA is the IT infrastructure service provider, IDS reports are submitted on the agency's behalf
- In the event that the IDS is unable to produce all of the reporting requirements, please contact CSRM



## What's coming?

- Release of the 2013 annual report on information security
- Recommendations based on the annual report
- Expand the risk management framework core incorporating additional categories/subcategories
- CSRM is considering facilitating a Commonwealth wide IT risk assessment



# Questions

## Questions?

You may also send any questions to :  
**[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)**



Virginia Information Technologies Agency

# Information Security Officer Manual

Bob Auton  
Small Agency ISO / Security Analyst,  
VITA



## ISO Manual Background

The ISO Manual is a 2013 project that was identified by the Information Security Council members. The purpose of the manual was to assist those ISOs who may have minimal resources to maintain their Agency's IT Security Program.

On the next slide we have a listing of ISO Manual Committee, who provided the documentation for the ISO Manual.



## ISO Manual Committee Members

Karen Ashby, Dept. for Aging and Rehabilitative Services,  
Cherrey Wallace, Dept. of Corrections,  
Theresa Fleming, Dept. of Medical Assistance Services,  
Melanie Seigler, Dept. of Forestry,  
Deborah Edwards, Dept of Treasury,  
Bill Freda, VITA, CSRM Project Support Personnel  
Bob Haugh, Co-Chair, Dept. of Emergency Management  
Bob Auton, Co-Chair, Dept. of Juvenile Justice\VITA



## Benefits of the ISO Manual

Provide information on IT security requirements for newly hired ISOs

Quick reference material for all ISOs

Provides alternate methods for completing required processes

Central location of information for newly implemented IT Security requirements



## Ensuring Future Benefits of the ISO Manual

In order for the ISO Manual to continue be a helpful tool in the future, we will need your help to identify efficient and alternate methods for implementing Commonwealth IT Security requirements!

Please let us know if you identify a more efficient method to implement a requirement that we may add to the ISO Manual documentation.

Please forward any information or requests for the ISO Manual to:

[CommonwealthSecurity@vita.gov](mailto:CommonwealthSecurity@vita.gov)



# ISO Manual Sections (Part 1)

1. So You've Just Been Appointed as Your Agency's Information Security Officer (10 Things You Should Do Immediately)
2. What is the Commonwealth's Information Security Governance Structure?
3. How Vulnerability Scanning can change your life and make you feel more secure!
4. The Agency's Information Security Program (The View From 50,000 Feet)
5. The Supporting Cast - Security Roles and Responsibilities
6. Business Impact Analysis (Or Finding Out What Your Agency Really Does)
7. Sensitivity Analysis (Without the Help of a Shrink)
8. Sensitive IT System Inventory and Definition
9. Risk(y) Assessment (Business)



## ISO Manual Sections (Part 2)

10. Information Security Training
11. Agency Level Security Policy (The ISO's Opportunity to be King/Queen for a Day)
12. Responding to Security Incidents
13. Disaster Recovery  $\neq$  Continuity of Operations
14. Exceptions, Exceptions, Exceptions
15. Audits Can Be Your Friends
16. Obtaining Information Security Reports from the Partnership (Who from and What)
17. Big Iron – Mainframe Security
18. COV Certification for ISOs



# ISO Manual Appendixes (Part 3)

Appendix A: An example Governance RACI Chart:

Appendix B: Commonwealth of Virginia Information Security Program Framework

Appendix C: The Supporting Cast - Security Roles and Responsibilities

Appendix D: Business Impact Analysis Template

Appendix E: Information System Security Plan

Appendix F: IT System and Inventory and Definition Document

Appendix G: Reports and Requests from Websites and Customer Care Center

Appendix H: ISO Certification Information

Appendix I: Summary of Steps to obtain COV ISO Certification

Appendix J: SEC-501 MAINTENANCE CALENDAR

Appendix K: Commonwealth of Virginia Acronyms



# Accessing the ISO Manual

The ISO Manual is located on the ITRM Policies, Standards and Guidelines webpage, under the Tools and Templates section.

The below is a link to the VITA webpage to access the ISO Manual:

<http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs>



# Questions





Virginia Information Technologies Agency

# Archer GRC in the Commonwealth

Benny Ambler  
Senior Manager, Security Governance  
VITA



## Archer GRC

- Archer is a Governance, Risk and Compliance (GRC) Application
  - Purchased and Deployed in 2013
  - Provides a consolidated repository to store and analyze our IT Assets and Risks
  - Helps provide an enterprise wide view of the state of security in the COV
  - Detailed tracking and analysis of people, assets and events



## Importing

- Imported the data from other systems and consolidated and added several tracking functions. Imports included:
  - Audit Program Data - IT Security Audit Plans, IT Security Audit Reports, Corrective Action Plans, Quarterly Status Reports and any open findings
  - Risk Management Data - Business Impact Analysis (BIA) and Risk Assessment (RA) submission information



## Consolidation

- Consolidated several other tracking functions into Archer
  - Information Security Officer (ISO) officially designated ISO Status and contact information
  - The COV ISO Certification Status and reporting functions
  - The use of the Commonwealth Enterprise Technology Resource (CETR) as the general system list.



## Improvements

- We need your assistance moving forward to further improve and enhance the use and functionality of Archer in the Commonwealth.
  - System Identification and Naming
  - APA Audits
  - Obtaining Access to Archer for the right people



## System Identification and Naming

- One of the biggest challenges we have is identifying which systems the agencies are referencing in their documents. We will ask that the system names be consistent across all documents moving forward.



## Document Flow

- CETR, is the official system list record of authority.
  - CETR contains all systems, those in production, retired, sensitive, not sensitive.
- BIA - each business process should align to an application in CETR.
  - Each business process should align to an application in CETR. This can be a many to many relationship, but any active system in CETR must include at least one business process in the BIA.



## Document Flow +

- The IT Security Audit Plan should also contain system names easily identifiable from CETR.
  - The IT Security Audit Plan is used to define sensitive systems. Systems should not be retired and should be marked as sensitive in CETR. But, the IT Security Audit plan may override CETR for sensitivity.



## Document Flow - Reporting

- IT Security Audit Reports, Corrective Action Plans, and Quarterly Reports should also follow the same naming.
- We should be able to identify a system in CETR as sensitive, and follow it from IT Security Audit Plan, Audit Report, and Corrective Action Plan (if it has findings) then follow the findings to closure on the Quarterly Status Reports.



## APA Audits

- Generally, the APA Audits are financial audits used to test the controls around a financial system. In the future an agency may be able to apply an APA audit to a sensitive system audit.
  - We will request that the system is clearly identified in the audit report.
  - And the report is identified as an IT Security Audit.



## Tips

- Risk Assessments for sensitive systems should be identifiable by name in CETR, as well.
- All of these documents are tied together in one system.
- We will be returning IT Security Audit Plan updates that do not align in CETR submitted in the future.
- We import the IT Security Audit Plan for Agencies that are not required to use CETR.
  - Independents and Higher Education



## Obtaining Access to Archer

- We recognize that agencies are structured differently in how they handle the activity of submitting compliance documents to the CISO.
- Currently ISO's may access Archer in read only mode.
- This requires 2 factor authentication
- Please note that access requests should originate from the ISO or have the ISO copied in the email.



## For Partnership Agencies

- acquire a token from eVA
- email the Request for access to Archer to [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)  
include:
  - name
  - title
  - email address



## For Non-Partnership Agencies

- email the request for access to Archer to [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov):
  - name
  - title
  - email address
  - mailing address (for setting up FIM account)
  - telephone number (for setting up FIM account)



# Questions?





Virginia Information Technologies Agency

# Upcoming Events





## Future ISOAG

**May 7**      1:00 – 4:00 pm @ CESC

**Keynote: Tony Douglas, Symantec**

*ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2014*



# IS Security Conference 4/3 & 4/4

Registration is now closed. We look forward to seeing you there!

## Information Security: Enabling the Business

Richmond, VA 2014



Secretary  
of  
Technology





# IS Orientation

**When: Thursday, June 5, 2014**

**Time: 1:00 pm to 3:30 pm**

**Where: CESC , Room 1211**

**Register here:**

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

**Next IS Orientation will be held on Sept 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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

2 April, 2014



**NORTHROP GRUMMAN**

# ADJOURN

## THANK YOU FOR ATTENDING

