Integrating the Federal Information Security Management Act (FISMA) and the CMMI: Partners or Problems?

Ronda Henning
rhenning@harris.com

Presentation Premise

- Federal Information Security Management Act (FISMA) evaluation criteria are embodied in NIST SP 800-53
- Evaluation criteria correspond to requirement families that measure compliance
- CMMI and SSE-CMM provide process specificity and a framework to address the FISMA criteria

The FISMA Life Cycle

HARRIS

Categorization of Information and Information System

FIPS 199 / SP 800-60

Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability, maps information types to specific categories

Risk Assessment

SP 800-26 / SP 800-30

Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, and availability would have on operations and assets

Security Planning

SP 800-18

Documents the security requirements and security controls planned or in place for the protection of information and information systems

Starting Point

Information & Information Systems

Security Control Selection and Implementation

SP 800-53 / FIPS 200

Management, operational, and technical controls (i.e. safeguards and countermeasures) planned or in place to protect information and information systems

Verification of Security Control Effectiveness (Certification)

SP 800-53A

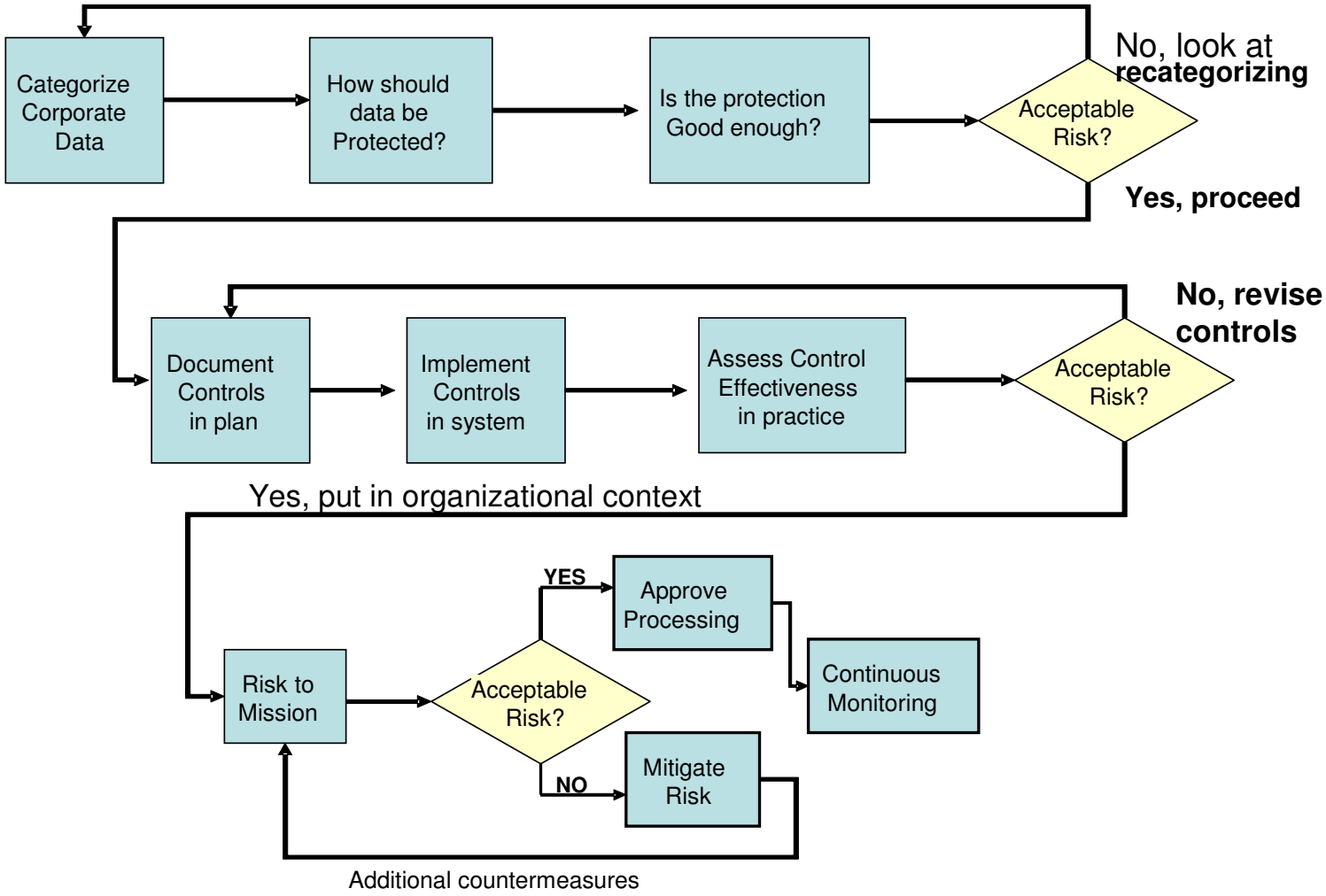
Measures the effectiveness of the security controls associated with information systems through security testing and evaluations

Security Authorization (Accreditation)

SP 800-37

The authorization of information systems to process, store, or transmit information, based on the effectiveness of security controls and residual risk

Risk Based Decisions

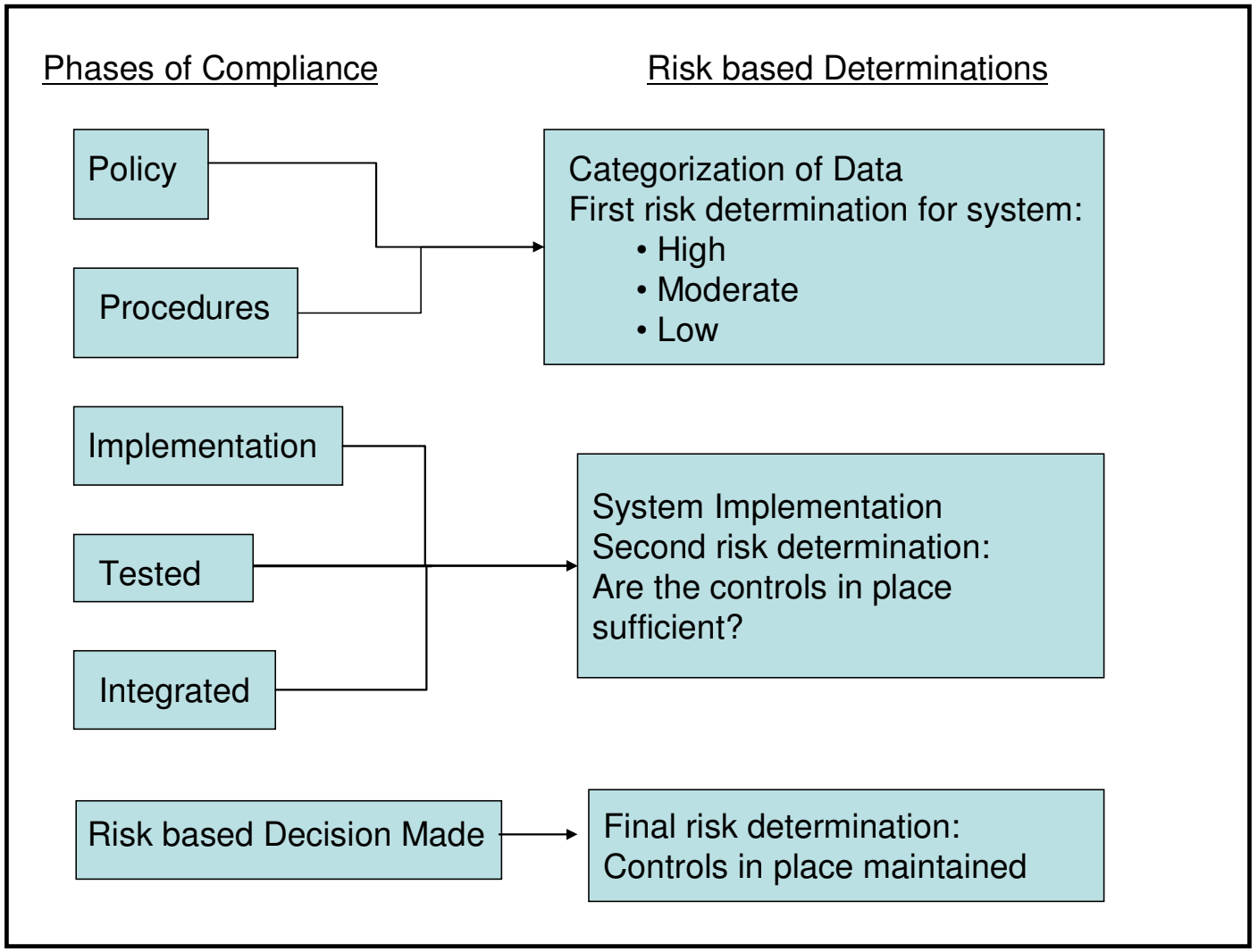


A Caveat

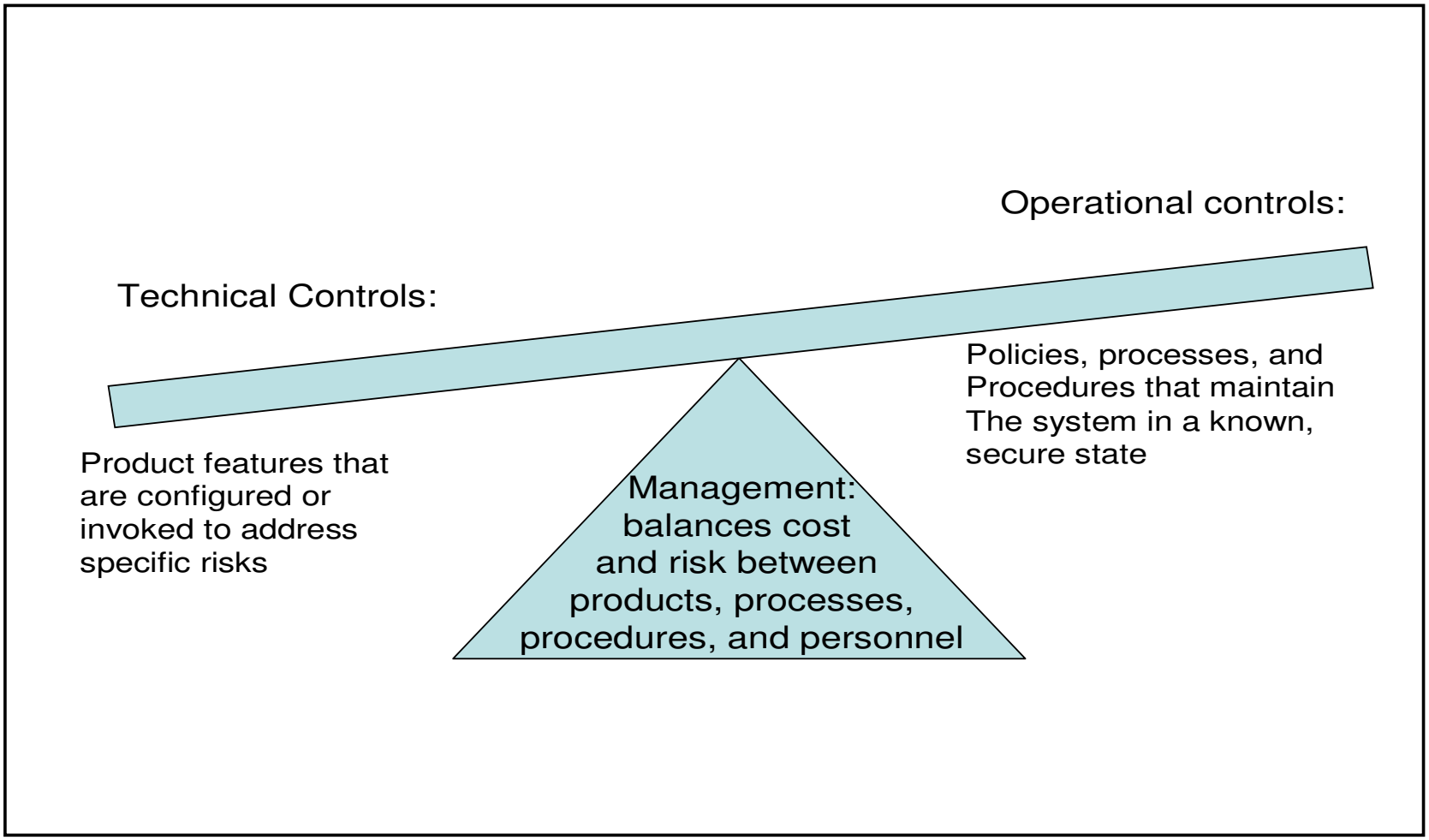
- Risk is “different”
  - Normally defined as impediments to achievement from perspective of mission functionality vs. cost or schedule
- In Security Parlance
  - Risk is the probability of compromise or exploitation of a vulnerability

Compromise is an impediment to the achievement of mission

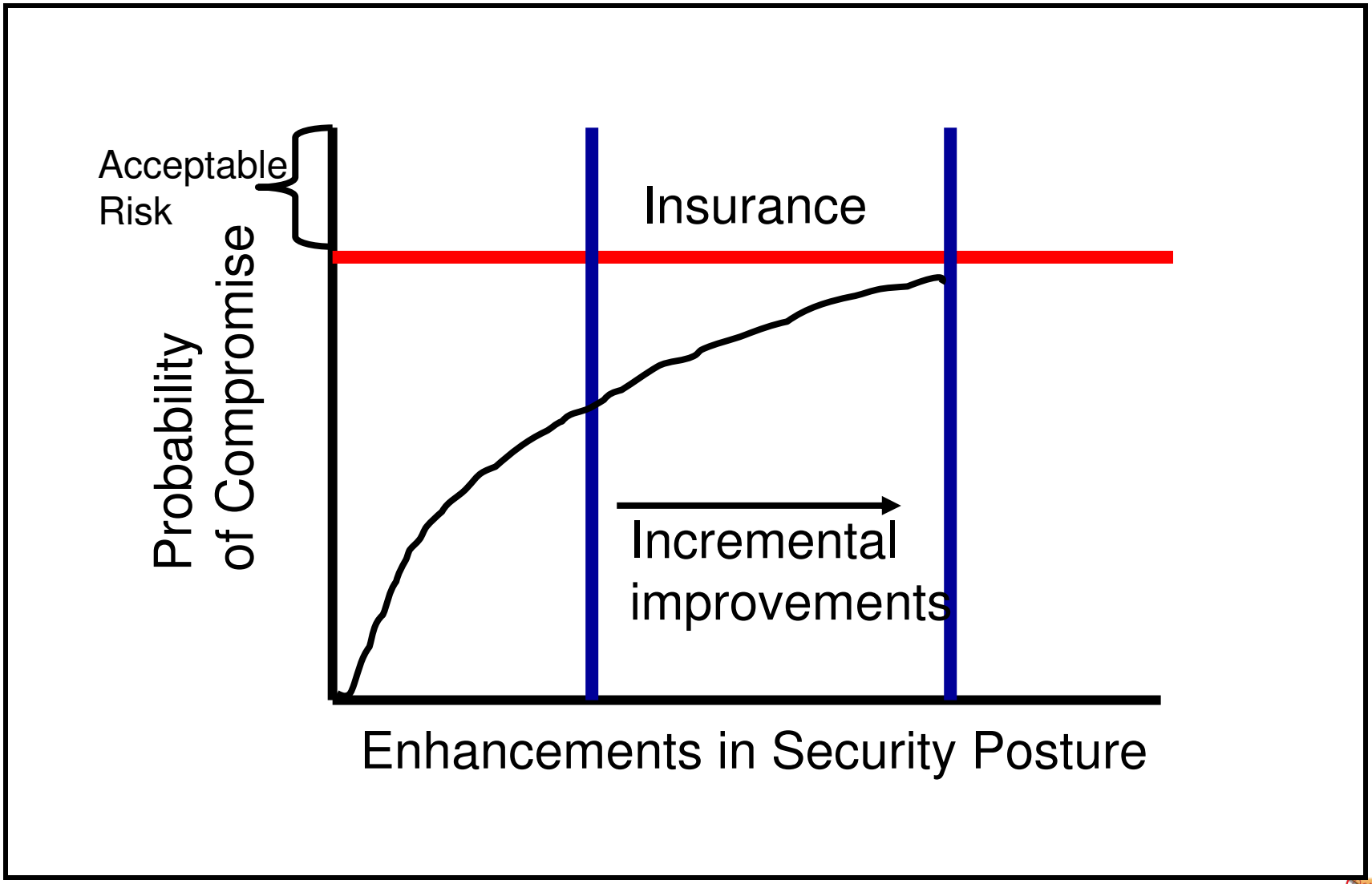
Compliance by Phase



Relationship among controls



Quantifiable Costs attached to Security Enhancements



FISMA Control Families

Management Controls

- Risk Assessment
- Planning
- System and Services Acquisition
- Certification & Accreditation (C&A)

Technical Controls

- Access Control
- Audit and Accountability
- Identification and Authentication
- System and Communications Protection

Operational Controls

- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

- Integrated guidance on product and process development activities
- Integrated content from varied disciplines
- Process framework areas are:
  - Project Management
  - Support
  - Engineering
  - Process Management

CMMI Families

HARRIS

Project Management

- Project Planning
- Project Monitoring and Control
- Supplier Agreement Management
- Integrated Project Management
- Risk Management
- Quantitative Project Management

Engineering

- Requirements Development
- Requirements Management
- Technical Solution
- Product Integration
- Verification
- Validation

Process Management

- Organizational Process Focus
- Organizational Process Definition
- Organizational Training
- Organizational Process Performance
- Organizational Innovation & Deployment

Support

- Configuration Management
- Process and Product QA
- Measurement & Analysis
- Decision Analysis & Resolution
- Causal Analysis & Resolution

FISMA to CMMI Correspondence

HARRIS

FISMA Family

Operational Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical & Environmental Protection
- Personnel Security
- System and Information Integrity

CMMI Family

Support
- Configuration Management
- Process and Product QA
- Measurement & Analysis
- Decision Analysis & Resolution
- Causal Analysis & Resolution

Engineering
- Requirements Development
- Requirements Management
- Technical Solution
- Product Integration
- Verification
- Validation

Process Management
- Organizational Process Focus
- Organizational Process Definition
- Organizational Training
- Organizational Process Performance
- Organizational Innovation & Deployment

FISMA to CMMI Correspondence

HARRIS

FISMA Family	CMMI Family
Technical Controls • Access Control • Audit and Accountability • Identification and Authentication • System and Communications Protection	**Engineering** • Requirements Development • Requirements Management • Technical Solution • Product Integration • Verification • Validation

FISMA to CMMI Correspondence

HARRIS

FISMA Family	CMMI Family
Management Controls	**Project Management**
• Risk Assessment	• Project Planning
• Planning	• Project Monitoring and Control
• System and Services Acquisition	• Supplier Agreement Management
• Certification & Accreditation (C&A)	• Integrated Project Management
	• Risk Management
	• Quantitative Project Management

Level of detail differs between FISMA and CMMI criteria

- The SSE-CMM was designed to address security specific activities

Engineering
- Administer Security Controls
- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability
- Build Assurance Argument
- Coordinate Security
- Monitor Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security

Project
- Ensure Quality
- Manage Configurations
- Manage Project Risk
- Monitor & Control Technical Effort
- Plan Technical Effort

Organizational
- Define Security Engineering Process
- Improve Security Engineering Process
- Manage Product Line Evolution
- Manage Sys. Engineering Support Env.
- Provide Ongoing Skills & Knowledge
- Coordinate with Suppliers

Mapping Goals, KPAs and FISMA:

HARRIS

FISMA Risk Assessment Control:

Risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

Maps to CMMI KPA

CMMI KPA:
Risk Management

Specific Guidance for Security Engineering

SSE-CMM KPA:

Manage Project Risk (PA 14):

- Develop Risk Management Approach
- Identify Risks
- Assess Risks
- Review Risk Assessment
- Execute Risk Mitigation
- Track Risk Mitigation

Basic Flow

HARRIS

- FISMA families explain what has to be done (tangible product)
- SSE-CMM defines specific process guidance that helps an organization develop the product
- CMMI provides the contextual framework for inclusion of FISMA families in an integrated set of engineering processes

In Summary

- Exact correspondence will vary:
  - Some organizations won't address all goals.
  - Compensating management controls can be traded against technical controls
- Goal is to define repeatable process:
  - Certification and accreditation required every 3 years
  - Ongoing monitoring requirements on an annual basis
  - Simpler to accommodate the requirements within existing processes
  - SSE-CMM and CMMI provide guidance and placeholders that can facilitate compliance

For More Information

- FISMA:
  - www.csrc.nist.gov
- SSE-CMM:
  - www.issea.org
- CMMI:
  - www.sei.cmu.edu