Opening Up a Second Front for Cyber Security and Risk Management

Annual Computer Security Applications Conference

December 4, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory


We The People

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…

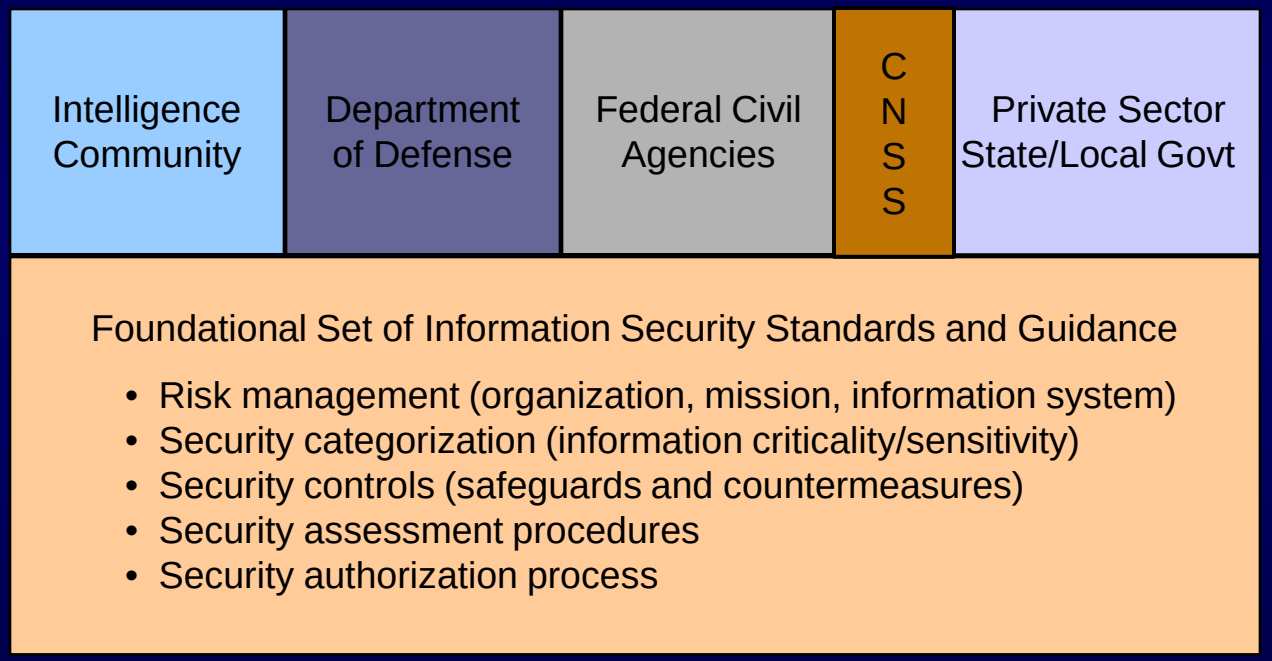
Unified Information Security Framework

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



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

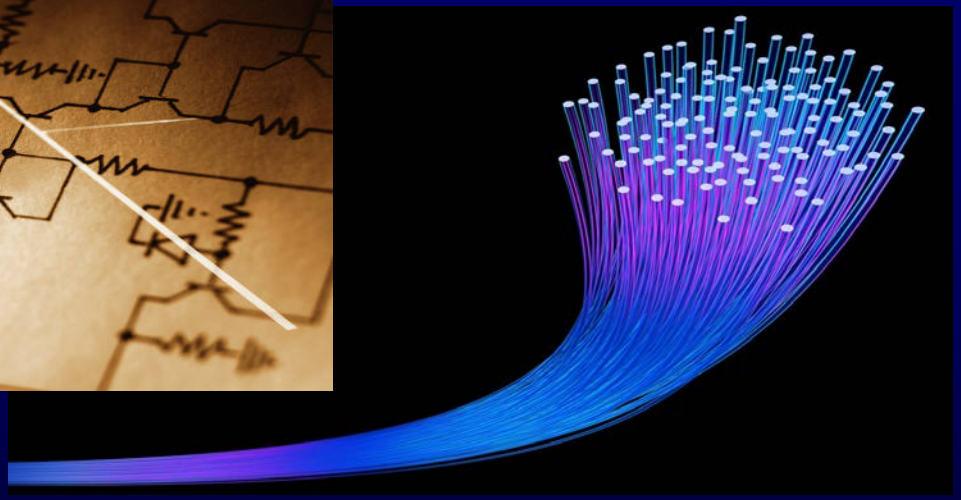
- NIST Special Publication 800-39
  Managing Information Security Risk: Organization, Mission, and Information System View
- NIST Special Publication 800-30
  Guide for Conducting Risk Assessments
- NIST Special Publication 800-37
  Applying the Risk Management Framework to Federal Information Systems
- 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

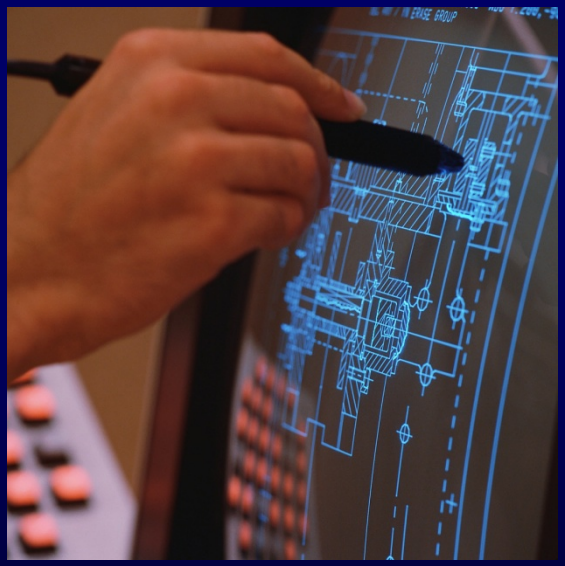
Complexity.

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.

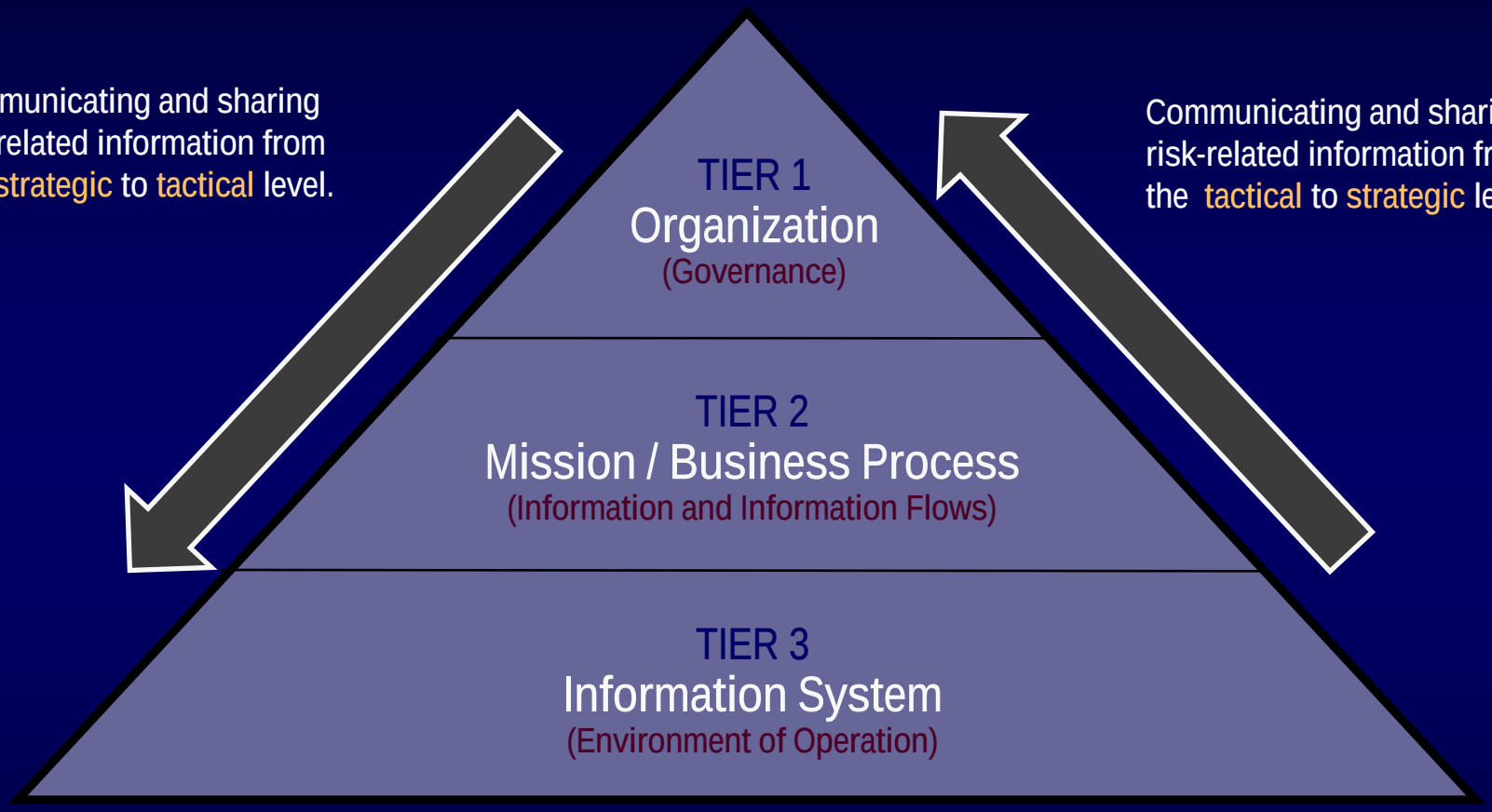


What can we do to change course?

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.

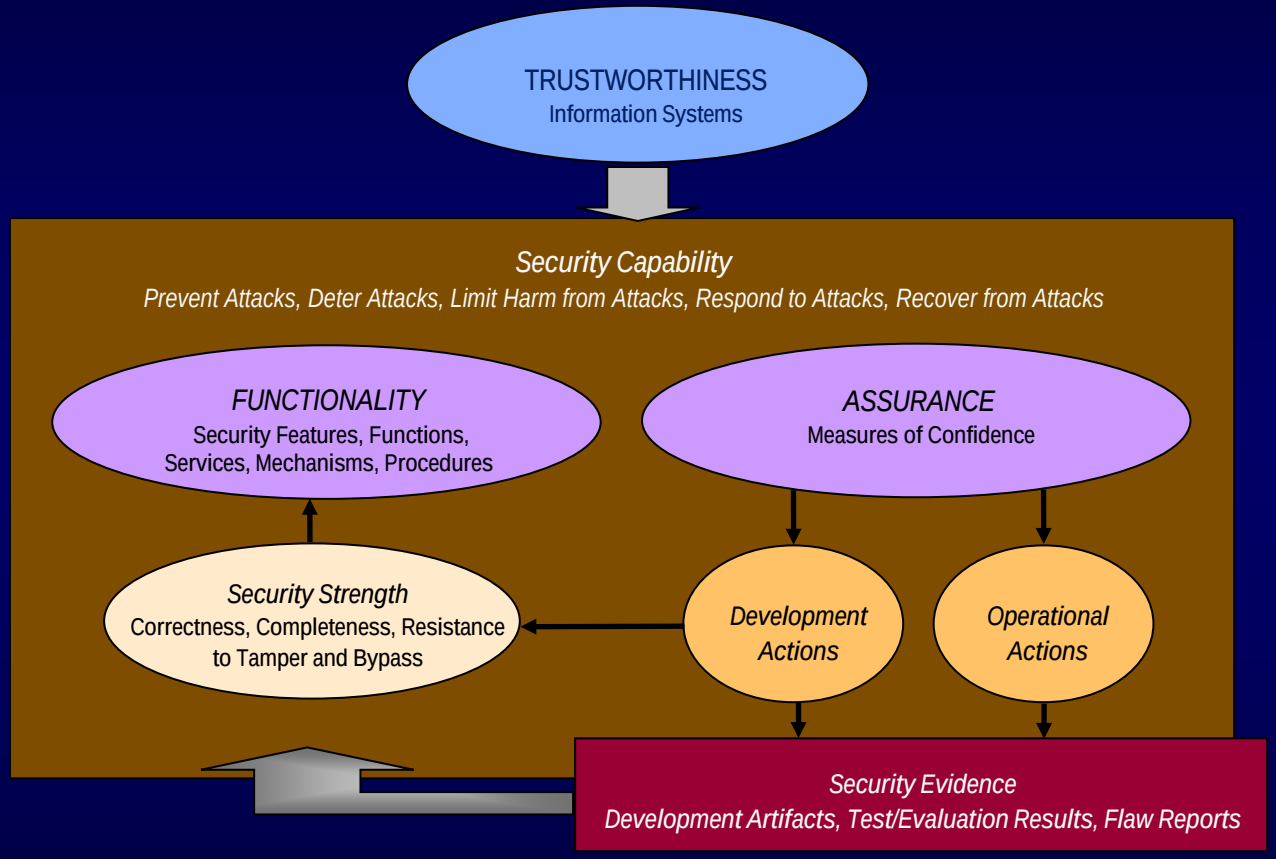
Functionality and Assurance.

They ride together…

What is observable in front of the wall.

What is observable behind the wall.

Assurance and Trustworthiness



Enables Understanding of Security Capability

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.

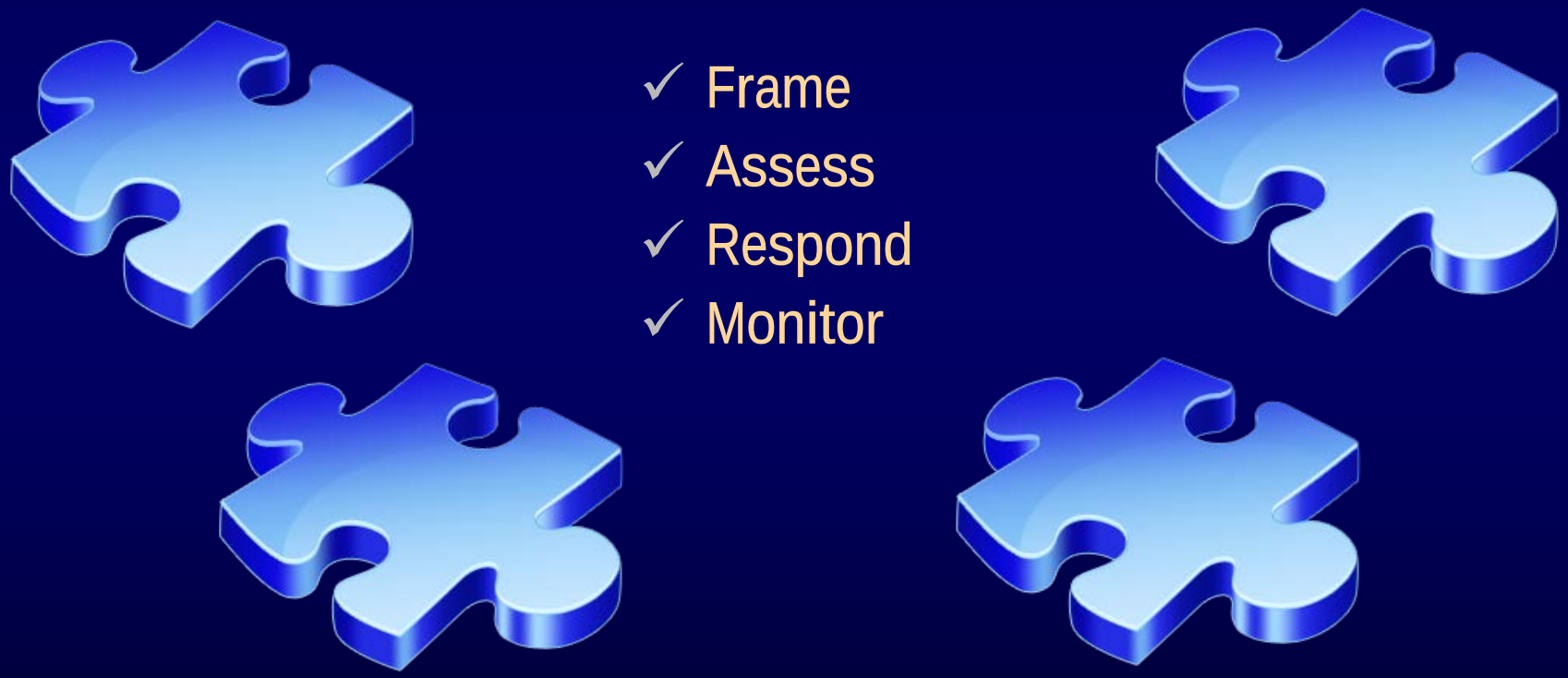
Powerful concepts that reduce risk…

Adversaries are not ten feet tall.

They have work factors and attack sequences that can be disrupted…

Managing risk.

Doesn't mean fixing everything…



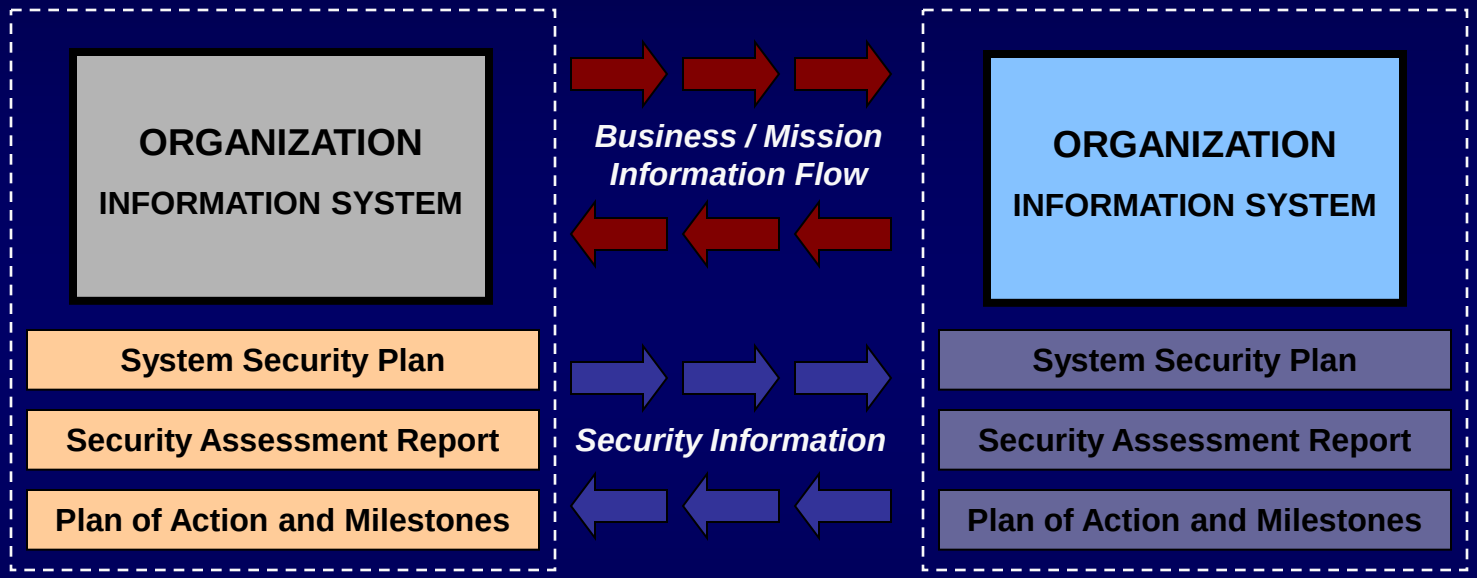
- ✓ Frame
- ✓ Assess
- ✓ Respond
- ✓ Monitor

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

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov