



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

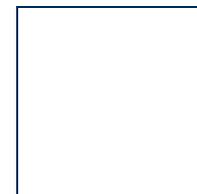
August 7, 2013



# ISOAG August 2013 Agenda

- |             |   |  |
|-------------|---|--|
| <b>I.</b>   | <b>Welcome &amp; Opening Remarks</b>  | <b>Michael Watson, VITA</b>  |
| <b>II.</b>  | <b>Incident Mgmt During Crisis Events</b>   | <b>Bennie Moore, Fed Res Bank</b>                                  |
| <b>III.</b> | <b>UC Irvine Info Sec Certification Prog<br/>&amp; Global Knowledge Offerings</b> | <b>Brian Breen, UC Irvine<br/>Kristen Miller, Global Knowledge</b> |
| <b>IV.</b>  | <b>DNS Amplification Attacks</b>  | <b>Eric Taylor, NG</b>   |
| <b>V.</b>   | <b>Risk Management Tool Demo</b>  | <b>Michael Watson, VITA</b>  |
| <b>VI.</b>  | <b>Upcoming Events &amp; Other Business</b>                                       | <b>Michael Watson, VITA</b>  |
| <b>VII.</b> | <b>Partnership Update</b>   | <b>Bob Baskette, VITA<br/>Eric Taylor &amp; Michael Clark, NG</b>  |

# Incident Management Planning



THE FEDERAL RESERVE BANK OF RICHMOND  
RICHMOND ■ BALTIMORE ■ CHARLOTTE

Bennie R. Moore, CBCP  
AVP Business Continuity  
August 7, 2013



# Disclaimer

**The views expressed in this presentation are mine and do not reflect those of the Federal Reserve Bank of Richmond, the Board of Governors of the Federal Reserve System, or any other agency or individual.**



# Discussion Objective and Topics

## Objective:

Provide information for an incident management approach

## Topics:

- Crisis Management Team (CMT) and Responsibilities
- Incident Management Plan
- Incident Management Process
- Additional Considerations
- Planning Resources





# Business Continuity Management Program

**The Business Continuity Management Program** gauges organizational risks and protects operations. Program planning components include:

- **Overall Direction** – Business Continuity Management Program Policy
- **Organization Level Plan** – Crisis Management Team Incident Management Plan
- **Business Area Level Plan** – Business Continuity Plans
- **Information Technology Infrastructure Plan** – Disaster Recovery Plan





# Incident Management Definitions

## **CRISIS EVENT**

A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.

## **INCIDENT MANAGEMENT**

The overall coordination of an organization's response to an event in an effective, timely manner with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.





# Crisis Management Team Definitions

- **Chair:** The Chief Operating Officer
- **Core Team Members:** The Chair, Business Continuity Officer and a limited number of key senior leaders only
- **Full Team Members:** Senior leaders representing all organizational areas; includes core team members
- **Functional Resources:** Provide business-area expertise and become engaged at the request of a CMT member based on the event
- **Alternates:** Each member / resource has pre-designated primary and secondary alternates





# Crisis Management Team Roles

## Core Team

- Contributes to initial event assessment
- Advises Chair on potential impacts and considering incident management initiation

## Full Team Members

- Fulfill pre-designated responsibilities
- Coordinate and communicate with respective area(s) of responsibility

## Functional Resources

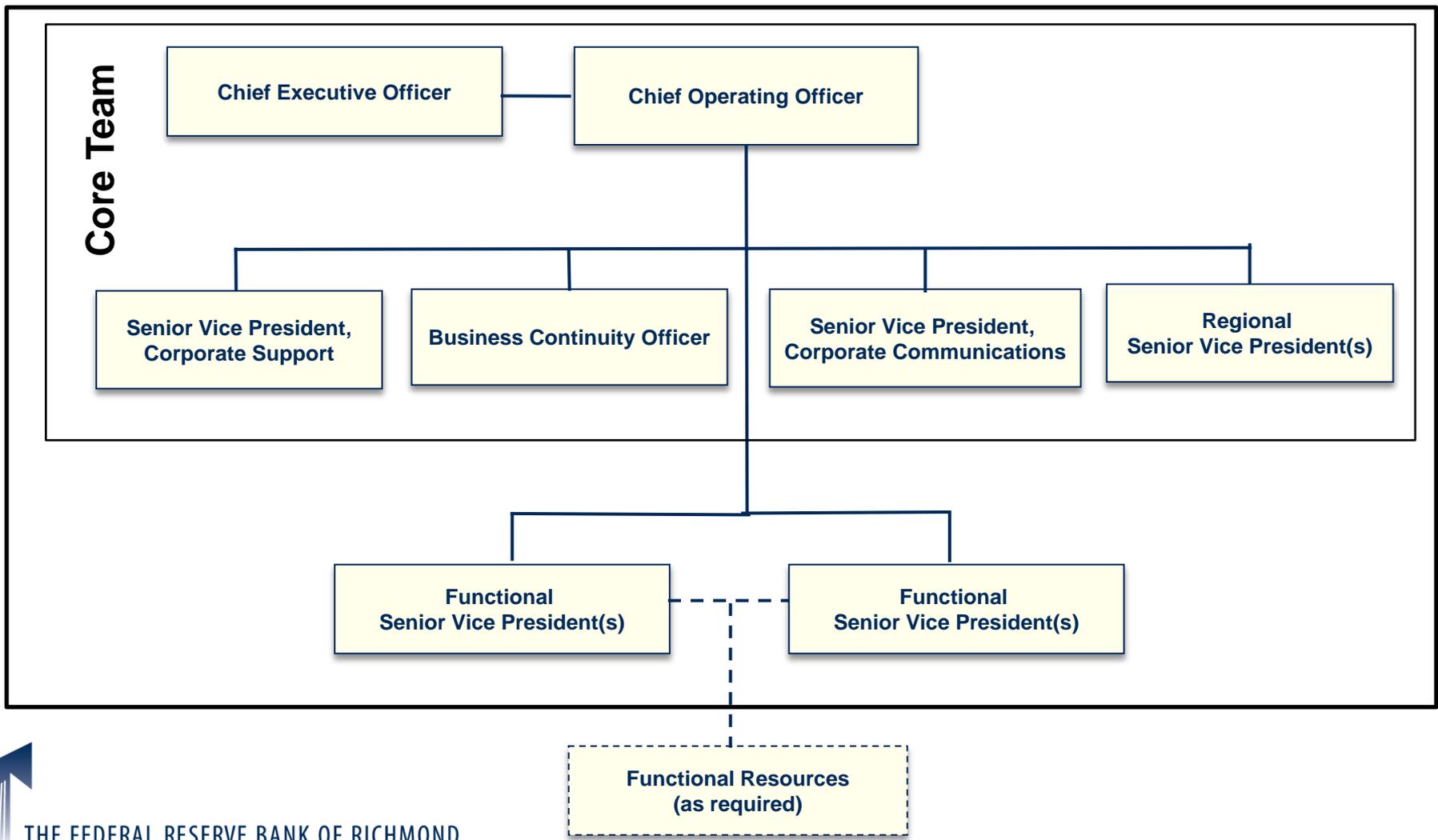
- Provide CMT business-area specific expertise





# Crisis Management Team Structure

Full Team





# Incident Management Plan Approach

- Manages events at the organizational level
- Utilizes an “All Hazards” planning approach based on Incident Command System (ICS) principles
- Responses are scoped to the event
- Supplemented with specific plans such as the Pandemic Response Plan, Emergency Procedures, etc.





# Incident Management Plan Structure

- **Plan Sections:** Define scope, roles/responsibilities and process
- **Appendices:** Contain reference materials to supplement plan sections (contact information, actions, and setup instructions)
- Corresponding checklist used to guide event actions
- Selected plan contact and reference information (contacts and telephone numbers, set-up instructions, etc.) condensed and loaded to individuals' mobile devices





# Incident Plan Structure Example

## **Section 1.0 - Plan Status and Approval**

## **Section 2.0 Overview and General Information**

- 2.1 Executive Summary
- 2.2 Scope
- 2.3 Policy
- 2.4 Objective
- 2.5 Assumptions

## **Section 3.0 Plan Strategy**

- 3.1 Incident Management Process
- 3.2 Management Team Members and Responsibilities
- 3.3 Incident Management Actions and Decisions Checklist
- 3.4 Incident Management Plan Supplements

## **Section 4.0 Plan Details**

- 4.1 Overview
- 4.2 Determine Phase
- 4.3 Initiate Phase
- 4.4 Assess Phase
- 4.5 Plan Phase
- 4.6 Execute Phase
- 4.7 Reassess Phase

## **Section 5.0 - Plan Administration and Maintenance**

## **Appendices**





# Incident Management Process

- Six, predetermined phases, consisting of multiple steps, considered to manage an incident
- Timeframe for phase/step progression depends on the situation being addressed
- Actions and decisions prioritized based upon:
  - Staff safety
  - Facility security
  - Facility operability
  - Supporting infrastructure operability (automated systems)
  - Critical operations
  - Less critical operations





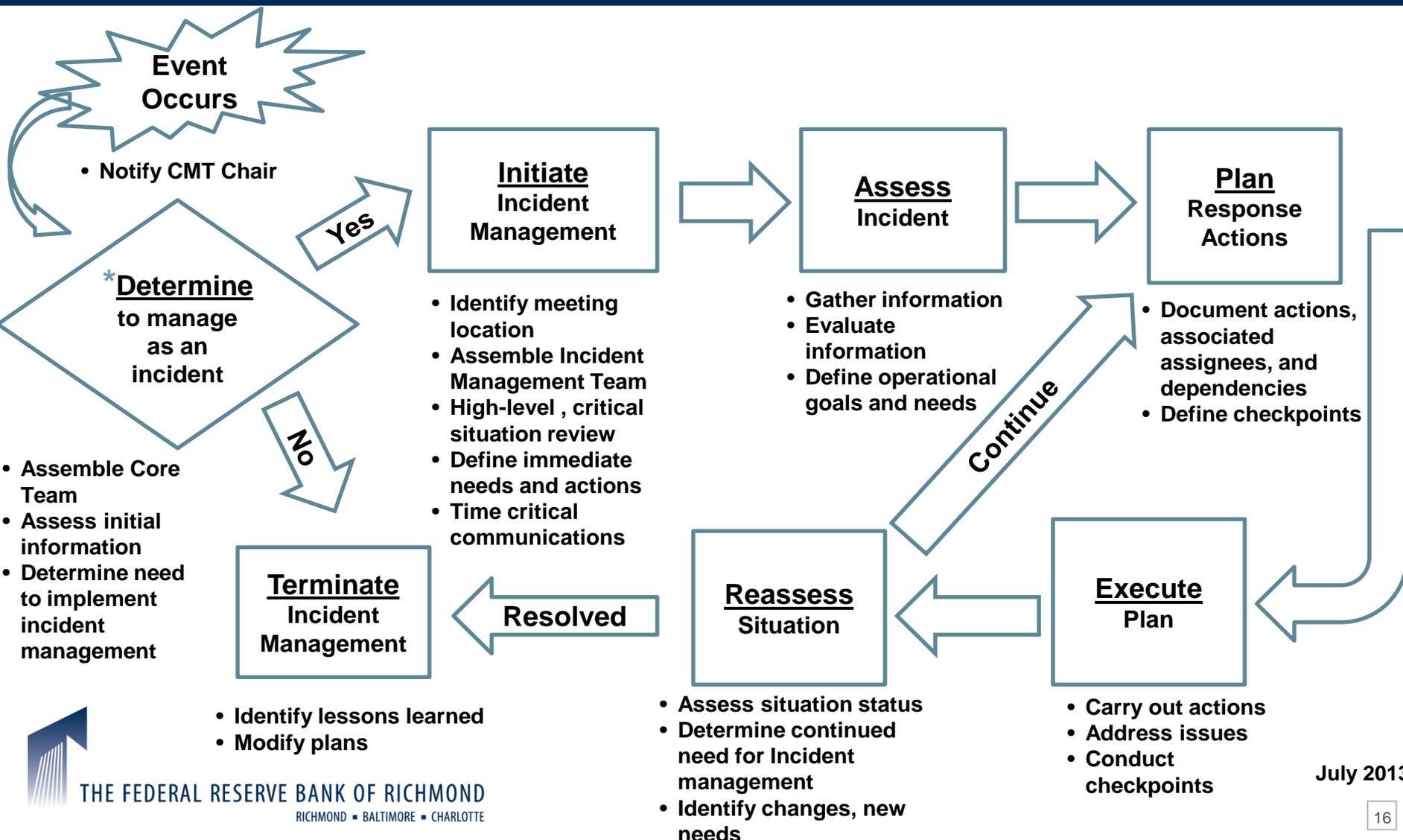
# Incident Management Process Phases

- 1. Determine:** Determine need to implement the incident management process
- 2. Initiate:** Begin steps to manage the event
- 3. Assess:** Conduct more comprehensive assessment of event scope and determine high-level actions
- 4. Plan:** Develop planned approach to manage the event
- 5. Execute:** Carry out the planned approach
- 6. Reassess:** Reassess the situation and actions taken; revise plans and implement changes or terminate incident management process





# Fifth District Incident Management Process





# Incident Management Actions and Decisions Checklist

- Developed to be a concise, quick reference guide for use during incidents
- Steps align with Incident Management Plan’s “All Hazards” approach, process phases, and narrative
- Intended to ensure the Crisis Management Team **considers each action and decision; not necessarily to implement each action**
- Steps follow a priority-based on staff safety, critical operations, inform constituents



# Incident Management Actions and Decisions Checklist

1 - DETERMINE PHASE    2 - INITIATE PHASE    3 - ASSESS PHASE    4 - PLAN PHASE    5 - EXECUTE PHASE    6 - REASSESS PHASE

**Phase Objective:** Event awareness and determine the need to activate the incident management process.

TASK		STATUS**				Notes/Comments
		<u>CMT/Dept Responsible</u>	<u>Staff Assigned Task/Time</u>	<u>Date/Time Due</u>	<u>Date/Time Done</u>	
<u>Consideration/Decision/Perform</u>						
<b>D.1 Initial decision makers (CO)***</b>						
D.1.1*	Assemble CMT Core - Specify Location	CMT Chair				
D.1.2	Activate Conference Bridge	BCO				
<b>D.2 Determine status of Staff Safety (SS)</b>						
D.2.1*	Type of event or threat	CMT Core				
D.2.2*	Immediate impact on staff	LEU & FM				
D.2.3*	Send immediate staff communication?	CMT Core, CC				
<b>D.3 Determine status of operations (CO &amp; RF)</b>						
D.3.1*	Determine impact to facility and operations	LEU & FM				
D.3.2*	Identify time critical decisions	CMT Core				
D.3.3*	Additional actions or decisions as required	CMT Core				
<b>D.4 Incident Management process activation (CO)</b>						
D.4.1*	Activate the Incident Management process? If activated, begin log of incident events.	CMT Chair				
D.4.2	If no, assign CMT member to monitor events	CMT Chair				
D.4.3	If no, determine requirements/times for status updates	CMT Chair				
<b>D.5 Determine Phase Completion checkpoint (CO &amp; RF)</b>						
D.5.1*	Determine Phase objective accomplished?	CMT				



# Initial Event Notification

- The CMT Chair is notified at the outset of an event that could potentially be managed as an incident
- Notification should be initiated by a predetermined set of individuals as follows:
  - Most senior leader available over a business area initially impacted
  - Law Enforcement
  - Other organizational areas having higher potential to be aware of an event at its inception





# Determine Phase

**Phase Objective:** Communicate event awareness and determine need to activate the Incident Management Process.

## Steps:

- Assemble Core Team
- Assess initial available information
- Factor potential, life-safety issues
- Identify operational impacts
- Determine need to implement Incident Management Process

**Key Factor:** Initial information assessed must be received from credible sources (pre-determined set)





# Determine Phase Checklist Steps - EXAMPLE

Consideration/Decision/Perform		CMT/Dept. Responsible
<b>D.1 Initial decision makers (CO)***</b>		
<b>D.1.1*</b>	<b>Assemble CMT Core - Specify Location</b>	<b>CMT Chair</b>
D.1.2	Activate Conference Bridge	BCO
<b>D.2 Determine status of Staff Safety (SS)</b>		
<b>D.2.1*</b>	<b>Type of event or threat</b>	<b>CMT Core</b>
<b>D.2.2*</b>	<b>Immediate impact on staff</b>	<b>LEU &amp; FM</b>
<b>D.2.3*</b>	<b>Send immediate staff communication?</b>	<b>CMT Core, CC</b>
<b>D.3 Determine status of operations (CO &amp; RF)</b>		
<b>D.3.1*</b>	<b>Determine impact to facility and operations</b>	<b>LEU &amp; FM</b>
<b>D.3.2*</b>	<b>Identify time critical decisions</b>	<b>CMT Core</b>
<b>D.3.3*</b>	<b>Additional actions or decisions as required</b>	<b>CMT Core</b>
<b>D.4 Incident Management process activation (CO)</b>		
<b>D.4.1*</b>	<b>Activate the Incident Management process? If activated, begin log of incident events.</b>	<b>CMT Chair</b>
D.4.2	If no, assign CMT member to monitor events	CMT Chair
D.4.3	If no, determine requirements/times for status updates	CMT Chair
<b>D.5 Determine Phase Completion checkpoint (CO &amp; RF)</b>		
<b>D.5.1*</b>	<b>Determine Phase objective accomplished?</b>	<b>CMT</b>



# Initiate Phase

**Phase Objective:** Initiate Incident Management Process to manage the event

## Steps:

- Identify team meeting location
- Notify and assemble Incident Management Team
- Conduct high-level situation, criticality review
- Identify time-critical issues
- Define immediate resource needs and actions
- Provide initial communications

**Key Factor:** Staff safety and time-related, critical communications should occur as soon as practical



# Initiate Phase Checklist - EXAMPLE

Consideration/Decision/Perform		CMT/Dept. Responsible
<b>I.1 Crisis Management Center (CO)</b>		
<b>I.1.1*</b>	<b>Identify CMT meeting location</b>	<b>CMT Chair, BCO</b>
<b>I.2 Notify CMT (IC)</b>		
I.2.1	Notify full CMT	CMT Chair
I.2.2	Assemble CMT in location and/or by teleconference.	BCO
<b>I.3 Event management (CO)</b>		
<b>I.3.1*</b>	<b>Assume events and actions record</b>	Team Scribe
<b>I.4 Time critical staff safety issues (SS)</b>		
<b>I.4.1*</b>	<b>Identify staff issues requiring immediate attention</b>	<b>CMT Core</b>
<b>I.4.2*</b>	<b>Issue instructions for staff</b>	<b>CMT Core</b>
<b>I.5 Relocation (CO )</b>		
I.5.1	Initiate possible activation of relocation site	BCO
<b>I.6 Notification (SS and CO)</b>		
<b>I.6.1*</b>	<b>Notify other affected organizations</b>	<b>CMT Core</b>
<b>I.7 Additional actions (CO &amp; RF)</b>		
<b>I.7.1*</b>	<b>Additional actions or decisions as required</b>	<b>CMT</b>
<b>I.8 Determine Phase Completion Checkpoint (CO &amp; RF)</b>		
<b>I.8.1*</b>	<b>Initiate Phase objective accomplished?</b>	<b>CMT</b>





# Assess Phase

**Phase Objective:** Perform a comprehensive assessment of the scope and severity of the event

## Steps:

- High-level impact assessments
  - Personnel
  - Business Operations
  - Facilities
- Initiate detailed, functional assessments
- Evaluate information to define operational goals

## Key Factors:

- Event scope and severity identified
- Initiate specific high level support actions to effectively manage it





# Assess Phase Checklist Steps - EXAMPLE

Consideration/ Decision/Perform		CMT/Dept. Responsible
<b>A.1 Personnel impact assessment affected areas (SS)</b>		
<b>A.1.1*</b>	<b>Assess impact to staff.</b>	<b>CMT</b>
<b>A.2 Initial high-level functional assessment (CO &amp; RF)</b>		
<b>A.2.1*</b>	<b>Critical functions operational?</b>	<b>Dept(s)</b>
A.2.2	Special expertise needed to manage this event?	BCO
<b>A.2.3*</b>	<b>Activate Communication Plan</b>	<b>Corp. Comm.</b>
<b>A.2.4*</b>	<b>Crisis Management Center resources suitable?</b>	<b>CMT Chair</b>
<b>A.3 Detailed functional assessment (CO)</b>		
<b>A.3.1*</b>	<b>Impact to critical functions; IT resources; customers; other</b>	<b>Dept(s)</b>
<b>A.3.2*</b>	<b>Non-critical functions, estimate time to reestablish operational level</b>	<b>Dept(s) / CMT</b>
<b>A.4 Alternate site recommendations (SS &amp; CO)</b>		
<b>A.4.1*</b>	<b>Alternate work site needed? Activation level?</b>	<b>CMT</b>
<b>A.4.2*</b>	<b>Functions to suspend?</b>	<b>CMT</b>
<b>A.5 Additional actions (CO &amp; RF)</b>		
<b>A.5.1*</b>	<b>Additional actions or decisions as required</b>	<b>CMT</b>
<b>A.6 Determine Phase Completion Checkpoint (CO &amp; RF)</b>		
<b>A.6.1*</b>	<b>Assess Phase objective accomplished?</b>	<b>CMT</b>





# Plan Phase

**Phase Objective:** Identify and prioritize response actions

**Steps:**

- Determine and prioritize operational response, ongoing actions, and internal and external communications
- Identify triggering events that would necessitate reviewing and possibly altering the planned approach
- Define and schedule status checkpoints

**Key Factors:**

- Requires actions be prioritized within both organizational and functional levels
- Actions and issues should be documented and tracked indicating associated assignees and dependencies





# Plan Phase Checklist Steps - EXAMPLE

Consideration/ Decision/Perform		CMT/Dept Responsible
<b>P.1 Determine / prioritize response action (SS, CO, RF)</b>		
<b>P.1.1*</b>	<b>Ensure safety and care of staff</b>	<b>CMT</b>
P.1.2	Need for staff assistance, temporary workers	HR
P.1.3	Coordinate secondary impact assessments?	Affected Dept(s)
P.1.4	Coordinate business areas' response actions	CMT
<b>P.1.5*</b>	<b>Define reassessment intervals or triggering events.</b>	<b>CMT</b>
<b>P.2 Determine / prioritize communication action (IC)</b>		
<b>P.2.1*</b>	<b>Internal communication efforts coordinated?</b>	<b>CC</b>
P.2.2	Telephone operator briefings and statement update	CC & CSS
P.2.9	Guidance to recover critical and non-critical business operations?	BCO
<b>P.3 Determine/prioritize external information distribution (IC)</b>		
<b>P.3.1*</b>	<b>External communication efforts coordinated?</b>	<b>CC</b>
<b>P.4 Continuing actions (CO &amp; RF)</b>		
<b>P.4.1*</b>	<b>Issue escalation and tracking process established?</b>	<b>CMT</b>
<b>P.4.2*</b>	<b>Status reporting method and schedule?</b>	<b>CMT Chair</b>
<b>P.5 Additional actions (CO &amp; RF)</b>		
<b>P.5.1*</b>	<b>Additional actions or decisions as required</b>	<b>CMT</b>
<b>P.6 Determine Phase Completion Checkpoint (CO &amp; RF)</b>		
<b>P.6.1*</b>	<b>Plan Phase objective accomplished?</b>	<b>CMT</b>





# Execute Phase

**Phase Objective:** Implement defined, response actions

**Steps:**

- Implement operational response plan (developed during Plan Phase)
- Address issues
- Conduct scheduled checkpoints

**Key Factor:** Situational awareness requires ongoing monitoring of changes impacting actions defined during planning process.





# Execute Phase Checklist Steps - EXAMPLE

Consideration/Decision/Perform		CMT/Dept Responsible
<b>E.1 Implement operational response plans (CO &amp; RF)</b>		
<b>E.1.1*</b>	<b>Evaluate staff well-being</b>	<b>Health Services &amp; Human Resources</b>
<b>E.1.2*</b>	<b>Execute Business Area BC plans</b>	<b>Affected Dept(s)</b>
<b>E.1.3</b>	Information Technology recovery coordinated with business areas?	Information Technology
<b>E.1.4*</b>	<b>Periodic progress updates to CMT</b>	<b>Affected Dept(s)</b>
<b>E.1.5*</b>	<b>Planned progress and reassessment checkpoints completed</b>	<b>Affected Dept(s)</b>
<b>E.1.6*</b>	<b>Situational changes requiring reassessment</b>	<b>CMT</b>
<b>E.2 Communication response actions (IC)</b>		
<b>E.2.1*</b>	<b>Implement other organization level plans developed in Plan Phase</b>	<b>Affected Dept(s) CMT</b>
<b>E.3 Additional actions (CO &amp; RF)</b>		
<b>E.3.1*</b>	<b>Additional actions or decisions as required</b>	<b>CMT</b>
<b>E.4 Determine Phase completion checkpoint (CO &amp; RF)</b>		
<b>E.4.1*</b>	<b>Execute Phase objective accomplished?</b>	<b>CMT</b>





# Reassess Phase

**Phase Objective:** Reassess event and response actions. Determine continued need for Incident Management Process

## Steps:

- Conduct a functional reassessment
- Conduct an event reassessment
- Determine continuing Incident Management process
- If continued, revise plans as necessary and implement alternate approaches
- If terminated, initiate actions to return to a normal operations status

**Key Factor:** Broadly communicate planning changes to account for other functional impacts





# Reassess Phase Checklist Steps - EXAMPLE

Consideration/Decision/Perform		CMT/Dept. Responsible
<b>R.1 Functional reassessment (SS, CO, IC &amp; RF)</b>		
<b>R.1.1*</b>	<b>Identify staff concerns</b>	<b>HR</b>
<b>R.1.2*</b>	<b>Status business functions</b>	<b>CMT</b>
<b>R.1.3*</b>	<b>Status of facility and security</b>	<b>LEU &amp; FM</b>
<b>R.1.4*</b>	<b>Status of automation resources</b>	<b>IT</b>
R.1.5	Additional information needed?	CMT
<b>R.2 Event reassessment (CO, IC, &amp; RF)</b>		
<b>R.2.1*</b>	<b>Identify updates or changes needed</b>	<b>CMT</b>
<b>R.2.2*</b>	<b>Implement changes per Execute Phase</b>	<b>CMT</b>
<b>R.2.3*</b>	<b>Communicate operating status change</b>	<b>CMT</b>
<b>R.3 Normal State (CO &amp; RF)</b>		
R.3.1	Initiate return to normal state actions?	CMT
<b>R.4 Incident Management process (CO)</b>		
<b>R.4.1*</b>	<b>Open actions or decisions</b>	<b>CMT</b>
<b>R.4.2*</b>	<b>Incident Management process complete</b>	<b>CMT</b>
<b>R.5 Lessons learned (CO)</b>		
<b>R.5.1*</b>	<b>Conduct Post Event Review</b>	<b>CMT Core, BCO</b>
<b>R.5.2*</b>	<b>Crisis Management and Business plans updated</b>	<b>Affected Dept(s)</b>
<b>R.6 Determine Phase Completion Checkpoint (CO &amp; RF)</b>		
<b>R.6.1*</b>	<b>Reassess Phase objective accomplished?</b>	<b>CMT</b>





# Post Event Actions

**Objective:** Improve plans based on what was learned during the event

**Steps:**

- Collect input from those involved with managing the event
- Evaluate actions taken
- Conduct a lessons-learned analysis
- Modify plans and implement changes

**Key Factor:** To be effective, evaluation must be non-judgmental on decisions made and actions taken





# Additional Considerations

- Pre-identify Team Meeting Locations
  - Onsite (multiple) and offsite
  - Telephone connectivity
  - Network connectivity (wired or wireless)
- Supply Storage
  - Near meeting locations
  - Office supplies
  - Phones
  - Network cords
  - Plan copies
- Plan Verification Approach
- Plan Maintenance





# Planning Resources

Organization	Website
Continuity Central	<a href="http://www.continuitycentral.com">www.continuitycentral.com</a>
Disaster Recovery Journal	<a href="http://www.drj.com">www.drj.com</a>
Disaster Resource	<a href="http://www.disaster-resource.com">www.disaster-resource.com</a>
FEMA Business Planning	<a href="http://www.ready.gov/business">www.ready.gov/business</a>
FEMA Training	<a href="http://training.fema.gov/EMI">training.fema.gov/EMI</a>
National Homeland Security	<a href="http://www.dhs.gov">www.dhs.gov</a>
Virginia Department of Emergency Management	<a href="http://www.vaemergency.gov">www.vaemergency.gov</a>

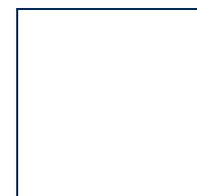




# Questions



# Incident Management Planning



THE FEDERAL RESERVE BANK OF RICHMOND  
RICHMOND ■ BALTIMORE ■ CHARLOTTE

Bennie R. Moore, CBCP  
AVP Business Continuity  
August 7, 2013



UCIRVINE | EXTENSION

**After Hours Certificate Programs**  
**On Site @ NGC, Chester**  
***Information Systems Security***

# Contact Information

## *Director of Corporate Training*

Brian Breen

(949) 824-1847 (Work)

[bbreen@uci.edu](mailto:bbreen@uci.edu)



## *NGC Student Services*

(949) 824-5933 (Work)

(949) 824-2090 (Fax)

[ngc@uci.edu](mailto:ngc@uci.edu)

## *Corporate Training Account Manager*

Missy Clayton

(949) 824-5736 (Work)

[missy.clayton@uci.edu](mailto:missy.clayton@uci.edu)

## *NGC BWI Contact*

Jocelyn Cenna

[jocelyn.cenna@ngc.com](mailto:jocelyn.cenna@ngc.com)

# Program Development

- Instructor Qualifications
  - Master's Degree
  - Professional Designations/Affiliation with Applicable Society
    - CISSP® Designation/Affiliation with (ISC)<sup>2</sup>
    - PMP® Designation/Affiliation with PMI
  - Subject Matter Experts / Practitioners



# Info Security Program Development

- Information Systems Security Certificate Program was developed with an Advisory Board of Industry Leaders and the School of Information and Computer Sciences at the University of California, Irvine.
- The curriculum is based upon:
  - Information Security Industry Standards
  - International Information Systems Security Certification Consortium(ISC)<sup>2</sup> 10 Domain Knowledge Areas in the CBK<sup>®</sup> Guide, 2nd Edition

# Program Curriculum

- Continuing Education Courses
- Preparation for the Certified Information System Security Professional (CISSP®) from (ISC)<sup>2</sup>
- Technical/Non-Technical Professionals Involved In:
  - Designing, Developing, Financing, Administering, and Managing Secured Information Systems and Networks



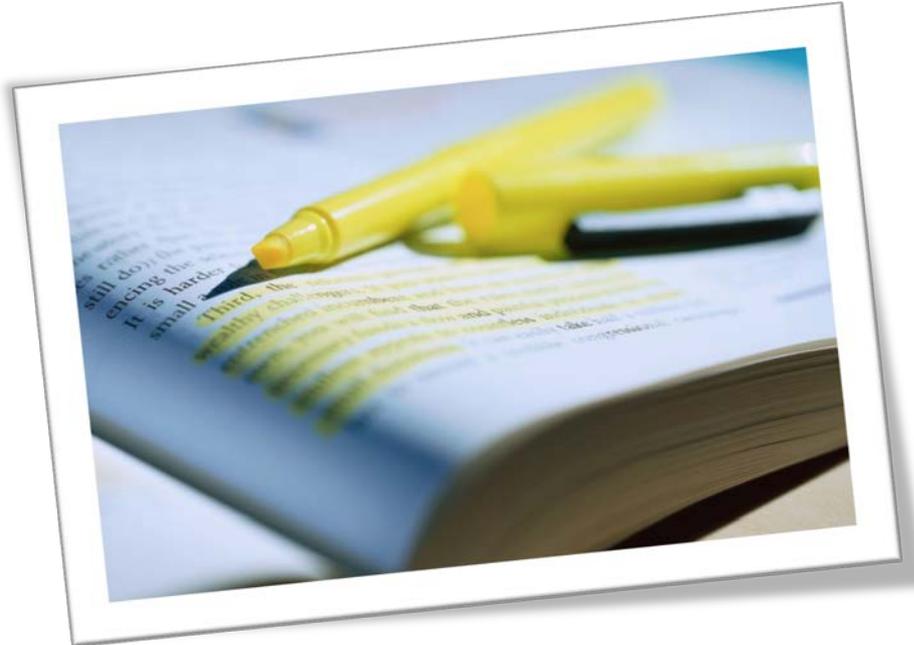
# Program Curriculum

- **Five Course Certificate Program**

- Three Required Courses
  - Body of Knowledge
- Two Elective Courses
  - Industry Specific

- **Certificate Completion**

- Must complete all 5 courses with grade of 'B' or better within 5 years



# Certificate Program Courses

## *Required Courses*

1. **Introduction to Information Systems Security** *(3.0 units)*
2. **Secure Systems** *(3.0 units)*
3. **Security Architecture and Design** *(3.0 units)*



# Certificate Program Courses

***2 Elective Courses*** (choose during 2<sup>nd</sup> Course)

## Information Systems Security Track

- 1. Host and OS Security**  
*(1.5 units)*
- 2. Applied Cryptography**  
*(3.0 units)*
- 3. Database Security**  
*(3.0 units)*
- 4. Network Security: Concepts & Technologies** *(3.0 units)*
- 5. Disaster Recovery Planning & Business Continuity** *(3.0 units)*

## Cyber Security Track

- 1. Introduction to Computer Forensics**  
*(3.0 units)*
- 2. Ethical Hacking** *(3.0 units)*
- 3. Reverse Engineering** *(1.5 units)*

# CISSP® Certification through (ISC)²

- Certified Information Systems Security Professional (CISSP®) Certification can be obtain through the International Information Systems Security Certification Consortium (ISC)²
- Certification is NOT administered through UCI

For more information please refer:

**[www.isc2.org/cissp](http://www.isc2.org/cissp)**

# CISSP® Certification through (ISC)²

## Eligibility Requirements

- High School Diploma/global equivalent
- 5 years security professional experience

- Bachelor's Degree/ global equivalent
- 4 years security professional experience

## Steps to Obtaining Credential

- Application Process + Multiple Choice Exam

## Exam Information & Fees

- 6 hours; 250 questions
- US \$549

## Credential Maintenance Cycles & Requirements

- 3 years; 120 CPE's (continuing professional education)
- Minimum of 20 CPE's per year

# Program Details

- **Absent for Class?**

- Advise/Coordinate with Instructor Prior to Absence
- Advise Teammates Prior to Absence
- Be Prepared to Make-up Missed Assignments
- Telecom can be Established as Needed



- **Work Required Outside of Class**

- Approximately 6-8 Hours of Work Per Week
- Some courses are structured on a team basis – others on an individual basis

# Class Information

## When?

- Start Date: September 3
- Offered 1 day per week: Tuesdays
- 5-9pm

## Where?

- NG, Chester

## Length?

- The programs will run approximately 10 months

# Registration Information

## Cost?

- \$600 for a 3.0 unit class
- \$525 for a 1.5 unit class
- + One Time Candidacy Fee of \$75
  - *Not collected until the end of program. UCI will prompt you.*

## Enrollment with UCI

- Please submit enrollment form for the first course via fax at (949)824-1728
- Payment is due no later than the first day of class to have access to course materials online
- Upon enrollment in the first course when your student account has been officially created, registration for all subsequent courses will occur on the NGC website.

# Your Account Information

## Accessing Grades & Account Info

- Grades, transcripts, enrollment confirmation, receipts, etc. are accessible via UC Irvine Extension Website
- In addition, all courseware is available electronically through “My Courses”
- **You must create a UCI account to access this information**



Global Knowledge®

# Upcoming Security Certifications

**Date: Wednesday August 7<sup>th</sup>, 2013**

**Presented by:  
Kristen Miller  
Global Knowledge**

# Session Overview

- **About the certifications**
  - Security+ and CISM
- **Upcoming sessions**
  - Security+ Boot Camp
    - October 7–11<sup>th</sup>
  - CISM Prep Course
    - November 12–14<sup>th</sup>
- **Location**
  - Northrop Grumman's CESC facility in Chester
- **Registration details**

# CompTIA Security +

- **Security+**
  - International, vendor-neutral certification
  - Demonstrates competency in these areas:
    - Network security
    - Compliance and operational security
    - Threats and vulnerabilities
    - Application, data and host security
    - Access control and identity management
    - Cryptography
- **Security+ not only ensures that candidates will apply knowledge of security concepts, tools, and procedures to react to security incidents, it ensures that security personnel are anticipating security risks and guarding against them.**

# CompTIA Security +

- **Security + Exam**

- 100 questions, 90 minutes to complete the exam
- A passing score is 750 out of 900 possible points
- Can be taken onsite with the class or at any Pearson VUE testing facility

- **Renewal can be achieved two ways:**

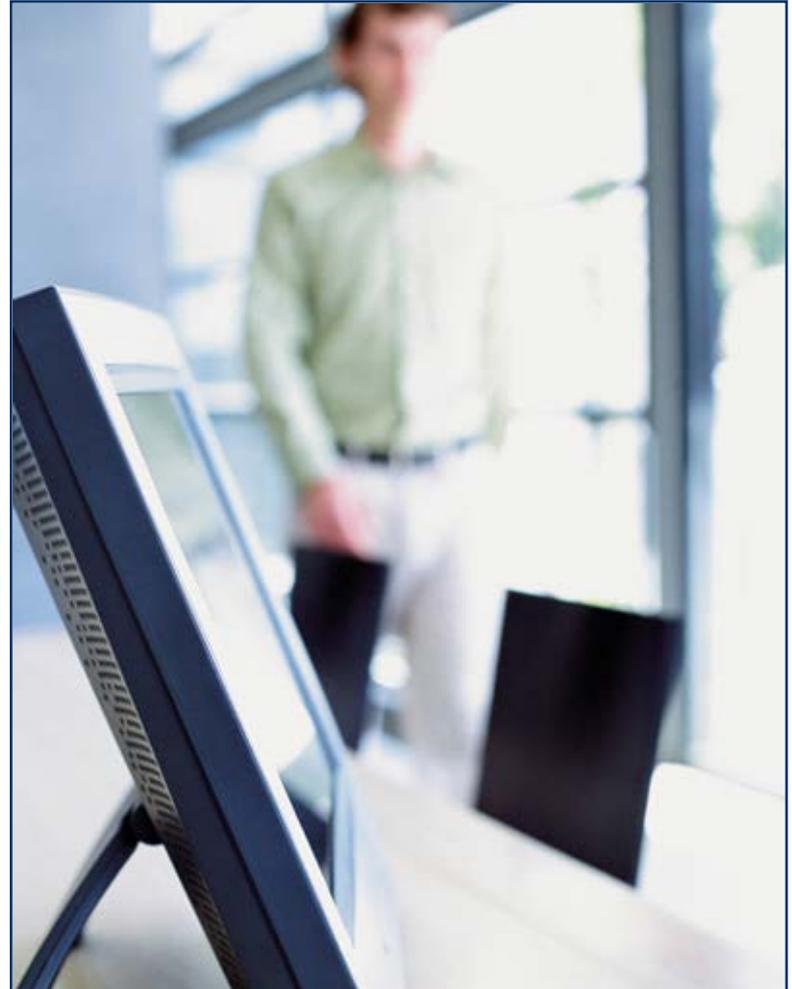
- Retake Exam – take the most current version of the CompTIA Security+ certification exam.
- CEU - earn 50 continuing education units per renewal period.
  - Earn CEUs by participating in qualified activities, such as publishing an article or white paper, obtaining another industry certification, additional security training or attending a relevant conference or event.

# Security+ Boot Camp Details

- **October 7- 11<sup>th</sup> from 8:00am – 6:00pm**
  - Class registration deadline is September 13<sup>th</sup>
  - Extended hours so you can test Friday afternoon
  - **\$ 1,625** per student
  - Pass Guarantee: Free retake voucher is provided
    - Assumes you took and failed the initial exam within 30 days of class
- **Course includes**
  - Pre-class online access to:
    - Security+ reading plan & Security+ Study guide
    - Security+ certification practice exams
  - During class, you'll have access to:
    - Security+ student manual
    - additional Security+ practice exam questions
    - Comprehension exercises, study digest, and quick reference card

# CISM – Certified Information Security Manager

- **Information Systems Audit and Control Association (ISACA)**
- **CISM**
  - Targets Tier II Security Management Professionals
  - Exam offered 2-3x a year
  - 200 multiple-choice questions
- **8570 compliancy**
- **Exam focuses on five domains:**
  - Security Governance
  - Risk Management
  - Security Program Development
  - Security Program Management
  - Incident Management and Response



# CISM – continued...

## ● Prerequisites

- Five years of experience with audit, IT systems, and security of information systems; systems administration experience; familiarity with TCP/IP; and an understanding of UNIX, Linux, and Windows.
- Requires intermediate-level knowledge of security concepts
  - Security+ Prep Course

## ● Who Needs to Attend

- Experienced ISM's and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

# CISM Prep Course

- **Date:** November 12 – 14
- **Hours:** 8:30 am – 4:30 pm
- **Fee:** \$1,100 per student
  
- **Class registration deadline: October 15<sup>th</sup>**
  - Seats are first come first serve
- **Exam fee and registration is separate**
  - See details on next slide

# CISM Exam and Maintenance with ISACA

- **Next exam in Richmond VA:** December 14<sup>th</sup>
- **Early Registration Deadline:** August 21
- **Final Registration Deadline:** October 25
  - Fees vary depending on how and when you register
  
- **Register and pay ISACA directly.**
  
- **CISM Maintenance:**
  - Annual maintenance fee
  - Attain and report an annual of 20 CPE hours.
  - Attain and report 120 CPE hours for a three-year reporting period.

# How to Register for Classes

- **Send payment to Kristen Miller**

- O: 252-756-4757 / [Kristen.miller@globalknowledge.com](mailto:Kristen.miller@globalknowledge.com)
  - ◆ Seats are first come first serve
  - ◆ Global Knowledge accepts company funded PO's or credit cards.

- **Overview**

- Security+ boot camp: October 7-11<sup>th</sup>
  - \$1,625
    - ◆ exam and guarantee included
- CISM Prep Course: November 12 – 14<sup>th</sup>
  - \$1,100
- Contact Kristen Miller with any questions!

*THE VALUE OF PERFORMANCE.*  
***NORTHROP GRUMMAN***

# **DNS Amplification Attacks**

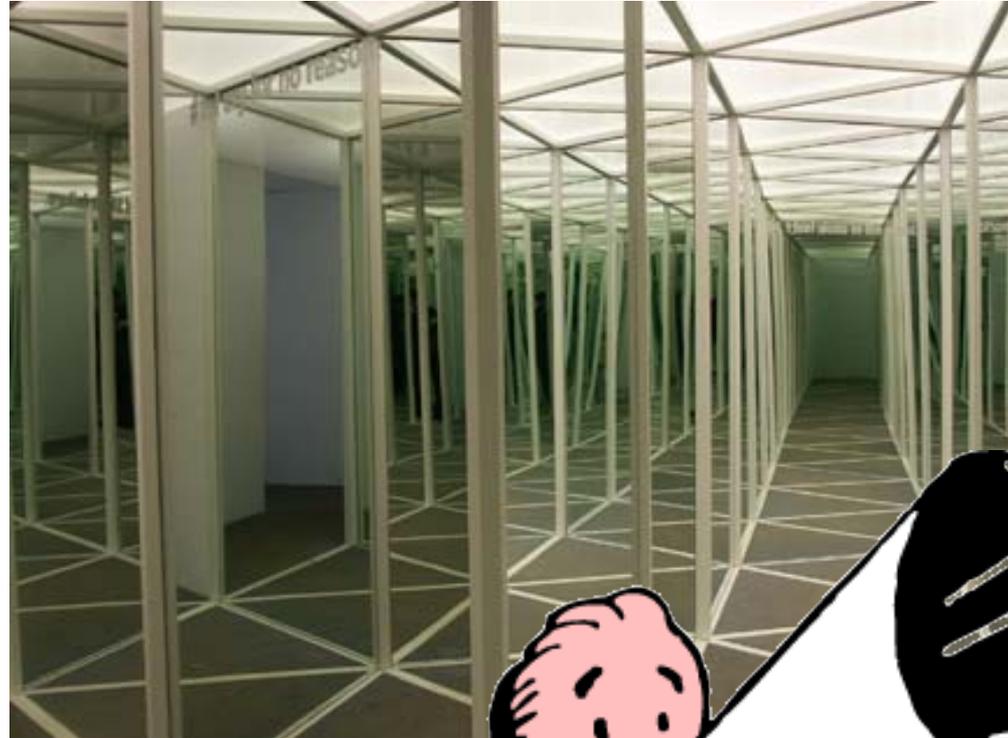
**David Cobaugh**

Northrop Grumman Cyber Administrator

David.Cobaugh@ngc.com

- What is it?
- What can it do?
- How can it be identified?
- Can it be mitigated?
- Current Events

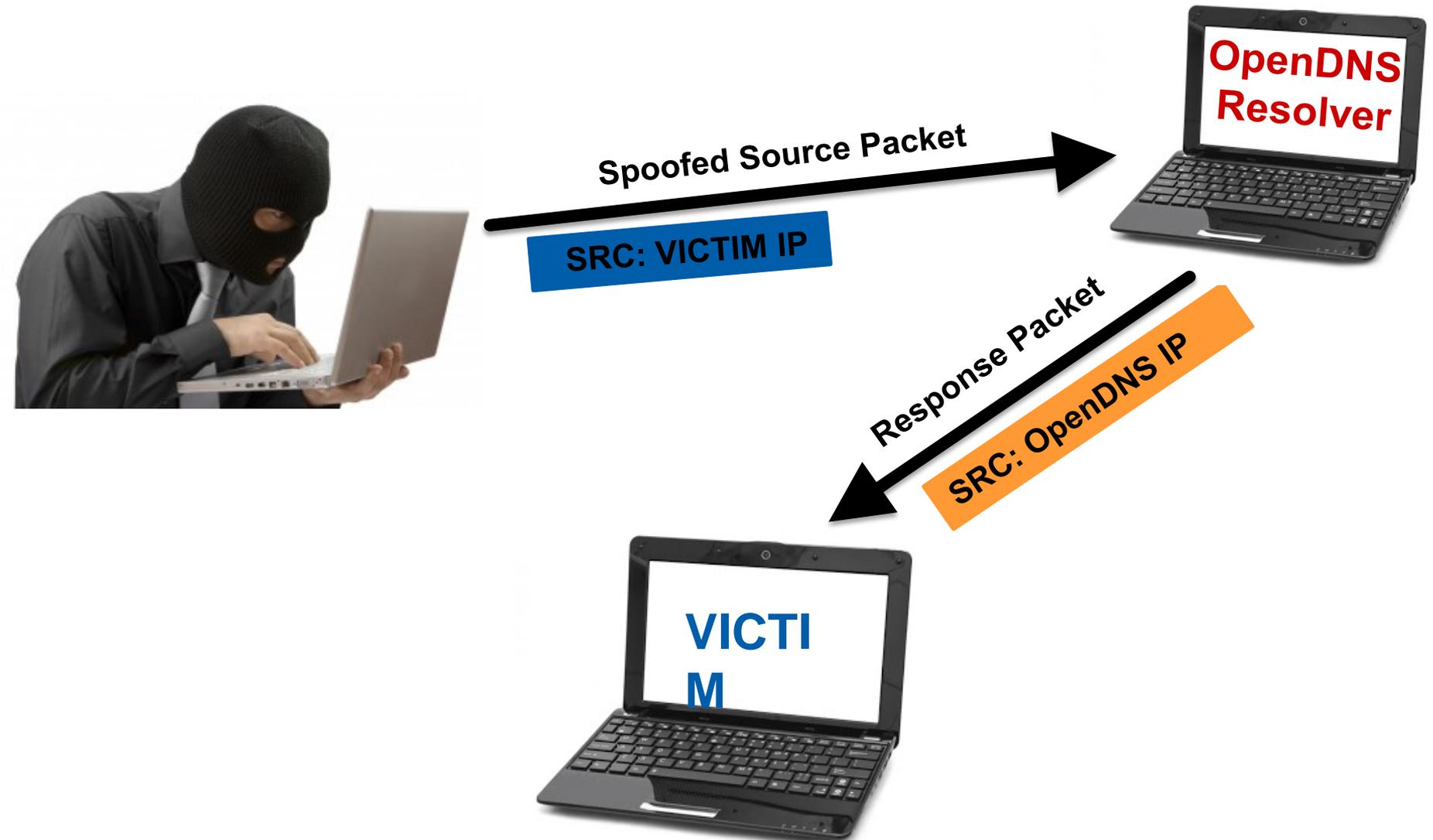
## Reflection



## Amplification



# DNS Amplification – Reflection example



## Execute 64 byte query

```
dcobaugh$ dig ANY isc.org @8.8.8.8
```

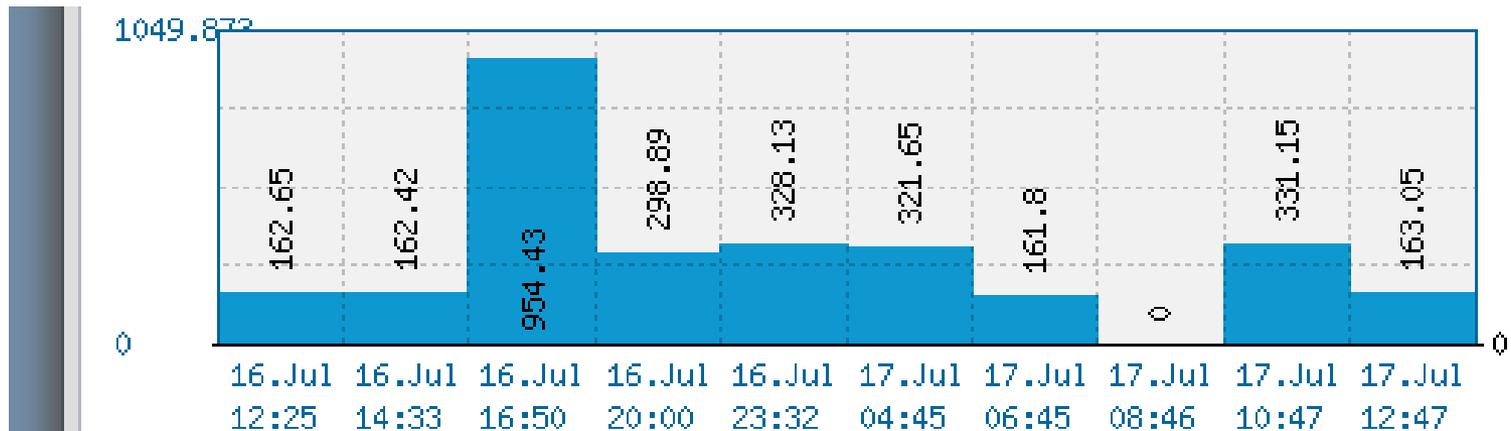
# DNS Amplification – Amplification Example continued

## Receive much larger response

```
;<<>> DiG 9.7.6-P1 <<>> ANY isc.org @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3791
;; flags: qr rd ra; QUERY: 1, ANSWER: 26, AUTHORITY: 0, ADDITIONAL: 0
;isc.org. 7187 IN NAPTR 20 0 "S" "SIP+D2U" "" _sip._udp.isc.org.
;isc.org. 7187 IN RRSIG NAPTR 5 2 7200 20130901004250 20130802004250 50012
;isc.org. tJqZK9kfHB8D9hh868rkVKe CnmzttN8HaA/en5bMUEVnztGZYxg2px9E9sEYwDg4LqGHDBVyYZGq066 yKSNx8xDmQuuNnyXTb
;; ANSWER SECTION=
isc.org. 3587 IN NSEC _adsp._domainkey.isc.org. A NS SOA MX TXT AAAA NAPTR
isc.org. 3587 IN RRSIG NSEC 5 2 3600 20130901004250 20130802004250 50012 i
vciB1zt1/KcB Zlscf8XXf6vJZsKJ0GfvPs 902tVF9ZUL31qEu0sQe2tZp53s/D0tMSEbIk0z7mpEChU6HjENkifEXw WRk6AJU7bhvI2ppTX/F
isc.org. 7187 IN DNSKEY 257 3 5 BEAAAA0hHQDBrhQbtphgq2wQUPEQ5t4DtUHxoMVFu2h
isc.org. /xyLYC06Krbdojwx8YMXLA5/KA+ u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPCLw+vT+U8eXEJm020jIS1ULgqy3 47cBB1zMnnz/4
isc.org. z Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xxzqZ7+ysyL K00edS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3o
isc.org. 7187 IN DNSKEY 256 3 5 BQEAAAABwuHz9Cem0BJ0JQT07C/a3McR6hMaufljs1d
isc.org. ZJnqTI8JyaFTw20M/ItBfh/hL2lm Cft207n3MfeqYtvjPnY7dWghYW4sVfH7VVEGm958o9nfi79532QeklXh x8pXWdeAaRU=
isc.org. 7187 IN RRSIG DNSKEY 5 2 7200 20130901004138 20130802004138 12892
kpH/GI+hyR63K VrwgJgkMA6I0fZCeS5PkH5uc 2825yGBkTkarKnLI7jhTQUY4W+snlBm+S18kaR1aiShSBbtJa+KlyYns paifU+jShseZXAZFR
isc.org. h+FZYm0Fi+8v5Lwh2bH4VRJNG2zaok8c0bhTCaE0yueY0gL6mAs00Y 1h95EuJSHQL5G08gRKEnm0EJmi+Fm5W2a0lVP6Icrvrf
isc.org. JZ7QCYpCE+v2+sq15vJIj0D6hYQ cIBj7A==
X/f6JUGYnpY0f 7187 IN RRSIG DNSKEY 5 2 7200 20130901004138 20130802004138 50012
isc.org. 9CI+gCd2Q9fsrkeoNuHXm8D+ ucmR5LHdTef5AGvLlSfjE3gvvBEoJEu17vBzxXoupMhb0PccyN5pZB2d AwHT1Fa1VVbCrrS5X
pCBTtKSwsZNd+ w=
isc.org. 7187 IN SPF "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16
28 ~all"
isc.org. 7187 IN RRSIG SPF 5 2 7200 20130901004250 20130802004250 50012 is
isc.org. NjBR7NcBVwYIdrMp/t6H5 XoeDZUP27BuwMR0KJq+H1Bapq/HI5c9TQ98a38guVPVyjAqXALDkFD5u zSQ9z1HWpkr4vKrGMNWB
15kYmX0QYsT16
isc.org. ;; Query time: 37 msec
isc.org. ;; SERVER: 8.8.8.8#53(8.8.8.8)
isc.org. ;; WHEN: Fri Aug 2 09:02:04 2013
isc.org. ;; MSG SIZE rcvd: 3030
```

**Spoof Source Address** – makes origin almost impossible to track down

**Bandwidth over-utilization** – can potentially cause network outages



The above graph displays service status activity for Networksolutions.com over the last 10 automatic checks. The blue bar displays the response time, which is better when smaller. If no bar is displayed for a specific time it means that the service was down and the site was offline.

**Service Status History :**

Date	Time	Ping Time	Date	Time	Ping Time
✓ 16.Jul.2013	12:25	162.65 ms.	✓ 16.Jul.2013	14:33	162.42 ms.
✓ 16.Jul.2013	16:50	954.43 ms.	✓ 16.Jul.2013	20:00	298.89 ms.
✓ 16.Jul.2013	23:32	328.13 ms.	✓ 17.Jul.2013	04:45	321.65 ms.
✓ 17.Jul.2013	06:45	161.8 ms.	17.Jul.2013	08:46	0
✓ 17.Jul.2013	10:47	331.15 ms.	17.Jul.2013	12:47	163.05 ms.

- Determine if your DNS servers are open resolvers
  - Open DNS Resolver Project [<http://openresolverproject.org>]
  - The Measurement Factory [<http://dns.measurement-factory.com>]
  - DNSInspect [<http://www.dnsinspect.com>]
  - Team Cymru Open Resolver Reports [<http://www.team-cymru.org/Services/Resolvers/>]
- Check DNS logs for large number of “ANY” requests with no matching
- Bandwidth over-utilization caused by influx of DNS UDP/53 traffic

- Little that can be done for complete mitigation
- Limit Recursion to authorized clients
  - Modify DNS configuration to only allow recursion only for the internal network
- Rate Limiting
  - Configure DNS and/or IPS to rate limit requests based on specific event rate in specified period of time.
- Block repeat offenders permanently



Highlight

 **Network Solutions**  
3 hours ago

The recent DDOS attack affecting some customers has now been mitigated. Customer websites should be resolving normally, and you should be able to readily access the Network Solutions site. If you continue to have issues, please contact our Customer Service team at 1-866-391-4357. Thanks to everyone for their patience as we resolved this issue.

Like · Comment 25



[Redacted name]

31 Jul

This terminal command launches as-if **DNS amplification** DDoS attack. send 64 bytes, get back >3000 #blackhat

[pic.twitter.com/vQYRKc3rfk](https://pic.twitter.com/vQYRKc3rfk)

Retweeted 6 times

Expand





# DNS Amplifier attack

DDoS attack uses over 1 million open recursive servers

- US-CERT [<http://www.us-cert.gov>]
- Team Cymru [<http://www.team-cymru.org>]
- Cloudflare [<http://blog.cloudflare.com>]
- Watchguard [<http://www.watchguard.com>]
- Security Bistro [<http://www.securitybistro.com>]
- Dell SecureWorks [<http://www.secureworks.com>]

***THE VALUE OF PERFORMANCE.***

***NORTHROP GRUMMAN***



- US-CERT [<http://www.us-cert.gov>]
- Team Cymru [<http://www.team-cymru.org>]
- Cloudflare [<http://blog.cloudflare.com>]
- Watchguard [<http://www.watchguard.com>]
- Security Bistro [<http://www.securitybistro.com>]
- Dell SecureWorks [<http://www.secureworks.com>]

***THE VALUE OF PERFORMANCE.***

***NORTHROP GRUMMAN***





# CSRM GRC Tool Overview

**Michael Watson**

Chief Information Security Officer

---

ISOAG

August 7<sup>th</sup>, 2013



## Agenda

- What is the VITA CSRM GRC tool?
- What data is in the GRC tool?
- What does CSRM do with your data?
- What is CSRM doing with this tool?
- How should agencies use the tool?
- What are the future plans for this tool and the risk management program?



## The IT GRCS Tool

- What does GRCS Stand for?
  - G – Governance
  - R – Risk
  - C – Compliance
  - S – Security
- Repository for information security program data
- Links together several VITA repositories of information to generate risk and compliance information



## What is in the tool?

- Annual report data points
- ISO status and certification data
- IT security audit program information
  - IT Security audit plans
  - Scheduled security audits
  - Audit reports
  - Identified findings
  - Remediation plans/Corrective action plans
- Risk management program information
  - Business processes
  - Agency criticality rating of those business processes
  - Risk findings from risk assessments
- Other agency data provided to VITA



## Where is the data coming from?

- Data has multiple possible sources
  - Agency submitted
  - Other VITA data sets
  - Northrop Grumman data



## Data provided by agencies

- All “Application” data is coming from CETR
  - Agencies who have system names that do not easily map to CETR will be contacted for clarification
  - Agencies who are not required to use CETR will have “Applications” created for them
- IT security audit program data
- Risk management program data
- ISO certification data
- Agency annual report data
  - Must be consistent to put it into the system



## VITA Data Sets

- CETR
  - Repository for applications, data sets, and technology used by agencies
- Partnership data
  - When necessary data will be pulled from partnership sources
    - Examples - EOL software and hardware and local admin rights issues
- Threat scans
  - Data identified from threat monitoring
- Security exception list
  - Status of exceptions will be listed
  - Process for exception renewal in a future phase
- Security incidents



# What does CSRM do with your data?

- Current
  - Normalize data against existing data sets
    - Compare to CETR, existing documentation, etc.
  - Identify findings within the data submitted
  - Identify a risk rating for findings
  - Evaluate the impact of existing risks to the agency
- Future
  - Identify risks that an agency will be subject to in the future
  - Create risk recommendations/findings
  - Enforce compliance and risk treatment



## What will CSRM do with the tool?

- Enhance reporting capabilities
  - Identify agencies carrying too much risk
  - Monitor remediation of risk at agencies
  - Show progress of agencies remediating risk
  - Identify operational issues increasing agency risk
- Make recommendations based on risk
  - Based on risk information recorded in the tool
  - Recommendations to AITR, ISO, agency head, secretary, and/or Commonwealth CIO
  - Can include recommendation to restrict IT investments until acceptable remediation is in place, underway, planned, or complete



## How Does CSRM Measure Agency Risk?

- Risk levels primarily based on findings
  - Qualitative evaluation
  - Findings are information security issues identified within an agency
  - Can come from any source
    - Security audit, risk assessment, operational data, etc.
- Finding criticality level based on several factors, examples include:
  - Business processes criticality level
  - Confidentiality of the data
  - Likelihood of occurrence
  - Magnitude of impact
  - Length of time finding open
  - Criticality of the application affected

► About

▼ General Information

Finding ID:	FND-15	Target:	Applications: <a href="#">Personnel Action Application (PAA)</a>
Agency:	<a href="#">Virginia Information Technologies Agency</a>	Agency Submit Date:	
Status:	Open	Authoritative Source References:	Authoritative Sources: <a href="#">AC-02 Account Management</a> Risk Register: <a href="#">RSK-6</a> Risk Register: <a href="#">RSK-20</a> Risk Register: <a href="#">RSK-52</a>
Category:	2012 VITA Risk Assessment Finding	Control Standards:	<a href="#">Access Authorization Process</a> <a href="#">Add</a>
Criticality:	●	Source Override:	Risk
Year:	2013	Date Closed:	
Source of Audit Finding:		Agency Finding Reference Field:	VITA Risk Assessment Finding PAA1
Magnitude of Impact:	●	Probability of Occurrence:	●

Workflow and Description

Response

▼ Workflow

Assigned to:	<a href="#">Shaw, Mauri</a>	Submit Date:	12/31/2012
Reviewer:	<a href="#">Smith, Jonathan M</a>	Review Status:	Awaiting Review
Submission Status:	In Process	Review Date:	

▼ Description

Name:	CIPR confidential data may be exposed or changed without management approval.		
Finding:	CIPR sensitive application audit log files are not reviewed for audit or security. <b>Risk Summary:</b> Potential harmful actions taken or not taken by System Administrators and or users would not be reviewed for audit or security.		
Response:	Remediate Risk		



# Where Does CSRM Get Risk Rating Data?

- IT Security Audit Program
  - Findings submitted by auditors
- Risk Management Program
  - Risk assessments
    - Results from risk assessments
  - Business Impact Analysis
    - Ratings provided from the BIAs submitted last year
  - Threat information
- Partnership Information
- Inherent Risk Calculations
  - The risk level when proper controls are not applied
- Residual Risk Calculations
  - The risk level when proper controls are applied
  - Exceptions should lower residual risk values



## What should agencies use the tool for?

- Review the current picture of agency risk based on CSRM data
  - Important to make sure agencies don't experience issues due to inaccurate data
- Prioritize risk mitigation steps based on most critical findings
- Obtain support from management to address agency risk
  - Include impact due to lack of risk mitigation



## Examples of Use

- Review annual report status
- Review ISO status and certification data
- Review IT security audit program status
- Review outstanding findings
- Review status of high risk findings
- Submit remediation and treatment plans based on risk rating
- Review security incident information
- Review business processes identified as critical



## Where do I go to see this information?

- The agency page will contain summary information
- Emails containing agency data points will be sent to agencies on a monthly basis
- Emails sent for pending expirations and expired information
- Dashboard will be available on sign-in



## Agency: Alcoholic Beverage Control



Record 1 of 127

First Published: 7/2/2013 1:10 PM Last Updated: 7/31/2013 11:14 PM

### About

#### General Information

Agency Name:	Alcoholic Beverage Control	Agency Acronym:	ABC
Web Site:	<a href="http://www.abc.virginia.gov">http://www.abc.virginia.gov</a>	Number of Employees:	2,639
Agency Number:	999	Authorized Users/Groups - Permissions:	ABC:ISO
Agency Secretariat:	Public Safety	Government Branch:	Executive Branch
Partnership Full Service Customer:	Yes		
Description:			

#### Agency Scorecard Data

ISO Certification Status:	<span style="color: green;">●</span>	Previous Year ISO Certification Status:	<span style="color: red;">●</span>
3 Year Audit Obligation:		3 Year Audit Obligation - Previous Year:	
Current Year Percentage of Audits Received:	0 %	Previous Year Percentage of Audits Received:	
Audit Plan Status:	<span style="color: green;">●</span>	Audit Plan Status - Previous Year:	<span style="color: green;">●</span>

#### Infrastructure Metrics

Total Applications:	45	Total Processes:	92
Total Sensitive Systems:	0	Total Critical Business Processes:	41
Total Information Assets:	0	Total Devices:	0
Total Products & Services:	0	Total Facilities:	0



## What do I do if I don't agree with CSRM?

- Check the data in the system first
  - Data could be out of date
  - Possible mistake
- Email Commonwealth Security if data is inaccurate or you would like to discuss further



## What are the future plans?

- Further refine the risk process
  - Move from qualitative to quantitative
- Refine agency risk ratings further
- Establish key risk indicators for predicting risk
- Allow direct edits by agencies
- Integrate more data into the tool



## ITGRCS Key Points

- Official repository for reporting
  - Annual report
  - Quarterly summary information
  - Risk recommendations
- Risk data repository
  - Identified findings will be monitored
  - Risk mitigation progress recorded
  - Exception repository



Virginia Information Technologies Agency

# Upcoming Events





## COVITS 2013

*COVITS is a forum to discuss technology requirements, share valuable lessons from actual case studies, and glimpse the future of government interaction with its customers.*

***September 9 & 10***

***Richmond Marriott***

500 East Broad Street, Richmond, VA 23219

***Register Here:*** <http://www.govtech.com/events/COVITS-2013.html>



# COVITS 2013: Governor's Technology Awards

The submission window for the  
**Governor's Technology Awards**  
is open through ***Friday, August 9***

The categories are:

- Cross-Boundary Collaboration on IT Initiatives
- IT as Efficiency Driver – Government to Citizen
- IT as Efficiency Driver – Government to Business
- IT as Efficiency Driver – Government to Government
- Innovative Use of Technology in Economic Development
- Innovative Use of Technology in Local Government
- Innovative Use of Technology in Education
- Innovative Use of Technology in Healthcare
- Innovative Use of Technology in Modeling and Simulation
- Innovative Commercialization of Technology Research

More information is available at:

<http://www.covits.org/awards.cfm>



# Information Security System Association

## ISSA

**DATE:** Wednesday, August 14, 2013

**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:** Roland Cloutier, Automatic Data Processing, Inc.

**TOPIC:** TBD

More info located here: <http://centva.issa.org/central-va-issa-feb-2013-meeting/>



# IS Orientation

**When: Thursday, Sept 5, 2013**

**Time: 10:00 am to Noon**

**Where: CESC , Room 1221**

**Register here:**

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

**Next IS Orientation will be held on Dec 5, 2013**



# DOA Training Offering

## Interviewing Techniques for Auditors

Instructor: Angela Nino (Wicklender-Zulawski)

**Date: September 18 & 19, 2013**

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

**Location: James Monroe Building  
DGS Conf. Rm. C, 1st FL**

**Cost: \$ 320.00**

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



# UC Irvine Information Security Cert Program

Information Systems Security professionals develop key knowledge of information systems security including access control, administration, auditing and monitoring, risk, response, and recovery. Gain the knowledge required to sit for the Certified Information Systems Security Professional (CISSP) exam.

**Date: September 3, 2013** thru **June 10, 2014**

**Time: 5:00 pm – 9:00 pm**

**Location: CESC**

**Register by August 9!**

**Information & Register:** [missy.clayton@unx.uci.edu](mailto:missy.clayton@unx.uci.edu)



## CISM Prep Course & Security+ Boot Camp Offering

Global Knowledge is hosting a CISM Prep Course and Security+ boot camp onsite at Northrop Grumman's CESC facility and we have seats available!

### CISM Prep Course

**Dates:** Tuesday Nov 12<sup>th</sup> – Thurs Nov 14<sup>th</sup>

**Time:** 8:30 am – 4:30 pm

**Cost:** \$ 1,100 -\$1,200      ***\*Register by August 9<sup>th</sup> to reserve seat!!***

### Security+ Boot camp

**Dates:** Monday Oct 7<sup>th</sup> – Friday Oct 11<sup>th</sup>

**Time:** 8:00 am – 6:00 pm

**Cost:** \$1,625      ***\*Register and pay by Sept 13 to reserve seat***

If you would like to register, please contact Kristen Miller at 252-756-4757 / [Kristen.miller@globalknowledge.com](mailto:Kristen.miller@globalknowledge.com) with payment or if you have any questions. Payment in the form of a company funded PO or credit card will secure your seat and is required before class starts.



## Future ISOAG Dates

**Sep 4                      1:00 – 4:00 pm @ CESC**

**Keynote Speaker: Dr. Larry Wortzel, Asia Strategies & Risk, LLC  
on “Chinese Cyber-Security Threat”**

**Oct 2                      1:00 – 4:00 pm @ CESC**

**Keynote Speakers: Hank Leininger, Kore Logic  
on “Passwords & Password Cracking”**

**And**

**Joe Segreti, Kore Logic  
on “Secure Source Code”**

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



## 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*

7 Aug, 2013



***NORTHROP GRUMMAN***



# ADJOURN

