Automated Security Support Tools

The Key to Successful FISMA Implementation

September 18, 2006

Dr. Ron Ross

Computer Security Division

Information Technology Laboratory

The Global Threat

- Information security is not just a paperwork drill…there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten our economic and national security…

FISMA Legislation

Overview

"Each federal agency shall develop, document, and implement an agency-wide information security 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…"

-- Federal Information Security Management Act of 2002

NIST's Responsibilities

- Develop necessary information security standards and guidance to allow federal agencies to demonstrate compliance to the legislation.
- Work with federal agencies, contractors, and industry to facilitate effective implementation of the security standards and guidance.

The FISMA Vision

- We are building a solid foundation of information security across the largest information technology infrastructure in the world based on comprehensive security standards and technical guidance.
- We are institutionalizing a comprehensive Risk Framework that promotes flexible, cost-effective information security programs for federal agencies.
- We are establishing a basic level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.

FISMA Implementation

- Effective implementation of FISMA requires three T's:
  - ***Training***
    - Understanding the legislation and the implementing security standards and guidance.
  - ***Transition Strategy***
    - Game plan for moving the enterprise from the old way of managing and implementing information security to the new FISMA paradigm.
  - ***Tools***
    - Why we are here today…collaboration among government agencies and industry to build consensus for a common specification language for expressing configuration settings and to promote the development of widely accessible databases and automated security support tools.

What is FISMA Compliance?

- Employing appropriate security controls in an information system—sufficiently robust to protect the mission or business case of the enterprise.
- Assessing the effectiveness of the implemented security controls to determine residual information system vulnerabilities and mission/business case risk.
- Making credible, risk-based decisions on placing the information system into operation or continuing its operation.

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system (criticality/sensitivity)
  - ✓ **Select** and tailor minimum (baseline) security controls
  - ✓ **Supplement** the security controls based on risk assessment
  - ✓ **Document** security controls in system security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls for effectiveness
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

The Risk Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53 / SP 800-30

Security Control Refinement

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Security Control Documentation

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Security Control Implementation

Implement security controls; apply security configuration settings

SP 800-53A

Security Control Assessment

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

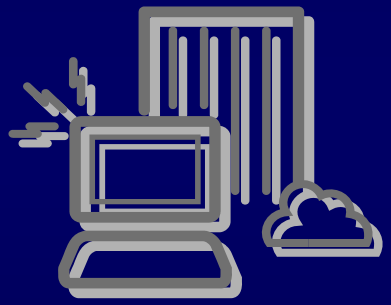
System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

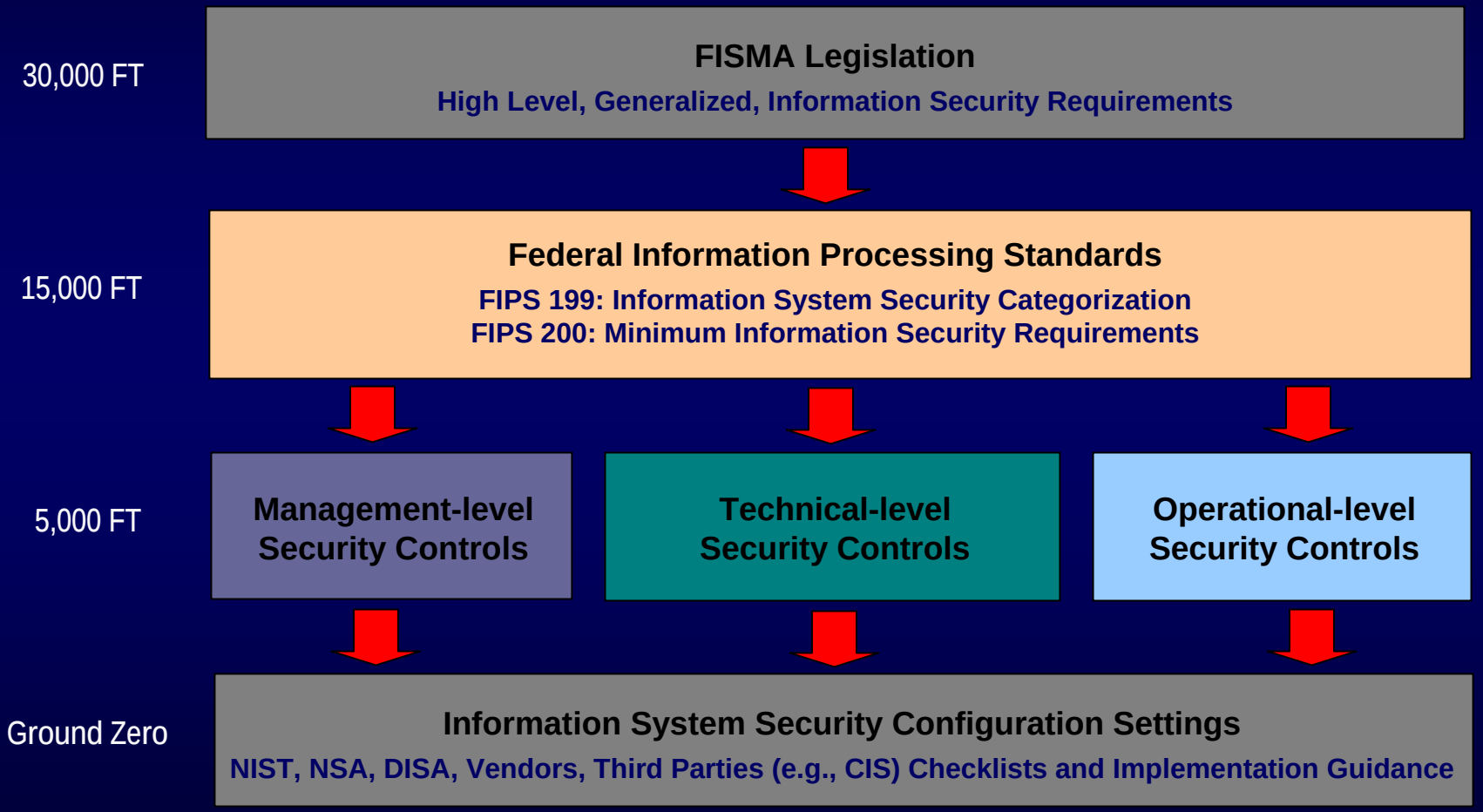
SP 800-37 / SP 8800-53A

Security Control Monitoring

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



FISMA Compliance Model



Secure Configuration Settings

The linkage between security controls and the information system…

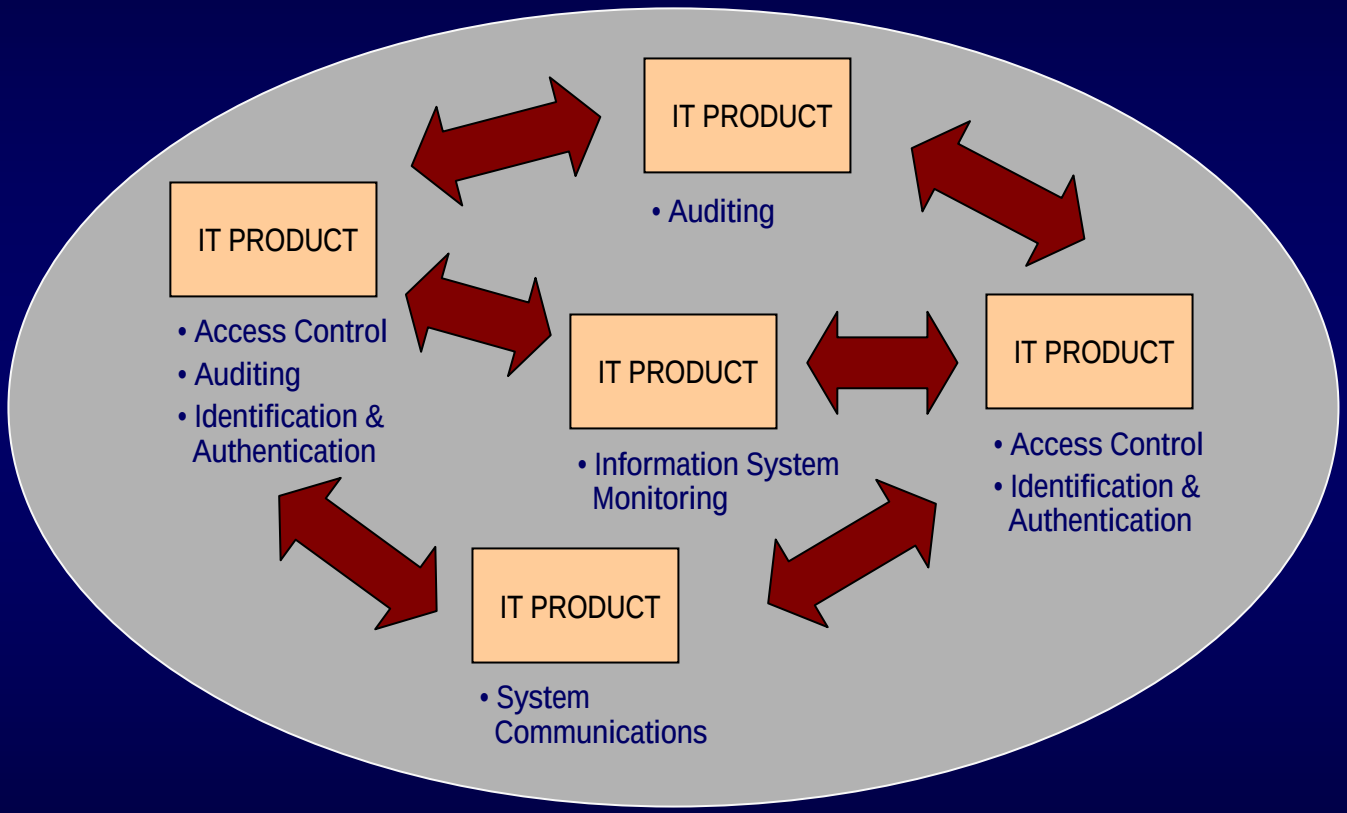
- Configuration settings are critically important in the implementation of selected security controls to ensure the full security capability of the controls can be obtained.
- Mandatory configuration settings, agency established and agency enforced, are a key provision of FISMA.

Information Systems View

Key Tasks…

- Determining which IT products implement designated security controls.
- Ensuring appropriate configuration settings are established and enforced for each IT product within the information system.

Information Systems View



Benefits of Automated Tools

(and standardized specification language)

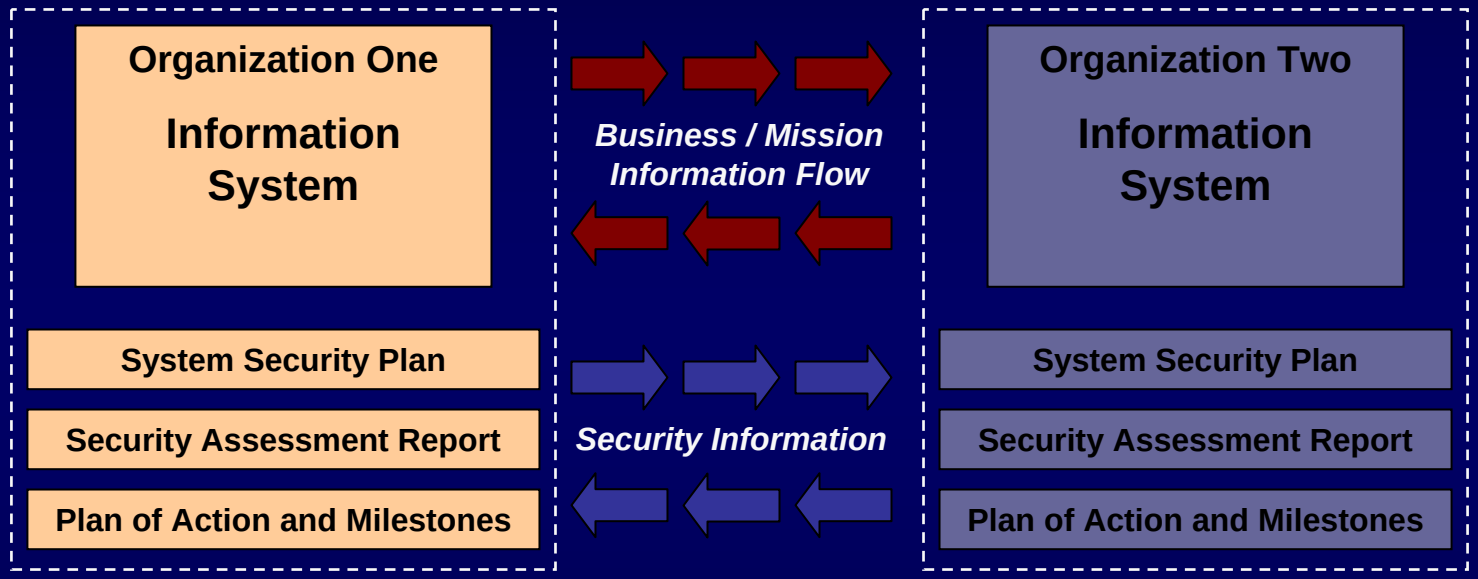
- Provide a consistent and comprehensive method of applying and verifying configuration settings for component IT products used in information systems.
- Reduce security implementation costs and provide greater efficiencies in managing configuration settings required by FISMA.
- Reduce the complexity associated with implementing configuration settings; make user-friendly and widely deployable.

Bottom Line

- Effective and efficient automated security support tools are ***essential*** to the success of FISMA…and to providing the necessary protection for federal information systems and those systems that support the United States critical infrastructure.

The Desired End State

Security Visibility Among Business/Mission Partners



Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…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

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
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov