High Level Policy meets Compliance

Dr. Hale
University of Nebraska at Omaha
Information Security and Policy– Lecture 5 (part 2)

Today's topics:

~~Introduction to Compliance and Security Controls~~

- ~~U.S. Compliance Laws~~
- ~~Industry standards (Common Criteria, PCI-DSS, ITIL)~~
- ~~Aligning Policy with Regulations and industry~~

Policy/security control frameworks

- Security Controls
- COBIT, ISO/IEC 27000, NIST SP800-53
- Focus on FISMA/NIST framework

[Conspicuous Lack of “Previously on” slide]

I promised..

Determine Compliance Requirements

Determine Compliance Requirements

First identify laws that you need to comply with.

Determine Compliance Requirements

Next identify industry regulations you want to comply with.

Determine Compliance Requirements

Both of these identifications should be integrated into an organizational risk assessment.
(i.e. those decision trees you've been working with)

Determine Compliance Requirements

Now examine and integrate security controls suggested/required by the selected laws/standards.*

Determine Compliance Requirements

*This is a big task

Determine Compliance Requirements

Lets start with the basics.

Definition:

A *Security Control* is a safeguard or countermeasure that is either preventative, detective, or corrective.

Think of controls as mandatory *policy guidelines* that target specific areas

Preventative Control

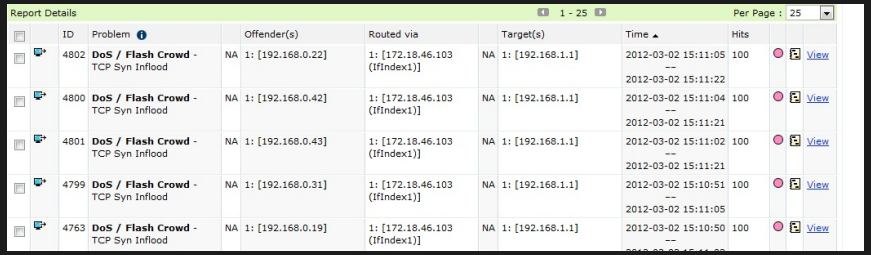
- Mitigates risks/attacks immediately by preventing attack success
  - e.g. firewall for port blocking
  - e.g. strong encryption for MiTM passive observation

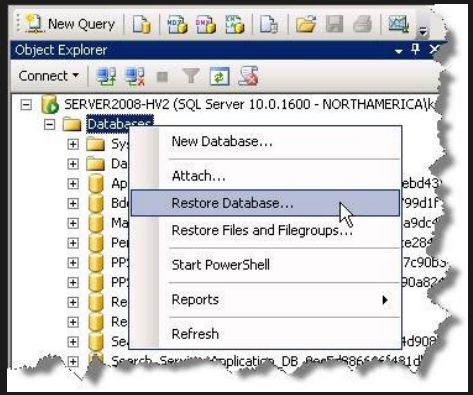
Detective Control

- doesn't prevent attacks
- alerts end-user or administrators of attack
- e.g. audit log review

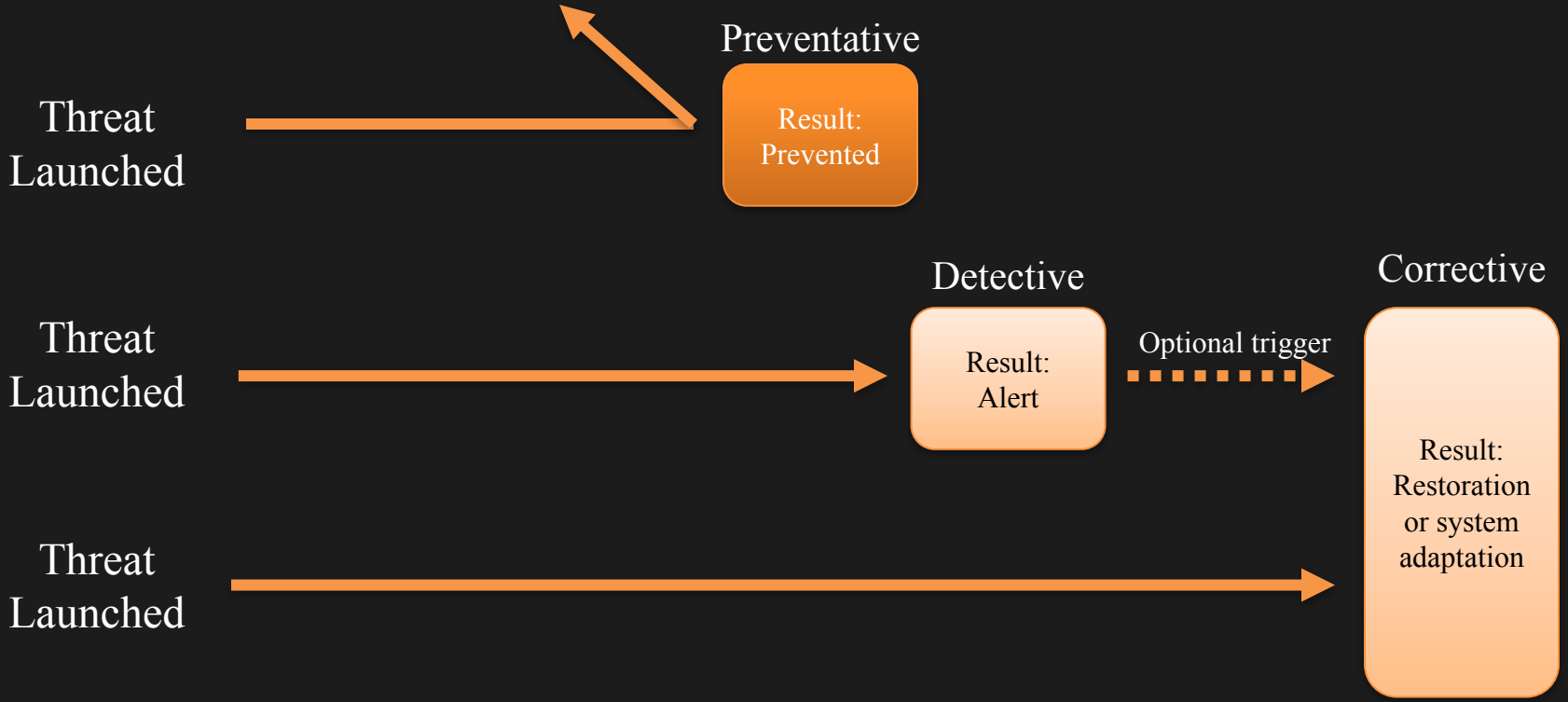
Corrective Control

- doesn't prevent or detect attacks
- limits the impact of attacks by restoring functionality or patching issues
- e.g. backup and recovery





Intro to compliance



Intro to compliance

Controls can be:

- technical (apply to systems, apps, networks, etc)
- operational/managerial (apply to people, organizations, etc)
- physical (apply to buildings, doors, etc)

Technical Controls

The ones most of you will deal with the most. (most-most)
Involve applying protections to systems, software components, networks, and/or data.

Operational Controls

The ones most of you will deal with even more (most-moster)
Dictate human behavior, requires training
May require employees, external staff, or managers to behave in certain ways
E.g. Not respond to phishing email

[small subset of] Operational Controls - Managerial

The ones most of you will rarely deal with (most-least)
May also dictate organizational behavior or structure
(e.g. annual reviews, planning requirements, designated officials, etc)

Note:

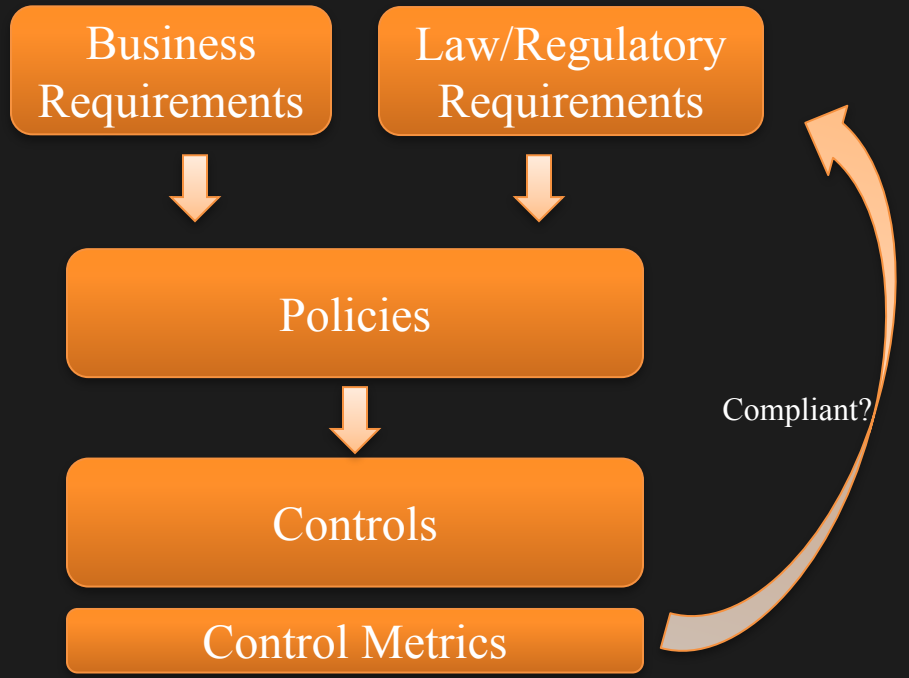
Sometimes managerial controls are split entirely into their own category (e.g. NIST)

Physical Controls

Dictates parameters that structure the real world
e.g. require hardware to be in a locked server closet,
have a guard posted at a door, or
use cameras for surveillance

Linking controls to requirements

- Laws / regulatory selections and business requirements set policy
- Policies should support business requirements and satisfy regulatory demands
- Controls implement Policies
- Metrics measure control satisfaction
- Satisfying metrics means being compliant with regulatory requirements



So how do I actually work with controls?

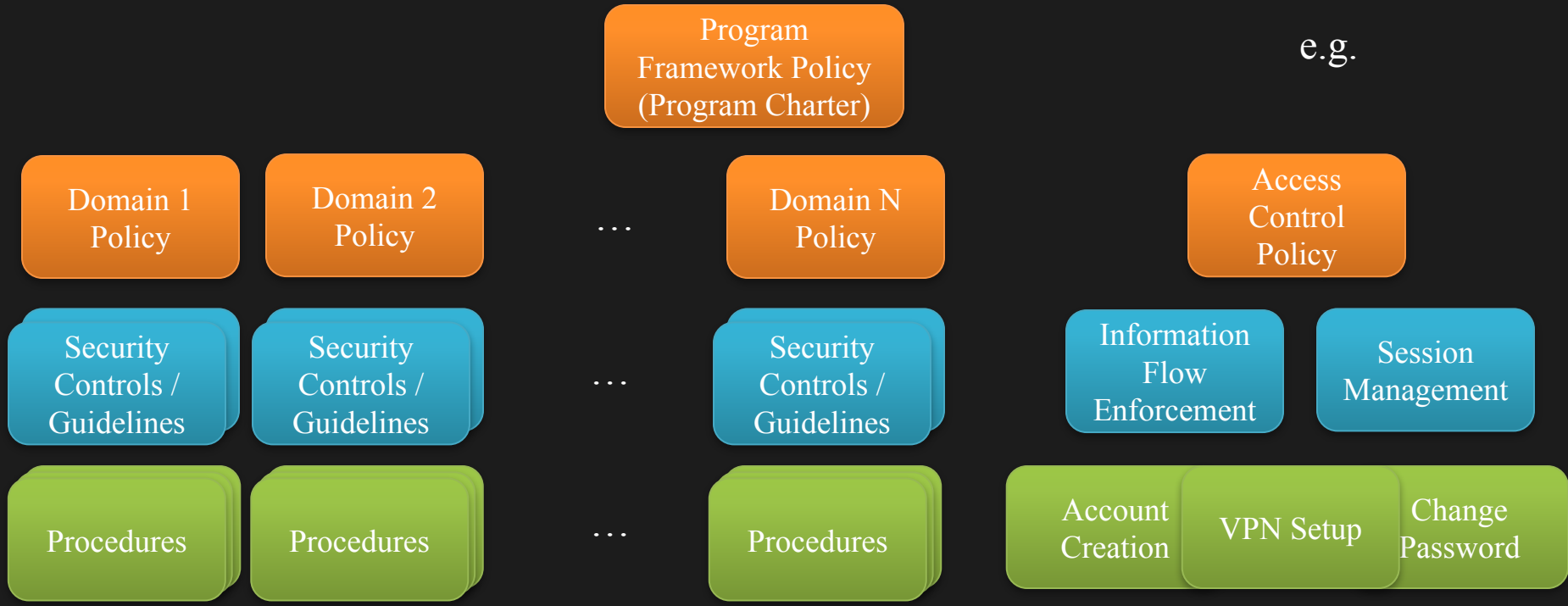
Policy Frameworks

This is where *control frameworks* come into play.

Definition:

A *Control Framework* is a structured collection of security controls that implements policy to create business value and minimize enterprise risks.

Control Framework



Policy Frameworks

You can build this yourself.

But why re-invent the (very well designed) wheel(s)

Policy Frameworks

(open) security control document players

Security Control Frameworks

Framework	Type of Organizations	Implements?
NIST SP 800-53 Recommended Security Controls for Federal Information Systems	Federal, Federal Contractors, some Industry	FISMA, Other federal risk management processes (SP 800-37), FIPS 199/200
NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Any, particularly Federal or Hospitals	HIPAA
Control Objectives for Information and related Technology (COBIT)	Industry	ITIL (compatible with 27000 series as well)
ISO/IEC 27000 series Information Technology Security Techniques Code of Practice for Information Security Management	Industry	Itself (it's a standard and a framework)
Common Criteria ISO/IEC 15408	Organizations that want to certify their systems or products	Itself (it's a standard and a framework)
DoDi 8500.01: Defense Department Cybersecurity Instruction	All DoD	Itself and a bunch of other related documents
Cloud Security Alliance CCM (Cloud Control Matrix)	Cloud vendors	COBIT, PCI, NIST, ISO 27000 series for cloud services

Policy Frameworks

What do security controls look like?

Policy Frameworks

What do security controls look like?

NIST: AU-12.c: Audit Generation

The information system generates audit records for the events defined in AU-2.d with the content defined in AU-3.

AU-2.d: Audit Events

The organization determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

AU-3: Content of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Policy Frameworks

What do security controls look like?

CC: FAU_GEN.1.1(c) Audit Data Generation

The TSF shall be able to generate an audit record of the following auditable events [assignment: other specifically defined auditable events]

Policy Frameworks

What do security controls look like?

I can’t show you COBIT or ISO 27000 Series Controls in these slides

Policy Frameworks

Policy Frameworks

We'll still talk about them (indirectly).
But the emphasis in this class will be on the FISMA family.

[GOTO NIST FISMA Slides]

Policy Frameworks

Federal Information Security Management Act

Applying NIST Information Security Standards and Guidelines

Presented to the State of California

April 20, 2008

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

A Unified Framework

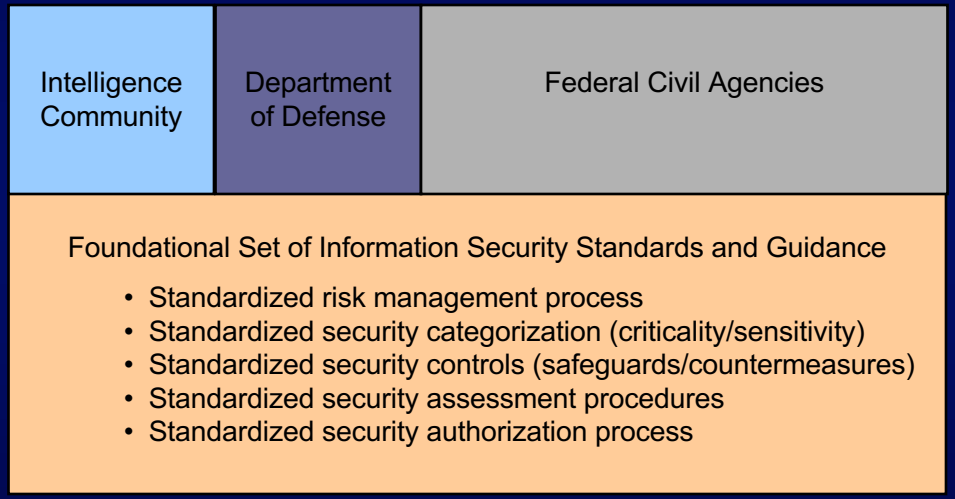
For Information Security

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



National security and non national security information systems

Risk-Based Protection Strategy

- Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for organizational information systems.
- Highly flexible implementation; recognizing diversity in mission/ business processes and operational environments.
- Senior leaders take ownership of their security plans including the safeguards/countermeasures for the information systems.
- Senior leaders are both responsible and accountable for their information security decisions; understanding, acknowledging, and explicitly accepting resulting mission/business risk.

Information Security Programs

Links in the Security Chain: Management, Operational, and Technical Controls

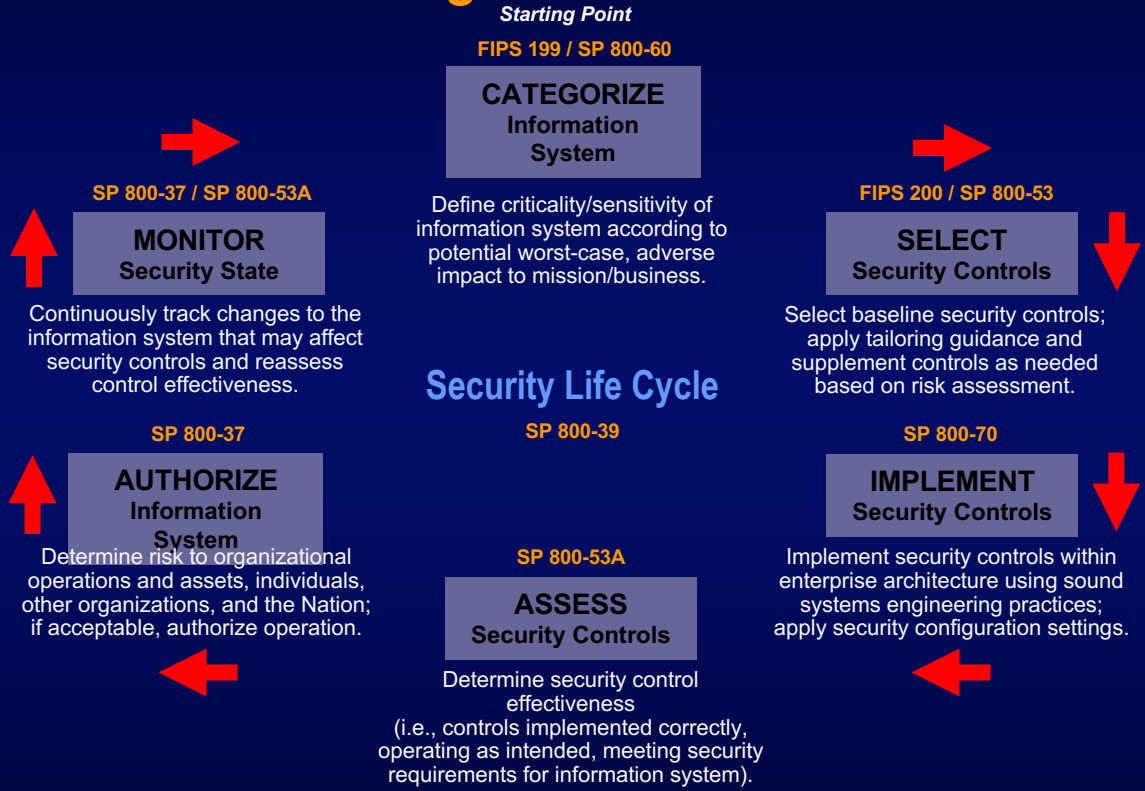
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation
- ✓ 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?

Strategic Planning Considerations

- Consider vulnerabilities of new information technologies and system integration before deployment.
- Diversify information technology assets.
- Reduce information system complexity.
- Apply a balanced set of management, operational, and technical security controls in a defense-in-depth approach.
- Detect and respond to breaches of information system boundaries.
- Reengineer mission/business processes, if necessary.

Risk Management Framework



RMF Characteristics

- The NIST *Risk Management Framework* and the associated security *standards* and *guidance* documents provide a process that is:
  - Disciplined
  - Flexible
  - Extensible
  - Repeatable
  - Organized
  - Structured

"Building information security into the infrastructure of the organization… so that critical enterprise missions and business cases will be protected."

Security Categorization

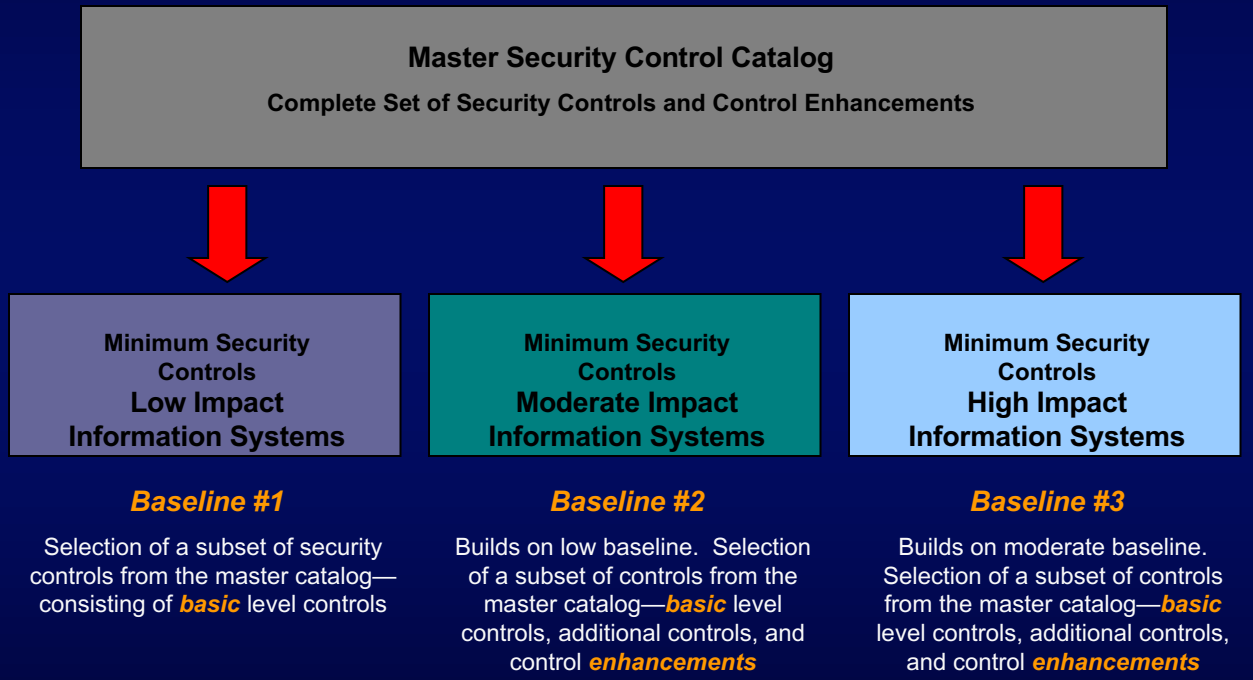
Example: An Enterprise Information System

Mapping Information Types to FIPS 199 Security Categories

SP 800-60

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Control Baselines

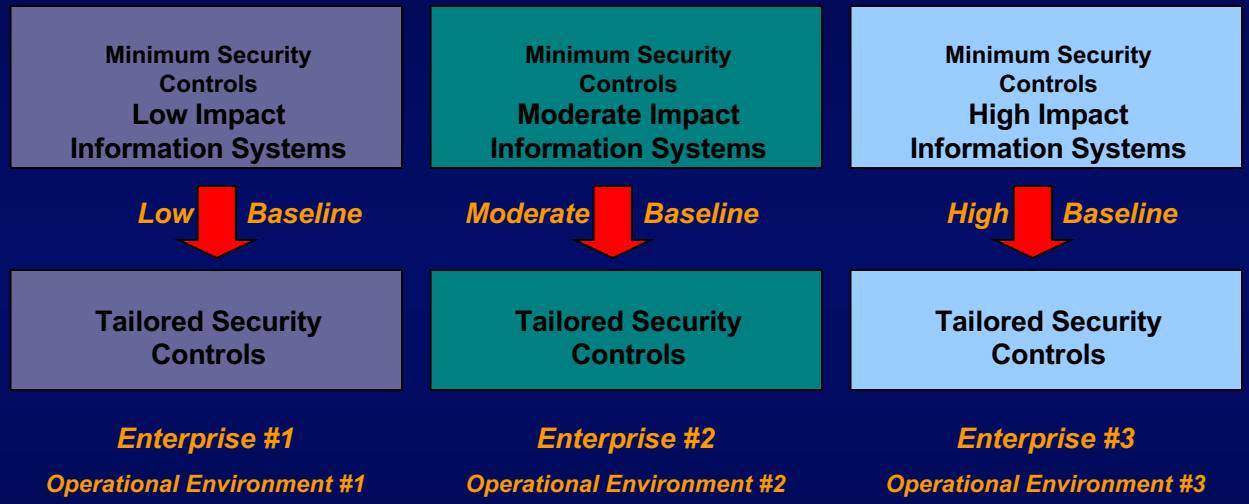


Tailoring Guidance

- FIPS 200 and SP 800-53 provide significant flexibility in the security control selection and specification process:
  - Scoping guidance;
  - Compensating security controls; and
  - Organization-defined security control parameters.

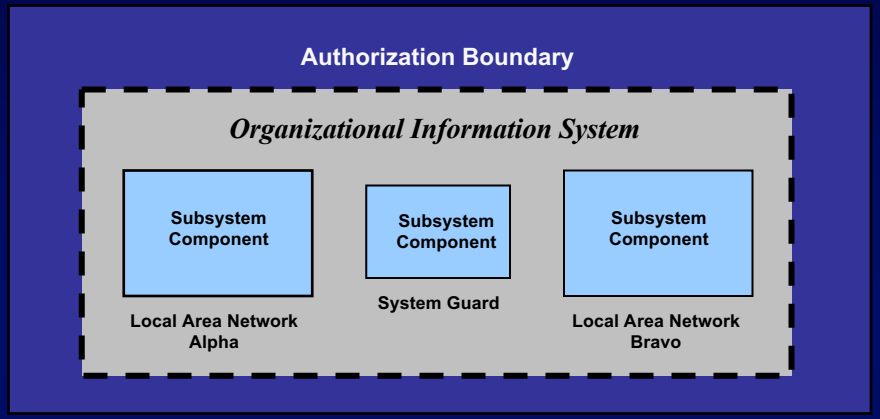
Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



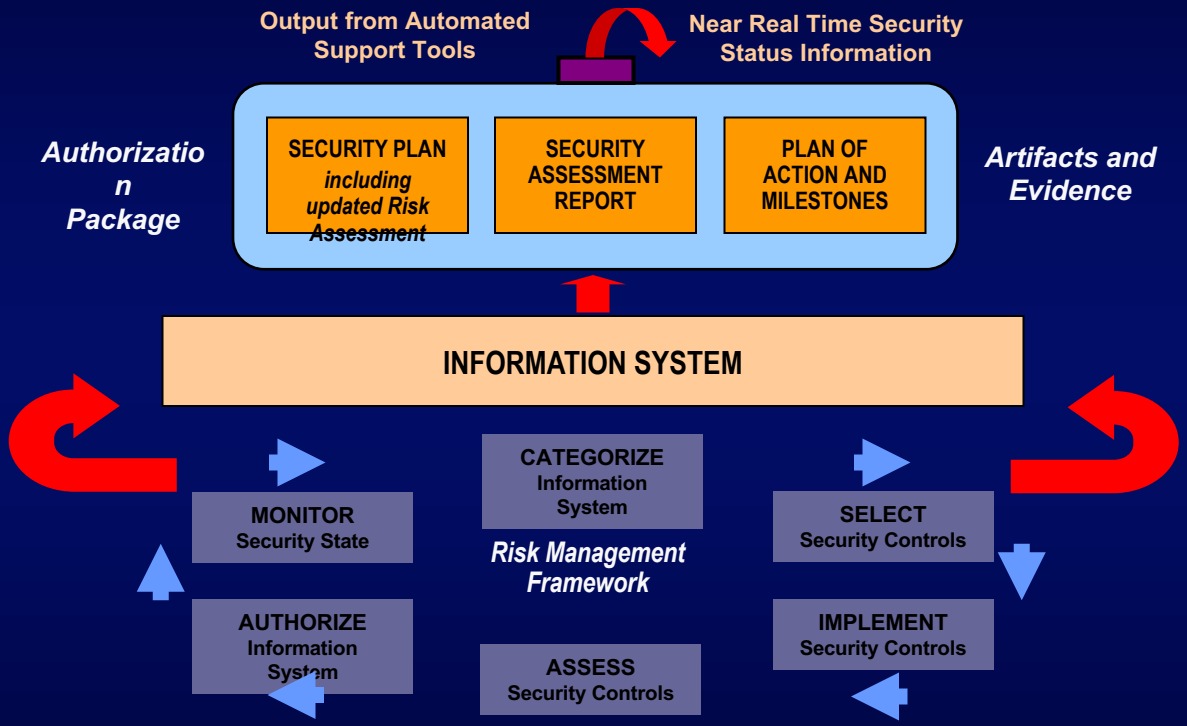
Cost effective, risk-based approach to achieving adequate information security…

Large and Complex Systems

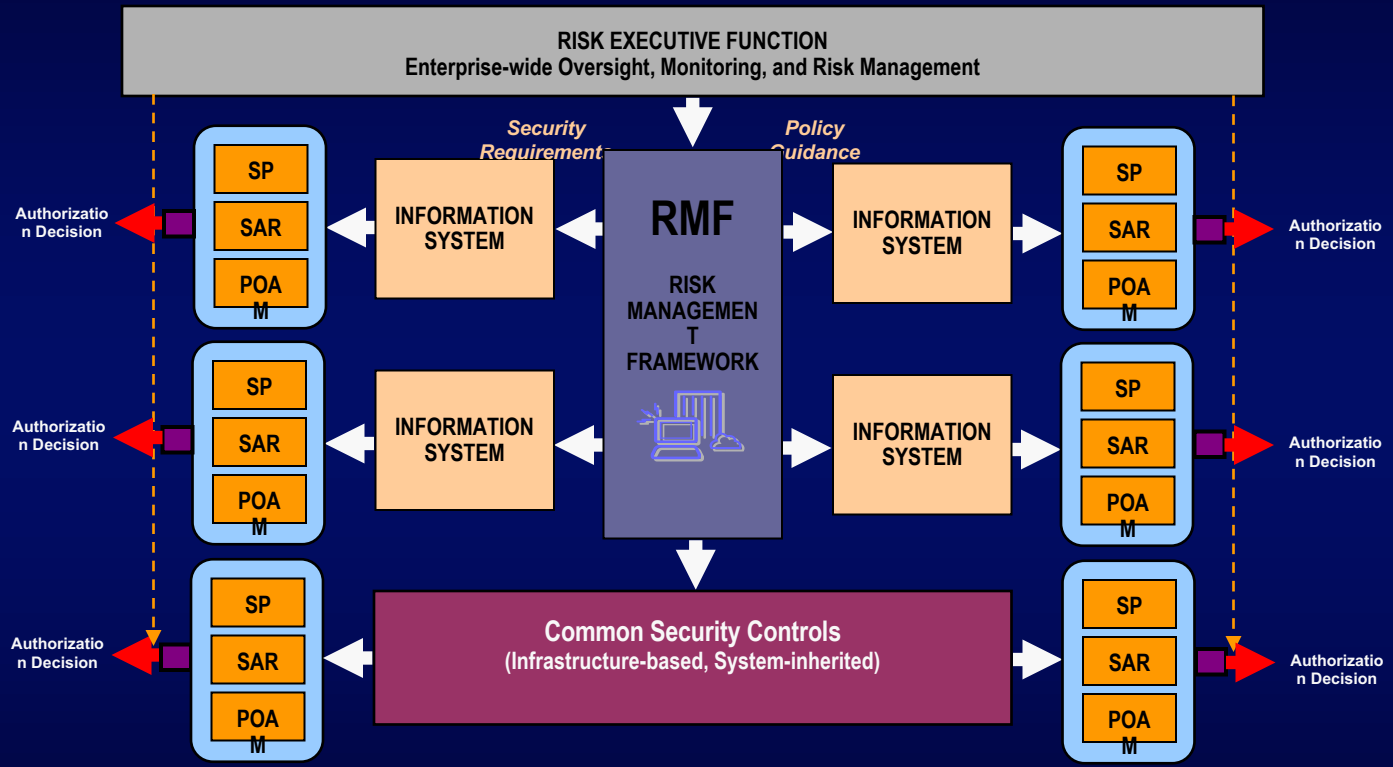


- System security plan reflects information system decomposition with adequate security controls assigned to each subsystem component.
- Security assessment procedures tailored for the security controls in each subsystem component and for the combined system-level controls.
- Security assessment performed on each subsystem component and on system-level controls not covered by subsystem assessments.
- Security authorization performed on the information system as a whole.

Applying the Risk Management Framework to Information Systems

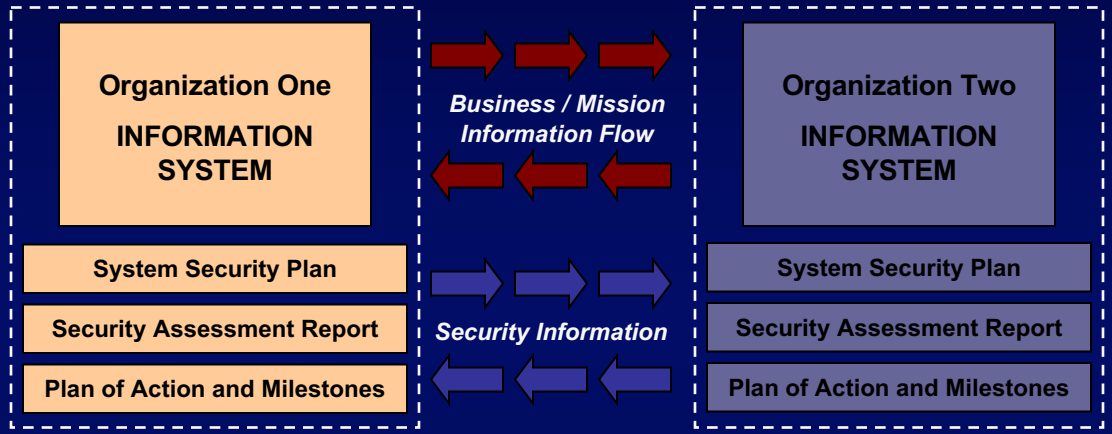


Extending the Risk Management Framework to Organizations



Risk Executive Function

Trust Relationships



Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve *visibility* into and *understanding* of prospective partner's information security programs…establishing a trust relationship based on the trustworthiness of their information systems.

Main Streaming Information Security

- Information security requirements must be considered *first order requirements* and are critical to mission and business success.
- An effective organization-wide information security program helps to ensure that security considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.

Enterprise Architecture

- Provides a common language for discussing information security in the context of organizational missions, business processes, and performance goals.
- Defines a collection of interrelated reference models that are focused on lines of business including Performance, Business, Service Component, Data, and Technical.
- Uses a security and privacy profile to describe how to integrate the Risk Management Framework into the reference models.

System Development Life Cycle

- The Risk Management Framework should be integrated into all phases of the SDLC.
  - Initiation (RMF Steps 1 and 2)
  - Development and Acquisition (RMF Step 2)
  - Implementation (RMF Steps 3 through 5)
  - Operations and Maintenance (RMF Step 6)
  - Disposition (RMF Step 6)
- Reuse system development artifacts and evidence (e.g., design specifications, system documentation, testing and evaluation results) for risk management activities.

FISMA Phase I Publications

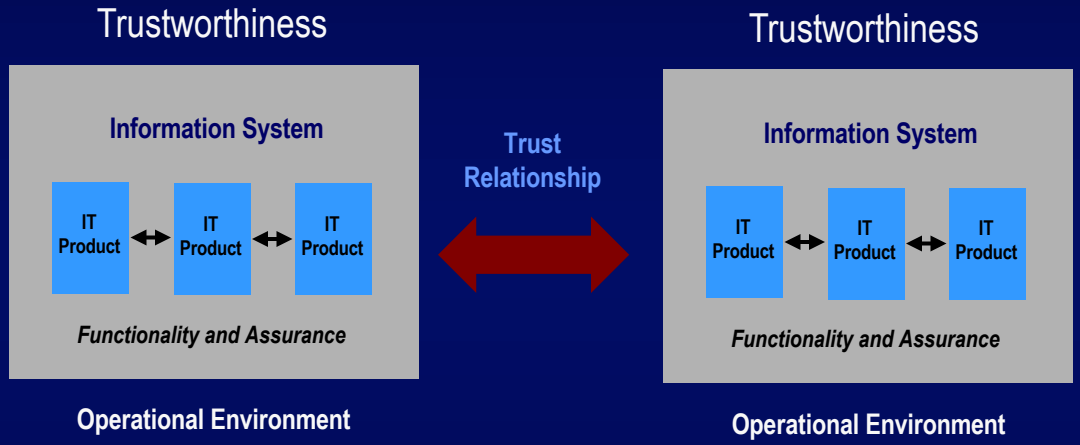
- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-39 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

FISMA Phase II

Demonstrating competence to provide information security services including—

- Assessments of Information Systems
  (Operational environments)
  - ***Security controls***
  - ***Configuration settings***
- Assessments of Information Technology Products
  (Laboratory environments)
  - ***Security functionality (features)***
  - ***Configuration settings***

FISMA Phase II



Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.

Training Initiative

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards and guidelines.
- Training initiative includes three components—
  - Frequently Asked Questions
  - Publication Summary Guides (Quickstart Guides)
  - Formal Curriculum and Training Courses
- NIST will provide initial training in order to fine-tune the curriculum; then transition to other providers.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Develop an enterprise-wide information security strategy and game plan.
- Get corporate “buy in” for the enterprise information security program—effective programs start at the top.
- Build information security into the infrastructure of the enterprise.
- Establish level of “due diligence” for information security.
- Focus initially on mission/business process impacts—bring in threat information only when specific and credible.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Create a balanced information security program with management, operational, and technical security controls.
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk.
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data.
- Harden the target; place multiple barriers between the adversary and enterprise information systems.

The Golden Rules

Building an Effective Enterprise Information Security Program

- Be a good consumer—beware of vendors trying to sell single point solutions for enterprise security problems.
- Don't be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes.
- Don't tolerate indifference to enterprise information security problems.

And finally…

- Manage enterprise risk—don't try to avoid it!

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

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

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

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

Matt Scholl
(301) 975-2941

Information and Feedback
Web:

Reading

Brotby 3 and 7, look at FISMA (with a cup of coffee), look at FIPS 199/200, look at NIST SP 800-53

Read: A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards - Constantine Gikas (will post link)

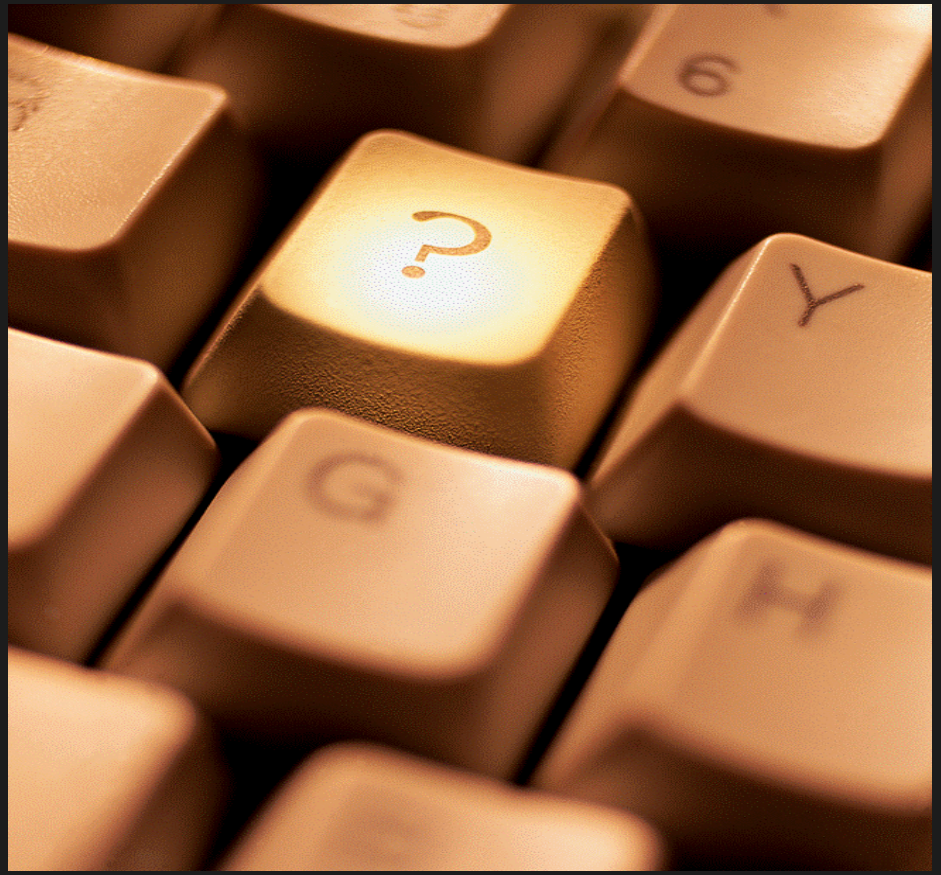
Homework

Policy Analysis assignment on github:
https://mlhale.github.io/CYBR3600/homework/projects/project-1.html

Next Time

I’m out of town

Questions?



Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_