




# The University of Texas System FISMA Overview

November 16, 2011

This presentation is intended solely for the information and internal use of UT System, the Academic Compliance Consortium, and the registered attendees of this webcast, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this presentation.

# Webinar Essentials

---

1. Session is currently being recorded, and will be available on our website at <http://www.utsystem.edu/compliance/SWCAcademy.html>.
2. Attendees are currently muted. If you wish to ask a question please click on the “Raise Hand” button . The webinar administrator will un-mute you at the appropriate time.
3. Be careful of turning down speaker volume to avoid feedback.
4. Questions may also be typed in the GoToWebinar *Question* panel.
5. CPE credit is available for this webinar for attendees who attend the live webinar. Please request credit by sending an email to the SWC Office at [systemwidecomp@utsystem.edu](mailto:systemwidecomp@utsystem.edu).
6. Please provide your feedback in the post-session survey.

# Agenda

---

- The Evolution of FISMA
  - FISMA Overview
  - FISMA Components
  - FISMA Applicability to Non-Federal Organizations
  - Understanding NIST's Role
- NIST's Risk Management Framework
  - Authorization Boundary
  - Continuous Monitoring and Automating Compliance
  - Benefits

# The Evolution of FISMA

# FISMA Overview

---

- The [E-Government Act \(Public Law 107-347\)](#) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the [Federal Information Security Management Act \(FISMA\)](#), requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

# FISMA's Core Components

---

- **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization
- **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system
- **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate
- **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks
- **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually
- A **weakness remediation process** for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization
- Procedures for detecting, reporting, and responding to **security incidents**
- Plans and procedures to ensure **continuity of operations** for information systems that support the operations and assets of the organization

# Evolution of FISMA - Highlights

---

- 2000 – Congress started modern quest to improve information security with Federal Agencies under Government Information Security Reform Act (GISRA).
- 2002 - GISRA's lack of enforcement mechanisms leads to the passing of FISMA
- 2003/4 - Congress starts issuing grades for FISMA compliance led by Rep. Tom Davis. Federal government recognizes security risks include outsourcing contractors, not just agency-owned assets.
- 2004/5 – Federal agencies expand risk profile to State agencies administering Federal programs. Pilot programs developed to understand the risks and close gaps.
- 2009 – Industry push for less documentation and more automation. Consensus Audit Guidelines (CAG) 1.0 released.
- 2010 – Rapid expansion of FISMA contract language in grant requests, RFPs, etc in commercial sector.

# FISMA's Applicability to Non-Federal Organizations

---

OMB clarified the reach of FISMA in its FY 2006 FISMA reporting instructions to Federal agencies.

*“Agency IT security programs apply to all organizations which possess or use Federal information on behalf of a Federal agency...including contractors, grantors, State and Local Governments, etc.”*

*“Agencies must ensure identical, not equivalent, security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation must, at a minimum, explicitly meet guidance from NIST.”* OMB 2006

# Federal Agencies expand enforcement of FISMA

---

Unlike the Office Civil Rights (OCR) for HIPAA, there isn't one federal agency responsible for FISMA compliance.

- Department of Labor
  - Developed grant program for Unemployment Insurance agencies to improve security posture in 2004/5
  - Granted \$8-12M annually to state UI agencies to meet FISMA standards
- Department of Education
  - Recognized security risks at private Loan Servicers, Collection Agencies and Guaranty Agencies
  - Implemented multi-year program to assess and certify using FIPS 200
  - Potential exists for Federal Student Aid to expand enforcement of FISMA to higher education – Title IV program and FERPA.
- Many other examples – SSA, CMS, DoD, NIH, VA

# Consensus Audit Guidelines (CAG)

---

In February 2009, a consortium of federal agencies and private organizations developed the Consensus Audit Guidelines Version 1.0. The 20 controls are a set of risk-based controls designed to mitigate the risks of attacks that frequently target the federal government, financial services, retailers and higher education institutions. Key points:

- CAG is currently up to Version 3.0 and can be found at <http://www.sans.org/critical-security-controls/>
- Focus of controls is on rigorous automation and measurement of control effectiveness.
- Organizations with limited resources can prioritize their remediation using the 20 controls recommended by the CAG.
- Detailed implementation and testing procedures provided by sponsoring organizations.
- Mapping to FIPS 200 control library, but compliance with FISMA requires additional documentation and implementation.
- Limited implementation and support within Federal government.

# Understanding NIST's role

---

- FISMA identified the National Institute of Standards and Technology (NIST) as the organization responsible for developing information security standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series) for non-national security federal information systems and assigned NIST some specific responsibilities, including the development of:
  - Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
  - Guidelines recommending the types of information and information systems to be included in each category; and
  - Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category.

# Key NIST Publications and Guidelines

---

NIST has two predominant publication series for information security - Special Publication 800 (SP) series and the Federal Information Processing Standards (FIPS) series. Knowledge of these and other NIST publications are essential for FISMA compliance.

NIST Publication	Description
<b>SP 800-18</b> - <i>Guide for Developing Security Plans for Federal Information Systems</i>	Document system controls in a system security plan (SSP)
<b>800-53/FIPS 200</b> - <i>Minimum Security Requirements for Federal Information and Information Systems</i>	Control library for information systems
<b>SP 800-53A</b> - <i>Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans</i>	Testing guidance for information systems
<b>SP 800-30</b> - <i>Risk Management Guide for Information Technology Systems</i>	Risk Assessments and Risk Management
<b>SP 800-37</b> - <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>	Certification and Accreditation lifecycle
<b>SP 800-137 IPD</b> - <i>DRAFT Information Security Continuous Monitoring for Federal Information Systems and Organizations</i>	Initial expectations for continuous monitoring under FISMA.
<b>FIPS 199/800-60</b> - <i>System Categorization and Guide for Mapping Types of Information and Information Systems to Security Categories</i>	Identification of the control baseline (low, moderate, high) for the information system

# NIST Security Control Requirements

---

- NIST categorizes FISMA principles into 18 security control families found in NIST Special Publication *800-53: Minimum Security Controls for Federal Information Systems*.
  - Each control area contains numerous requirements, based on the sensitivity level of the system.
- NIST controls often cover most controls in other frameworks such as ISO, NIST and PCI DSS

## Management Controls

- RA – Risk Management
- PL – Planning
- SA – System & Services Acquisition
- CA – Security Assessment & Authorization
- PM – Program Management

## Operational Controls

- PS – Personnel Security
- PE – Physical & Environmental Protection
- CP – Contingency Planning
- CM – Configuration Management
- MA – Maintenance
- SI – System & Information Integrity
- MP – Media Protection
- IR – Incident Response
- AT – Awareness & Training

## Technical Controls

- IA – Identification & Authentication
- AC – Access Control
- AU – Audit & Accountability
- SC – System & Communications Protection



# What does FISMA Compliant really mean?

---

- For non-Federal agencies, compliance with NIST 800-53
- Completion of the following core documents

## Required Documentation

Authorization Boundary/ Security Categorization (FIPS 199)

System Security Plan (NIST 800-18)

Risk Assessment (800-30)

Security Assessment Report (800-30, 800-37)

Contingency Plan/Disaster Recovery Plan (800-34)

Privacy Impact Assessment

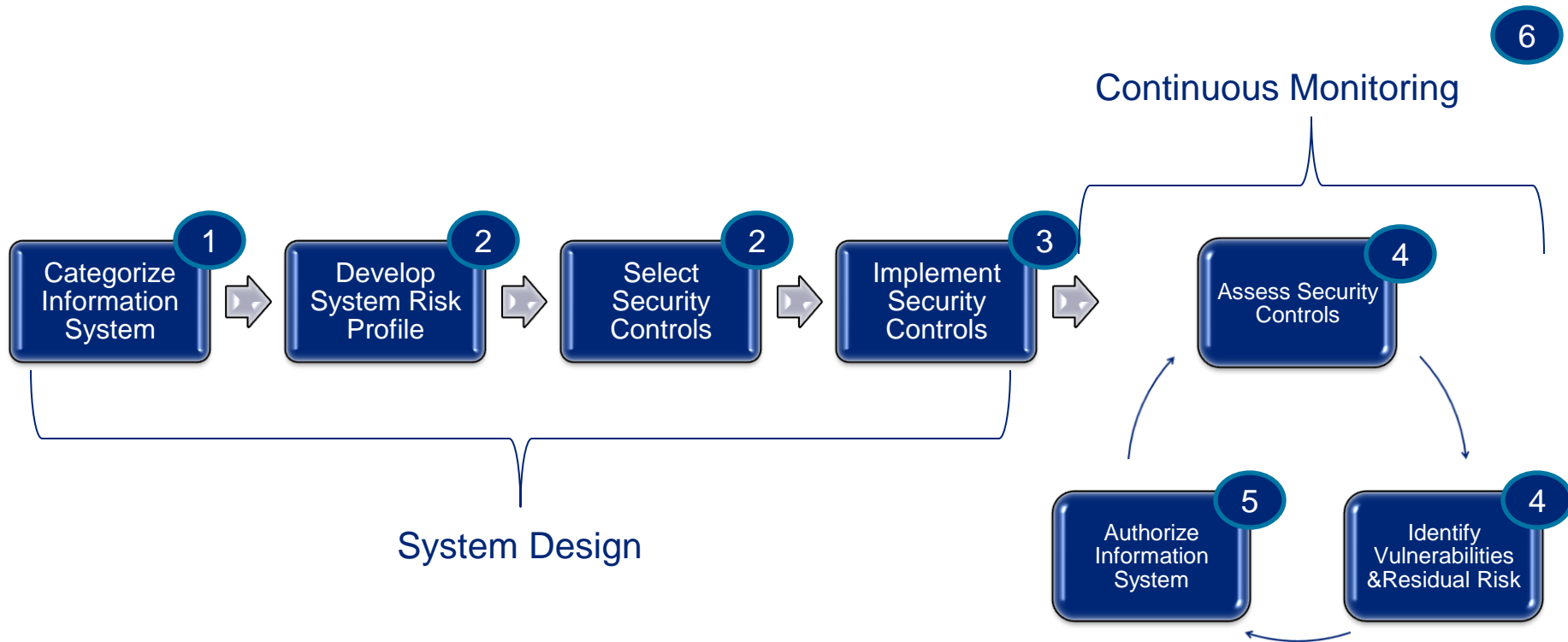
Plan of Action and Milestones (POA&M)

- Additionally, some agencies require Certification and Accreditation
  - Formal program of system boundary authorization
  - Self Assessment, 3<sup>rd</sup> Party Attestation (SOC2), Federal certification

# NIST's Risk Management Framework

# NIST's Risk Management Framework (RMF)

NIST describes the RMF model as a series of six repeating steps designed to identify the security mechanisms necessary for an IT system, implement those protections, and validate their proper operation over the systems' lifecycle.



# Key success criteria for each step in the RMF

---

- Step 1: Categorize Information System: Has the organization completed a **security categorization** of the information system including the information to be processed, stored, and transmitted by the system? Has the organization **registered** the information system for purposes of management, accountability, and oversight?
- Step 2: Select Security Controls: Has the organization allocated all security controls to the **information system** as system-specific, hybrid, or common controls? Has the organization identified **authorizing officials** for the information system and all common controls inherited by the system?
- Step 3: Implement Security Controls: Has the organization documented how **common, system-specific and hybrid controls** inherited by organizational information systems have been implemented?
- Step 4: Assess Security Controls: Has the organization developed a comprehensive **plan** to assess the security controls employed within or inherited by the information system? Has the organization considered the appropriate level of assessor **independence** for the security control assessment?
- Step 5: Authorize Information System: Did the organization take the necessary **remediation actions** to address the **most** important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report? Did the organization develop an appropriate **authorization package** with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?
- Step 6: Monitor Information Security Controls: Is the organization effectively monitoring changes to the **information system** and its **environment of operation** including the effectiveness of deployed **security controls** in accordance with the continuous monitoring strategy?

# Authorization Boundary Overview

---

The Authorization Boundary is a logical and physical boundary that groups Information Technology assets with the same mission and security requirements and determines the complexity of a system's certification.

The Authorization boundary definition process needs to strike a balance between expanded boundaries and tighter boundaries in order to allow for the right level of testing and security controls to be applied.

## What constitutes Accreditation Boundaries?

- General Support Systems (GSS)
  - Major Applications (MAs)
- Functional & Development Tools
  - System Interconnections

## Why Do we need an Accreditation Boundary?

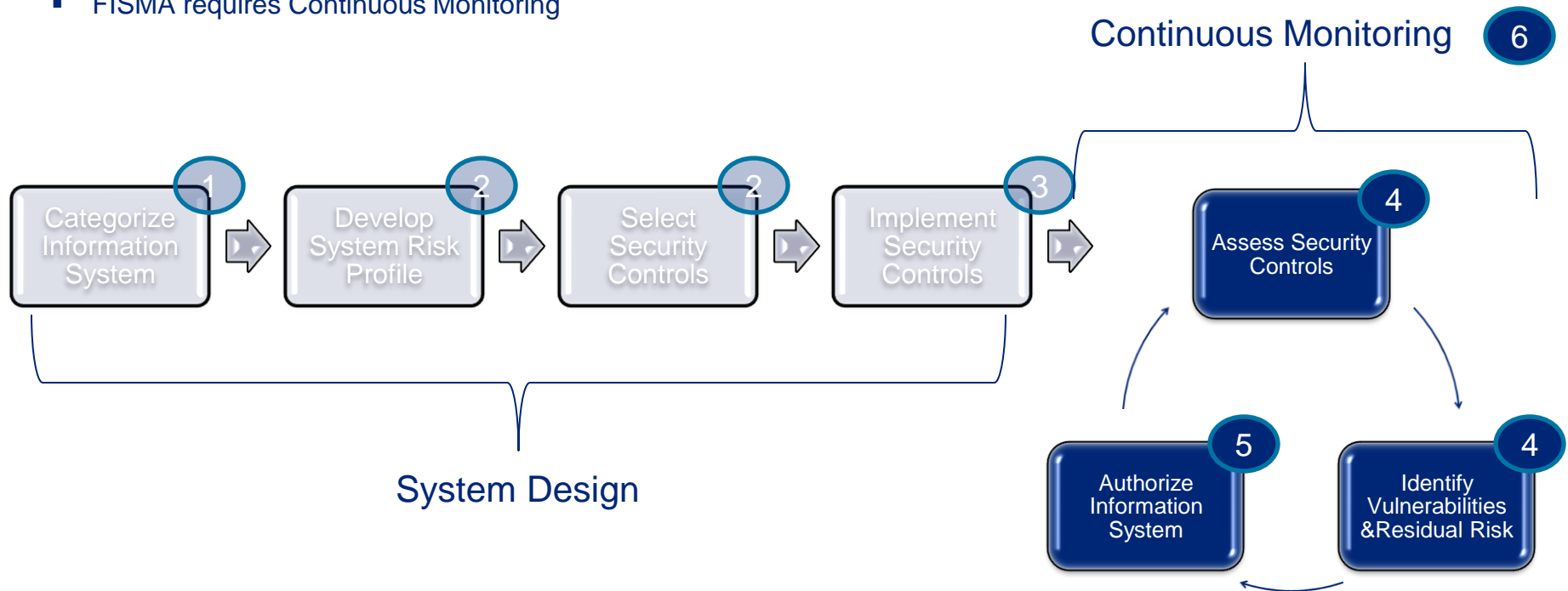
- Certification & Accreditation
- Clear decision authority

**Effective Authorization Boundaries promote an effective security posture for an organization's Information Systems**

# Continuous Monitoring

Continuous monitoring is one of six steps in the Risk Management Framework (RMF) described in NIST Special Publication 800-37, Revision 1, *Applying the Risk Management Framework to Federal Information Systems* (February 2010). The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.

- Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation (including threat space).
- Authorizing Officials' risk-based decisions (i.e., security authorization decisions) should consider how continuous monitoring will be implemented organization-wide as one of the components of the security life cycle represented by the RMF.
- FISMA requires Continuous Monitoring



Q&A

**Deloitte.**