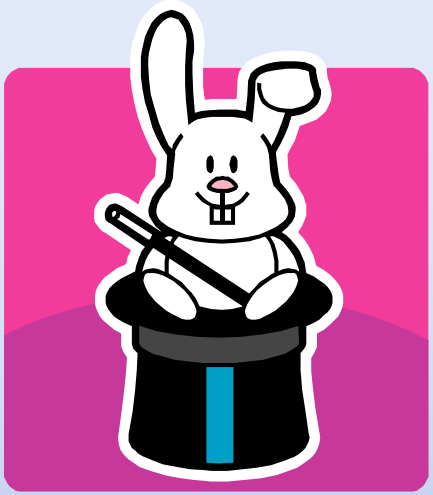
NIST Implementation Mission Possible

2011 Montana Government
Information Technology Conference
December 7, 2011

Presented by:
Lynne Pizzini, CISSP, CISM, CIPP
Information Systems Security Officer
State Information Technology Services Division
444-9127
lpizzini@mt.gov



Lynne Pizzini, CISSP, CISM, CIPP
Lyn-nerd the Clown
Information Systems Security Officer
State Information Technology Services Division

Outline – Mission Possible

- Compliance Smorgasbord
- Overview of NIST
- Special Publications and 800-53
- Security Controls Overview
- Special Publications and ISO 27000
- NIST and Risk Management
- Policies and Procedures
- Implementation
- Review

Are you working on an Impossible Mission?

OR a Mission that is Possible?

How do you get from Impossible to Possible?

Your Assignment, if you wish to accept this mission…

Compliance!

Compliance Smorgasbord

NIST

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

PCI Security Standards Council
PARTICIPATING ORGANIZATION

ISO International Organization for Standardization

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

IRS
Department of the Treasury
Internal Revenue Service

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

The State of Montana CIO has Chosen NIST

This is our umbrella of protection for information systems.

Choose NIST!

What is NIST ?

Nothing is Secure in Technology
Need Information Security Tools
Need Idiot-proof Security Theme

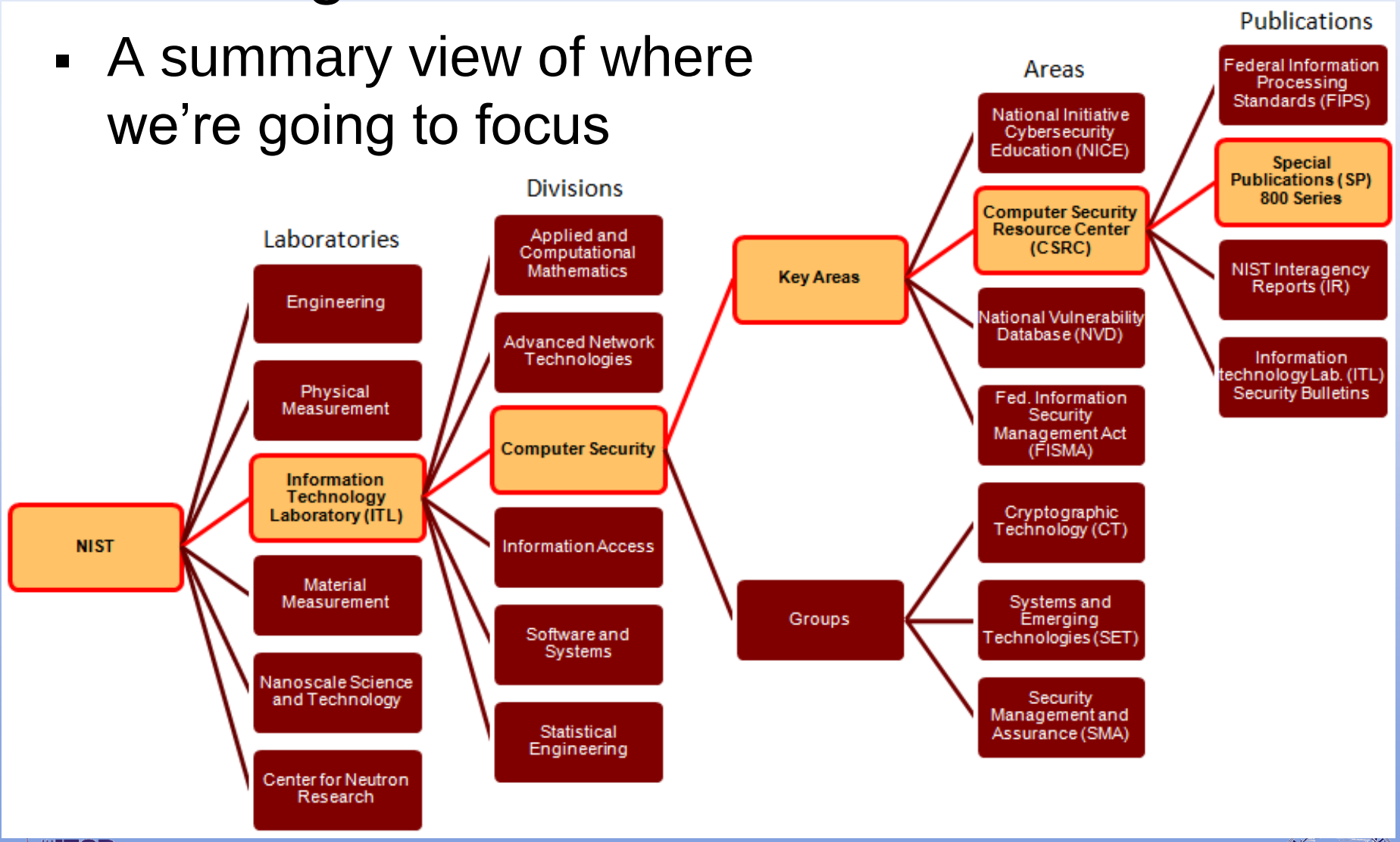
National Institute of Standards and Technology
Federal Standards from FISMA

Using NIST

- Why use NIST for building a security program?
  - “NIST is complicated.”
  - “I don’t understand it.”
- It’s valuable…
  - Comprehensive
    - Covers gaps in other standards
    - Interconnected with a number of other standards
    - Detailed information and guidance
  - Cross compliance capability
    - Offers a framework that can be applied to multiple enterprise regulatory scenarios
  - Use what you want!
    - If you’re not part of or provide IT services to Federal information systems take from it what you need

NIST Organization

- A summary view of where we're going to focus



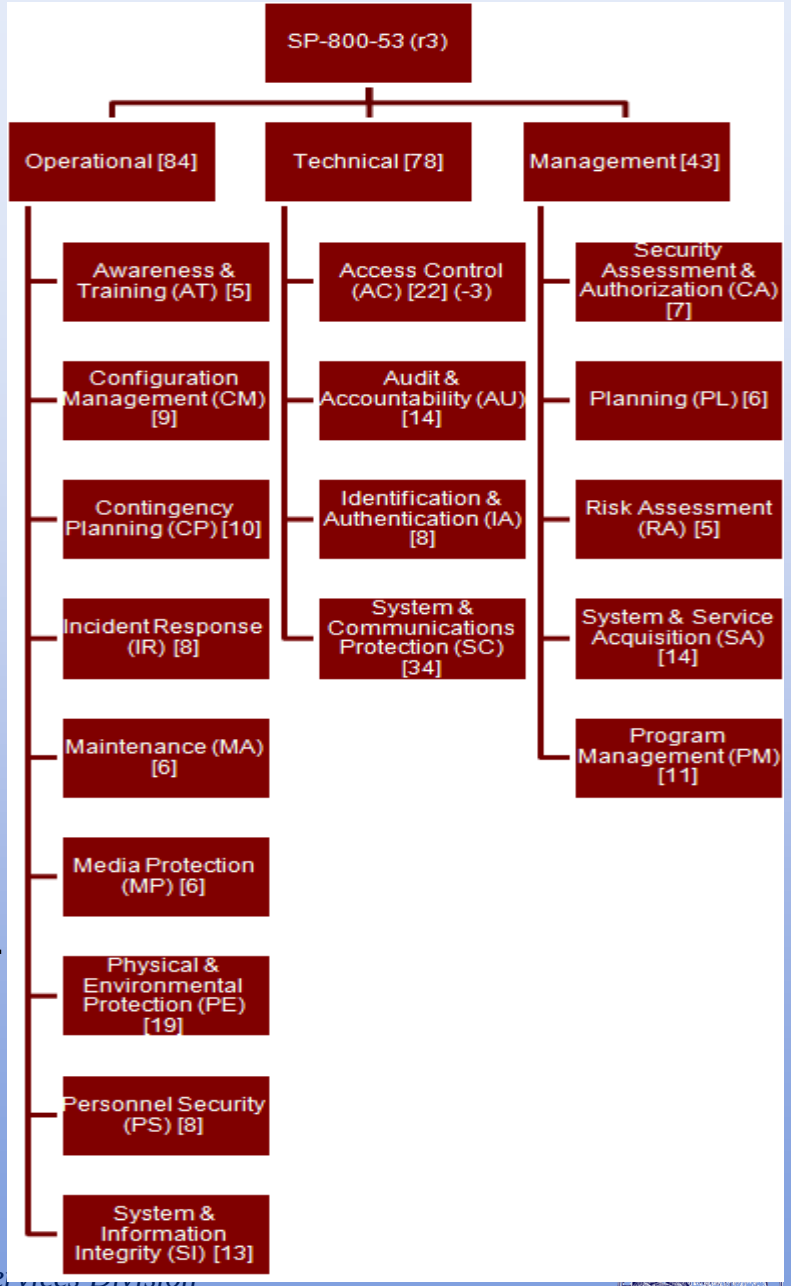
SP800-53 rev.3, Aug 2009

Recommended Security Controls for Federal Information Systems and Organizations

- Primary focus for this session
  - Broad and comprehensive, a center point
- Genesis
  - Developed by the Joint Task Force Transformation Initiative Interagency Working Group to:
    - Produce a unified information security framework that includes a consistent process for selecting and specifying safeguards and countermeasures
  - Developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Management Act (FISMA)
  - FISMA requires federal agencies comply with Secretary of Commerce approved Federal Information Processing Standards (FIPS)
    - FIPS-200
      - Minimum Security Requirements for Federal Information and Information Systems
      - Mandates SP800-53
- Compliance with FISMA, FIPS, and applicable SP's is the responsibility of the Office of Management and Budget (OMB)

800-53 Structure

- Control Organization
  - 3 Classes
  - 18 Families
  - 205 Controls
- Wait… 18 families?
  - FIPS-200 defines 17 families
    - 800-53 adds an additional Program Management (PM) family (Appendix G) provides for security controls at the organizational level, not information system level



Controls Overview

- Control section
  - Provides a statement(s) defining the control with specific security-related activities or actions
    - Acts as the basis for selection and auditing
- Supplemental guidance
  - Provides common areas of applicability, gaps, and related controls, but no requirements
    - Meant to assist in defining, developing, and implementing
- Control enhancements
  - Defines security capability statements to address systems that require greater protection, used when:
    - Build in additional control functionality, and/or
    - Increase the strength of the control
    - Are numbered sequentially for prioritization

FAMILY: ACCESS CONTROL **CLASS: TECHNICAL**

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organizationdefined frequency]:*

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100

Baseline Controls

- Although risk is used, selecting the appropriate specific controls can be a challenge
- Baseline controls are provided as a starting point for the control selection process
  - Low, moderate, and high impact based on system criticality and is hierarchical
  - Prioritization is based on the application of identified security controls relative to impact
    - Includes LOW/MED/HIGH control enhancements, additional control characteristics that should be applied in a prioritized manner based on impact

Baseline Controls (2)

Priority Code	Sequencing	Action
Priority Code 1 **(P1)**	FIRST	Implement P1 security controls first.
Priority Code 2 **(P2)**	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 **(P3)**	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code **(P0)**	NONE	Security control not selected for baseline.

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected

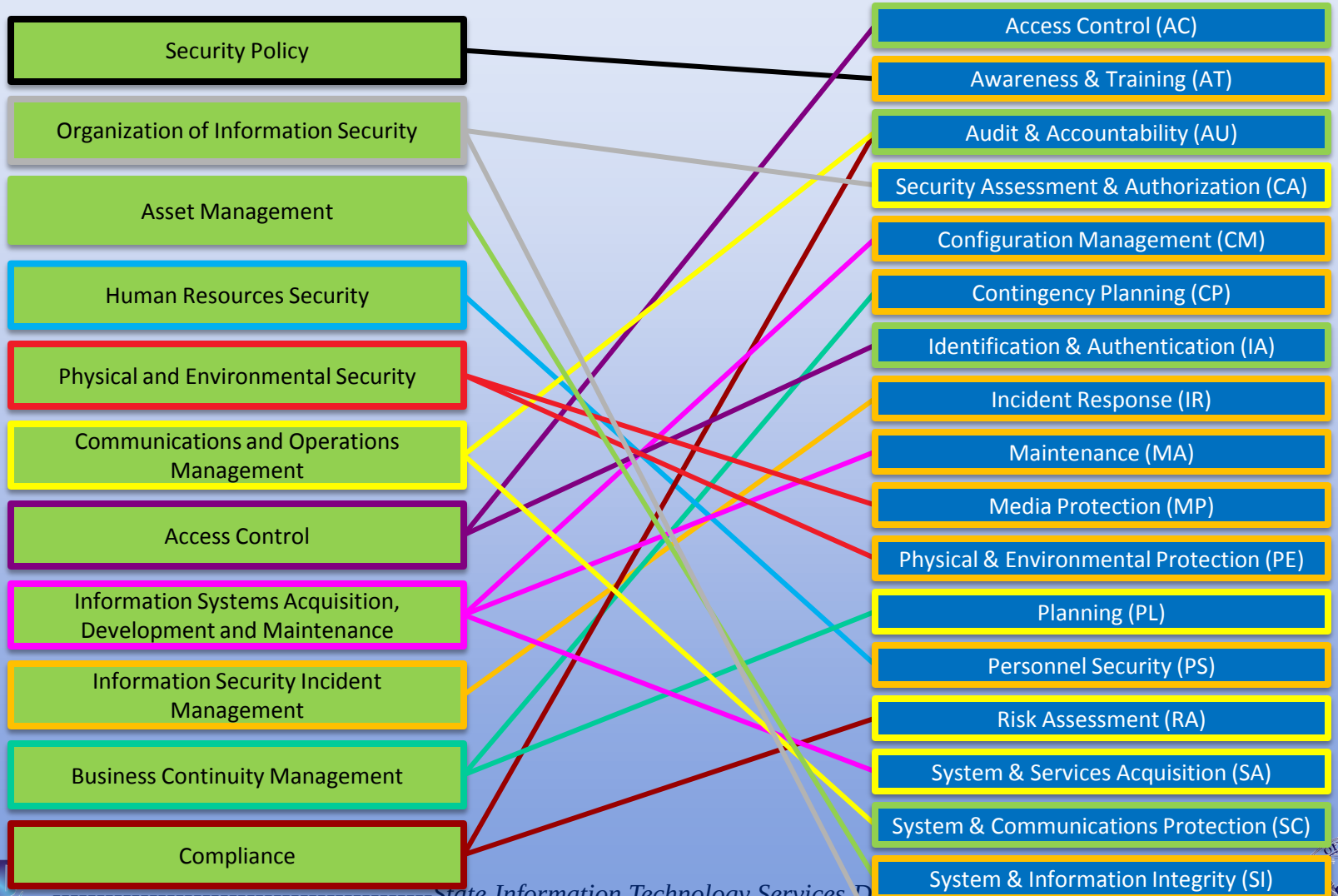
Common Controls

- Controls that are inheritable and cross domain
- Typically broad controls, such as
  - Program management
  - Incident response
  - Physical and environmental controls
  - Personnel security controls
  - Contingency planning
  - Security awareness and training
- Usually manifest in an organization-wide information security program plan
- Represents NIST's attempt to recognize an opportunity to group controls based on scope and specificity
  - Non-common controls are system-specific controls or hybrid controls (where system specific controls have common attributes)

SP800-53 and ISO-27002

- Many programs are based on ISO
- How does 800-53 map to ISO?
  - 800-53, Appendix H, pg. H-2 (PDF pg.213)
- ISO-27002
  - Provides for 11 major areas (clauses) with 185 controls
  - Begins with the expression of risk management
  - Intended as an information security management system
  - Based on guidance and recommended conditions
- SP800-53
  - Based on the same “concept” and intent, organized differently
  - Predominantly based on a control framework with management and risk as part of that framework
  - More granular with specific controls tied to other SP’s

Primary Mapping Eye Chart



800-53 to ISO

800-53	ISO
AC-1	11.1.1
	11.4.1
	15.1.1
AC-2	6.2.2
	6.2.3
	8.3.3
	11.2.1
	11.2.2
	11.2.4
	11.7.2
AC-3	11.2.4
	11.4.5
AC-4	10.6.2
	11.4.5
	11.4.6
	11.4.7
AC-5	10.1.3
	10.6.1
	10.10.1
AC-6	11.2.2
AC-7	11.5.1
AC-8	11.5.1
	15.1.5
AC-9	11.5.1
AC-11	11.3.2
AC-12	11.3.2
	11.5.5
AC-13	10.10.2
	11.2.4
AC-15	7.2.2
AC-16	7.2.2
AC-17	11.4.2
	11.4.3
	11.4.4
AC-18	11.4.2
	11.7.1
	11.7.2
AC-19	11.7.1
AC-20	6.1.4
	9.2.5
	11.7.1

800-53	ISO
AT-1	5.1.1
	8.2.2
	15.1.1
AT-2	6.2.3
	8.2.2
	10.4.1
	11.7.1
	13.1.1
	14.1.4
	15.1.4
AT-3	8.2.2
	10.3.2
	11.7.1
	13.1.1
	14.1.4
AT-5	6.1.7
AU-1	10.1
	15.1.1
AU-2	10.10.1
AU-3	10.10.1
	10.10.4
AU-4	10.10.3
AU-5	10.10.3
AU-6	10.10.2
	10.10.4
	13.2.1
AU-7	10.10.3
AU-8	10.10.6
AU-9	10.10.3
	15.1.3
	15.3.2
AU-10	10.8.2
	10.9.1
	12.3.1
AU-11	10.10.1
	15.1.3
CA-1	6.1.4
	10.3.2
	15.1.1
CA-2	6.1.8
	15.2.1
	15.2.2

800-53	ISO
CA-3	10.6.2
	10.9.1
	11.4.5
	11.4.6
	11.4.7
CA-4	10.3.2
CA-5	15.2.1
CA-6	10.3.2
CA-7	15.2.1
	15.2.2
CM-1	12.4.1
	12.5.1
	15.1.1
CM-2	7.1.1
	15.1.2
CM-3	10.1.2
	10.2.3
	12.4.1
	12.5.1
	12.5.2
	12.5.3
CM-4	10.1.2
CM-5	11.6.1
CM-8	7.1.1
	15.1.2
CP-1	5.1.1
	10.4.1
	14.1.1
	14.1.3
	15.1.1
CP-2	10.3.2
	10.4.1
	10.8.5
	14.1.3
	14.1.4
CP-3	14.1.3
	14.1.4
CP-4	10.5.1
	14.1.5
CP-5	14.1.3
	14.1.5
CP-6	10.5.1

800-53	ISO
CP-7	14.1.4
CP-8	14.1.4
CP-9	10.5.1
	11.7.1
CP-10	14.1.4
IA-1	15.1.1
IA-2	11.2.3
	11.4.2
	11.5.2
	11.4.2
IA-3	11.4.3
	11.7.1
IA-4	11.2.3
	11.5.2
IA-5	11.5.2
	11.5.3
IA-6	11.5.1
IR-1	10.4.1
	13.1
	13.2.1
	15.1.1
IR-2	13.1.1
IR-3	14.1.5
IR-4	6.1.6
	13.2.1
	13.2.2
IR-6	6.1.6
	6.2.2
	6.2.3
	13.1.1
	13.1.2
IR-7	14.1.3
MA-1	10.1.1
	15.1.1
MA-2	9.2.4
MA-4	11.4.4
MA-5	6.2.3
	9.2.4
MP-1	10.1.1
	10.7
	15.1.1
	15.1.3

800-53	ISO
MP-2	10.7.3
MP-3	7.2.2
	10.7.3
	10.8.2
	15.1.3
MP-4	10.7.1
	10.7.2
	10.7.3
	10.7.4
	15.1.3
MP-5	10.8.3
MP-6	9.2.6
	10.7.1
	10.7.2
PE-1	15.1.1
PE-2	9.1.2
	9.1.6
PE-3	9.1.1
	9.1.2
	9.1.5
	9.1.6
	10.5.1
PE-4	9.2.3
PE-5	9.1.2
	11.3.3
PE-6	9.1.2
PE-7	9.1.2
PE-8	9.1.2
PE-9	9.2.2
	9.2.3
PE-10	9.2.2
PE-11	9.2.2
PE-12	9.2.2
PE-13	9.1.4
	9.2.1
PE-14	9.2.1
	10.5.1
	10.7.1
PE-15	9.1.4
	9.2.1
PE-16	9.1.6
	9.2.7
	10.7.1

800-53	ISO
PE-17	11.7.2
PE-18	9.2.1
PL-1	6.1
	15.1.1
PL-2	6.1
PL-3	6.1
PL-4	7.1.3
	8.1.3
	15.1.5
PL-5	15.1.4
PL-6	15.3.1
PS-1	8.1.1
	15.1.1
PS-2	8.1.2
PS-3	8.1.2
PS-4	8.1.3
	8.3
	11.2.1
PS-5	8.3.1
	8.3.3
	11.2.1
PS-6	6.1.5
	8.1.3
PS-7	6.2.1
	6.2.3
	8.1.1
	8.1.2
	8.1.3
	8.2.1
	8.2.2
	11.2.1
PS-8	8.2.3
	11.2.1
RA-1	4.1
	15.1.1
RA-2	7.2.1

800-53	ISO
RA-3	4
	4.1
	4.2
	6.2.1
	10.10.2
	10.10.5
	12.5.1
	12.6.1
	14.1.1
	14.1.2
RA-4	4.1
RA-5	12.6.1
SA-1	12.1
	15.1.1
SA-2	10.3.1
SA-4	12.1.1
SA-5	10.7.4
SA-6	15.1.2
SA-7	15.1.2
SA-8	12.1
SA-9	6.2.1
	6.2.3
	10.2.1
	10.2.2
	10.6.2
SA-10	12.5.1
	12.5.2
SA-11	12.5.1
	12.5.2
SC-1	10.8.1
	15.1.1
SC-2	11.4.5
SC-3	11.4.5
SC-4	10.8.1
SC-5	10.8.4
	13.2.1
SC-7	11.4.6
SC-8	10.6.1
	10.8.1
	10.9.1
SC-9	10.6.1
	10.8.1
	10.9.1

800-53	ISO
SC-10	11.5.6
SC-11	10.9.2
SC-12	12.3.1
	12.3.2
SC-14	10.7.4
	10.9.3
SC-16	7.2.2
	10.8.2
	10.9.2
SC-17	12.3.2
SC-18	10.4.1
	10.4.2
SI-1	15.1.1
SI-2	10.10.5
	12.4.1
	12.5.1
	12.5.2
	12.6.1
SI-3	10.4.1
SI-4	10.6.2
	10.10.1
	10.10.2
	10.10.4
SI-5	6.1.7
	10.4.1
SI-7	12.2.1
	12.2.2
	12.2.4
SI-9	12.2.1
	12.2.2
SI-10	10.7.3
	12.2.1
	12.2.2
SI-11	12.2.1
	12.2.2
	12.2.3
	12.2.4
SI-12	10.7.3
	12.2.4

Areas of 800-53 / ISO Gaps

- Areas where 800-53 addresses specific features that are not as obvious in ISO

AC-10	Concurrent Session Control
AC-14	Permitted Actions Without Identification Or Authentication
AT-4	Security Training Records
CM-6	Configuration Settings
CM-7	Least Functionality
IA-7	Cryptographic Module Authentication
IR-5	Incident Monitoring
MA-3	Maintenance Tools
MA-6	Timely Maintenance
PE-19	Information Leakage
SA-3	Life Cycle Support
SC-6	Resource Priority
SC-13	Use Of Cryptography
SC-15	Collaborative Computing
SC-19	Voice Over Internet Protocol
SC-20	Secure Name / Address Resolution Service (Authoritative Source)
SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)
SC-22	Architecture And Provisioning For Name / Address Resolution Service
SC-23	Session Authenticity
SI-6	Security Functionality Verification
SI-8	Spam Protection

SP800-53 as the Center Point

- This is where the real value of NIST SP's comes to light
  - Can have a tangible impact to existing programs
  - Act as targeted guidance in creating a program
- Each connected SP from 800-53 is
  - A complete standard
  - Contains implementation guidance
  - Provides additional information to other practices
  - Provides mappings to regulations
  - Offers a control framework

Other Interesting SP's

- Even when using ISO, 800-53 mapping to other SP's can provide guidance in improving and building comprehensive security program features
  - Some popular ones…
    - 800-39: Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View (updated)
    - 800-40: Creating a Patch and Vulnerability Management Program
    - 800-50: Building an Information Technology Security Awareness and Training Program
    - 800-61: Computer Security Incident Handling Guide
    - 800-64: Security Considerations in the System Development Life Cycle
    - 800-124: Guidelines on Cell Phone and PDA Security

Other More Recent Interesting SP's

- 800-121: Guide to Bluetooth Security
- 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- 800-125: Guide to Security for Full Virtualization Technologies
- 800-146: Cloud Computing Synopsis and Recommendations
- 800-153: Guidelines for Securing Wireless Local Area Networks

Is this Mission Possible?

Montana's 5 Year Plan

1. Gap Analysis (Risk Assessment)	2008
2. Write Policies and Procedures	2009 – 2010
3. Implementation of Policies and Procedures	2010 – 2011
4. Education, Education, Education	2010
5. Continue Writing Procedures	2011 – 2012
6. More Education	2011
7. Continue Implementing Procedures	2012
8. Even More Education	2012
9. Review and start over	2013

The next step in your mission…

Gap Analysis

Also known as a Risk Assessment

Getting Started

- As with any standards-based security program development you have to start with a Risk Assessment
- Basic questions
  - What security controls are needed to adequately mitigate identified risk?
  - Have identified controls been implemented, is there a plan, and what compensating controls are needed?
  - What is the desired level of assurance that the selected control (as implemented) is effective?

Risk Assessment

- There are roughly 70 different risk management and assessment models available in the industry today
  - Not including the several hundred risk tools out there
- In <u>very</u> simple terms…
  - Risk assessment is:
    - Evaluating the probability of an event and level of potential impact
  - Security is:
    - The controls that protect assets from threats
- Many organizations assess risk using different “philosophies”

Risk and NIST

- There are a number of ways to assess risk to determine meaningful security controls (and investments)
  - Where you start can/will impact where you end
    - Vulnerability based
    - Threat based
    - Control capability based
    - Compliance based
    - Asset based
    - Others?
- NIST take the approach of system-based risk relative to mission objective
  - “The risk to organizational operations and assets, individuals other organizations, and the Nation associated with the operations of an information system”
- Guidance:
  - SP800-30 Risk Assessment
  - SP800-39 Developing Risk Management Strategy

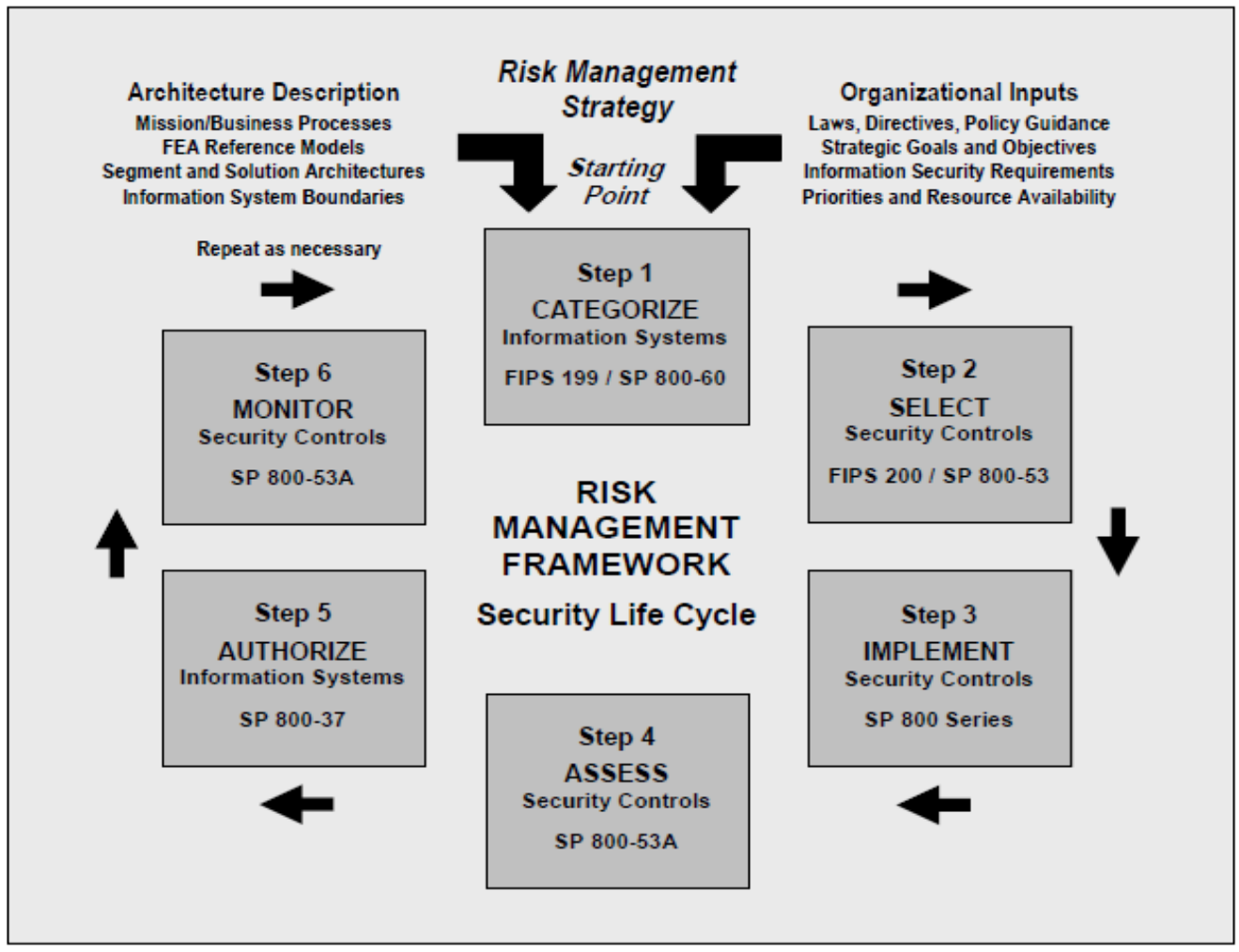
Enterprise Applicability & Risk

- A key “twist” from traditional security programs to a NIST-based security program
  - It all starts with information classification, defining:
    - Value to the business
    - Criticality to business operations/functions and achieving objectives
    - Lifecycle management of information assets relative to business cycles
      - Also change in value over time
  - Classification leads to “system” classification
    - System can be a: server, networks, applications, locations, or a combination
  - System classification leads to system criticality

NIST's Key Activities in Managing Risk

- Categorize* the information system and the information processed, stored, and transmitted by that system
- Select* initial set of baseline controls based on impact level and minimum security requirements and tailor
- Implement the security controls and describe how the controls are employed within the information system and its environmental operation
- Assess the security control using the appropriate procedures to determine the extent controls are implemented correctly, operating as intended, and producing the desired outcome
- Authorize information system operation based on risk determination and/or risk acceptance
- Monitor* controls continually to assess effectiveness, documenting changes, impact analysis of changes, and control reporting

NIST's Risk Management Strategy



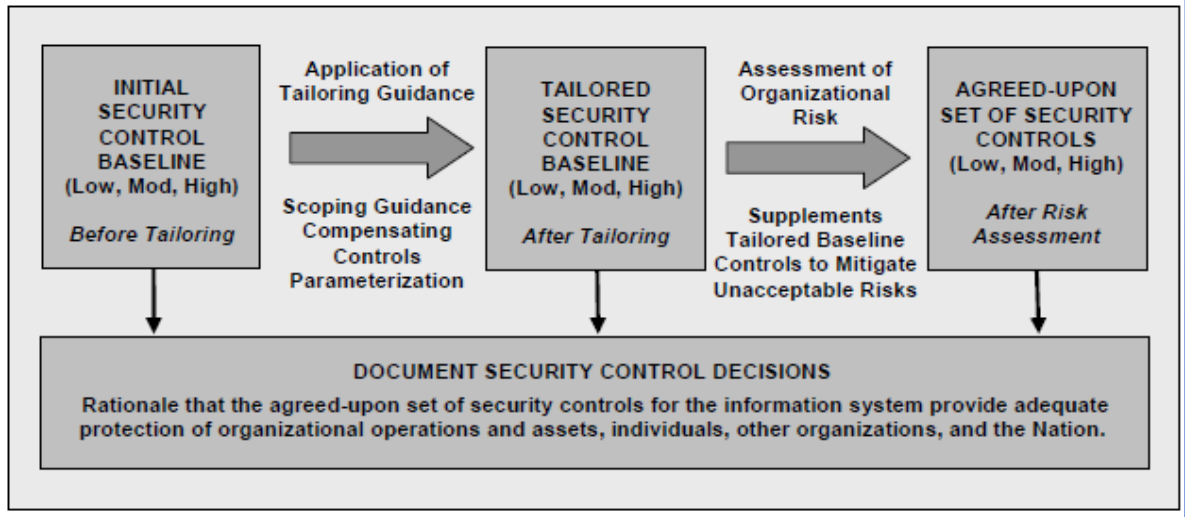
Categorization of Information System

- SP800-60 Guide for Mapping Types of Information and Information Systems to Security Categories (SC)
- Seeking to determine low, moderate, or high impact relative confidentiality, integrity, and availability
- SCIS = (conf,impact),(integrity,impact),(avail,impact)
  - Potential impact is a “high water mark” of the different information types that are processed, stored, and transmitted by targeted system

Info Sys	Conf	Integ	Avail	Impact
SAP	High	Mod	Low	**High**
TGGS	Mod	Low	Mod	**Mod**
CRM	Low	Mod	Low	**Mod**
UCC	Low	Low	Low	**Low**

Selecting Controls

- Selecting initial baseline controls
- Tailoring baseline controls
  - Scoping to determine applicability and implementation of specific controls
  - Compensating security controls to adjust and provided an equivalent set deemed more feasible to implement
  - Organizational-defined parameters in security controls relative so explicit assignment



Gap Analysis Process for State of Montana

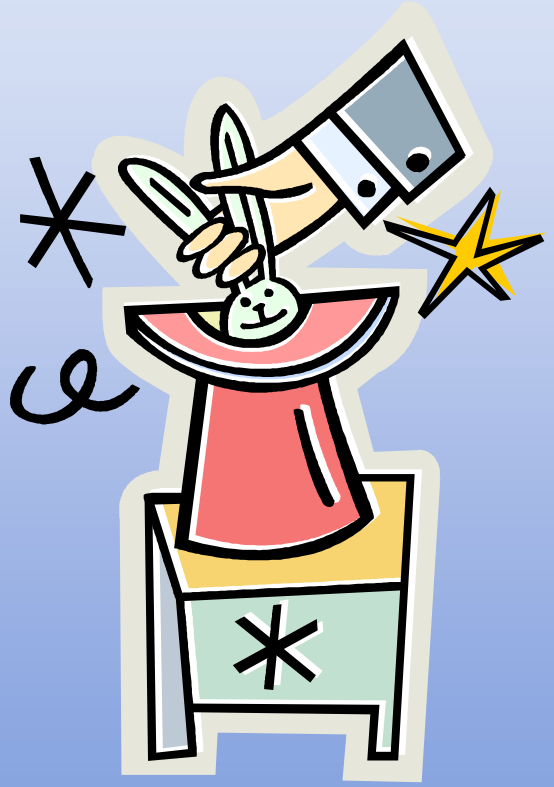
NIST 800-53 Rev3

Templates

Presentation to Executive Team

Assignments

Risks and Controls



The next step in your mission…

Policies and Procedures

Policies and Procedures

Standard format - Templates

Easy – KISS principle

One or many?

Policy and Procedure Requirements

- Formal process
- Purpose, scope, roles, and responsibilities
- Management Commitment
- Coordination among organizational entities
- Compliance process

The next step in your mission…

Implementation

Implementation

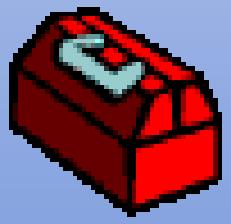
Start at the Top:

- Management Class
- Technical Class
- Operational Class

Implementation

Education

Processes and Tools



“Seven Times” Rule for Education

Implementation of a Good Security Program

The last step in your mission…

Review

Review

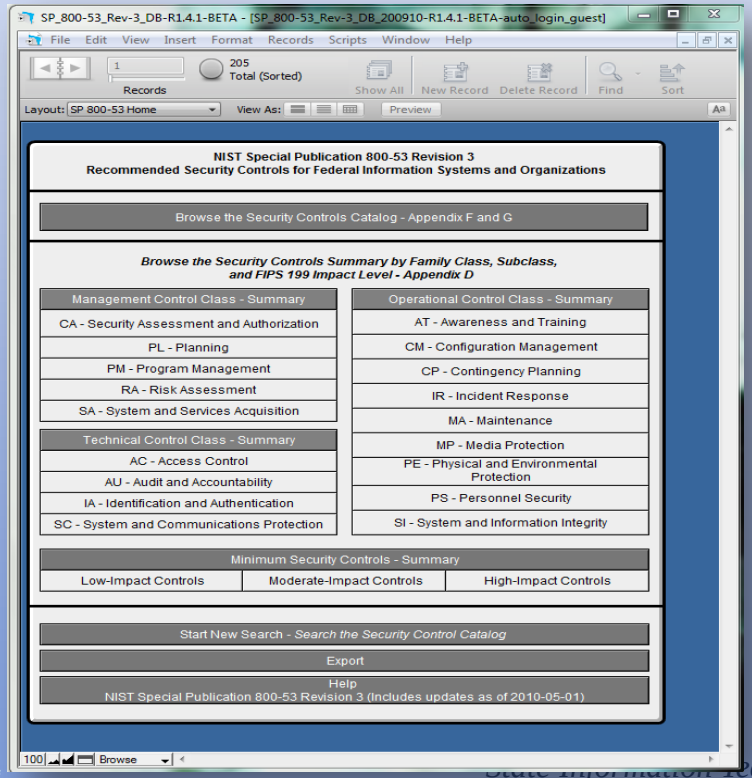
- Start over
- Gap Analysis
- Draft SP800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations

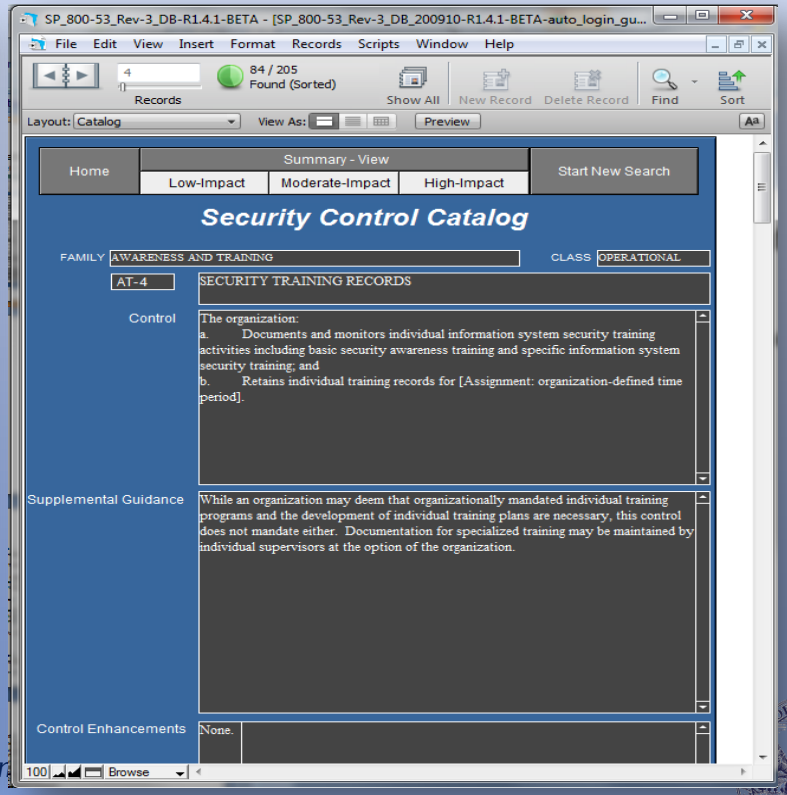
Challenges/Pitfalls

- NIST 800-53 is – at its heart - a controls framework, supported by multiple management, implementation, and program defining features
  - In other words…big……..HUGE
- Challenges for some…
  - Quantifying and categorizing security
  - Clarity in criticality
  - Monitoring (the biggest challenge for most – requires a great deal of commitment)
- Pitfalls for some…
  - Taking it on in one shot - - success unlikely for typical enterprises
  - Cycles in focus and inability to maintain consistency

Assistance – 800-53 Database

- Tools: http://csrc.nist.gov/groups/SMA/fisma/support_tools.html
- On-line database: http://web.nvd.nist.gov/view/800-53/home
- Database Application: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/SP_800-53_Rev-3_database-R1.4.1-BETA.zip





Conclusions

- NIST's approach to security is
  - Comprehensive
  - Well-designed
  - Effectively supported
- Highly applicable to the enterprise
  - Leverage 800-53A for an initial assessment
- Great Information - Use what you want

Resources

- NIST:

http://csrc.nist.gov/publications/PubsFL.html

- Guide to NIST Publications:

http://csrc.nist.gov/publications/CSD_DocsGuide.pdf

- NIST 800-53 Rev3

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

Final Comment

This process will not self destruct in 60 seconds.

Summary

- Compliance Smorgasbord
- Overview of NIST
- Special Publications and 800-53
- Security Controls Overview
- Special Publications and ISO 27000
- NIST and Risk Management
- Policies and Procedures
- Implementation
- Review

ANY QUESTIONS?