



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

February 6, 2013



# ISOAG February 2013 Agenda

- |      |   |   |
|------|---|---|
| I.   | Welcome & Opening Remarks   | Michael Watson, VITA                    |
| II.  | Opening Up A Second Front<br>For Cyber Security & Risk Management | Dr. Ron Ross, NIST                      |
| III. | Clicker Millionaire   | Ed Miller, VITA                         |
| IV.  | Upcoming Events & Other Business                                  | Michael Watson, VITA                    |
| V.   | Partnership Update  | Bob Baskette, VITA<br>Michael Clark, NG |
| VI.  | Microsoft End of Life   | Bob Baskette, VITA                      |

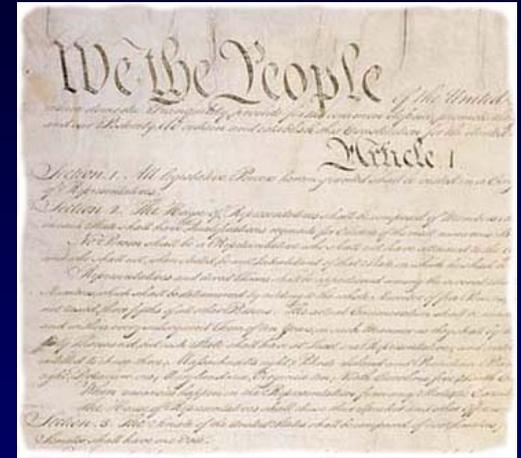
# Opening Up a Second Front for Cyber Security and Risk Management

Dr. Ron Ross

*Computer Security Division  
Information Technology Laboratory*



The seeds of information security and privacy in the digital age, were planted in United States Constitution over two centuries ago...



# The United States Constitution

“WE THE PEOPLE of the United States, in Order to form a more perfect Union, establish Justice, ensure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America...”

Information security and privacy,  
traditional societal values, are  
at greater risk today due to the  
ever increasing size of our  
*digital footprint...*



# Why Is Cyber Security Important?

- Because many information systems in the public and private sectors that are part of the U.S. critical infrastructure are extremely vulnerable to hostile cyber attacks and other threats...
- These systems must be more *reliable, trustworthy, and resilient.*



# Conventional Threats

- *What do we worry about?*
  - Hostile cyber attacks
  - Natural disasters
  - Structural failures
  - Human errors of omission or commission



# Advanced Persistent Threat

*An adversary that —*

- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations—
  - To exfiltrate information.
  - Undermine / impede critical aspects of a mission, program, or organization.
  - Position itself to carry out these objectives in the future.

# The First Front.

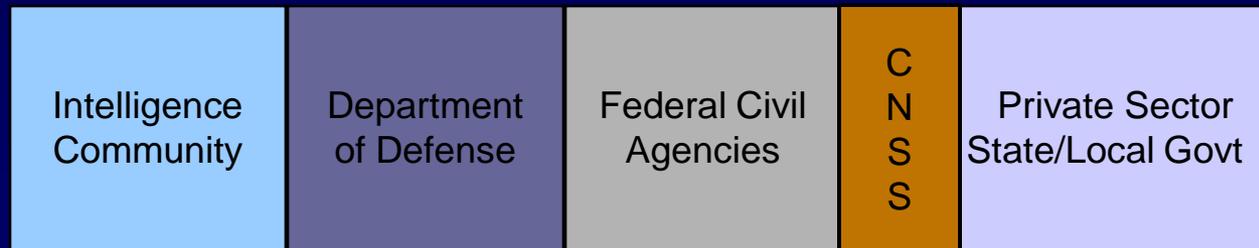
*What we have accomplished...*

# Unified Information Security Framework

## The Generalized Model

**Unique  
Information  
Security  
Requirements**

*The “Delta”*



**Common  
Information  
Security  
Requirements**

Foundational Set of Information Security Standards and Guidance

- Risk management (organization, mission, information system)
- Security categorization (information criticality/sensitivity)
- Security controls (safeguards and countermeasures)
- Security assessment procedures
- Security authorization process

National security and non national security information systems

# Joint Task Force Transformation Initiative

- In 2012, completed development of comprehensive security guidelines that can be adopted by all federal agencies including the national security community.
- Flexible and extensible tool box includes:
  - *An enterprise-wide risk management process.*
  - *State-of-the-practice, comprehensive, security controls.*
  - *Risk management framework.*
  - *Risk assessment process.*
  - *Security control assessment procedures.*

# Unified Information Security Framework

- **NIST Special Publication 800-39**  
*Managing Information Security Risk:  
Organization, Mission, and Information System View*
- **NIST Special Publication 800-30**  
*Guide for Conducting Risk Assessments*
- **NIST Special Publication 800-37**  
*Applying the Risk Management Framework  
to Federal Information Systems*
- **NIST Special Publication 800-53**  
*Recommended Security Controls for Federal  
Information Systems and Organizations*
- **NIST Special Publication 800-53A**  
*Guide for Assessing the Security Controls  
in Federal Information Systems and Organizations*

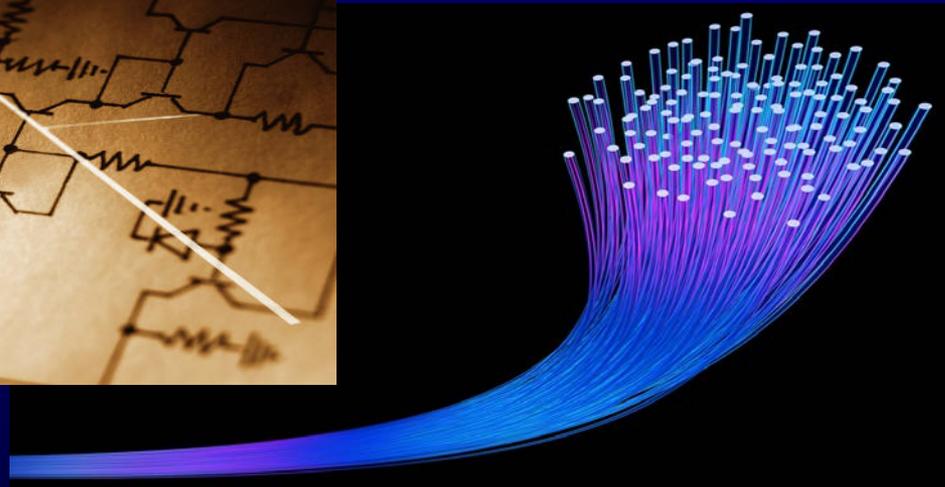


# The Second Front.

*What we need to accomplish...*

*The federal cyber security strategy...*

# Build It Right, Then Continuously Monitor



# Unconventional Threats

*What should we worry about?*



*Complexity*

*Connectivity*



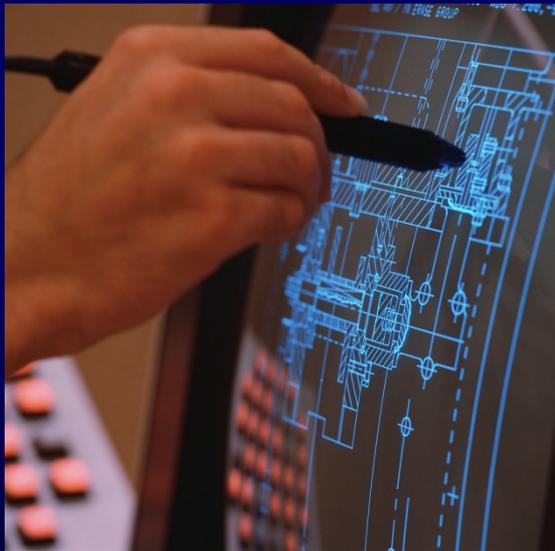
*Culture*

# Complexity.

*Ground zero for our current problems...*

If we can't understand it –  
*we can't protect it...*

We need to build our security programs like NASA builds space shuttles—using the *integrated project team* concept.



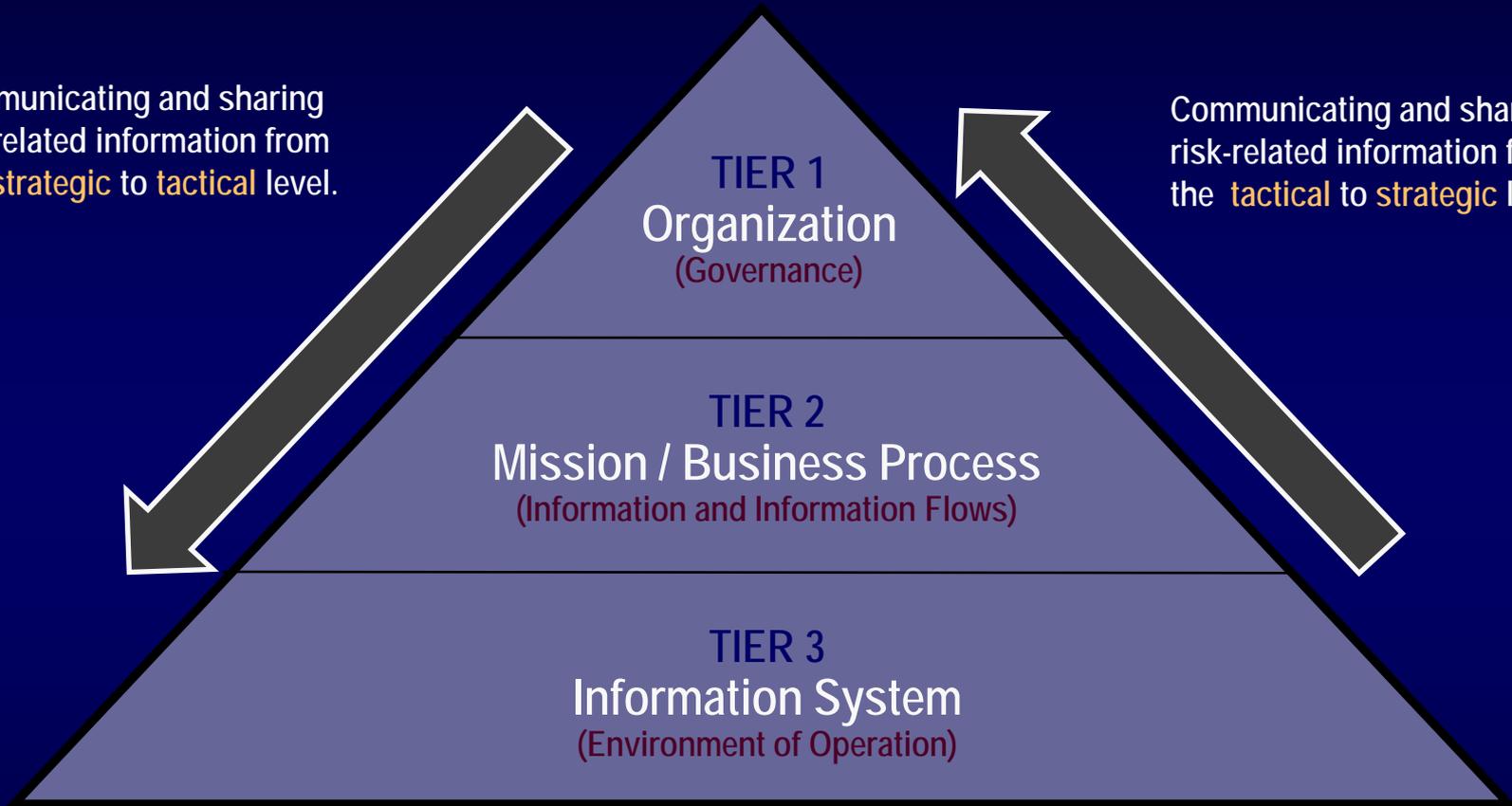
What can we do to change course?

*Simplify, Specialize, and Integrate...*

# STRATEGIC RISK FOCUS

Communicating and sharing risk-related information from the **strategic** to **tactical** level.

Communicating and sharing risk-related information from the **tactical** to **strategic** level.



# TACTICAL RISK FOCUS

# A New Approach for Information Security

- Work directly with mission/business owners and program managers.
- Bring all stakeholders to the table with a vested interest in the success or outcome of the mission or business function.
- Consider information security requirements as mainstream functional requirements.
- Conduct security trade-off analyses with regard to cost, schedule, and performance requirements.
- Implement enforceable metrics for key officials.

# Increasing Strength of IT Infrastructure

- Simplify.
  - Reduce and manage *complexity* of IT infrastructure.
  - Use enterprise architecture to streamline the IT infrastructure; *standardize, optimize, consolidate* IT assets.
- Specialize.
  - Use guidance in SP 800-53, Rev 4 to *customize security plans* to support specific missions/business functions, environments of operation, and technologies.
  - Develop effective *monitoring strategies* linked to specialized security plans.

# Increasing Strength of IT Infrastructure

- Integrate.
  - Build information security requirements and controls into mainstream organizational processes including:
    - *Enterprise Architecture.*
    - *Systems Engineering.*
    - *System Development Life Cycle.*
    - *Acquisition.*
  - Eliminate information security programs and practices as stovepipes within organizations.
  - Ensure information security decisions are risk-based and part of routine *cost, schedule, and performance* tradeoffs.

# Defense-in-Depth



## Links in the Security and Privacy Chain: Security and Privacy Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical and personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring
- ✓ Privacy protection
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

*Adversaries attack the weakest link...where is yours?*

# Defense In Depth is a Good Strategy

*Until it fails...then what?*

# Resilience.

*The only way to go for critical missions  
and information systems...*

# Dual Protection Strategies

*Sometimes your information systems will be compromised even when you do everything right...*

- **Boundary Protection**

Primary Consideration: *Penetration resistance.*

Adversary Location: *Outside defensive perimeter.*

Objective: *Repel the attack.*



- **Agile Defense**

Primary Consideration: *Information system resilience.*

Adversary Location: *Inside defensive perimeter.*

Objective: *Operate while under attack, limit damage.*

# Agile Defense

- Boundary protection is a necessary but not sufficient condition for *Agile Defense*.
- Examples of *Agile Defense* measures—
  - Compartmentalization and segregation of critical assets.
  - Targeted allocation of security controls.
  - Virtualization and obfuscation techniques.
  - Encryption of data at rest.
  - Limiting privileges.
  - Routine reconstitution to known secure state.

*Bottom Line: Limit damage of hostile attack while operating in a (potentially) degraded or debilitated state...*

# Special Publication 800-53, Revision 4.

*Big changes on the way...*

# Gap Areas Addressed

- Insider threat.
- Application security.
- Supply chain risk.
- Security assurance and trustworthy systems.
- Mobile and cloud computing technologies.
- Advanced persistent threat.
- Tailoring guidance and overlays.
- Privacy.

# SP 800-53 Rev 4 Driving Major Changes

(1 of 2)

- Special Publication 800-82 (Industrial Control System Security) undergoing major changes.
  - *Phase I: ICS Appendix from SP 800-53, Revision 3, moving to SP 800-82 (simultaneous release with SP 800-53, Revision 4).*
  - *Phase II: Full update to SP 800-82 by September 2013.*
- Privacy requirements and controls will be part of standard lexicon and coordinated with security requirements.
- Overlay concept promotes specialization of security plans for federal agencies; potential significant expansion of use by private sector (voluntary basis).

# SP 800-53 Rev 4 Driving Major Changes

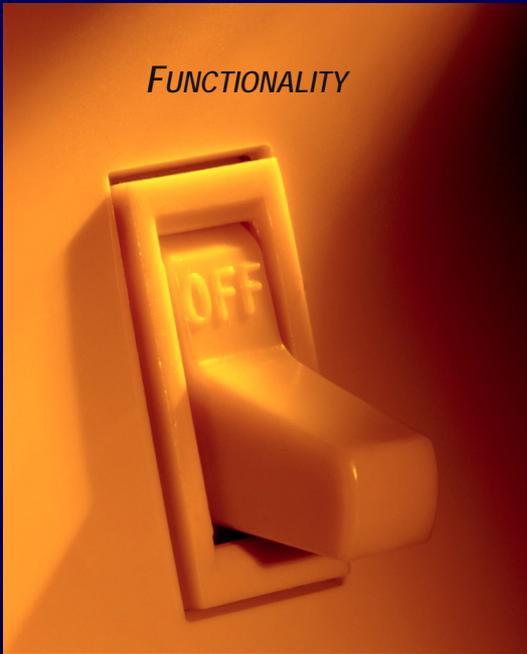
(2 of 2)

- Special Publication 800-160 (Security Engineering Guideline) targeted for publication in late 2013.
  - *Security controls in SP 800-53, Revision 4, addressing trustworthy systems, assurance, and system resilience.*
  - *Exploring the possibility of system resiliency appendix in SP 800-53.*
- Opening up new discussions on the concept of assurance.
  - *How federal agencies can obtain IT products and information systems with greater assurance.*
  - *SP 800-53, Revision 4, (internal) mapping to Common Criteria (ISO/IEC 15408) requirements.*
- Impacting ISO/IEC 27001 and 27002.

# Functionality and Assurance.

*They ride together...*

*FUNCTIONALITY*



What is observable in front of the wall.

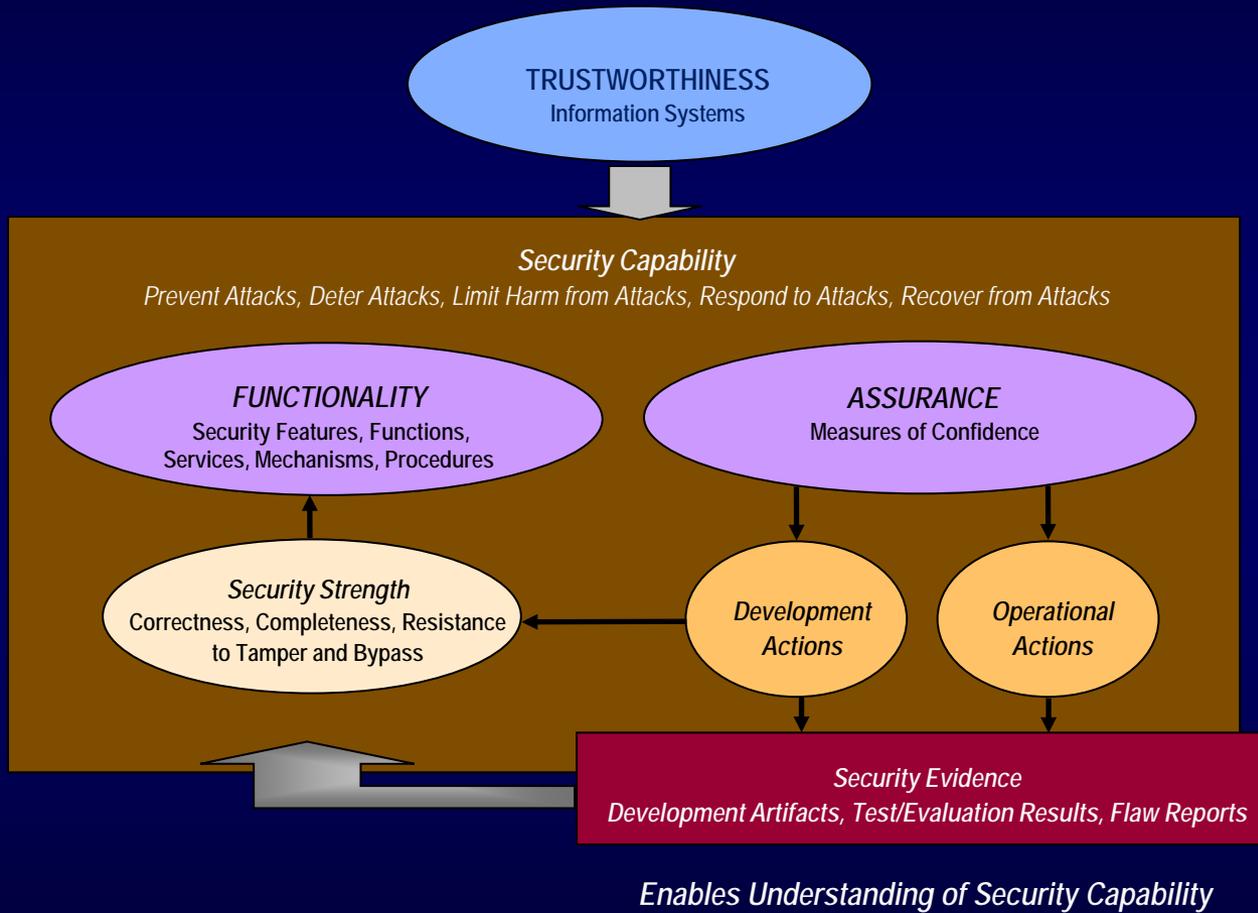
What is observable behind the wall.



*ASSURANCE*



# Assurance and Trustworthiness



Assurance.

*You don't need it until you need it...*

# Rebranding the Concept of Assurance

*Making the assurance argument for today's practitioners—*

- Objectives for Special Publication 800-53, Revision 4
  - What is assurance?
  - Why is assurance important?
  - When is assurance needed?
  - How are organizations obtaining assurance now?
  - How can organizations obtain increased levels of assurance in the future?

# Trustworthiness and Assurance

- Significant changes to security controls and control enhancements—
- Configuration Management (CM) family.
- System and Services Acquisition (SA) family.
- System and Information Integrity (SI) family.

*Applying best practices in software application development at all stages in the SDLC.*

# Significant Updates to Security Controls

- Development processes, standards, and tools.
- Developer security architecture and design.
- Developer configuration management.
- Developer security testing.
- Developer-provided training.
- Supply chain protection.

# Minimum Assurance – Appendix E

- Appendix E has been completely revised.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.

Table E-1  
Minimum Assurance for Low Impact Baseline

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-5, SA-9
IA	IA-1	SC	SC-1, SC-41
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

And after we build it right.

*What next?*

# Continuous Monitoring

- Determine effectiveness of risk responses.
- Identify changes to information systems and environments of operation.
- Verify compliance to federal legislation, Executive Orders, directives, policies, standards, and guidelines.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

And until we build it right.

*What should we do?*

# Important Stop-Gap Actions

- For high-end adversaries launching sophisticated and well-coordinated cyber attacks targeting: U.S. critical infrastructure; federal mission-essential functions and systems; and private sector industries—
  - ✓ Develop, implement, and exercise robust contingency plans to support full scale continuity of operations;
  - ✓ Implement continuous monitoring programs; and



Some random thoughts.

*In not so random order...*

Information security is hard.

*But it is important...*

Think strategic.  
*Execute tactical...*

Information has value.

*But not all information is valuable...*



Least privilege and least functionality.

*Powerful concepts that reduce risk...*

Adversaries are not ten feet tall.

*They have work factors and attack sequences  
that can be disrupted...*



# Managing risk.

*Doesn't mean fixing everything...*



- ✓ **Frame**
- ✓ **Assess**
- ✓ **Respond**
- ✓ **Monitor**



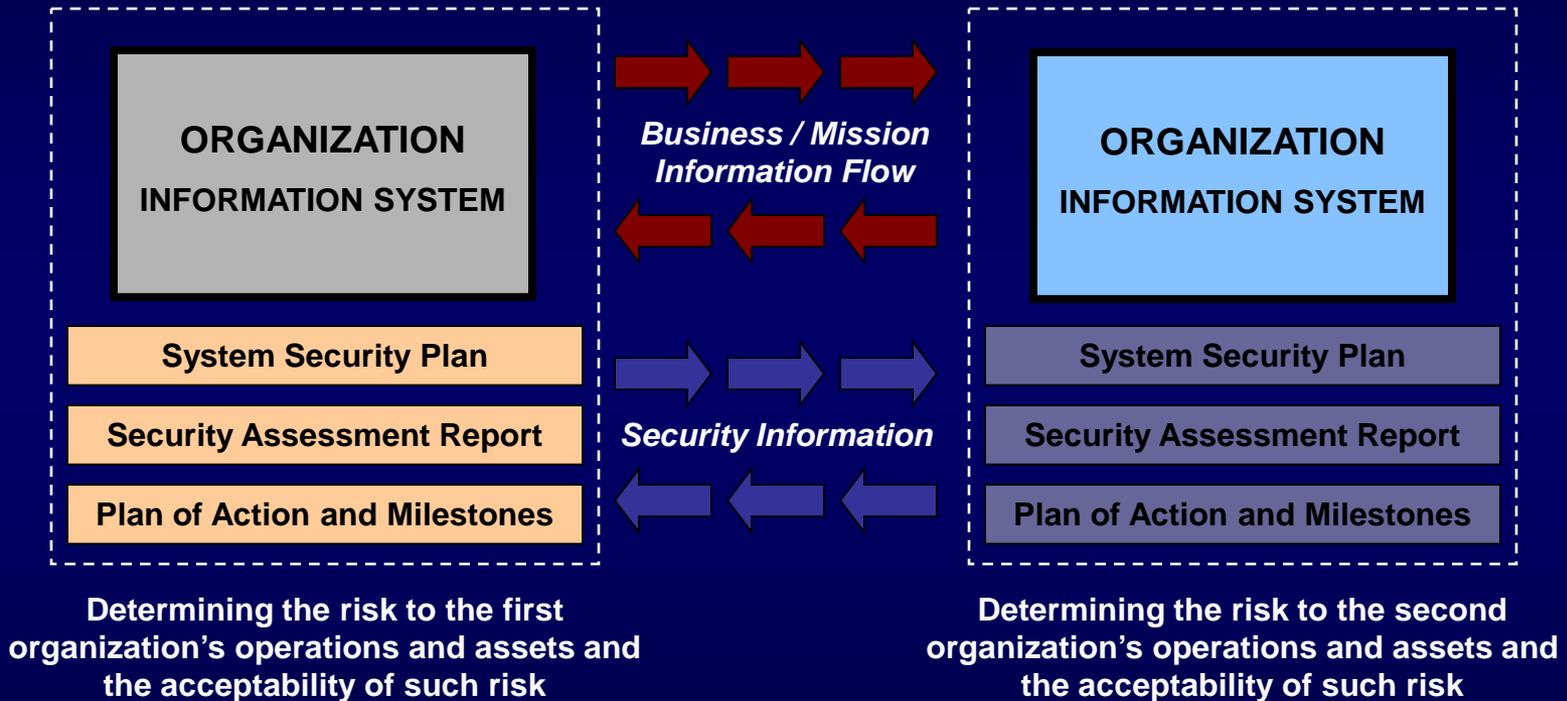
# Risk Tolerance.

*How you know when to stop deploying  
security controls...*



# The Desired End State

## *Security Visibility Among Business/Mission Partners*



The objective is to achieve *visibility* into prospective business/mission partners information security programs establishing levels of security due diligence and trust.

# Contact Information

100 Bureau Drive Mailstop 8930  
Gaithersburg, MD USA 20899-8930

## *Project Leader*

Dr. Ron Ross  
(301) 975-5390  
ron.ross@nist.gov

## *Administrative Support*

Peggy Himes  
(301) 975-2489  
peggy.himes@nist.gov

## *Senior Information Security Researchers and Technical Support*

Pat Toth  
(301) 975-5140  
patricia.toth@nist.gov

Kelley Dempsey  
(301) 975-2827  
kelley.dempsey@nist.gov

Arnold Johnson  
(301) 975-3247  
arnold.johnson@nist.gov

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)

Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)



## Clicker Millionaire

Who Wants to be a  
SEC501/NIST SP 800-53  
*Clicker Millionaire?*

Ed Miller CISA, CISM, CIA, CIPP/IT



# Clicker Millionaire Rules

We're playing as teams. Not individually.

We go through every question. Each question is worth progressively more points than the previous question.

There is no elimination if you miss a question.

No Life Lines. No Poll the Audience. No 50/50.  
However, you may Phone Bob.

The clicker software won't let me go up to 1 million so the scores are adjusted down a little.

# Team Scoring

- Team scores are the average of the total team.
- For example, let's say there are 10 teammates answering a 1000 point question. 7 answer correctly and 3 answer incorrectly.

$$(7 \text{ correct} \times 1000) + (3 \text{ incorrect} \times 0) = 7000$$

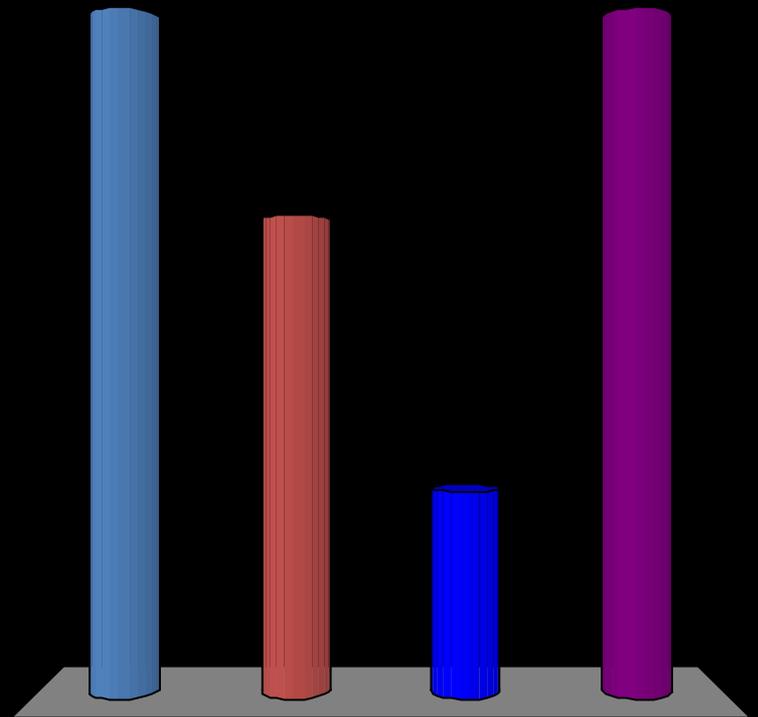
$$7000 / 10 \text{ teammates}$$

$$= 700 \text{ points}$$

- Here we go!

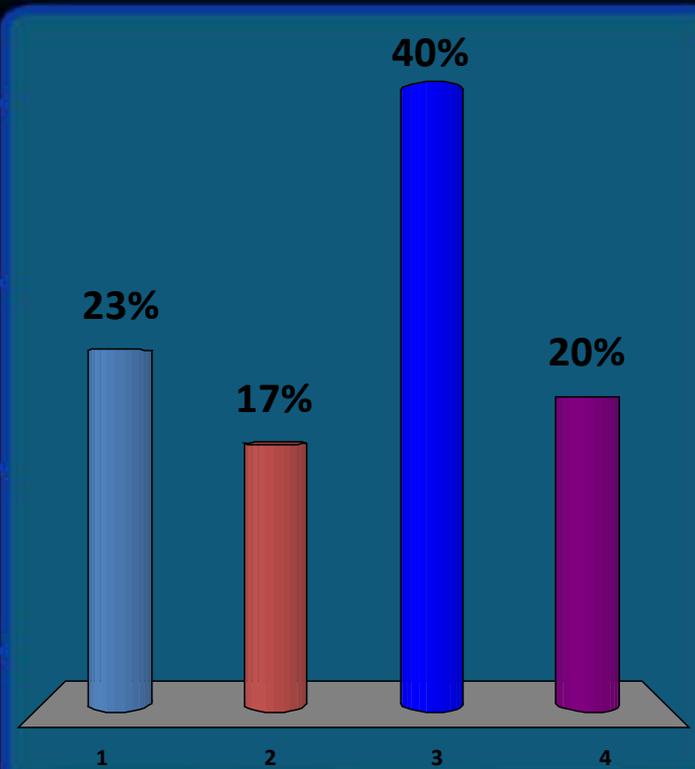
# Please select your birth month.

1. Jan-Feb-Mar
2. Apr-May-Jun
3. Jul-Aug-Sep
4. Oct-Nov-Dec



# What security control family is identified by “AC”?

1. Authorization Control
2. Authentication Compliance
3. Awareness Compliance
4. Access Control

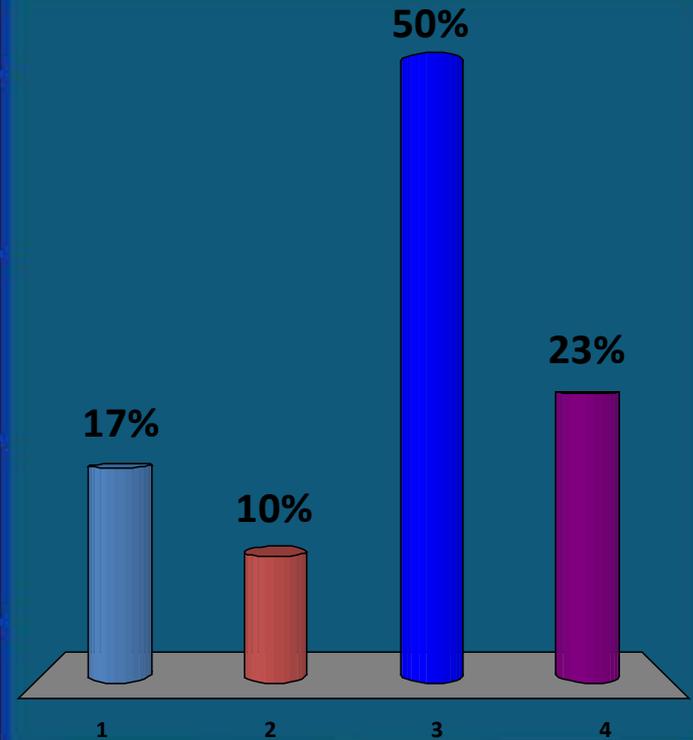


1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# What security control family is identified by “PS”?

1. Physical Security
2. Planning for Systems
3. Personnel Security
4. Program Structuring



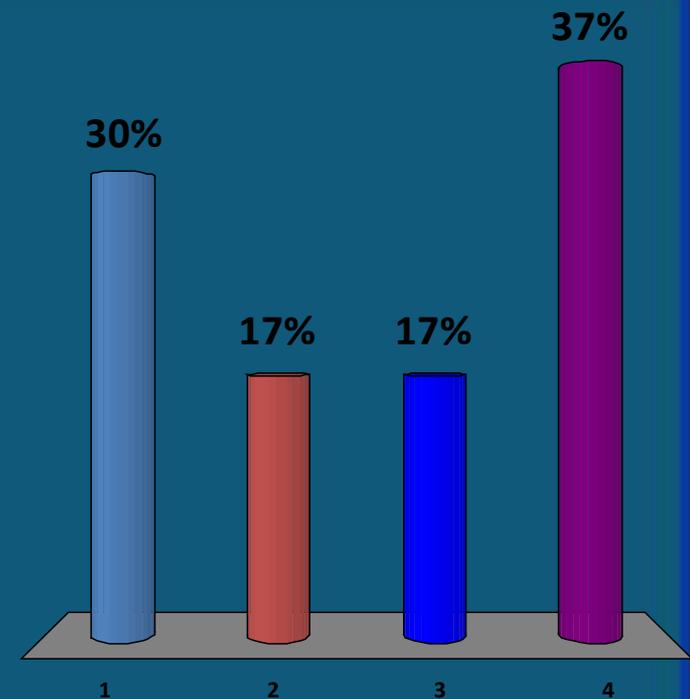
1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000

2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# What security control family is identified by “CM”?

1. Configuration Mgmt
2. Compliance Mgmt
3. Certification Mgmt
4. Contingency Mgmt

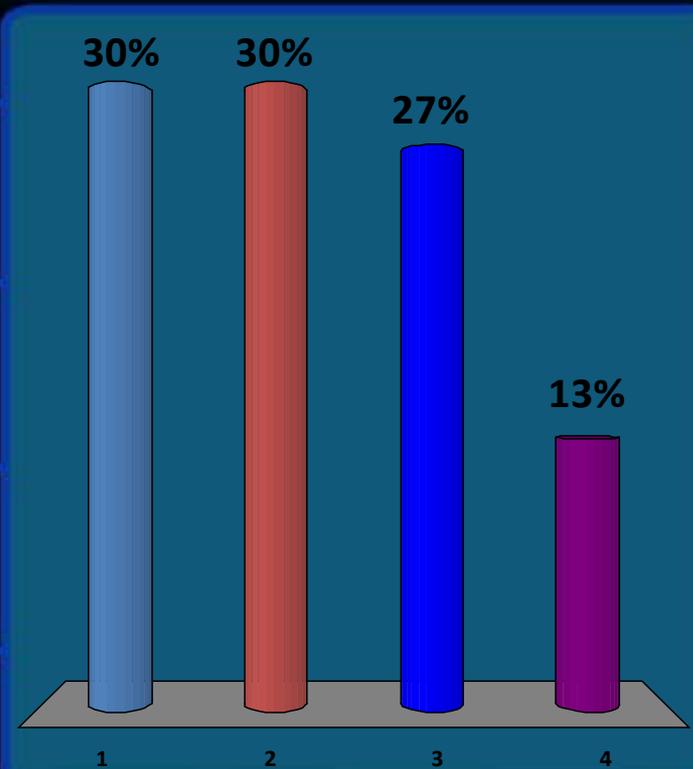


1 - 5   3 - 20   5 - 40   7 - 100   9 - 300   11 - 500   13 - 2000  
2 - 10   4 - 30   6 - 50   8 - 200   10 - 400   12 - 1000   14 - 5000

**15 - 10000**

# What security control family is identified by “MA”?

1. Management
2. Maintenance
3. Monitoring Apps
4. Media Access

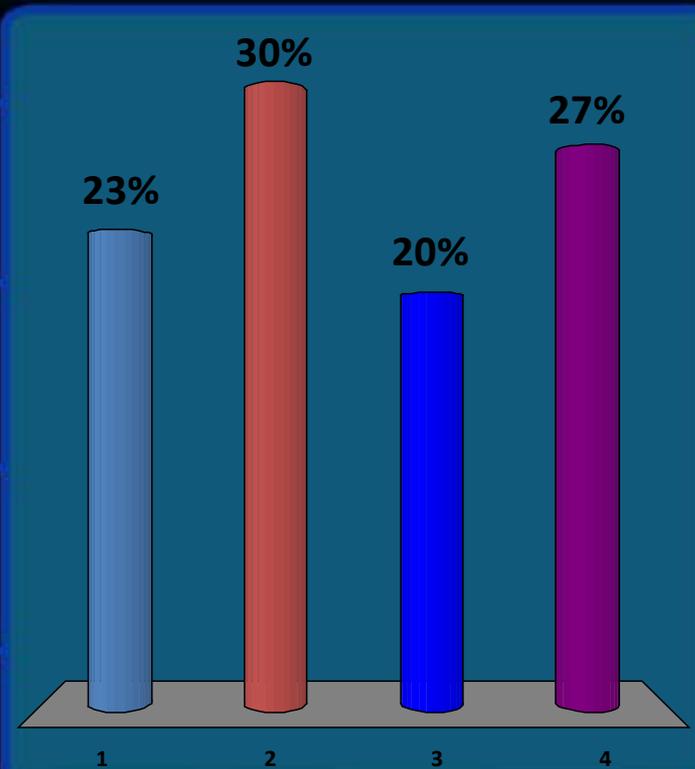


1 - 5   3 - 20   5 - 40   7 - 100   9 - 300   11 - 500   13 - 2000  
2 - 10   4 - 30   6 - 50   8 - 200   10 - 400   12 - 1000   14 - 3000

**15 - 10000**

# What security control family is identified by “SC”?

1. Security Compliance
2. System & Communications Protection
3. System Compliance
4. Secure Communications



1 - 5    3 - 20    **5 - 40**    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# Team Scores

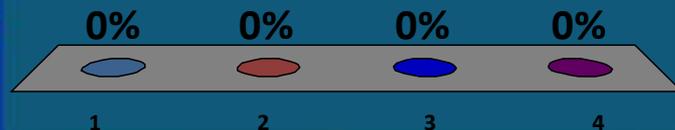
Points	Team
35	Apr-May-Jun
35	Jan-Feb-Mar
35	Oct-Nov-Dec
15	Jul-Aug-Sep

# Top 5 Participant Scores

Points	Participant	Points	Participant
100	10	45	19
100	18	40	13
90	2	40	25
90	28	15	9
80	7	10	1
75	17	10	16
65	4	10	20
60	12	10	21
60	3	10	24
50	29	10	27

A hacker drops a virus on a USB drive in the parking lot hoping an employee will pick it up. In addition, to “SI3 Malicious Code Protection”, what control would best mitigate this risk?

1. CM3-Configuration Change
2. AT2-Sec Awareness Training
3. SA3-Life Cycle Support
4. CP2-Contingency Planning

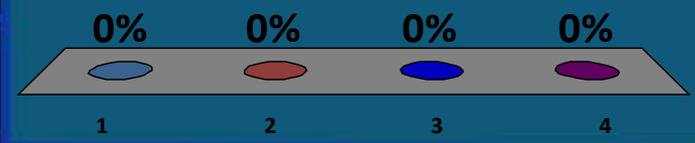


1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

RA5, Vulnerability Scanning control, requires vulnerability scans for publicly facing systems at least once every \_\_\_\_\_.

- 1. 60 days
- 2. 90 days
- 3. 120 days
- 4. year



1 - 5	3 - 20	5 - 40	7 - 100	9 - 300	11 - 500	13 - 2000
2 - 10	4 - 30	6 - 50	8 - 200	10 - 400	12 - 1000	14 - 3000

**15 - 10000**

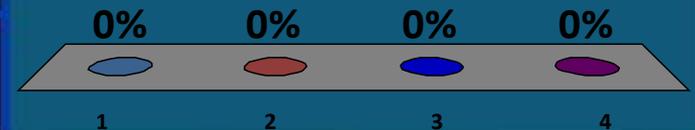
PE5: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining \_\_\_\_\_ .

1. printer supplies

2. the output

3. paper

4. biometric tokens



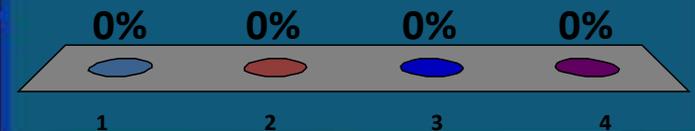
1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000

2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

Name this control: Allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions & business functions.

1. PS3-Personnel Screening
2. PS6-Access Agreements
3. AC5-Separation of Duties
4. AC6-Least Privilege

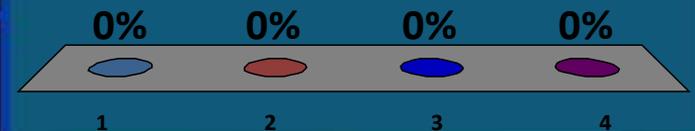


1 - 5	3 - 20	5 - 40	7 - 100	9 - 300	11 - 500	13 - 2000
2 - 10	4 - 30	6 - 50	8 - 200	10 - 400	12 - 1000	14 - 5000

**15 - 10000**

Which of the following controls is probably the *least useful* in defending against insider threats?

1. AU6-Audit Review, Analysis & Reporting
2. PS3-Personnel Screening
3. SI3:Malicious Code Protection
4. PS4-Personnel Termination



1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# Team Scores

**Points**      **Team**

**Points**      **Team**

# Top 5 Participant Scores

**Points**

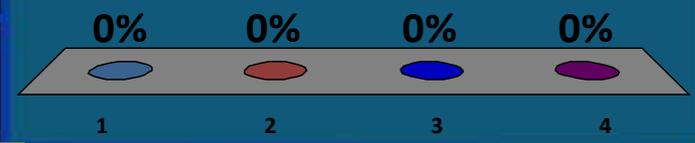
**Participant**

**Points**

**Participant**

Writing secure software requires integrating security in all phases of software development.  
Which control best enforces this idea?

1. SA3-Life Cycle Support
2. SA11-Security Testing
3. AC4-Information Flow Enforcement
4. AT3-Security Training

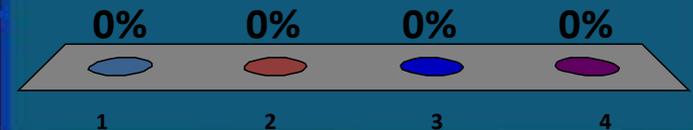


1 - 5	3 - 20	5 - 40	7 - 100	9 - 300	11 - 500	13 - 2000
2 - 10	4 - 30	6 - 50	8 - 200	10 - 400	12 - 1000	14 - 3000

**15 - 10000**

# An information system contingency plan, per CP-2, should document all but what?

1. Essential mission functions
2. Recovery objectives
3. Configuration baselines
4. Roles & responsibilities

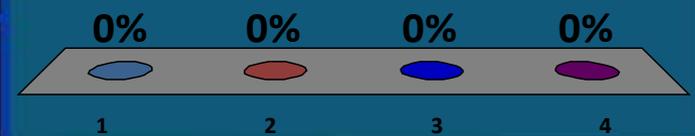


1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    **12 - 1000**    14 - 5000

**15 - 10000**

IR4, Incident Handling, requires that incident handling activities be coordinated with the activities for \_\_\_\_\_?

1. RA5-Vulnerability Scanning
2. SI3- Malicious Code Protection
3. PL2-System Security Planning
4. CP2-Contingency Planning

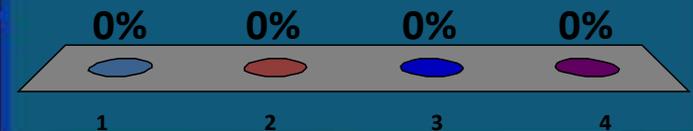


1 - 5	3 - 20	5 - 40	7 - 100	9 - 300	11 - 500	13 - 2000
2 - 10	4 - 30	6 - 50	8 - 200	10 - 400	12 - 1000	14 - 5000

**15 - 10000**

Name the control: The organization includes a determination of information security requirements for the information system in mission/business process planning.

1. CA1-Security Assessment & Authorization
2. PL6-Security Related Activity Planning
3. SA2-Allocation of Resources
4. CM1-Configuration Mgmt



1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# Team Scores

**Points**      **Team**

**Points**      **Team**

# Participant Scores

**Points**

**Participant**

**Points**

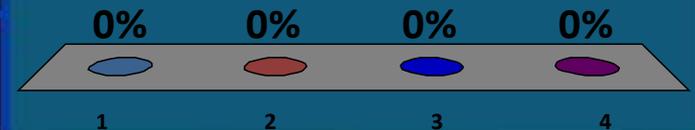
**Participant**



**AND NOW FOR  
THE FINAL QUESTION**

# Dr. Ross holds both Masters and Ph.D. degrees in Computer Science from?

1. West Point
2. Massachusetts Institute of Technology
3. US Naval Postgraduate School
4. Virginia Military Institute



1 - 5    3 - 20    5 - 40    7 - 100    9 - 300    11 - 500    13 - 2000  
2 - 10    4 - 30    6 - 50    8 - 200    10 - 400    12 - 1000    14 - 5000

**15 - 10000**

# Team Racing Scores

# Final Team Scores

**Points**

**Team**

**Points**

**Team**

# Final Top 5 Participant Scores

**Points**

**Participant**

**Points**

**Participant**

**THANKS FOR PLAYING**  
**“WHO WANTS TO BE**  
**A SEC501/NIST 800-53**  
**CLICKER MILLIONAIRE?”**

**NEXT SLIDE PLEASE**



## RECENT SURVEYS

We recently sent out 2 surveys to the ISO's.

The **Kid Safe Poster Contest** voting ends on COB Friday, February 8<sup>th</sup>.

The **ISO Resources Survey** ends on COB Friday, February 15<sup>th</sup>.

JUST ONE MORE SLIDE



## NEW SURVEY

The IS Council has formed a committee to develop an information security conference and training session to be held sometime in the spring of 2014.

You will be receiving a survey requesting your opinions on what you would like to see in a conference of that type.

Look for that survey to come out in the next day or two. **THANK YOU!**



Virginia Information Technologies Agency

# Upcoming Events





# Information Security System Association

## ISSA

**DATE:** Wednesday, Feb 13, 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:** Charles Greene

**TOPIC:** *"Thanks for Recovering....Now I can Hack You!"*

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



## AITR Meeting

**When: Wednesday, February 13, 2013**

**Time: 9:00 to 11:00 am**

**Location: CESC**



## IS Orientation

**When: Tuesday, March 7, 2013**

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

**Where: CESC , Room 1221**

**Register here:**

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

Next IS Orientation will be held on June 6, 2013



## Future ISOAG Dates

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

**Keynote Speaker: Lyn Rahilly, Privacy Officer**

**U.S. Customs and Immigration Enforcement**

**Apr 3                      1:00 – 4:00 pm @ CESC**

**Keynote Speaker: Lori Broache,**

**Continuity Management Solutions**

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

**Keynote Speaker: Todd Dergenski,**

**Senior Security Administration, ODU**

**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*

Feb 6, 2013



***NORTHROP GRUMMAN***



# Microsoft End of Life / End of Support Dates

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Microsoft End of Life

Slides have been  
intentionally omitted

# ADJOURN

