



# ISOAG Meeting July 6 , 2016

Welcome to CESC!

---





# ISOAG July 6, 2016 Agenda

**I. Welcome & Opening Remarks**

**Mike Watson, VITA**

**II. The Internet of Things,  
Big Data, Smart Grid, Health IT**

**Ellen Nadeau, NIST, Cyber Policy Strategist**

**III. Archer Reporting/Analysis**

**Mark Martens, VITA & Joy Young, VITA**

**IV. VITA Centralized/Shared  
ISO & Audit Services**

**Ed Miller, VITA**

**V. Upcoming Events**

**Mike Watson, VITA**

**VI. Partnership Update**

**Northrop Grumman**



# Welcome and Opening Remarks

Michael Watson

July 6, 2016

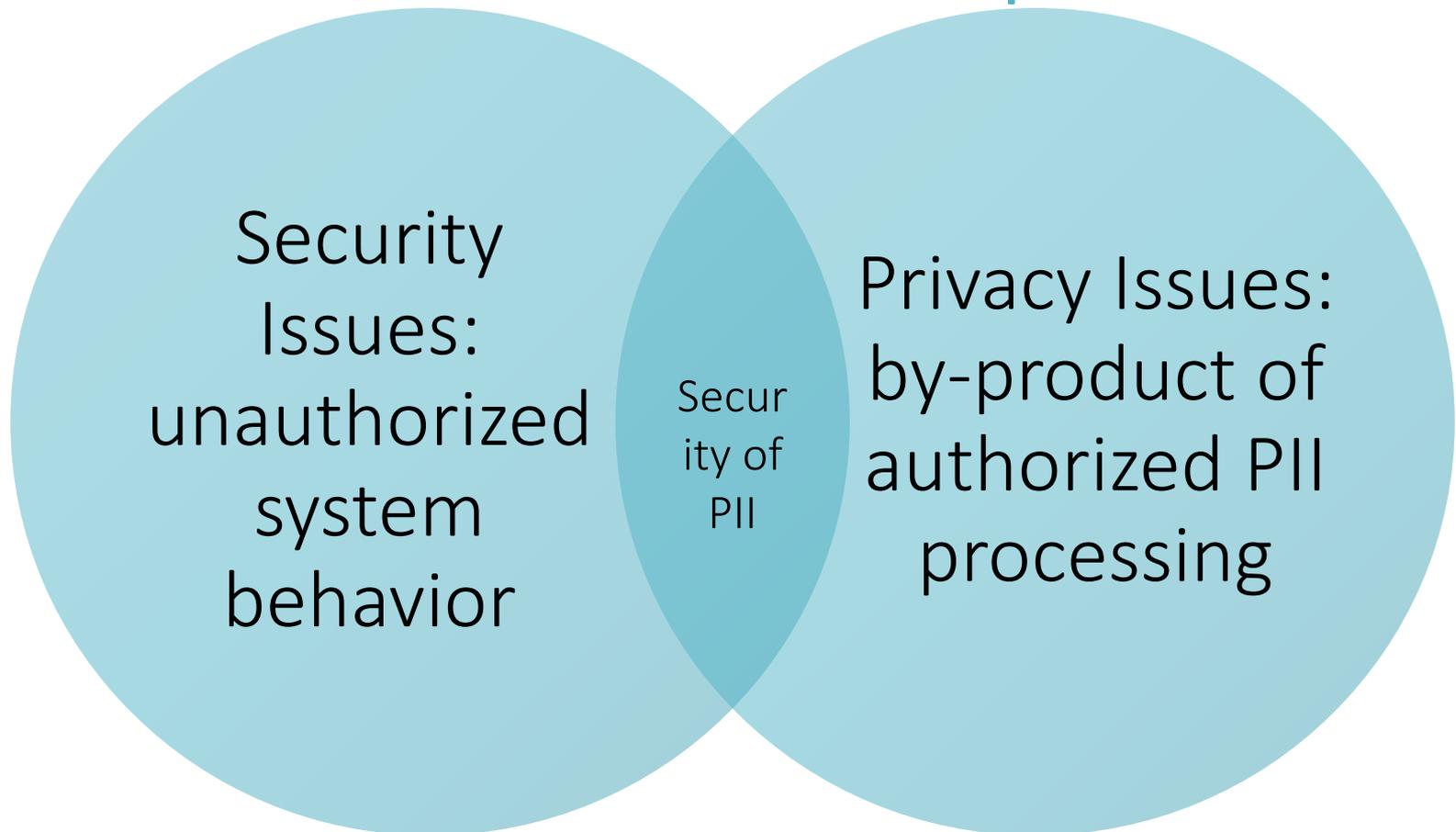


Ellen Nadeau, NIST

July 6, 2016

# Using Risk Management to Improve Privacy in Information Systems

# Information Security and Privacy: Boundaries and Overlap



# Identifying Risk

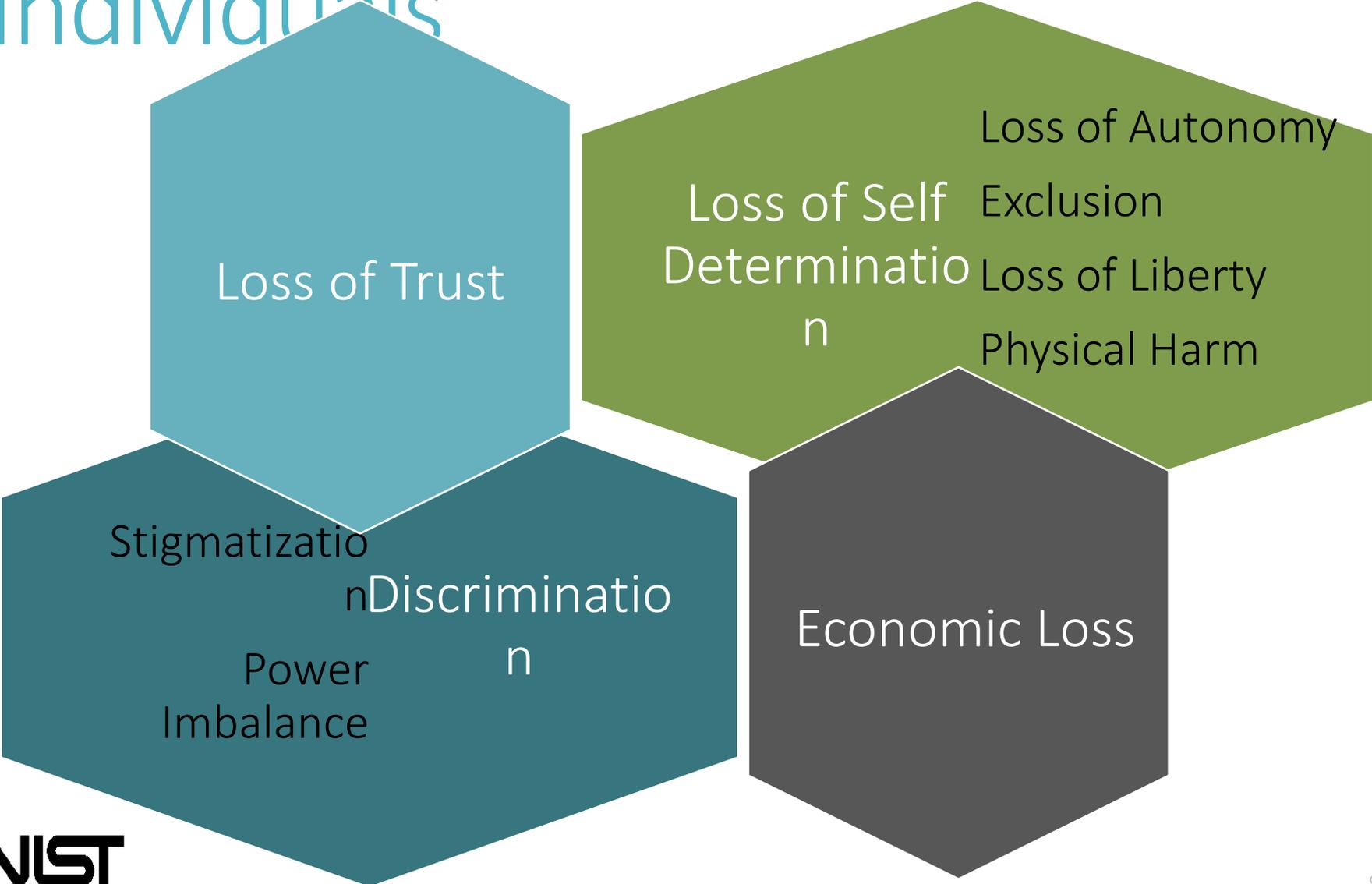
A measure of the extent to which an entity is threatened by a potential circumstance or event

A function of:

- Likelihood of occurrence
- Adverse impact that would occur

$$\text{Security Risk} = \text{Vulnerability} * \text{Threat} * \text{Impact}$$

# Potential Problems for Individuals



# Privacy Risk Equation

Privacy Risk = Likelihood of a Problematic Data  
Action \* Impact

**Likelihood** is

determined by contextually-based analysis that a data action is likely to create a problem for representative set of

**Impact** is determined by an analysis of the adverse affects on an organization of creating the potential for privacy problems

*Note: Contextual analysis is the comparison of Data Actions, the personal information on which they act, and contextual considerations*

# Risk can never be eliminated and so it must be

## MANAGED

### Risk Responses

- Accept risk
- Avoid risk
- Mitigate risk
- Transfer/share risk

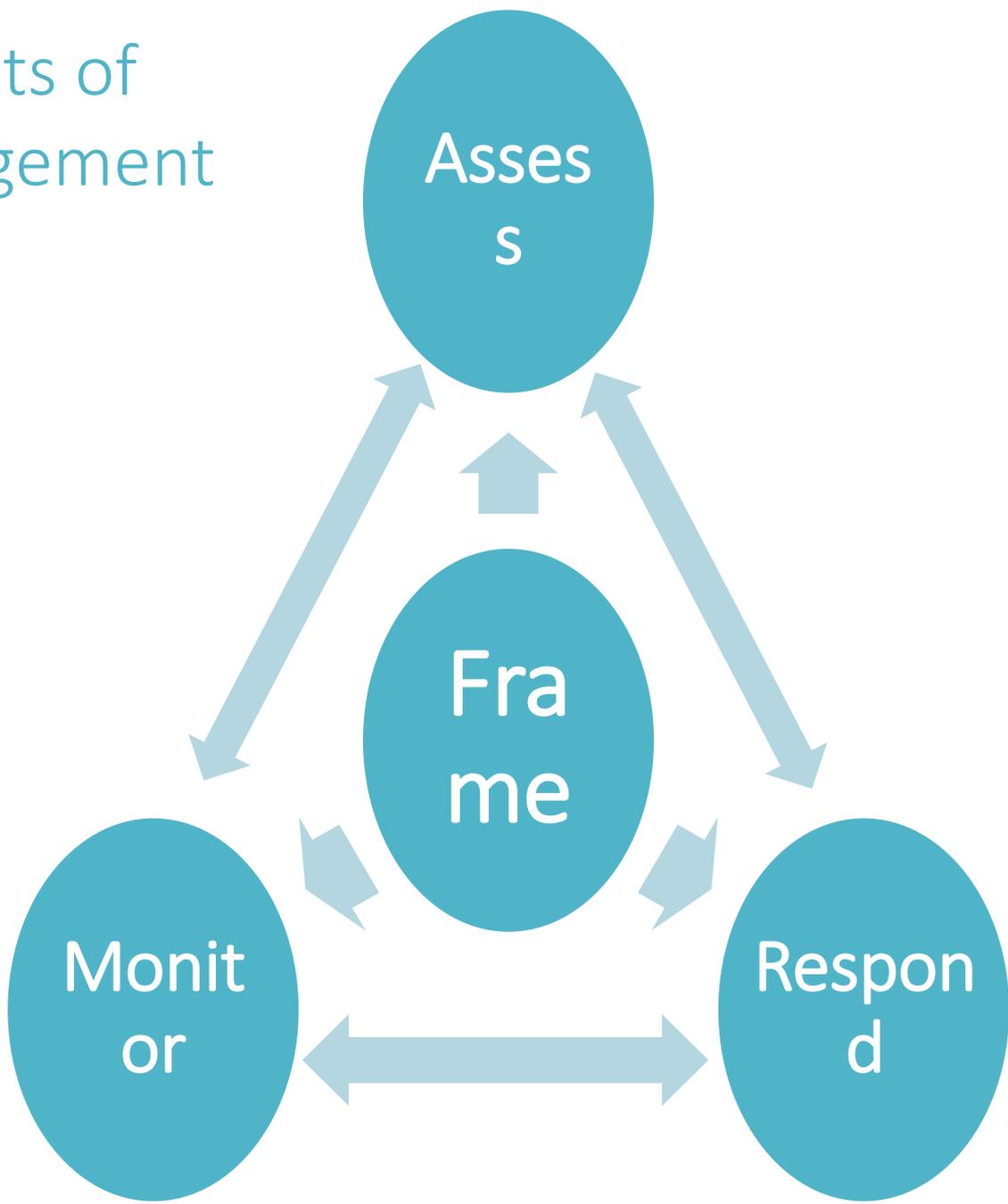
### Risk Decisions

- Organization-wide process
- Optimization factors include: mission objectives; other risk areas (financial, legal, etc.)



# Privacy Risk Assessment Methodology

Components of Risk Management



# Frame Business Objectives

Frame the business objectives for the system(s), including the organizational needs served.

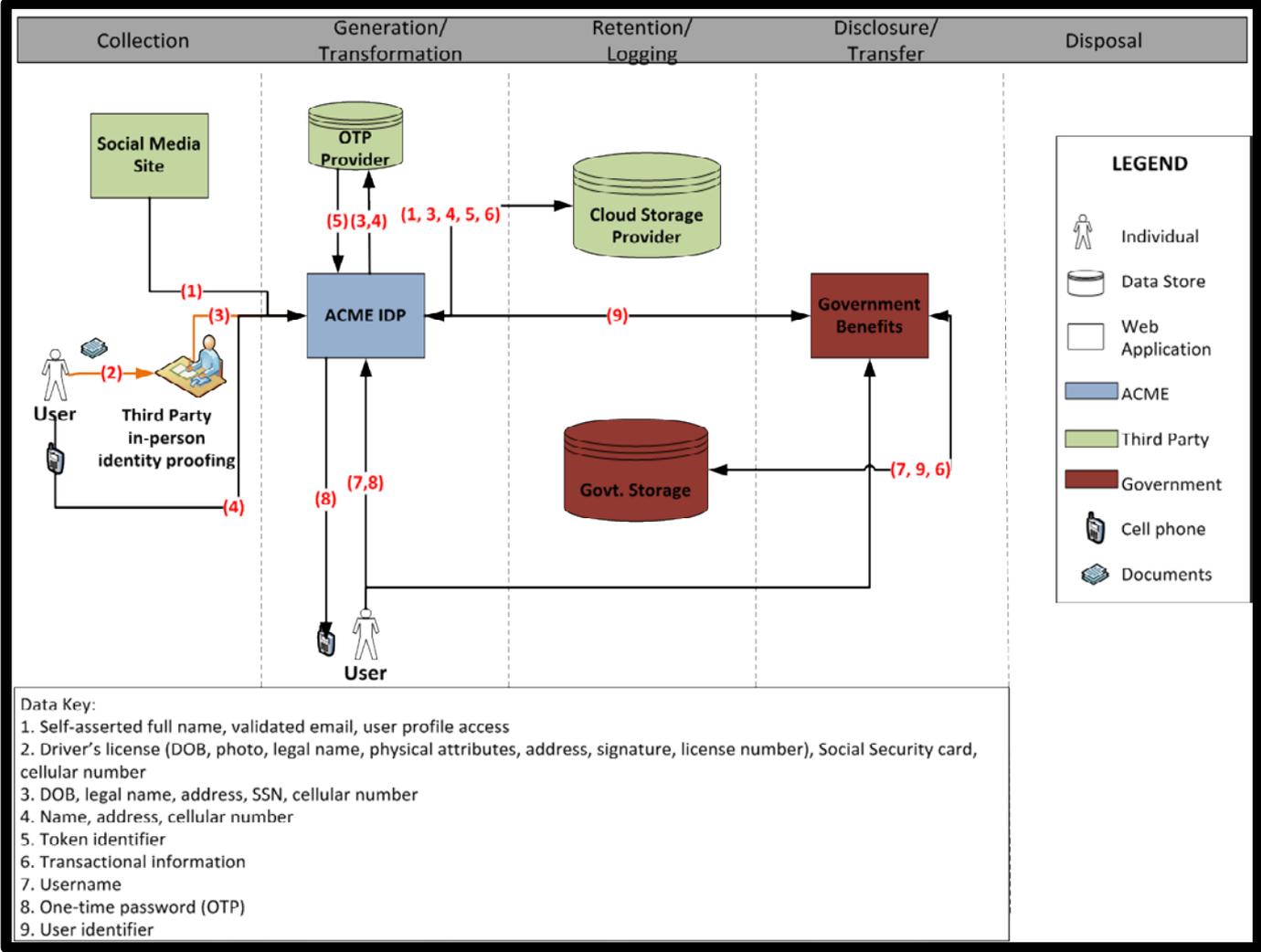
- Describe the functionality of your system(s).
- Describe the business needs that your system(s) serve.
- Describe how your system will be marketed, with respect to any privacy-preserving functionality.

# Frame Privacy Governance

Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

- Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the pilot must operate.
- Identify any privacy-related principles or other commitments to which the organization adheres (FIPPs, Privacy by Design, etc.).
- Identify any privacy goals that are explicit or implicit in the organization's vision and/or mission.

# Assess System Design – Data Actions



# Assess System Design - Context

## Example:

An individual wishes to use ACME IDP service to augment a social credential with identity proofing and a second authentication factor to create a stronger credential. This stronger credential will be used to access government benefits.

Data Action	Personal Information	Specific Context	Summary Issues
Collection from the Social Media Site	<ul style="list-style-type: none"> <li>- Self-Asserted Full Name</li> <li>- Validated Email</li> <li>- List of Friends</li> <li>- Profile Photograph</li> </ul>	<ul style="list-style-type: none"> <li>- One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user's social media presence and ACME IDP</li> <li>- Social credential linking is visible to user</li> <li>- Linking of social credential simplifies access to government benefits system</li> <li>- User profile may contain information the user considers sensitive</li> <li>- User profile may contain information from other users not participating in the system</li> </ul>	<ul style="list-style-type: none"> <li>- Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose</li> <li>- Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?</li> <li>- How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?</li> <li>- Will the user understand ACME will have</li> </ul>

### Example Contextual Factors

#### Organizational

*System includes both government benefits agency and commercial service providers*

*Multiple privacy policies governing system*

*Public perception: high expectation of privacy with government benefits agency, low expectation with social credential provider*

*Relationships: No pre-existing relationship with ACME IDP, regular interactions with government benefits agency, regular interactions with social credential provider*

#### System

*Personal information is not intended to be made public*

*New system, no history with affected individuals. Low similarity with existing systems/uses of social identity.*

*Four parties sharing personal information: one public institution, three private*

*ACME will use 3rd party cloud provider*

#### User

*High sensitivity about government benefits provided by system*

*Users exhibit various levels of technical sophistication*

*Potential user confusion regarding who "owns" the various segments of each system*

*20% of users use privacy settings at social provider*

# Assess Privacy Risk

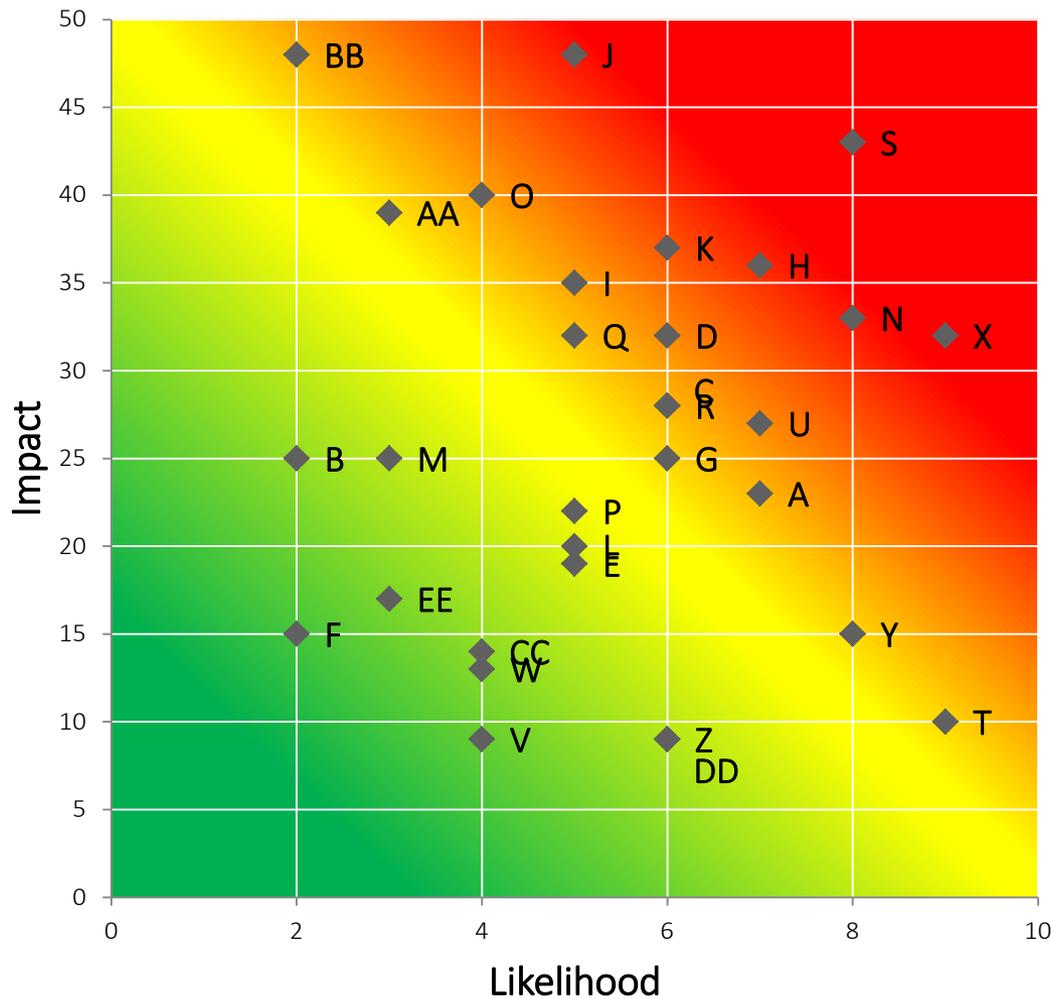
SAMPLE TABLE

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	<ul style="list-style-type: none"> <li>-Appropriation</li> <li>-Induced disclosure</li> <li>-Surveillance</li> <li>-Unanticipated Revelation</li> </ul>	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	7
			Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.	2
	Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?	-This summary issue will be associated with another data action.		NA
	How will percept organization's priva willingness to con			

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Business Impact Factors					Total Business Impact (per Potential Problem)
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	<ul style="list-style-type: none"> <li>-Appropriation</li> <li>-Induced disclosure</li> <li>-Surveillance</li> <li>-Unanticipated Revelation</li> </ul>	Stigmatization	7	6	6	4		23
			Power Imbalance	7	6	8	4		25
	How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?	<ul style="list-style-type: none"> <li>-Induced disclosure</li> <li>-Surveillance</li> </ul>	Loss of Trust	7	6	8	7		28

# Assess Privacy Risk

Problem Prioritization Heat Map



# Resources

NIST Privacy Engineering Website:

[http://csrc.nist.gov/projects/privacy\\_engineering/index.html](http://csrc.nist.gov/projects/privacy_engineering/index.html)

Draft NISTIR 8062:

<http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8062>

Contact me: [ellen.nadeau@nist.gov](mailto:ellen.nadeau@nist.gov)



Virginia Information Technologies Agency

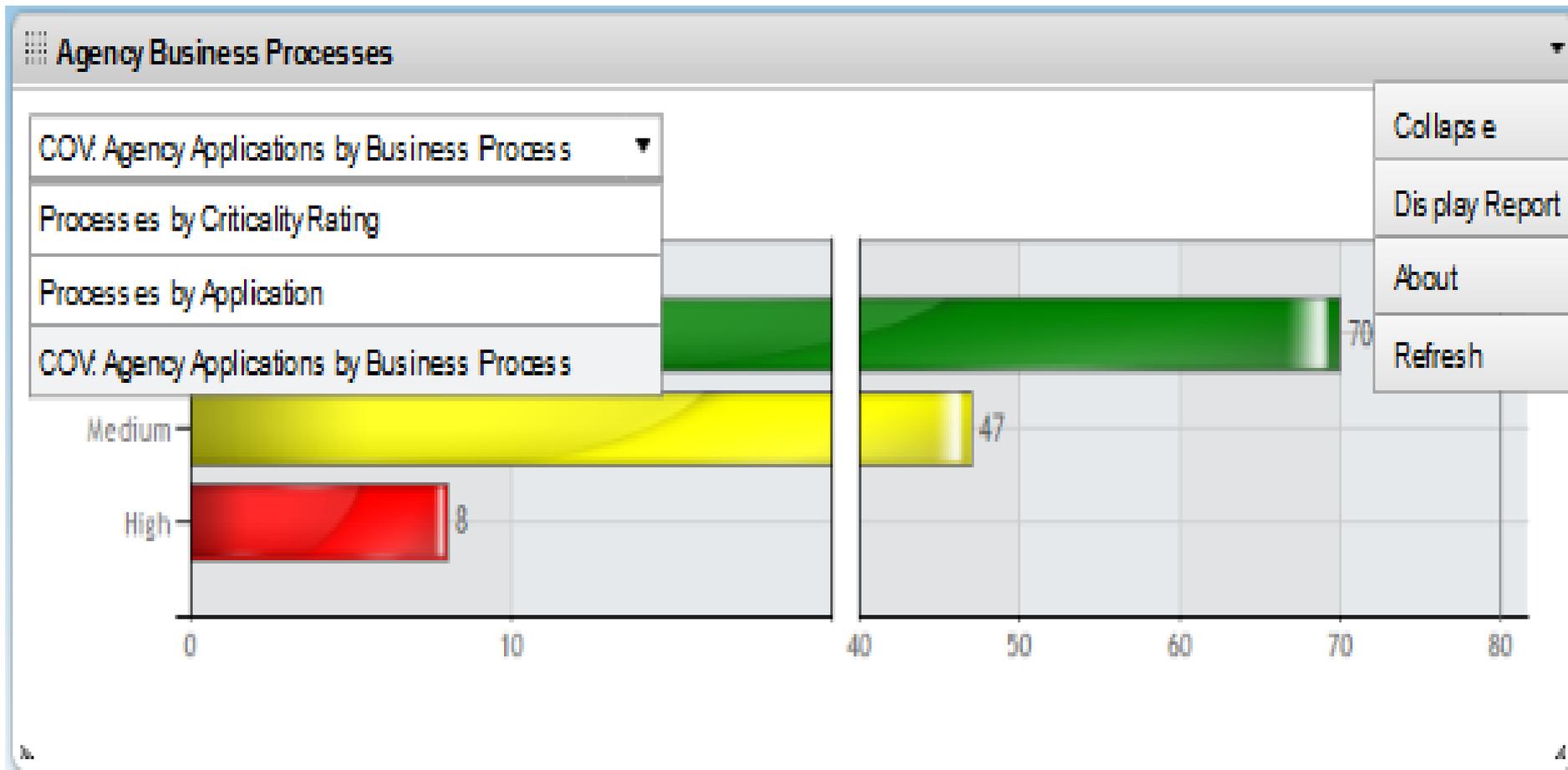
# Archer Reporting Overview & 2015 Annual Report Preview

Mark Martens & Joy Young  
Information Assurance Analysts

---

ISOAG  
July 6<sup>th</sup> , 2016

# Dashboard Reports





## Key Fields

Virginia Information Technologies Agency

**Enterprise Governance Risk and Compliance**

Agency Workspace

Preferences Reports Help Logout Search: Agency Management

Add/Change Datasets (Information) | Add/Change Devices | Change Applications | Device Reports | Dataset Reports | Questionnaire Reports | Application Reports | IT Security Audit Plans | IT Risk Assessment Plans | Applications without Business Processes

### Business Processes

1 to 50 (of 100)

Refresh Export Print Email

#### COV: Agency Applications by Business Process

Agency	Process Name	Business Purpose	Compliance Rating	Content ID	Criticality Rating	Process ID	Risk Rating	Applications
Agency: Virginia Information Technologies Agency								
Virginia Information Technologies Agency	Accounts Payable	Processes vendor invoices received for processing at MTA in accordance with the VA Prompt Payment Act and other policies	Not Rated		🟡	BPID-251159		Cardinal Interface eVA Interface Peoplesoft Financials
Virginia Information Technologies Agency	Accounts Receivable (Non-State)	Processes and deposits all cash receipts, including checks, received for processing at MTA	Not Rated		🟡	BPID-251121		Peoplesoft Financials
Virginia Information Technologies Agency	Accounts Receivable (State)	Update customer accounts for payments, ensure adequate cash flow to MTA to cover agency obligations	Not Rated		🟡	BPID-251117		Cardinal Interface Peoplesoft Financials
Virginia Information Technologies Agency	Advance the quality & maturity of ITIM implementation & support (Both PMD & ITIM Division)	Conceptualize & develop new ITIM based programs, processes, & supporting tools. Advance selected programs, processes, & tools through the VITA ITIM/PMD approval processes. § 59.1-496 The CIO shall develop and recommend to the Secretary of Technology all investments of a million dollars or more	Not Rated		🟢	BPID-251087		Commonwealth Enterprise Technology Repository EBA - Enterprise Business Architecture Application and Tools Oracle Primavera Portfolio Management (OPPM) VITA Security Asset Inventory and Risk Management (RSA ARCHER)
Virginia Information Technologies Agency	Agency IT strategic planning process	§ 2.2-2017 Review information management and information technology plans submitted by agencies and public institutions for high-priority and	Not Rated		🟢	BPID-251085		Commonwealth Enterprise Technology Repository EBA - Enterprise Business Architecture Application



# Application Sensitivity

## ▼ General Information

<b>Agency:</b>	<a href="#">Virginia Information Technologies Agency</a>	<b>Agency Number:</b>	136
<b>Application Name:</b>	VITA Architecture Review	<b>Application ID:</b>	APPID-205903
<b>Technologies:</b>		<b>Application Type:</b>	
<b>Last Updated:</b>	5/6/2016 12:09 PM	<b>IT Security Audits (IT Systems Scheduled to Audit):</b>	<a href="#">SA-212161</a> <a href="#">SA-221118</a> <a href="#">SA-226914</a>
<b>Description:</b>	Review new application development <a href="https://ssi01.apps.vita.virginia.gov/var/">https://ssi01.apps.vita.virginia.gov/var/</a>		
<b>Contains Data Sensitive to Confidentiality:</b>	No	<b>Customer Impacting Information:</b>	
<b>Contains Data Sensitive to Integrity:</b>	No	<b>Vital Business Function:</b>	
<b>Contains Data Sensitive to Availability:</b>	No	<b>COV Inherited Record Permissions:</b>	APA:ISO Commonwealth Security Groups CSRM Incident Response CSRM Risk Management - Manager CSRM Risk Management Group CSRM Security Analyst CSRM Security Architecture and Operations CSRM Sysadmin CSRM-Contractors NG Incident Response Group NG Information Assurance VITA:ISO
<b>Recovery Time Objective (RTO):</b>		<b>Recovery Point Objective (RPO):</b>	
<b>Customer Impacting:</b>	Yes	<b>Service Model:</b>	
<b>Sensitive System:</b>	Yes		

## Crisp Rat



## Crisp Rat



## Crisp Rat



## Crisp Rat





# Helper Icon

▼ Agency Scorecard Data			
ISO Certification Status:	N/C		
3 Year Audit Obligation:	N/C	3 Year Audit Obligation - Previous Year:	N/C
Audit Plan Status:	N/C	Audit Plan Status -	N/C
Current Year Percentage of Audits Received:	N/C		
Current Year Percentage of Quarterly Updates Received:	0%		
Business Impact Analysis Status:	Pass		
3 Year Risk Assessment Obligation:	84%	Previous Year 3 Year Risk Assessment Obligation:	
Risk Assessment Plan Status:	●	Previous Year Risk Assessment Plan Status:	●
IDS Quarterly Reports:	●	Previous Year IDS Quarterly Reports:	
Vulnerability Scanning:	●	Previous Year Vulnerability Scanning:	
Primary ISO is Certified:	Yes		
Data Set Inventory:			

**3 Year Audit Obligation** ✕

X% - The percentage of audit work completed as measured against the agency's security audit plans over the past three years  
 N/A - Not applicable as the agency had no audits due  
 N/C - The agency head has not submitted a current security audit plan



# Creating Reports

**Applications** ? X

New Modify Save Reports Delete 1 to 100 (of 133) Refresh Export Print Email

**Search Results** Options

Drag a column name here to group the items by the values within that column.

Application ID	Agency	Application Name ▲	Description	Criticality Rating
APPID-205806	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Agency IT Strategic Plans for Budget Biennium 2002-2004 App</a>	Allows users to search (by Secretariat or Agency) for PDFs of Agency IT Strategic Plans.	Not Rated
APPID-205807	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Agency IT Strategic Plans for Budget Biennium 2004-2006 App</a>	Allows users to search (by Secretariat or Agency) for PDFs of Agency IT Strategic Plans.	●
APPID-205808	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">AITR Web Site</a>	Web site used by AITR's	Not Rated
APPID-205810	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Assistant to the Governor for Workforce Website</a>	Web site design and content management.	●
APPID-224688	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Broadband Zip Code Search (public)</a>	The state broadband contracts provide an alternative for low cost internet and broadband services for commonwealth customers. These contracts have minimal service performance guarantees (SLAs) and service term commitments.	●
APPID-205811	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Budget and Resource Forecasting - CSS (BARF) (retired, not in use)</a>	VITA's Resource Forecasting Application to assist VITA with rate setting and to provide customers with VITA computer services expense projections.	Not Rated
APPID-205812	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Budget and Resource Forecasting - CSS (BARF) (retired, not in use)</a>	VITA's Resource Forecasting Application to assist VITA with rate setting and to provide customers with VITA computer services expense projections.	Not Rated



# Modifying Reports

Available	Selected
<p>Find: <input type="text"/> Name <input type="button" value="🔍"/></p> <p>[-] Applications</p> <ul style="list-style-type: none"><li>[-] Add New Relationship</li><li>[-] 3 Year Audit Obligation - Helper</li><li>[-] 3 Year Audit Obligation - Previous Year - Helper</li><li>[-] 3 Year Audit Obligation - TEST - Domain Family Helper</li><li>[-] 3 Year Audit Obligation - TEST - Helper</li><li>[-] Active Usage Quantity</li><li>[-] Agency</li><li>[-] Agency IT RA Current and Sensitive System - Helper</li></ul>	<p>Applications</p> <ul style="list-style-type: none"><li>Application ID <input type="button" value="✕"/></li><li>Agency <input type="button" value="✕"/></li><li>Application Name <input type="button" value="🔑"/></li><li>Description <input type="button" value="✕"/></li><li>Criticality Rating <input type="button" value="✕"/></li></ul>
<p><input type="checkbox"/> <b>Statistics Mode</b> Return search results in the form of a statistics report by grouping and aggregating field values.</p>	



# Add New Relationship

Available	Selected
<p>Find: <input type="text"/> Name <input type="button" value="🔍"/></p> <ul style="list-style-type: none"><li>Applications<ul style="list-style-type: none"><li>Add New Relationship</li><li>3 Year Audit Obligation - Helper</li><li>3 Year Audit Obligation - Previous Year - Helper</li><li>web Category</li><li>Web Service</li><li>Year Last Major Update/Upgrade</li><li>Year Placed in Service</li></ul></li><li>Findings</li></ul>	<p><b>Applications</b></p> <ul style="list-style-type: none"><li>Application ID <input type="button" value="✕"/></li><li>Agency <input type="button" value="✕"/></li><li>Application Name <input type="button" value="✕"/></li><li>Description <input type="button" value="✕"/></li><li>Criticality Rating <input type="button" value="✕"/></li></ul> <p><b>Findings</b> <input type="button" value="✕"/></p> <p>No Fields Selected.</p>
<p><input type="checkbox"/> <b>Statistics Mode</b> Return search results in the form of a statistics report by grouping and aggregating field values.</p>	<p><a href="#">Configure Relationships</a></p>



# New Relationships are Complicated

+	APPID-205881	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Sharepoint (VI)</a>	File sharing sharepoint service	
-	APPID-221181	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Telecommunications Inventory Billing System (TIBS)</a>	Provides Customer billing, asset/inventory, and service order capabilities for all telecommunications goods and services (voice, data, cellular, pager)	
Finding ID ▲		Policies			
<a href="#">FND-1331</a>		<a href="#">CM-02 Baseline Configuration</a>			
<a href="#">FND-1332</a>		<a href="#">CM-02 Baseline Configuration</a>			
Page 1 of 1 (2 records)					
+	APPID-205893	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">Vendor Invoice Payment &amp; Reconciliation</a>	VITA Vendor Invoice Payment & Reconciliation Used to track the status of Telecommunication vendor payments	
-	APPID-205902	<a href="#">Virginia Information Technologies Agency</a>	<a href="#">VITA Application Security</a>	VITA Application Security provides role based security to applications	

# Enforce Relationships

Search Records: Applications

Search

Agency IT RA Current and Sensitive

Statistics Mode Return search results

Configure Relationships

Add New

### Advanced Search Configuration

**Relationship Options**

The Options dropdown menu for each related application provide options for establishing the specific relationship type and allow you to remove the relationships.

- [-] Applications
  - [-] Findings
    - Enforce Relationships

OK Cancel

Field To Evaluate	Operator	Value	Relationship	Actions
1. Agency			And	
2. Sensitive System	Equals	* Yes	And	
3. Status	Does Not Equal	* No longer in use - retired	And	
4. Policies	Equals	* AC-02 Account Management	And	

Advanced Operator Logic:  Example (1 AND 2) OR 3



# Filtering Reports

## ▼ Filters



Select filtering options, including filter by value, cross reference, users/groups and date ranges.

Field To Evaluate	Operator	Value(s)
1. Agency	Contains	* Virginia Information Technologies Agency
2. Sensitive System	Equals	* Yes
3. Status	Does Not Equal	* No longer in use - retired

Advanced Operator Logic:

Example (1 AND 2) OR 3



# Sorting Reports

## ▼ Sorting



Select fields from the list below to sort your data. You can choose to sort ascending or descending and also to group data if desired.

	Field		Order
1.	<input type="text" value="Application Name"/>	...	<input type="text" value="Ascending"/>
2.	<input type="text"/>	...	<input type="text" value="Ascending"/>

# Exporting Reports

**Applications**

View Modify Save Reports Delete

**Search Results**

Drag a column name here to group the items by the

Application ID	Agency
APPID-205820	<a href="#">Virginia Information Technologies Agency</a>
APPID-205821	<a href="#">Virginia Information Technologies Agency</a>
APPID-205822	<a href="#">Virginia Information Technologies Agency</a>
APPID-205859	<a href="#">Virginia Information Technologies Agency</a>

**Applications: Export Options**

**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 other application that can read text files.
-  **XML File** Generates an XML file that can be opened in Internet Explorer or any other application that can read a text file.

Refresh Export

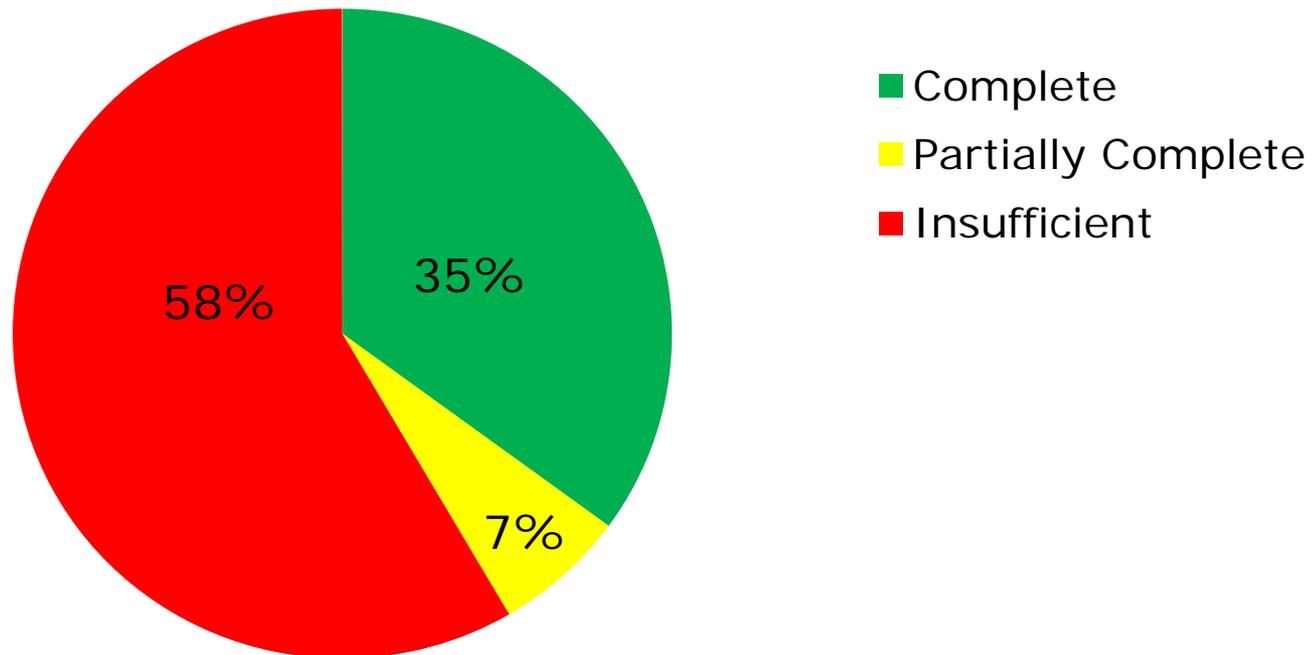
Options

	Criticality Rating
... and eVA charges ... users access billing ... for all service types.	●
... and hosted ... and decentralized	●
... allows authorized ... (PMIS, CIPPS, ... to view employee	Not Rated
... contact data within ... NG employees ... automated feed. In ... ts extracted. This ... y the PeopleService	●

...fault.aspx.

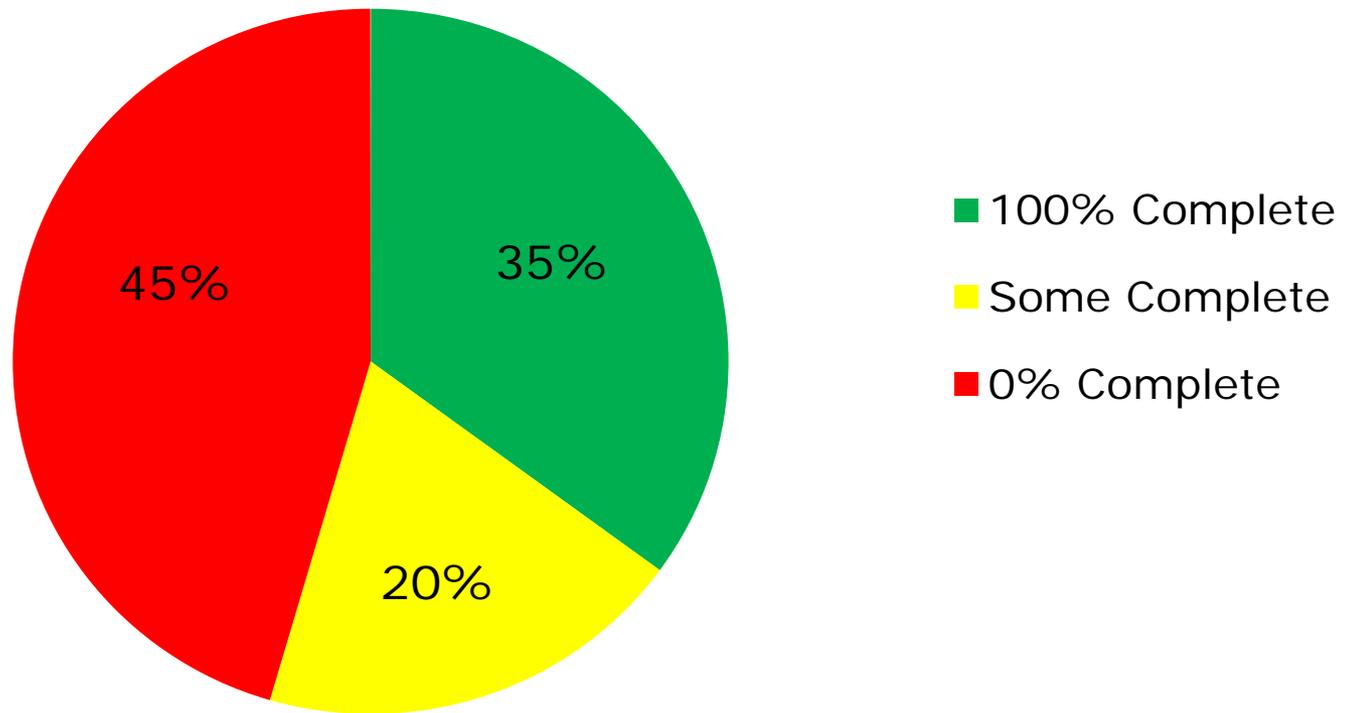
# Overall Risk Program

## Commonwealth Overall Risk Program Score



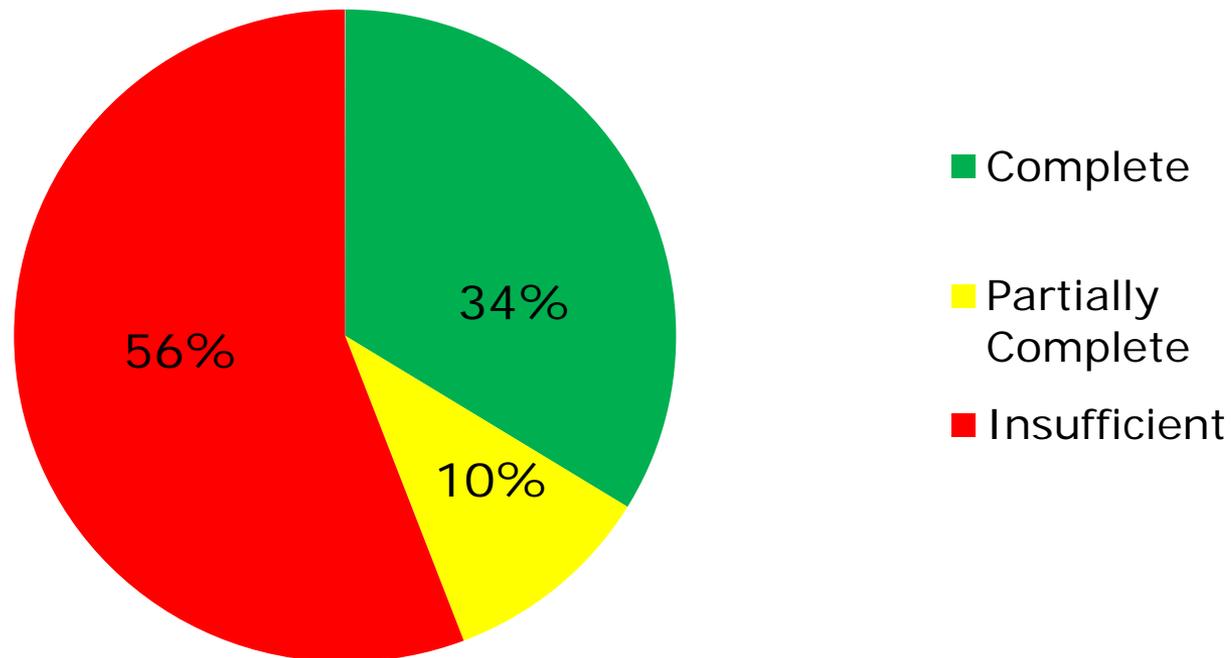
# Risk Assessment Obligation

## 3 Year Risk Assessment Obligation



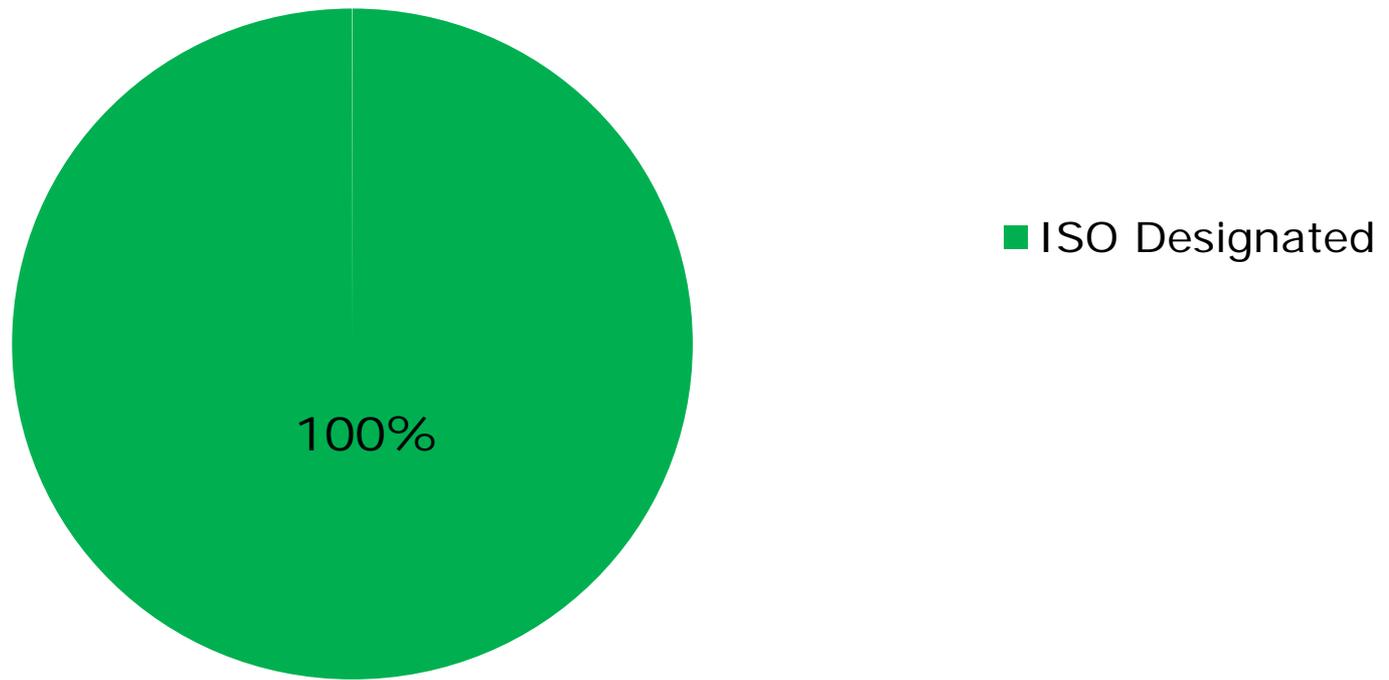
# Overall Security Audit Program

## Commonwealth Overall Audit Program Score



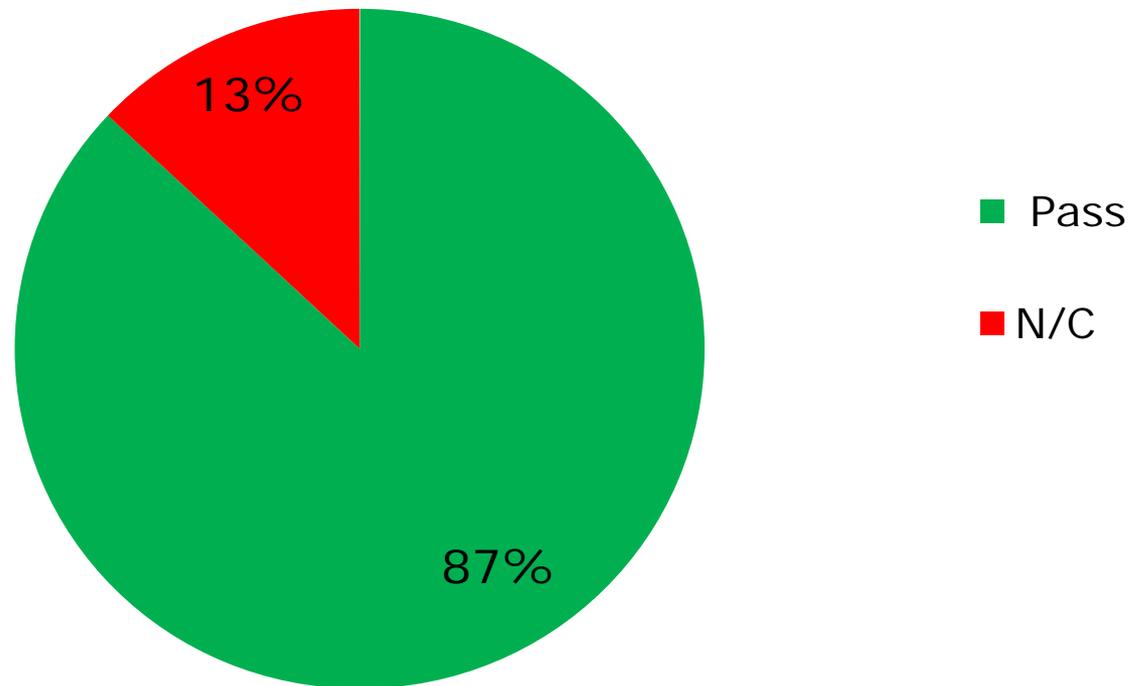
# Designation of an ISO

## ISO Designation



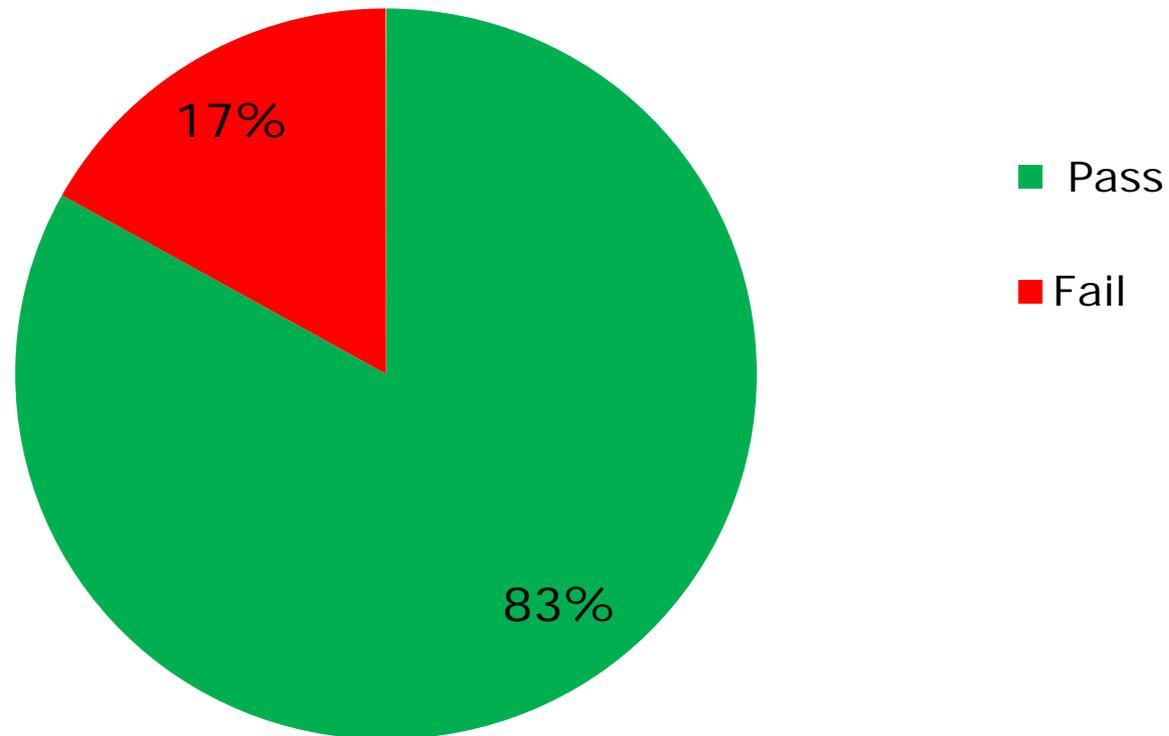
# ISO Certification Status

## ISO Certification



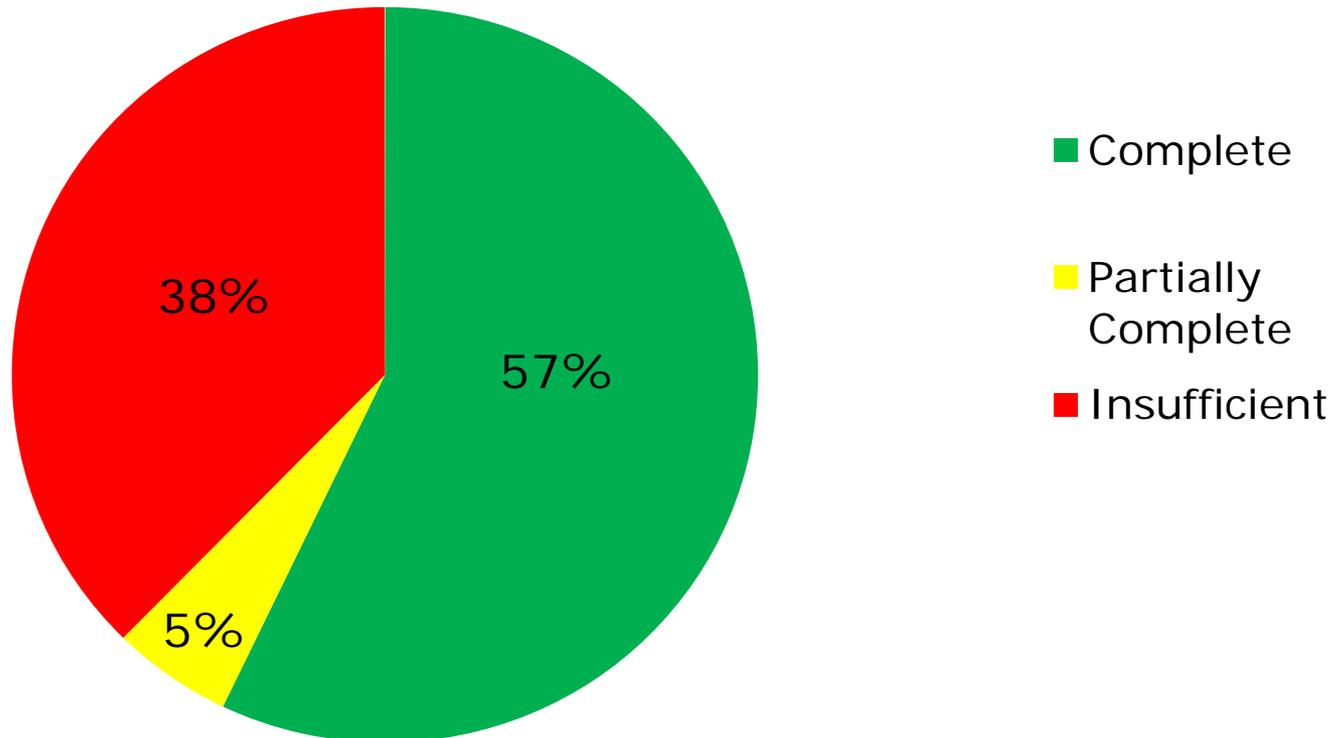
# Submission of IT Security Audit Plan

## IT Security Audit Plan Status



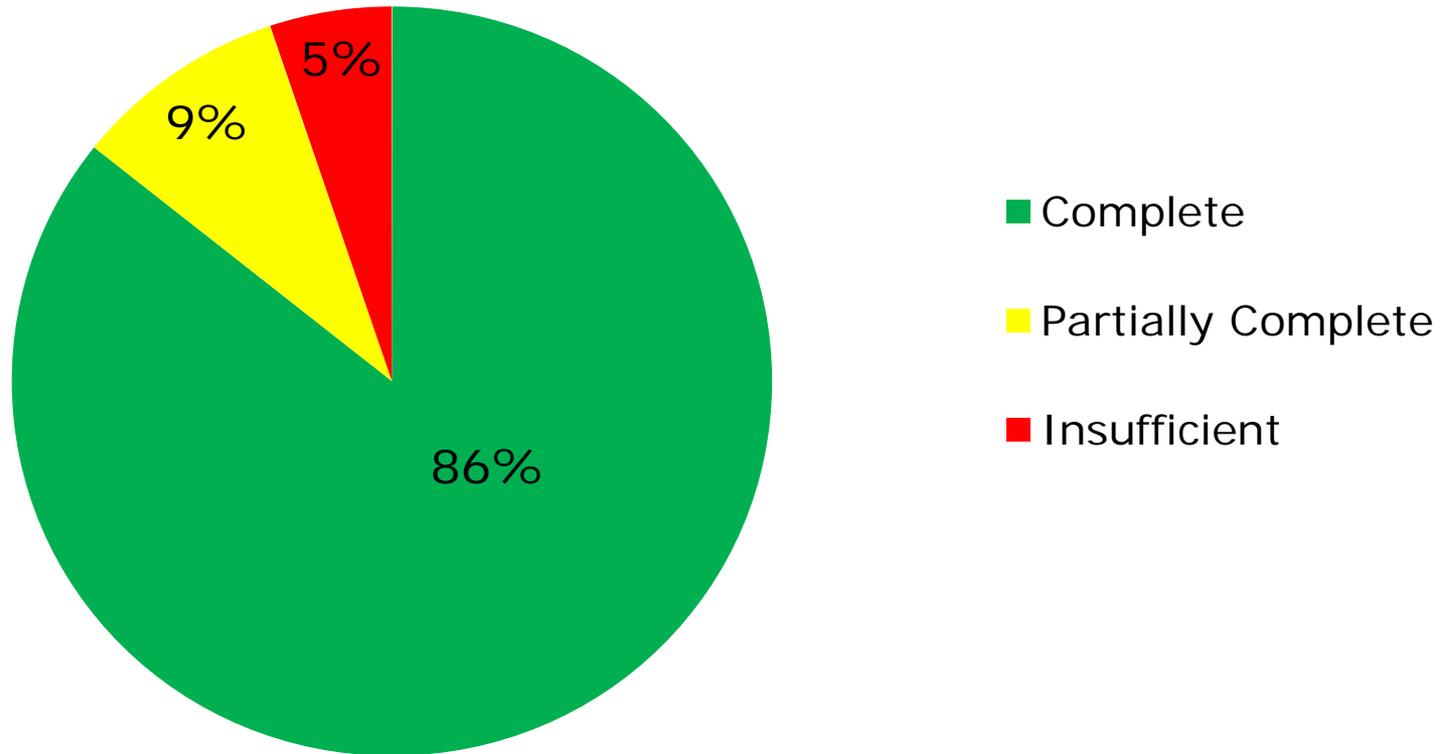
# Submission of IT Security Audit Reports

## Audit Reports



# Submission of Quarterly Updates (CAPs)

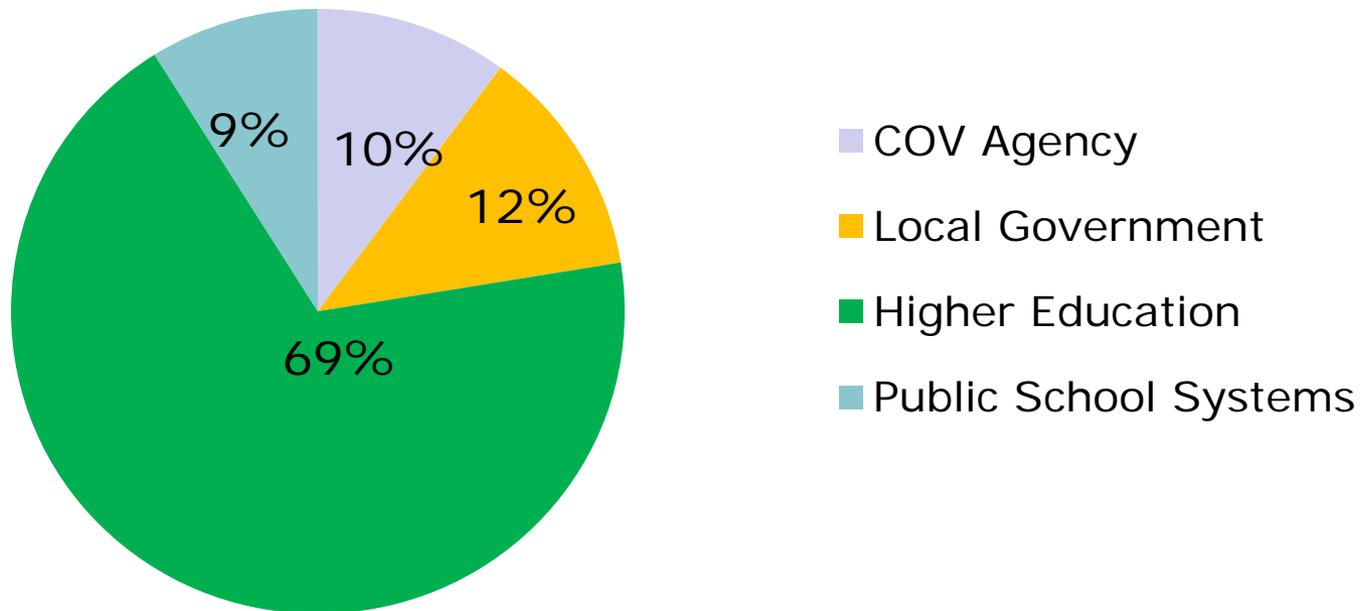
## Quarterly Updates Received



# Investigations

## Percentage of Investigations 2015

Source: MS-ISACS





## Issues Identified

- No significant improvement in agency IT security audit programs or risk programs
  - Agencies are not conducting IT security audits
  - Findings are not addressed in a timely manner
  - Lack of IT Security audits and Risk Management practices hinders the ability to determine risk



## Issues Identified (cont.)

- Information security program compliance became a factor in evaluating information technology investment funding and off premise hosting requests
- Access control continues to be a significant area of weakness
  - 26 percent of all security audit findings
  - 32 percent of all security exception requests



# Questions

????????????????

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



# VITA Centralized/Shared ISO & Audit Services

Ed Miller, VITA

July 6, 2016



Virginia Information Technologies Agency



WHAT THE BEST COMPANIES DO



Virginia Information Technologies Agency

**CEB**

**Subscription**

*Corporate Executive Board*

**Ed Miller**

**IT Security Governance**



**WHAT THE BEST COMPANIES DO**



## CEB

- CEB is a best practice insight and technology company. They can provide you with information, i.e. tools, templates, case studies, etc. regarding what matters—and what works—in areas of IT risk management.
- We have renewed our commonwealth-wide subscription to the CEB Information Risk Council for another year.



## CEB

- To take full advantage of the CEB website, you need an account to login.
- All commonwealth employees should have access or be able to get access. The website address is [www.cebglobal.com](http://www.cebglobal.com)
- This subscription just got renewed, so give it a few days before you try.



Virginia Information Technologies Agency

# Agency IT Strategic Plan

Ed Miller  
IT Security Governance





# Agency IT Strategic Plans

- Agency IT Strategic Plans are due September 1st.
- In addition to your agency's normal planning, it is important to address the impact that the IT infrastructure sourcing effort will have on your agency
- The VITA website has helpful information & guidance on preparing the IT Strategic Plan (search for ITSP)



## Agency IT Strategic Plans

- CSRM will be issuing new ORIs (operational risk/issues) soon.
- Many ORIs will be triggered from the Annual IT Security Report. If your agency is RED on IT Audit or IT Risk Management, you will receive an ORI and you will need to address this in your ITSP.
- For any new ORIs and for any previously issued ORIs, please keep us updated with remediation steps. Let us know when it has been **remediated** and what has been done to remediate it.



# Centralized ISO & Security Audit Services

Ed Miller  
IT Security Governance





## General Assembly Session 2016

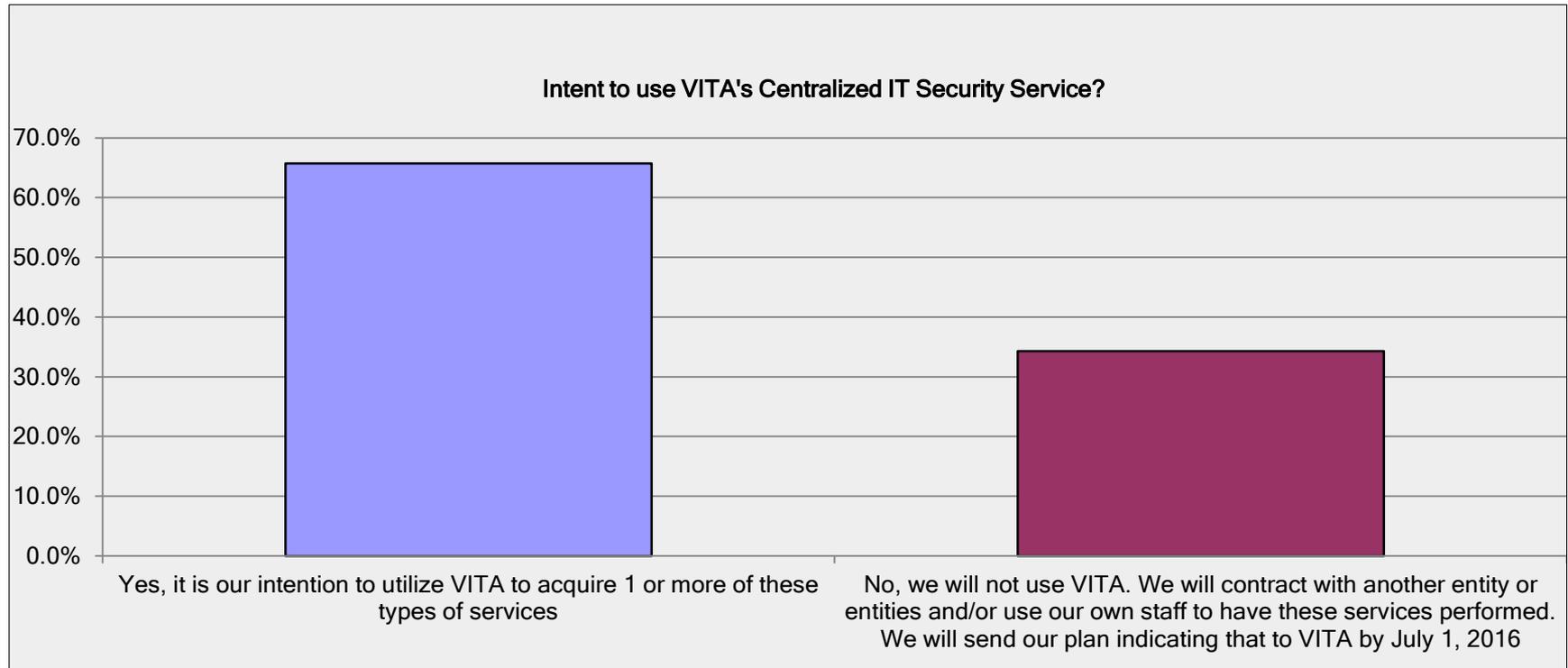
- HB30 was introduced to support the Governor's budget related to state agency cyber security.
- The bill B.1: "(VITA) shall operate an **information technology security service center** to support the information technology security needs of agencies .... "
- "Support for participating agencies shall include, but not be limited to, **vulnerability scans**, information technology **security audits**, and **Information Security Officer services**."



## Funding

- This bill includes funding to help agencies obtain resources to fix auditing and ISO issues.
- DPB has created a cost estimate model for each service (Audit or ISO).
- Your DPB analyst can help you determine your funding and how it is sourced to your agency.

# Participation in Shared Audit/ISO Services



- 65% yes, 35% no



## General Assembly Session 2016

**3. Agencies electing to participate in the information technology security service center shall enter into a memorandum of understanding with (VITA).**



## MOU/Work Request Form

- The MOU will be in the format of a Work Request Form, 1 form for Audit Services and 1 form for ISO Services.
- For the agencies wishing to use a service, CSRMM will pre-populate the form with your agency's estimated funding.
- Please contact your DPB analyst for information about your funding.
- The Work Request will be in effect for 3 years.



## Funding Model Example

The DPB funding model, using their spreadsheet formulas for the salary of an auditor and the # of hours an audit would take to complete, determined that VITA could do your agency's audits for \$X amount. Your agency's funding was then set for \$X amount and spread out over the next 3 fiscal years, approximately 1/3 of the total amount per year:

- $X = \$$  Total Amount of Funding Approved for Your Agency for a Service
- FY17:  $1/3(X)$
- FY18:  $1/3(X)$
- FY19:  $1/3(X)$

So regardless of when VITA performs the work, it takes us 3 years to recover the funds for doing the work. So if we audit in Year 1, you pay approximately 1/3 now, 1/3 in year 2 and 1/3 in year 3. If we don't audit until Year 3; you still pay 1/3 in year 1, 1/3 in year 2 and 1/3 in year 3. Either way, you get the audits for the same cost.

That's why this is a 3 year commitment.



## Funding Model Example

Whether you choose to use VITA's Centralized services or choose to contract with another vendor or use contingent labor, the funding is still available to your agency to use for this purpose.

Again, please contact your DPB analyst for specific information.



## General Assembly Session 2016

“4. **Non-participating agencies *shall*** be required by **July 1** each year to ***notify*** the Chief Information Officer of the Commonwealth ***that the agency has met the requirements*** of the Commonwealth's **information security standards**. If the ***agency has not met the requirements*** of the Commonwealth's information security standards, the agency ***shall report*** to the Chief Information Officer of the Commonwealth ***the steps and procedures*** the agency is implementing in order to satisfy the requirements.”



## Non-Participating Agency Plans

If you are not using the service, VITA is required to collect your plan for bringing your agency into compliance.

The simplest way for everyone is to just re-confirm your agency's *IT Security Audit Plans* and *IT Risk Assessment Plan*.

The difference is that now CSRM is going to have to actively monitor agency progress on their plans.

So, the plan has to be realistic and workable.



## Non-Participating Agency Plans

The newly updated IT Security Audit Plans and Risk Assessment Plans are essentially the same as the old ones.

There is now a drop-down box for selecting the “auditor” or “assessor” that will be used: Contractor, Internal Staff, APA, etc.

Note: If you select APA for audits, we will want confirmation from the APA when you submit the audit report that the audit meets the requirements of an IT Security Audit per SEC501 and SEC502. We want to know exactly what was in scope.



## Centralized Services Directors

We finally were approved for a Director of Centralized IT Security Audit Services and a Director for Centralized ISO Services.

Look for those positions to be posted very soon.



## Next Steps

- For agencies that have noted their intention to use the Centralized Services, we are in the process of getting their MOU/Work Request Forms finalized.
- For agencies that do not intend to use the Centralized Services, they are currently sending us their plans to achieve compliance with the commonwealth's IT Security Standards. If you have not done so, please do it.

# Any Questions?





Virginia Information Technologies Agency

# Upcoming Events





## Future ISOAG

**August 3, 2016 1:00 - 4:00 pm @ CESC**

**Speakers: June Jennings, OSIG  
&  
Irina Piven, Federal Reserve Bank**

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2016***



## Future ISOAG

**August 31, 2016 1:00 - 4:00 pm @ CESC**

**Speakers: Paul Grassi, NSTIC**

**&**

**Alyson Intihar, RSA**

**This meeting will be in place of the  
September Meeting**

**ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2016**



## IS Orientation

**When: Thursday, September 29, 2016**

**Time: 10:00 am to 12:00 pm**

**Where: CESC , Room 1221**

**Register here:**

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

# ADJOURN

## THANK YOU FOR ATTENDING

