



Virginia Information Technologies Agency

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

November 7, 2012



# ISOAG November 2012 Agenda

- |      |                                       |   |
|------|---------------------------------------|---|
| I.   | Welcome & Opening Remarks             | Michael Watson, VITA                        |
| II.  | UVA IT Audit & Special Investigations | Kevin Savoy, UVA                            |
| III. | BIA Overview                          | Ed Miller, VITA                             |
| IV.  | COV IS Council Committees             | Michael Watson, VITA                        |
| V.   | Data Points                           | Michael Watson, VITA                        |
| VI.  | Upcoming Events & Other Business      | Michael Watson, VITA                        |
| VII. | Partnership Update                    | Bob Baskette, VITA<br>and Michael Clark, NG |

*UVA*

*IT Special Investigations /  
Forensics*

**Kevin Savoy, CPA, MBA, CISA, CISSP**  
*Director of Hospital and IT Audits*

# Agenda

- ▶ Why forensics
- ▶ Our typical procedures
- ▶ Pornography
- ▶ Fraud
- ▶ Cyber hacks
- ▶ Working with law enforcement
- ▶ Going to court
- ▶ Conclusion

# UVA

- Founded 1819 by Thomas Jefferson
- 1,700 acres
- \$2 billion budget
- 21,100 Students
- Number 2 public University in the US (US News & World Report)
- 577 bed teaching hospital
- 18,000 plus employees
  
- As you can see UVA is a small city in and of itself and requires the needs of special investigations and forensics.

## UVA Special Investigations/Forensics

- ▶ Per UVA policy Internal Audit handles fraud, pornography, and sensitive administrative investigations.
- ▶ Per UVA policy UVA Police handle criminal investigations.
- ▶ Per policy ITS handles investigations of cyber attacks and compromise of IT system resources.
- ▶ In reality Internal Audit has been involved in all of the above types of cases as all three units work with one another....

## Internal Audit

- ▶ We have performed over 100 IT forensic cases.
- ▶ The cases have involved pornography, fraud, theft, personnel policy infractions, cyber theft of funds, and more.
- ▶ We have received information that leads to investigations from several source such as employees, family members of employees, management, the general public, law enforcement, and private industry

## Typical Procedures

- ▶ An investigation is generated by a tip or request
- ▶ Per policy, Internal Audit must receive permission from the VP over the computer resource in order to review the hard drives and memory
- ▶ The decision must be made on whether a particular investigation can proceed in the open or must it be handled in a clandestine manner (the majority are handled clandestine due to sensitivity of the investigation and to protect innocent individuals)

## Typical Procedures **IMPORTANT**

- ▶ Internal Audit treats all special investigations and forensics as if the case may go to court.
- ▶ Even minor administrative actions can often have unforeseen consequences such as lawsuits.
- ▶ So that said. We use standard written procedures and “check sheets” we have developed for our work and document as we go.

## The gist of what we do....

- ▶ Determine who the closest person to the computers is that we can trust to keep our activities confidential (could be a supervisor, could be a Department Chair, could be a Dean, Provost etc...)
- ▶ Determine when we will go in to make copies of hard drives and who will give us physical access to computers. Usually we go in late at night or middle of the night....
- ▶ We take photos of all equipment and of the office, lab, etc.
- ▶ Have chain of custody form signed by person giving us access

## The gist of what we do

- ▶ We remove hard drive(s) and make binary copies to BRAND NEW hard drives
- ▶ Use Logicube Quest copier that provides a hash tag report and adapters for SATA and IDE drives.
- ▶ Copying a Terabyte hard drive will take a few hours so bring some work or a book!!
- ▶ We then close up the system, place all furniture back to match our photos taken earlier and depart.

## The gist of what we do

- ▶ The copy of the drive is then taken to the office where we make a second working copy for our forensics.
- ▶ The original copy is placed into a safe that only I and the Chief Audit Executive has access to
- ▶ We then proceed to review the second copy of the hard drive(s)
- ▶ For Windows based systems we will drop into DOS to run “find commands”, the same for Linux and so forth...
- ▶ After running commands at the operating system level we then use Encase Forensics.....

## The gist of what we do

- ▶ We document every procedure we do along with pertinent information such as time stamps to files we are interested in
- ▶ We conclude the investigation which results in a memo of our findings that goes to the President, other senior management, UVA Police and ITS.
- ▶ The end results have been arrests, employee dismissals, and employee administrative actions...

## Thars gold in them thar hills

- ▶ Most systems today keep a myriad of information that point to how a workstation or laptop was used.
- ▶ Most users are unaware of many of the standard features of Windows or Apple or Linux that track usage
- ▶ Some savvy users may hope that you don't know this also

# Many topics

- ▶ Hidden files
- ▶ Internet viewing and downloading history
- ▶ Last files accessed
- ▶ Last programs run
- ▶ File/Folder search history
- ▶ Temporary files

## Hidden files

- ▶ Some files are so well hidden that they will not show up in Windows explorer or MS-DOS directory listing.
- ▶ These reside in blind directories..but as long as you know the file names which are listed in the following slides you can find them.

# Internet files

## ▶ Internet cookies

- *Cookies are placed on your machine by websites to supposedly make your next visit to that website more enjoyable!*

## ▶ Internet history

- *Keeps a list of where you have been by address (URL)*

## ▶ Temporary internet files

- *Is where parts of a website are cached in your computer to make it quicker to reload next time you visit that site*

# Temporary Files

- ▶ Windows creates a myriad of temporary files during the course of operations (usually when a new program is installed etc)
- ▶ These programs are supposed to delete these files when done but often do not.
- ▶ Use search feature for key word “temp” to find many of these folder locations
- ▶ Often these files are there even if the user deleted the programs that spawned the temporary files

## The old standby

- ▶ Recycle bin if not emptied still has deleted files.
- ▶ 3rd party software available to recover deleted files and erase the files we have gone over in this presentation.

## Yeah I know what you are saying...

- ▶ The past few slides are based on ancient history but the files are still out there, just under different folders (some protected system folders some not)
- ▶ Encase is what we use for the most part after reviewing in DOS or Linux.
- ▶ We are usually looking for pictures, movies, chats, searches, temp files, anything that is pertinent to the case

# Pornography Investigations

- ▶ Commonwealth law and UVA Policy prohibit state employees viewing and downloading of sexually explicit material via state resources.
- ▶ The Audit Department does not go out of its way to look for this activity. We act when it is reported to us.
- ▶ Must have permission from the President or Vice President of the area to review someone's computer activities.

# Morality Police?

- ▶ I and my staff are not here to enforce morality.
- ▶ What employees do at home (unless criminal) that does not effect UVA is none of my business.

## A couple of years ago

- ▶ Ten investigations of staff / faculty.
- ▶ Nine (9) employees have left the institution.
- ▶ Egregious cases where employees were downloading thousands of pictures/movies.
- ▶ Some using peer-to-peer file sharing with users around the world.
- ▶ Some using “pagesucker” software to download whole websites.

## What are the risks?

- ▶ Potential for Hostile Workplace lawsuits.
- ▶ Drain on IT resources (bandwidth, drive space).
- ▶ Pornography is infamous as a means to entice users to sites that are ripe with security risks such as viruses, Trojan horse backdoor software etc.
- ▶ Criminal activity such as child pornography.

## CODE OF VIRGINIA 2.2-2827.

## Restrictions on state employee access to information infrastructure.

- ▶ Except to the extent required in conjunction with a bona fide, agency-approved research project or other agency-approved undertaking,
- ▶ **no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content.**
- ▶ Agency approvals shall be given in writing by agency heads, and any such approvals shall be available to the public under the provisions of the Virginia Freedom of Information Act (§ [2.2-3700](#)).

## Degrees of Pornography

- ▶ Audit Department realizes that evidence of sexually explicit material can be left behind from accidental hit of a sexually explicit web site or received unsolicited via e-mail.
- ▶ We factor that into our investigations.

## Technical Issues – Peer to Peer File Sharing (P2P)

- ▶ University environment is a sharing environment. We do NO content filtering.
- ▶ P2P allows users to download parts of files from one another.
- ▶ Your computer may have 10 percent of a file the rest of the world is looking for. Thus you become a server for those users.

## P2P continued

- ▶ It works great and was designed so everyone would not have to hit just one site to download a movie or whatever and thus overwhelm it.
- ▶ Two individuals were using it to collect and distribute adult pornography from UVA.
- ▶ It can be made into an automated process where you type the fetish that you are interested in and you begin to download and trade files with other Internet users.

## P2P risks

- ▶ Potential is there to download and trade movies and pictures that you are unaware of.
- ▶ In essence, UVA or any business could become a server for child pornography if not careful.

## Page Sucker and Vampire

- ▶ Examples of software that allow one to download the majority of the contents of a web site so that it is stored and viewed off line.
- ▶ One individual found to be doing this.
- ▶ The user assumption is that they will not be caught through Internet logs.

## Generic log ins

- ▶ Many computers have generic logins so that it becomes hard to track offending parties.
- ▶ However, wherever possible it is best to institute individualized logins for accountability. (No one likes to be blamed en masse for another user's indiscretions).

## Local Support Partner (LSP's role)

- ▶ A few cases were brought to our attention when an LSP went to his manager to state that a user's system had sexually explicit material on it.
- ▶ In those case's the employee complained that his system was slow. (That will happen when you store 1000's of porn movies and pictures on your system!!)

## LSP's role

- ▶ According to the UVA General Counsel's office, employees of the University generally are not at risk of personal liability for reporting potential legal and policy violations, if following set policy in good faith.

## Other uses for monitoring

- ▶ In one of our cases an investigation was non-conclusive. Some evidence pointed to validation of the anonymous allegation.
- ▶ Due to the seriousness of the allegation, the employee was told that a condition of their continued employment would be the monitoring of their computer usage.

# Virginia DHRM Policy

- ▶ *No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access...*

## Virginia DHRM Policy continued

- ▶ ...Agencies have a right to monitor any and all aspects of their computer systems including, but not limited to, sites, instant messaging systems, chat groups, or news groups visited by agency users, material downloaded or uploaded by agency users, and e-mail sent or received by agency users. Such monitoring may occur at any time, without notice, and without the user's permission...

# Problems with physical keylogging

- ▶ Can be detected by users if they snoop around their USB connections.
- ▶ Must place on the system without arousing suspicion.

# Keylogging / Monitoring Software

- ▶ Generally undetectable software that hides deep in memory while running.
- ▶ Combines key strokes with images.
- ▶ Very Low resource overhead so that user does not notice degradation in performance.
- ▶ Example that we use:
  - Spector Pro

## Who should know?

- ▶ We inform as few employees as possible when monitoring. This avoids rumors and innuendos from spreading.
  - Always executive management is told
  - Sometimes the user's supervisor is told
  - Never are peers told

# Confidentiality

- ▶ Monitoring often encompasses aspects of an employee's **personal** life that may or may not be pertinent to the investigation.
- ▶ Confidentiality is a must. Only a select few in the Audit Department working on the case are allowed to read monitoring results.
- ▶ In addition, all materials follow a chain of custody form. All materials are placed in a locked safe, behind the director's locked office door, behind a pass key entrance of the audit department.

## In conclusion

- ▶ We do not go out of our way to monitor employees.
- ▶ It is one of the harder aspects of our job emotionally.
- ▶ However if done professionally you will often be complimented for aiding in resolving embarrassing personnel issues.

# Fraud and Cyber Hacks

- ▶ We have worked with law enforcement on thefts, fraud, and cyber theft.
- ▶ Rash of laptop thefts where we pinpointed access point and building of a stolen computer. Went to court on this one.

## Cyber Hack at UVA Wise

- ▶ Our comptroller's wire transfer fund was hacked.
- ▶ Hackers placed Zeus key logging software on machine
- ▶ Hacker captured login credentials to bank and wired \$1M to China
- ▶ We worked on site and with FBI and Internal Revenue Service.
- ▶ Ultimately the funds were “refunded”

## Working with law enforcement

- ▶ They need to gain your trust. That is done by showing them what you do.
- ▶ Their aim is often the same as yours but often more intense
- ▶ Prepare every case as if it could go to court
- ▶ Keep a constant line of communication and be prepared to turn investigation over to them once it crosses the line to criminality (child pornography, theft, etc)
- ▶ Often we have done work administratively that law enforcement can't do easily, then turned it over if a potential crime exists.

## Going to court

- ▶ Just state the fact. Don't stretch and make suppositions unless asked and tell the judge and jury when you are not sure.
- ▶ Have everything documented
- ▶ Have used proper collection and evidence storage techniques
- ▶ Be certified as much as possible, CISA, CISSP, GCFA etc.
- ▶ Be prepared to be challenged as to your expertise and do not be offended
- ▶ Trials by judge usually are more strict than jury trials

## Conclusion

- ▶ Determine who in you agency will do forensics (could be and outside entity if you are small or do not have expertise)
- ▶ Determine proper techniques and document your results
- ▶ At UVA we are creating a hotshot team between Audit, ITS, and UVA PD so that we can work on projects in tandem when necessary or cover for one another if someone is unavailable.....
- ▶ Encryption is going to make this a whole lot harder
- ▶ Questions??????? or email me [Savoy@virginia.edu](mailto:Savoy@virginia.edu)



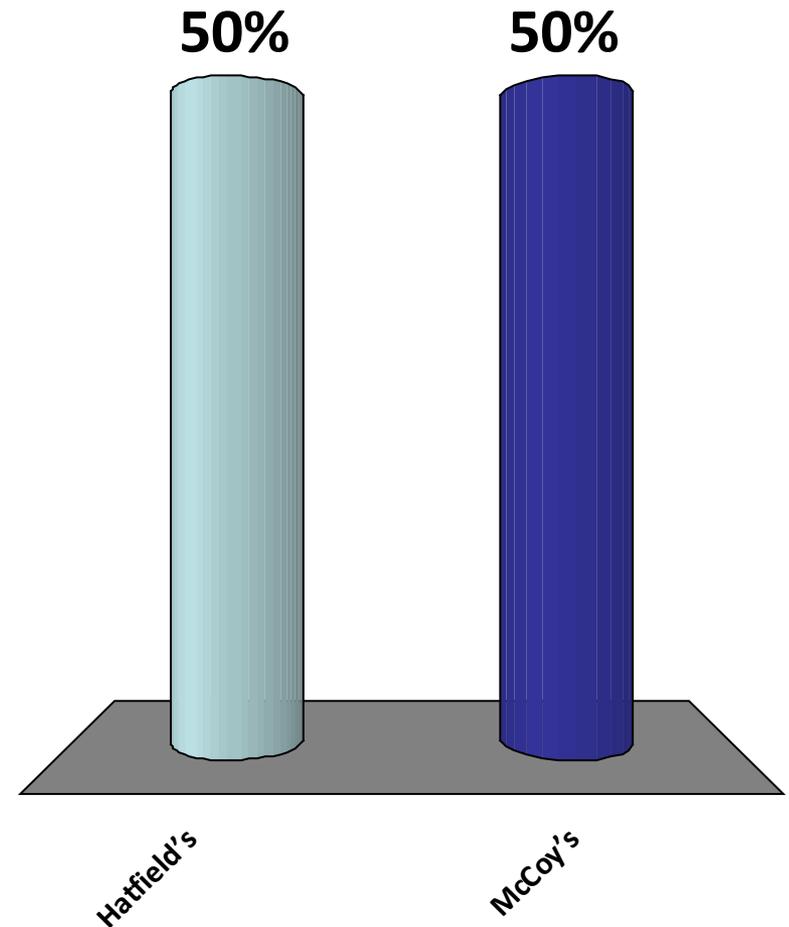
*Virginia Information Technologies Agency*

# Business Impact Analysis Overview

Ed Miller  
CISA CIA CISM CIPP/IT

# Please select a Team.

1. Hatfield's
2. McCoy's



OUR COMPUTERS ARE DOWN,  
SO WE HAVE TO DO  
EVERYTHING MANUALLY...



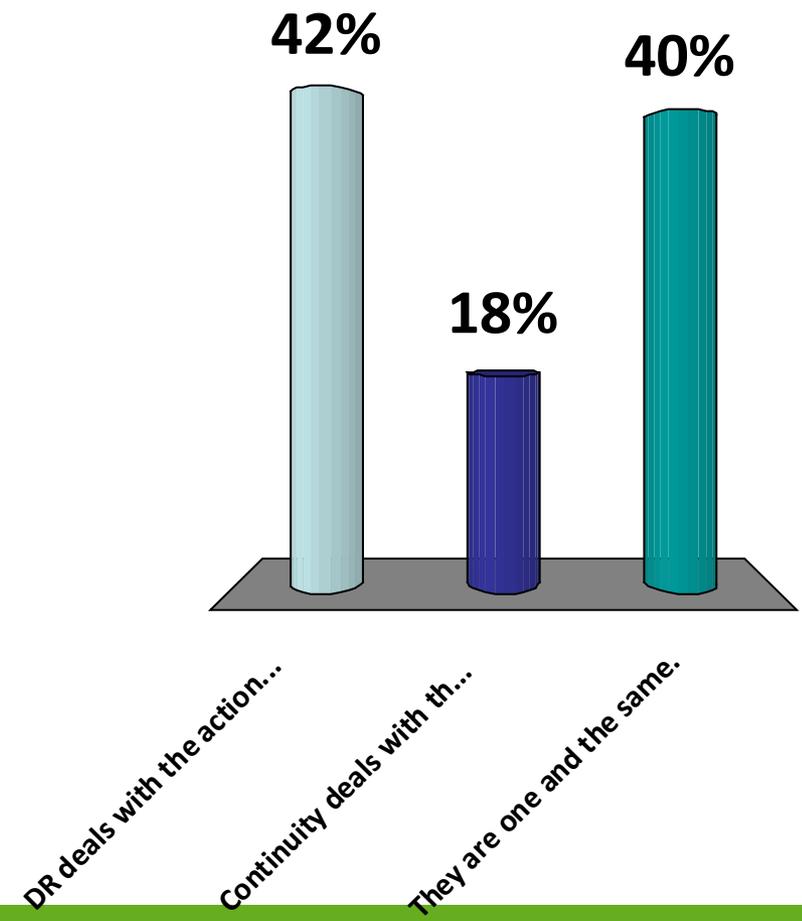


# Contingency Planning

- NIST SP 800-34
  1. Develop contingency planning policy
  2. Conduct the **BIA**
  3. Identify preventative controls
  4. Create contingency strategies
  5. Develop an information system contingency plan
  6. Ensure plan testing, training and exercise
  7. Ensure plan maintenance

# What is the difference between continuity of operations & disaster recovery?

1. DR deals with the actions to take place immediately following a disaster, Continuity deals with the actions needed to take place to keep operations running over a longer period of time.
2. Continuity deals with the actions to take place immediately following a disaster, DR deals with the actions needed to take place to keep operations running over a longer period of time.
3. They are one and the same.





## How does contingency planning affect security?

- Security pillars: C-I-A
  - Confidentiality
  - Integrity
  - Availability
- Contingency planning *directly* supports **availability**. Confidentiality and integrity are still important.



## Industry Standards & Frameworks

- ISO 27001: Requirements for *Information Security Management Systems*. Section 14 addresses business continuity management.
- ISO 27002: *Code of Practice for Business Continuity Management*.
- ISO 22301: "*Societal security-Preparedness and Continuity Management Systems-Requirements*", specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your recovery from disruptive incidents.



# Industry Standards & Frameworks

- NIST 800-34
  - *Contingency Planning Guide for Information Technology Systems.*
  - Seven step process for BCP and DRP projects
  - From U.S. National Institute for Standards and Technology
- NFPA 1600
  - *Standard on Disaster / Emergency Management and Business Continuity Programs*
  - From U.S. National Fire Protection Association



## Industry Standards & Frameworks

- ASIS (American Society for Industrial Security): *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use Standard.*
- FEMA: *Federal Executive Branch National Continuity Program & Requirements; Federal Continuity Directives (FCD1/FCD2)*



# What is a BIA?

Per *SEC501-06* and also *SEC501-07*

- **2.2. Business Impact Analysis**

Business Impact Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions.

**Note:** The requirements ... address only the IT and data aspects of BIA and do not require agencies to develop a BIA separate from the BIA that could be used to develop an agency's Continuity of Operations Plan (COOP). Agencies should create a single BIA that meets both the requirements of this Standard and can be used to develop the agency COOP.



## What is a BIA?

- Per *VDEM Guide to Identifying Mission Essential Functions (MEFs) and Business Process Analyses (BPAs)*
- A Business Impact Analysis (BIA) is a useful tool in identifying an agency or institution's PBFs. The BIA process is beyond the scope of this guide; however, you may refer to your agency or institution's internal standard procedures...



## Goals of the BIA

- 1. Criticality Prioritization:** every critical business unit must be identified & prioritized and the impact of a disruptive event must be evaluated.
- 2. Downtime Estimation:** what is the maximum tolerable period of time a critical process can remain interrupted.
- 3. Resource Requirements:** identification of the resources & inter-dependencies required to support the critical function.

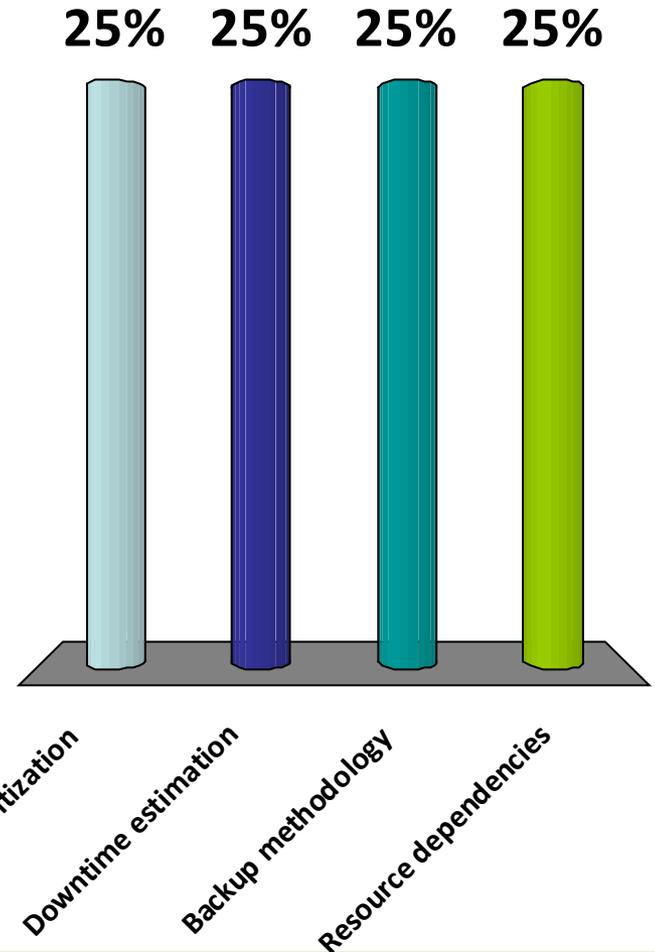


## Steps of a BIA

- In general, most BIA processes will follow these steps:
  - **Identification.** Identify what the the function is/does. Look at org charts, identify business units, people, processes.
  - **Impact assessment.** Analyze the impact if the function were lost: financial loss, operational expenses, public confidence loss, life/safety loss, legal/regulatory impacts, or sensitive data loss.
  - **Acceptable downtime.** Document how long the function can be disrupted before losses occur.
  - **Resource requirements:** What resources, IT systems or other dependent processes relate to this function.
  - **Documentation.** Summarize & document this information for management review and approval.

# Which of the following is not a goal of a BIA?

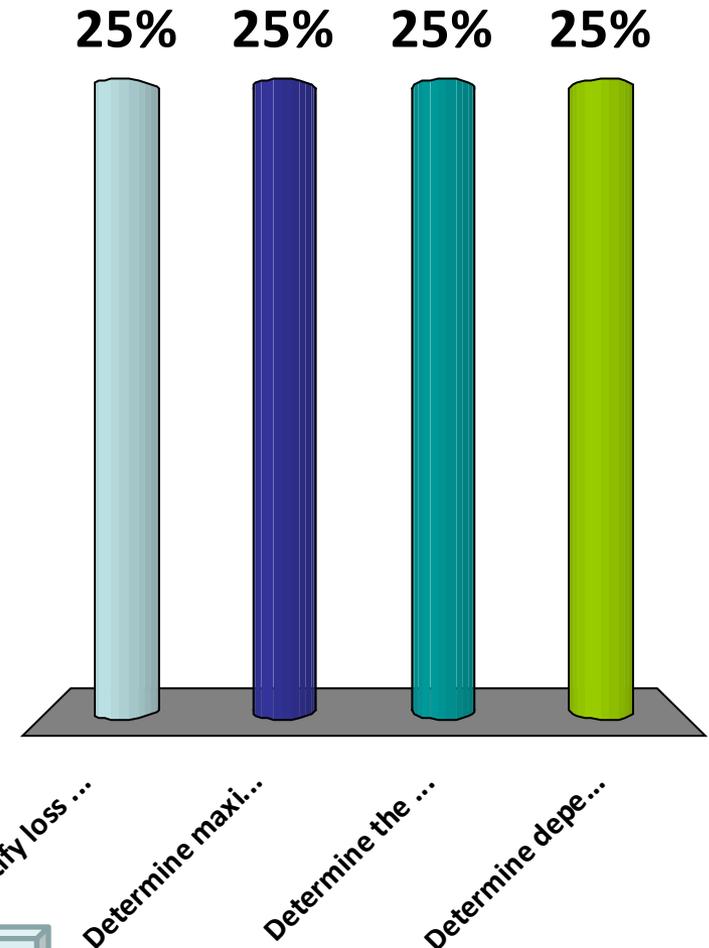
1. Criticality prioritization
2. Downtime estimation
3. Backup methodology
4. Resource dependencies



**Answer Now**

# What is not a function of a BIA?

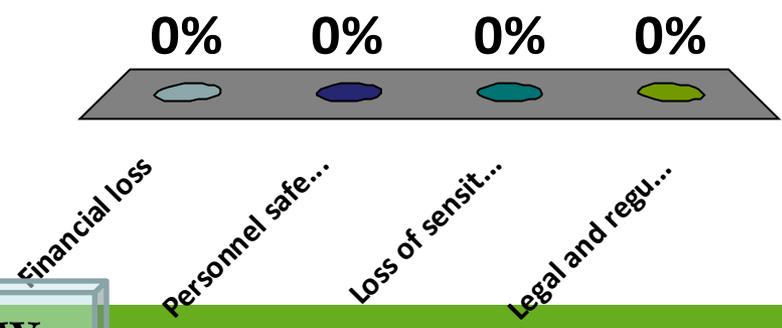
1. Quantify loss due to outage
2. Determine maximum tolerable downtime
3. Determine the types of incidents that may cause a disruption
4. Determine dependent resources



**Answer Now**

# Which of these has the highest impact in a disaster?

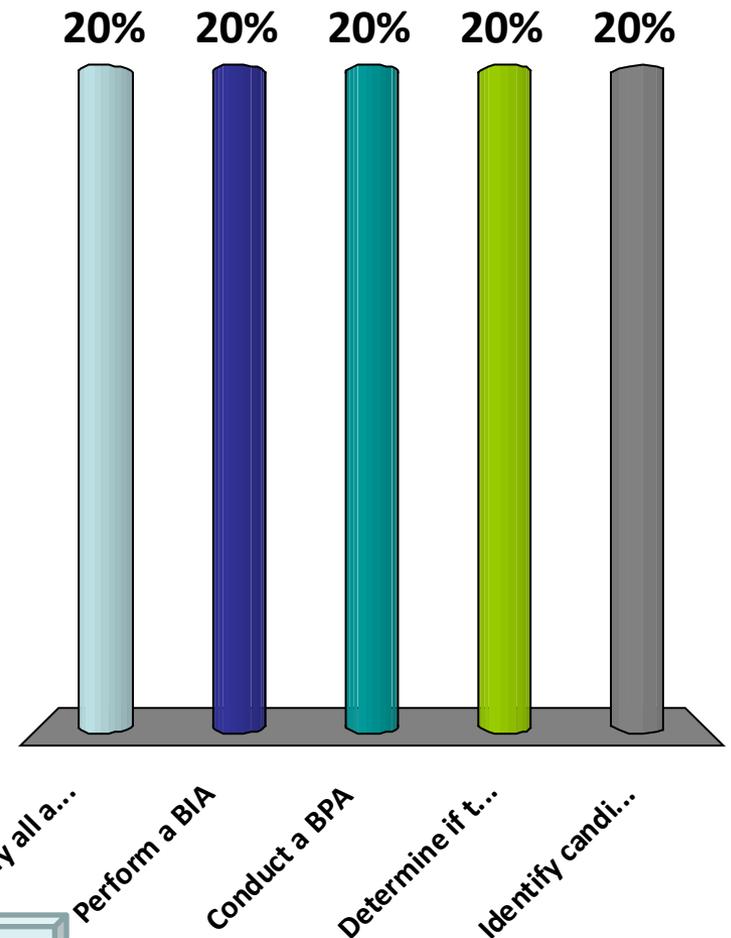
- 1. Financial loss
- 2. Personnel safety
- 3. Loss of sensitive data
- 4. Legal and regulatory implications



Answer Now

# What is the first step in developing a Continuity Plan?

1. Identify all agency functions
2. Perform a BIA
3. Conduct a BPA
4. Determine if the function is a MEF or PBF
5. Identify candidate MEF's



**Answer Now**

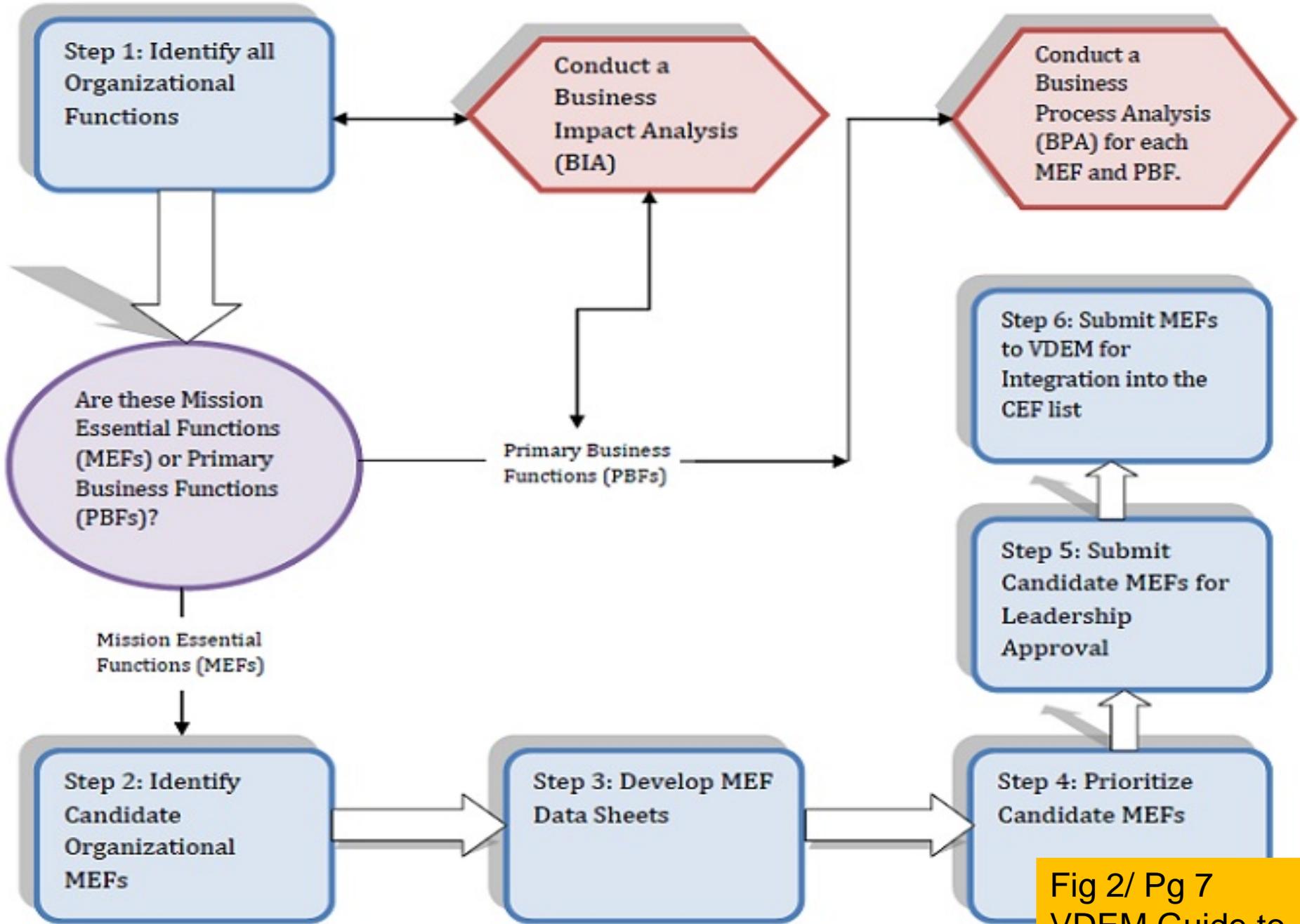


Fig 2/ Pg 7  
VDEM Guide to  
MEF and BPA



# Team Scores

0	Team 1
0	Team 2
0	Team 3
0	Team 4
0	Team 5



# Participant Scores

0	Participant 1
0	Participant 2
0	Participant 3
0	Participant 4
0	Participant 5

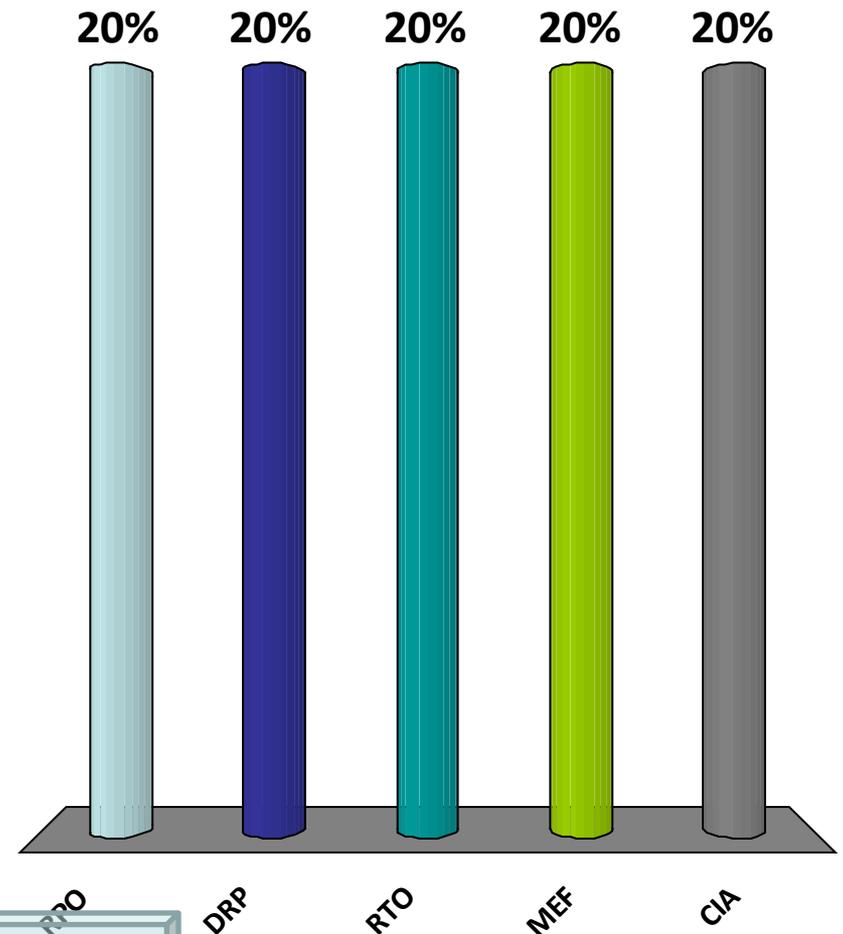


## Fastest Responders (in seconds)

- 0 Participant 1
- 0 Participant 2
- 0 Participant 3
- 0 Participant 4
- 0 Participant 5

An agency's BIA has determined that a critical IT system must be back online in 24 hours. What best describes that?

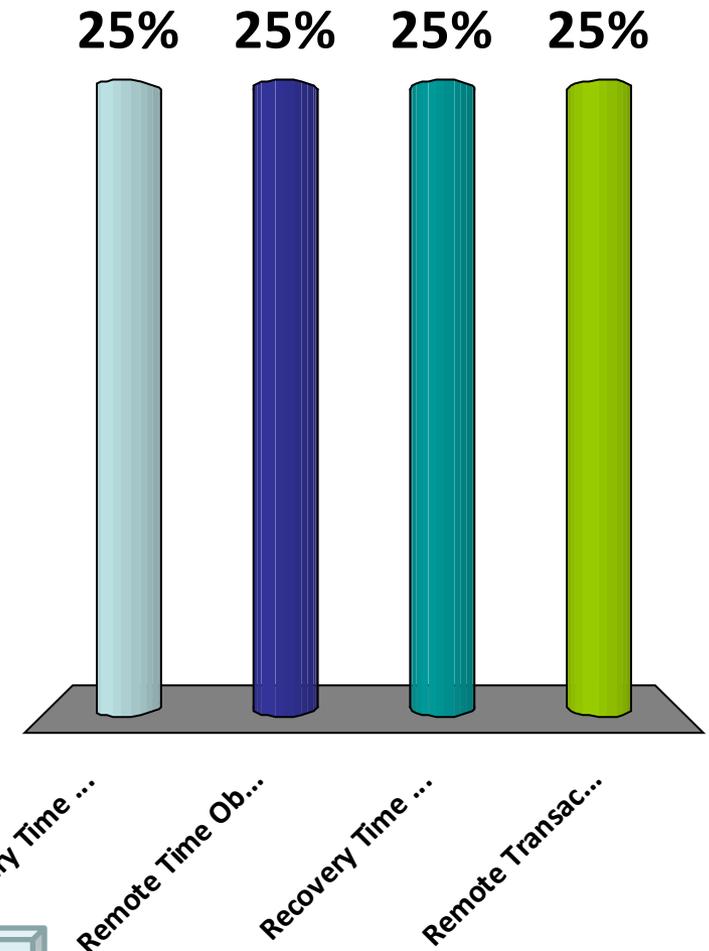
- 1. RPO
- 2. DRP
- 3. RTO
- 4. MEF
- 5. CIA



Answer Now

# What does RTO stand for?

1. Recovery Time Operation
2. Remote Time Objective
3. Recovery Time Objective
4. Remote Transaction Operation



**Answer Now**



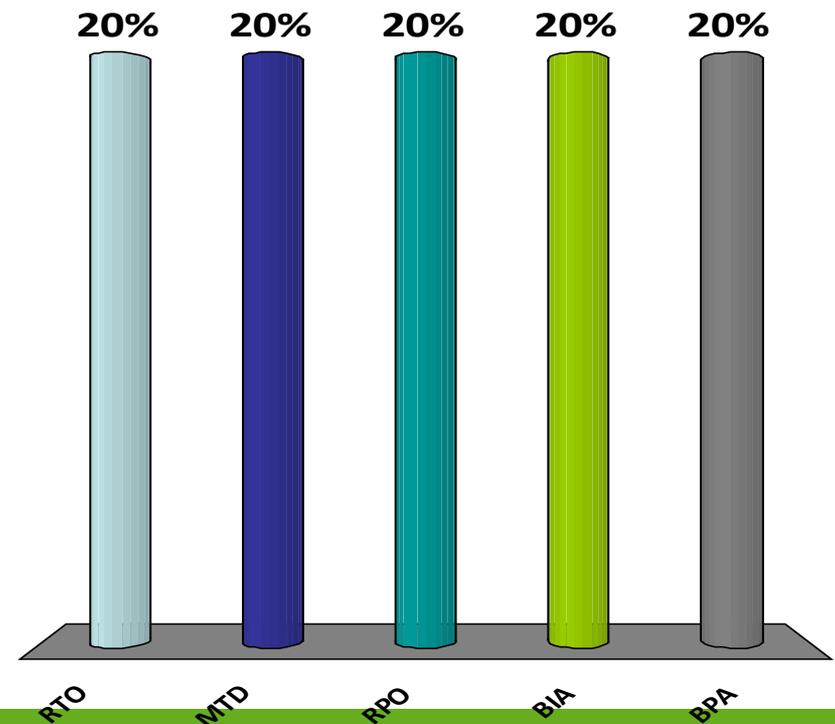
## RTO – Recovery Time Objective

- The RTO is the period of time in which systems, applications or functions must be recovered after an outage in order to avoid unacceptable consequences associated with a break in business continuity.

# The point in time to which data must be restored in order to resume processing transactions ?

(Its directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup)

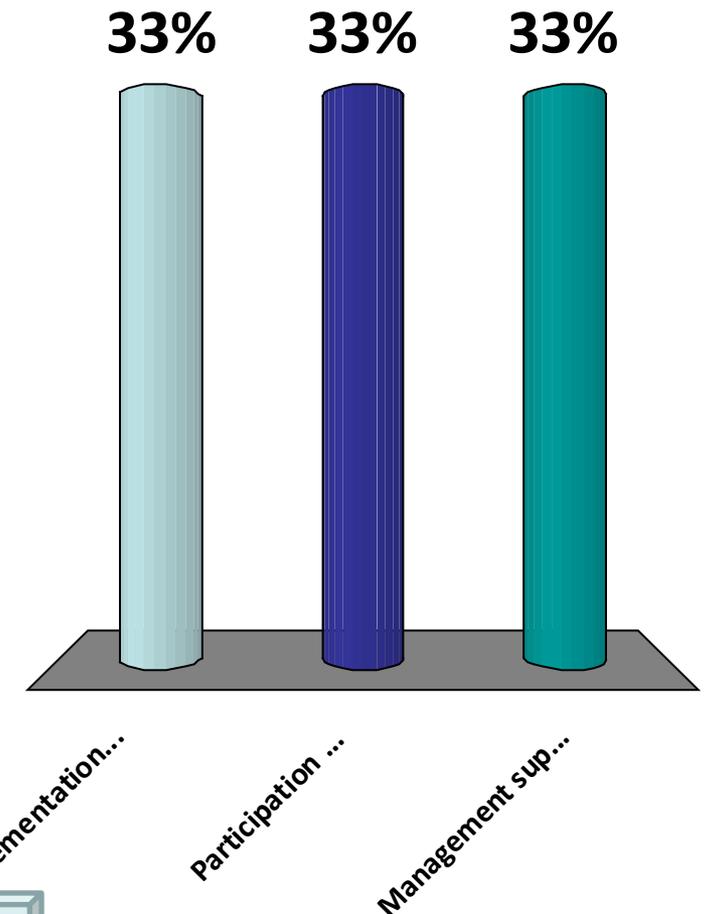
1. RTO
2. MTD
3. RPO
4. BIA
5. BPA



Answer Now

# What is the most crucial element of developing a BIA?

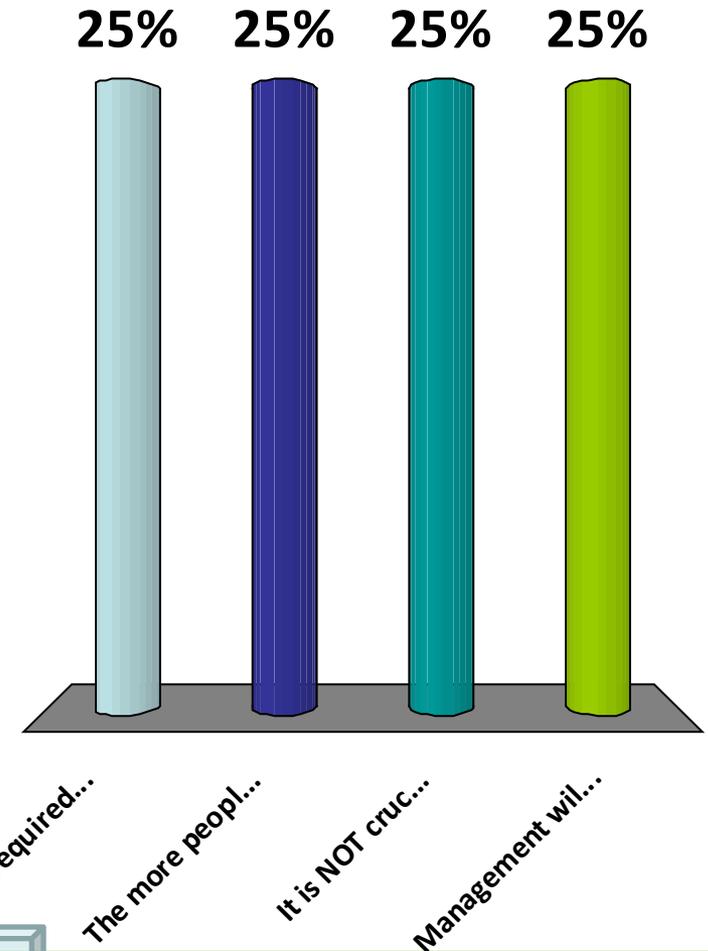
1. Implementation, testing & follow-through
2. Participation by every business unit
3. Management support



Answer Now

# During development of the BIA, a high degree of interaction & communication is crucial to the process. Why?

1. It is required by SEC 501
2. The more people talk about it, the more awareness will increase
3. It is NOT crucial & should not be interactive as it will most affect operations
4. Management will more likely support it



**Answer Now**



## What's is a BPA?

- BPA – Business Process Analysis
- A BPA is a systematic method of identifying and documenting all of the elements necessary to accomplish each MEF and PBF.
- While MEF's and PBF's identify *what* needs to be accomplished, the BPA identifies *how* it is accomplished.

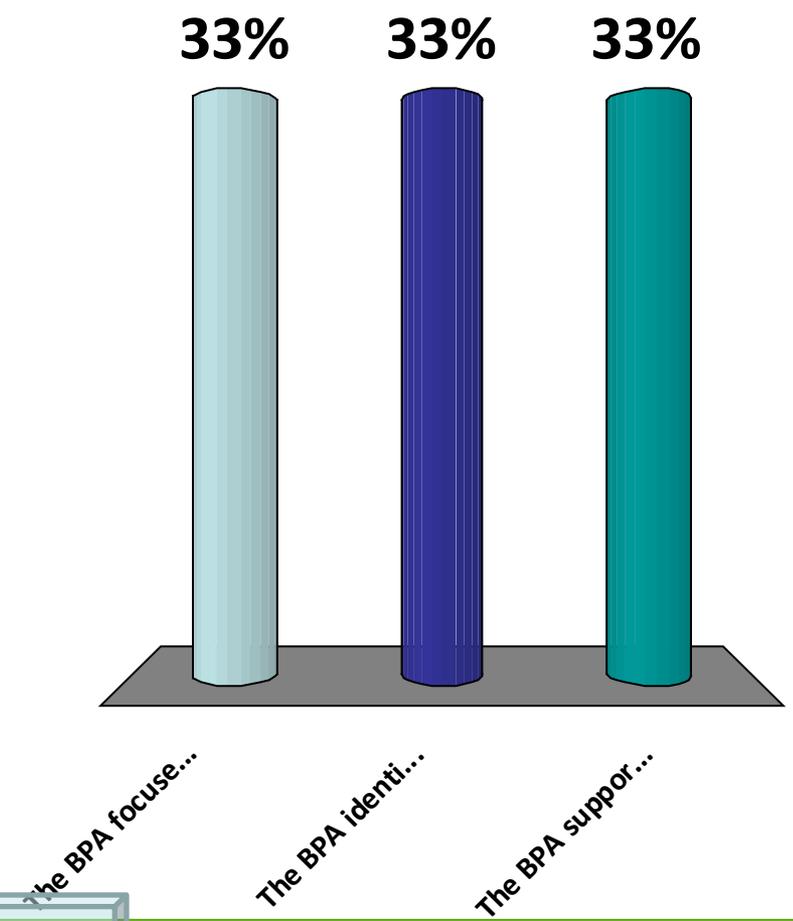


## Keep in mind

- MEF's and their supporting PBF's have high availability requirements. They are not deferrable.
- BIA's should be able to map over to your MEF and PBF worksheets.

# VDEM requires a Business Process Analysis (BPA). What is the main difference between a BPA and a BIA?

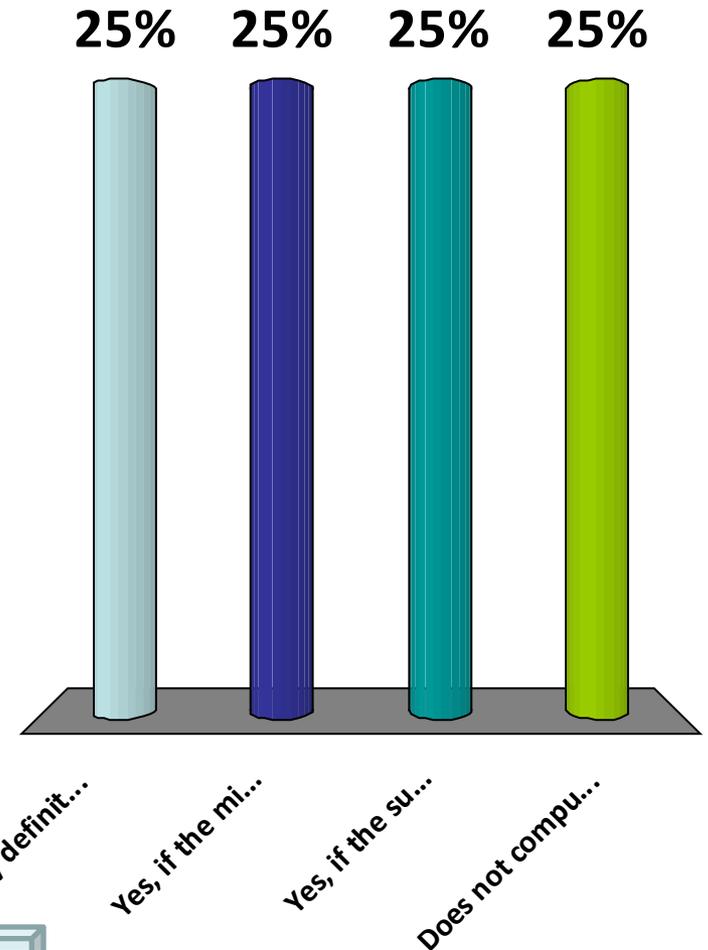
1. The BPA focuses on how to accomplish the function, the BIA focuses on the consequences of not doing the function.
2. The BPA identifies PBF's (primary business functions), while the BIA identifies MEF's (mission essential functions)
3. The BPA supports the function prioritization for the COOP, while the BIA supports IT resource prioritization for the DR Plan.



**Answer Now**

# Can you have non-essential mission functions?

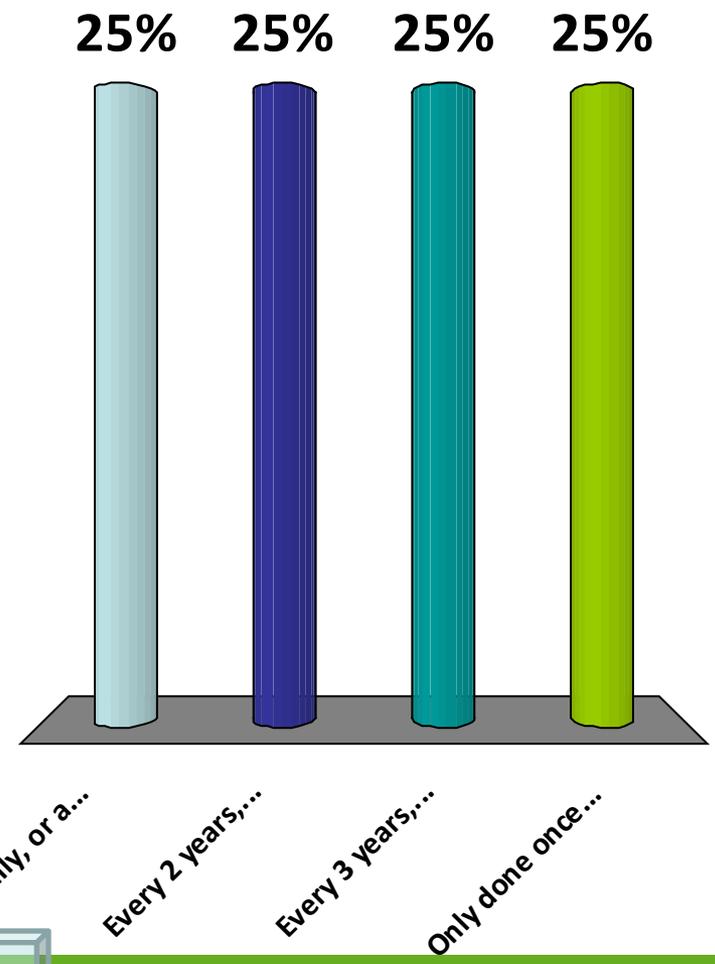
1. No, by definition a mission function is essential
2. Yes, if the mission function can be deferred
3. Yes, if the supporting PBF's are not essential
4. Does not compute



**Answer Now**

# How often do BIA's need to be revised?

1. Annually, or as needed.
2. Every 2 years, or as needed
3. Every 3 years, or as needed
4. Only done once and then start over



**Answer Now**



# Participant Scores

0	Participant 1
0	Participant 2
0	Participant 3
0	Participant 4
0	Participant 5



## Fastest Responders (in seconds)

- 0 Participant 1
- 0 Participant 2
- 0 Participant 3
- 0 Participant 4
- 0 Participant 5



# Racing Leader Board



# Team Scores

0 Team 1

0 Team 2

0 Team 3

0 Team 4

0 Team 5



## Q & A

- Thank you



*Virginia Information Technologies Agency*

# COV IS Council Committees

Michael Watson  
Chief Information Security Officer



# COV IS Council Committees

## Proposed Committees for 2013

1. **Scope & Percentage of IT Budget**
2. **IT Standards & Policies**
3. **Repository for IT Projects/Policies/Guidelines**
4. **IS Conference**
5. **ISO Manual**
6. **IPv6**
7. **BYOD Strategy**
8. **IT Legislature**



## COV IS Council Committees

### Committees will consist of:

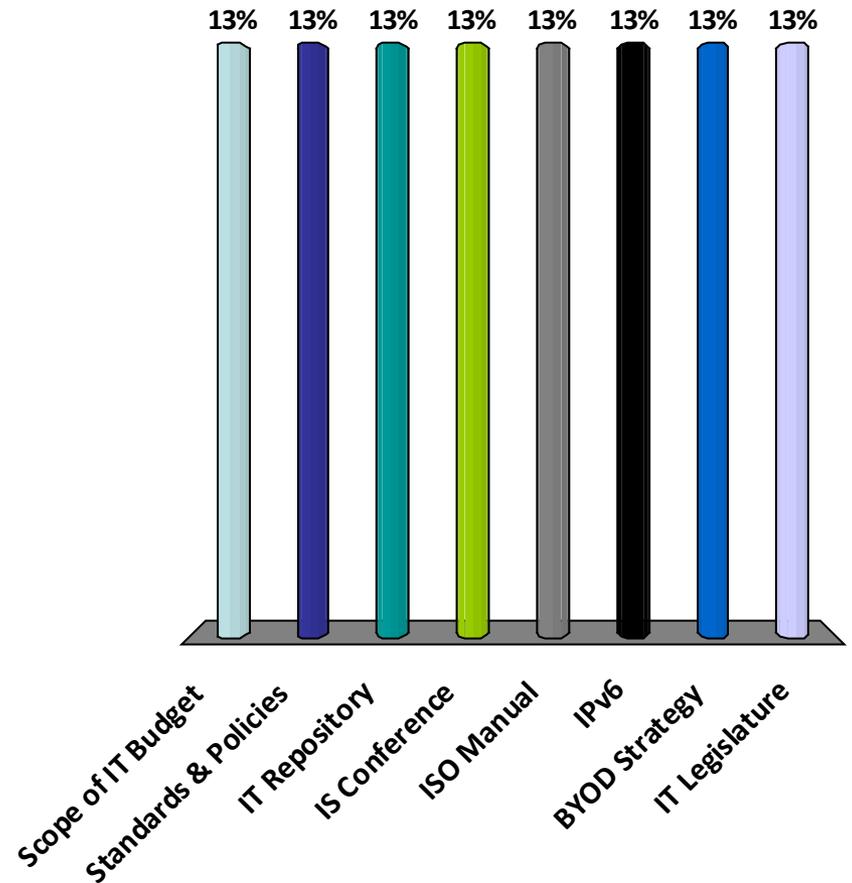
- \* 5 – 10 people
- \* Chairmen will be IS Council Members
- \* Will Meet Every Other Month
- \* Deliverables will be achieved in 6 –12 months



# Choose Top 5 Committees

In order of Preference

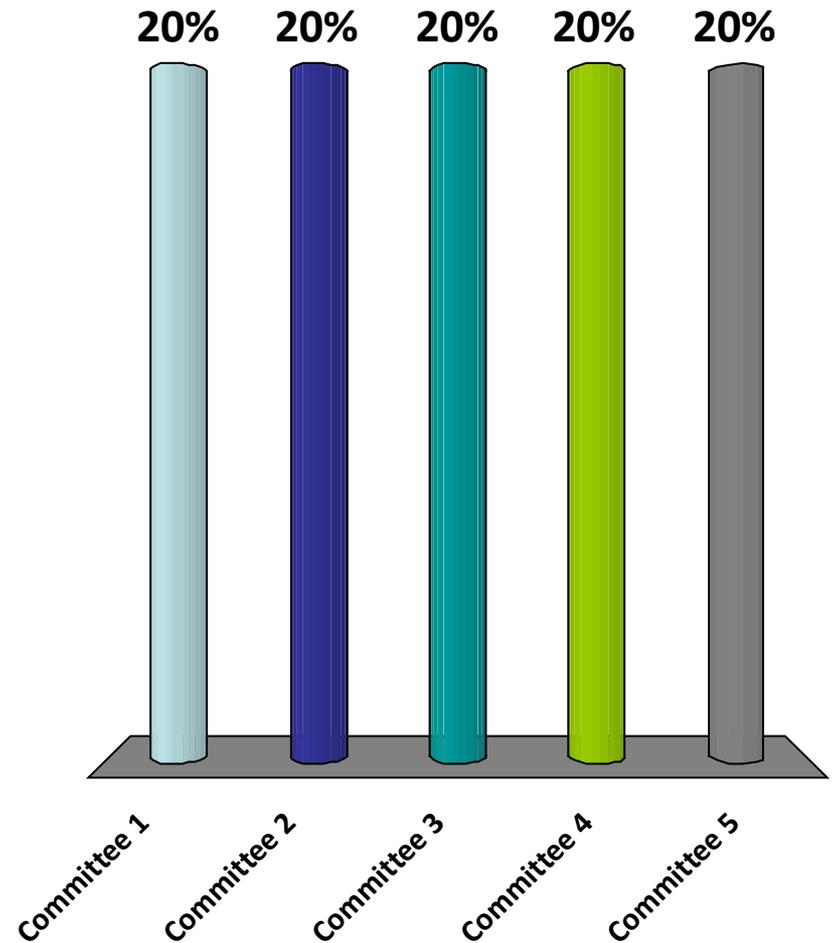
- A. Scope of IT Budget
- B. Standards & Policies
- C. IT Repository
- D. IS Conference
- E. ISO Manual
- F. IPv6
- G. BYOD Strategy
- H. IT Legislature





# Which Committee would you like to assist with?

- A. Committee 1
- B. Committee 2
- C. Committee 3
- D. Committee 4
- E. Committee 5





# COV IS Council Committees

## Meeting Day

**Date:** Monday, November 26

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

**Location:** CESC room 1222

**Register:** at [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)  
*Include the proposed committee you would like to serve on*



# COV IS Council Committee

**Questions  
Or  
Comments?**



2012  
Commonwealth Security Annual Report

Michael Watson  
Chief Information Security Officer



## § 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 - 2012 Overall Audit Program Scores

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

**ISO Designated:** The Agency Head has:

Yes - designated an ISO with the agency within the past two years

No – not designated an ISO for the agency since 2006

Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

**ISO Certification**

N/A– The certification program is pending, and scheduled to start in 2013.

**Attended IS Orientation:**

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"



# Detailed Agency Information Security - 2012 Overall Audit Program Scores Con't

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

**Security Audit Plan Received:** The Agency Head has:

**Current** - submitted a Security Audit Plan for the period of fiscal year (FY) 2012-2014 or 2013-2015 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2012, Audit Plans submitted shall reflect 2013-2015)

**No** - not submitted a Security Audit Plan since 2006

**Exception** – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

**Expired** –submitted a Security Audit Plan on file that does not contain the current three year period fiscal year (FY) 2012-2014 or 2013-2015

**Pending** –submitted a Security Audit Plan that is currently under review

**2012 - Percentage of Audit Reports Received per the Audit Plan:** The Agency Head or designee has:

**%** – submitted % of Audit Reports or planned audits listed on submitted Audit Plan

**N/A** - not had Security Audits scheduled to be completed

**Pending** –submitted a Corrective Action Plan that is currently under review

**2012 - Percentage of CAPs Received:** The Agency Head or designee has:

**%** – submitted % of CAPs for planned audits listed on submitted Audit Plan

**N/A** - not had Security Audits scheduled to be completed

**Pending** –submitted a Corrective Action Plan that is currently under review



# Detailed Agency Information Security - 2012 Overall Audit Program Scores Con't

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

**2012 - Percentage of Quarterly Updates Received:** The Agency Head or designee has:

**%** – submitted % of QUs for all open findings per CAPs submitted

**N/A** - not had Security Audits scheduled to be completed

**Pending** –submitted a Corrective Action Plan that is currently under review

**3 year - Percentage of Audit Obligation Completed:**

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.”*

Agencies that did not submit an IT Security Audit Plan by 2009 were not in compliance and therefore there is no data to report on for 2012. Systems that have been removed from audit plans within the three-year period due to retirement of the system or reclassification to non-sensitive are not counted.

**%** – Sensitive systems listed on agency IT Security Audit Plans vs. audits conducted in the last 3 years

**Pending** – currently under review

**Exception** – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



# Secretariat: Administration

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
CB	Yes	N/A	0	Current	0	0	N/A	0
DGS	Yes	N/A	0	Current	0	0	0	25
DHRM	Yes	N/A	0	Current	0	0	N/A	100
DMBE	Yes	N/A	1	Expired	0	0	N/A	0
OISG	Yes	N/A	0	Expired	N/A	N/A	N/A	0
SBE	Yes	N/A	1	Expired	N/A	N/A	N/A	0

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Agriculture & Forestry

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOF	Yes	N/A	1	Current	0	0	N/A	100
VDACS	Yes	N/A	0	Current	100	100	94.44	100

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Commerce & Trade

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
BOA	Yes	N/A	1	Current	100	100	N/A	100
DBA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DHCD	Yes	N/A	0	Current	0	0	0	80
DMME	Yes	N/A	6	Expired	0	0	N/A	57
DOLI	Yes	N/A	0	Expired	0	0	N/A	0
DPOR	Yes	N/A	0	Expired	N/A	N/A	25	100
TIC	Yes	N/A	0	Expired	N/A	N/A	N/A	0
VEC	Yes	N/A	0	Current	33.33	33.33	22.22	44
VEDP*	Yes	N/A	1	Expired	0	0	N/A	0
VRA	No	N/A	0	Expired	N/A	N/A	N/A	0
VRC	Yes	N/A	1	Current	0	0	0	100

\* VEDP includes VTA and VNDIA

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Education

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOE	Yes	N/A	1	Current	100	100	77.78	100
FCMV	Yes	N/A	0	Expired	N/A	N/A	N/A	100
GH	Expired	N/A	0	Expired	N/A	N/A	N/A	0
JYF	Yes	N/A	0	Current	0	0	N/A	100
LVA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
NSU	Yes	N/A	4	Current	Pending	Pending	Pending	Pending
RBC	Yes	N/A	1	Expired	N/A	N/A	N/A	100
SCHEV	Yes	N/A	0	Expired	0	0	N/A	0
SMV	Yes	N/A	0	Current	N/A	N/A	N/A	100
SVHEC	Yes	N/A	0	Expired	N/A	N/A	N/A	100
UMW	Yes	N/A	1	Current	100	100	33.33	100
VCA	Yes	N/A	0	Expired	0	0	N/A	100
VMFA	Yes	N/A	2	Current	0	0	0	0
VSDB	Yes	N/A	0	Expired	0	0	N/A	0
VSU	Yes	N/A	2	Current	100	100	53.12	78

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Finance

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOA	Yes	N/A	0	Expired	0	0	0	25
DPB	Yes	N/A	0	Expired	N/A	N/A	0	0
TAX	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
TD	Yes	N/A	0	Expired	0	0	N/A	0

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Health & Human Resources

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
CSA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DBHDS*	Yes	N/A	1	Current	N/A	N/A	0	83
DHP	Yes	N/A	0	Current	N/A	N/A	N/A	67
DMAS	Yes	N/A	6	Current	N/A	N/A	N/A	0
DRS**	Yes	N/A	0	Current	33.33	33.33	50	36
DSS	Yes	N/A	1	Current	0	0	0	22
VDH	Yes	N/A	1	Current	57.14	57.14	64.29	39
VFHY	Yes	N/A	0	Expired	0	0	N/A	100

\* DBHDS includes VCBR

\*\* DRS includes DBVI, VDA, VDDHH,VBPD, and WWRC

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Natural Resources

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DCR	Yes	N/A	0	Current	0	0	0	67
DEQ	Yes	N/A	1	Current	100	100	N/A	67
DGIF	Yes	N/A	2	Pending	Pending	Pending	Pending	Pending
DHR	Yes	N/A	0	Current	N/A	N/A	N/A	0
MRC	Yes	N/A	1	Current	N/A	N/A	N/A	100
VMNH	Yes	N/A	0	Expired	N/A	N/A	N/A	0

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Public Safety

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
ABC	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
CASC	Yes	N/A	0	Expired	N/A	N/A	N/A	100
DCJS	Yes	N/A	2	Expired	N/A	N/A	N/A	0
DEM	Yes	N/A	2	Expired	0	0	N/A	0
DFP	Yes	Yes	0	Expired	0	0	N/A	100
DFS	Yes	N/A	1	Current	66.67	66.67	0	75
DJJ	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
DMA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DOC*	Yes	N/A	5	Current	100	100	70.59	83
DVS**	Yes	N/A	0	Current	N/A	N/A	N/A	100
VSP	Yes	N/A	0	Current	50	50	77.27	89

\*DOC includes VPB

\*\* DVS includes VWM

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Technology

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
IEIA	Yes	N/A	2	Expired	0	0	N/A	0
VITA	Yes	N/A	3	Current	0	0	100	33

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Transportation

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DMV	Yes	N/A	0	Expired	0	0	0	100
DOAV	Yes	N/A	2	Current	0	0	N/A	0
DRPT	Yes	N/A	0	Expired	N/A	N/A	N/A	0
MVDB	Yes	N/A	0	Expired	N/A	N/A	N/A	100
VDOT	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
VPA	No	N/A	0	Expired	N/A	N/A	N/A	0

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Independent Branch Agencies

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
IDC	Yes	N/A	1	Current	0	0	8.33	80
SCC	Yes	N/A	1	Expired	66.67	66.67	73.33	100
SLD	Yes	N/A	0	Current	100	100	45.45	50
VCSP	Yes	N/A	1	Current	0	0	N/A	100
VOPA	Yes	N/A	2	Expired	N/A	N/A	N/A	0
VRS	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
VWC	Yes	N/A	1	Current	0	0	N/A	17

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Others

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
GOV	Yes	N/A	0	Current	0	0	N/A	0
OAG	Yes	N/A	2	Current	N/A	N/A	0	100

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Risk Management Program

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
XYZ	Yes	Pending	No

**All documentation received as requested information about the agency's RA(s), BIA, or IDS reports.**

**Yes** – Agency has submitted RA, BIA or IDS Report(s)

**No** – Agency has not submitted RA, BIA or IDS Report(s)

**Pending** – Agency has submitted RA, BIA or IDS Report(s) that is currently under review

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Administration

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
CB	No	Pending	Yes
DGS	No	No	Yes
DHRM	No	Pending	Yes
DMBE	No	No	Yes
OISG	No	No	No
SBE	No	No	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Agriculture & Forestry

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOF	No	Pending	Yes
VDACS	Yes	Pending	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Commerce & Trade

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
BOA	No	Pending	Yes
DBA	No	No	Yes
DHCD	No	No	Yes
DMME	No	Pending	Yes
DOLI	No	No	Yes
DPOR	No	Pending	Yes
TIC	No	Pending	Yes
VEC	No	No	Yes
VEDP*	No	No	Yes
VRA	No	No	No
VRC	No	Pending	Yes

\* VEDP includes VTA and VNDIA

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Education

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOE	Yes	Pending	Yes
FCMV	No	No	Yes
GH	No	No	Yes
JYF	No	No	Yes
LVA	No	No	Yes
NSU	No	Pending	Yes
RBC	No	No	No
SCHEV	No	No	Yes
SMV	No	No	Yes
SVHEC	No	No	No
UMW	No	No	No
VCA	No	No	Yes
VMFA	No	No	Yes
VSDB	No	No	Yes
VSU	Yes	Pending	No



# Secretariat: Finance

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOA	No	No	Yes
DPB	No	No	Yes
TAX	Pending	No	Yes
TD	No	Pending	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Health & Human Resources

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
CSA	No	No	Yes
DBHDS*	No	No	Yes
DHP	Yes	Pending	Yes
DMAS	No	Pending	Yes
DRS**	No	No	Yes
DSS	No	Pending	Yes
VDH	No	No	Yes
VFHY	No	No	Yes

\* DBHDS includes VCBR

\*\* DRS includes DBVI, VDA, VDDHH,VBPD, and WWRC

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Natural Resources

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DCR	No	No	Yes
DEQ	No	Pending	Yes
DGIF	No	No	Yes
DHR	No	No	Yes
MRC	No	Pending	Yes
VMNH	No	No	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Public Safety

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
ABC	No	Pending	Yes
CASC	No	No	Yes
DCJS	Pending	Pending	Yes
DEM	No	Pending	Yes
DFP	Pending	Pending	Yes
DFS	No	Pending	Yes
DJJ	Yes	Pending	Yes
DMA	No	No	Yes
DOC*	Pending	Pending	Yes
DVS**	Yes	Pending	Yes
VSP	No	Pending	Yes

\*DOC includes VPB  
 \*\* DVS includes VWM

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Technology

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
IEIA	No	No	Yes
VITA	Yes	Yes	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Transportation

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DMV	No	Pending	Yes
DOAV	No	Pending	Yes
DRPT	No	No	Yes
MVDB	No	No	Yes
VDOT	No	Pending	Yes
VPA	No	No	No

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Independent Branch Agencies

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
IDC	No	No	Yes
SCC	No	No	No
SLD	No	No	No
VCSP	No	No	No
VOPA	No	No	No
VRS	No	No	No
VWC	No	No	No

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Others

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
GOV	No	No	Yes
OAG	No	No	Yes

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



## 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, 2012**



# Questions ???????

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



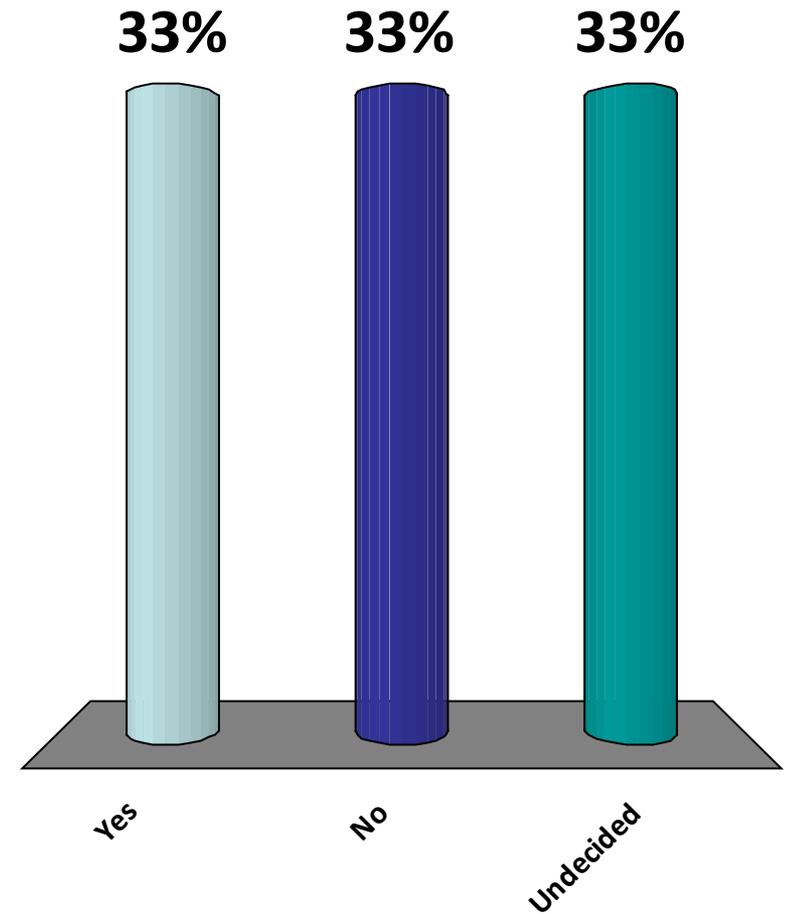
Virginia Information Technologies Agency

# Upcoming Events



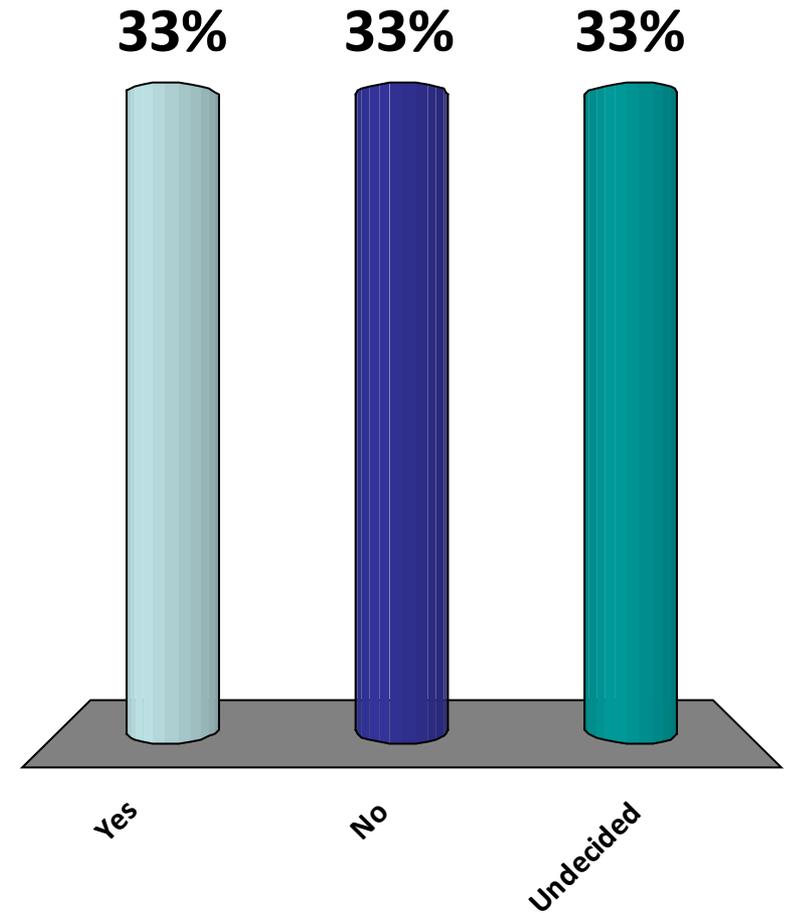
# Keynote Speaker – Kevin Savoy

- A. Yes
- B. No
- C. Undecided



# BIA Presentation – Ed Miller

- A. Yes
- B. No
- C. Undecided

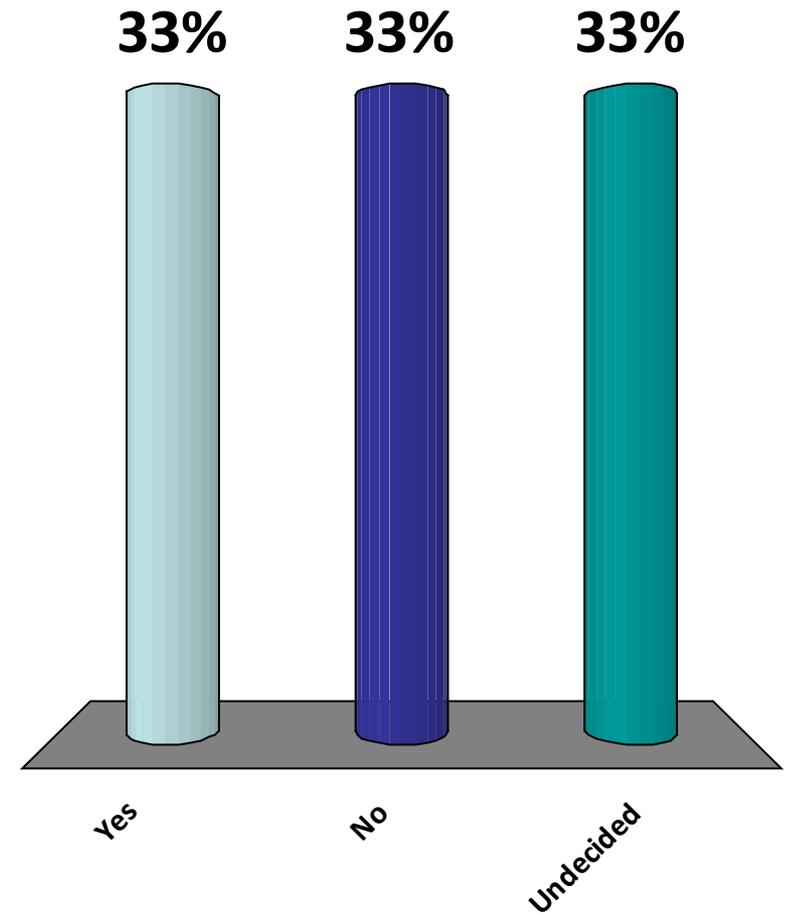




# Do today's topics meet your needs?

And would you like more of the same?

- A. Yes
- B. No
- C. Undecided





# Information Security System Association

## ISSA

**DATE:** Wednesday, Nov 14, 2012

**LOCATION:** Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

**TIME:** 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

**COST:** ISSA Members: \$20 & Non-Members: \$25

**SPEAKER:**

**TOPIC:** Secure Processors & Hardware Security Modules



# DSIA Training

## Fraud and Detection for Government Auditors

Instructor: Courtenay Thompson

**Date:** December 4 & 5, 2012

**Time:** 8:15-4:45

**Location:** James Monroe Building  
DOE Conf. Rm., 22nd FL

**Cost:** \$ 320.00

**Register:** <https://hrtraining.doa.virginia.gov>



## Future ISOAG Dates

**Dec 5**                      **1:00 – 4:00 pm @ CESC**

**Keynote Speaker: Brian Miller, Syrinx Technologies**  
**on “Pentesting”**

**Jan 9**                      **1:00 – 4:00 pm @ CESC**

**Keynote Speaker: David Frei, Capitol One**  
**on “Mobile Device Risk Assessment”**

**Feb 6**                      **1:00 – 4:00 pm @ CESC**

**Keynote Speaker: Dr. Ron Ross, NIST**

**ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2013**



# IS Orientation Sessions

Tuesday - Nov 13, 2012

9:00 – 11:30a  
(CESC)

Email [CommonwealthSecurity@VITA.virginia.gov](mailto:CommonwealthSecurity@VITA.virginia.gov) if you are interested in attending.

**IS Orientation also available via webinar!**



## 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*

Nov 7, 2012



***NORTHROP GRUMMAN***



# ADJOURN

