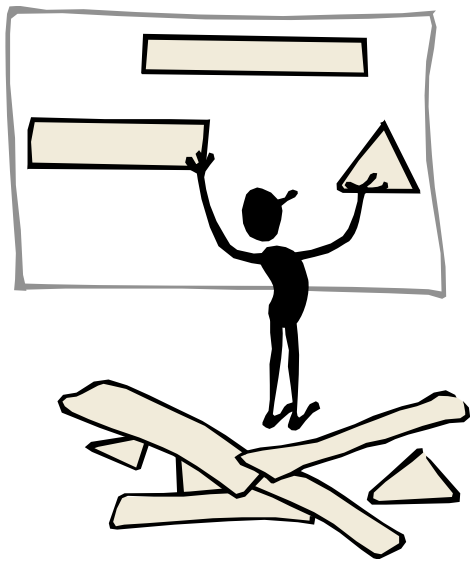
# *Federal Information Security Management Act (FISMA) Operational Controls and Their Relationship to Process Maturity*

Ronda Henning
rhenning@harris.com

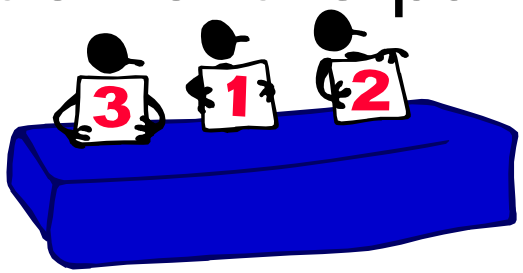
- Proper preparation and planning makes later phases of the System Development Life Cycle easier to conquer.



NOTE: FISMA is used as a representative standard. Insert the security guidance document of your choice in the context of this presentation.

# About FISMA

- The Federal Information System Management Act (FISMA)
- Consists of  17distinct families of security requirements
- Mandates quarterly vulnerability reporting and annual progress reports to GAO
- The framework for how to report is left to the interpretation of the parent agency



# FISMA Control Families

## Management Controls

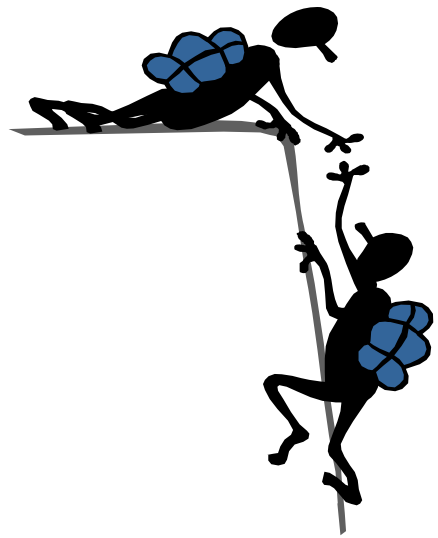
- Risk Assessment
- Planning
- System and Services Acquisition
- Certification & Accreditation (C&A)

## Technical Controls

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

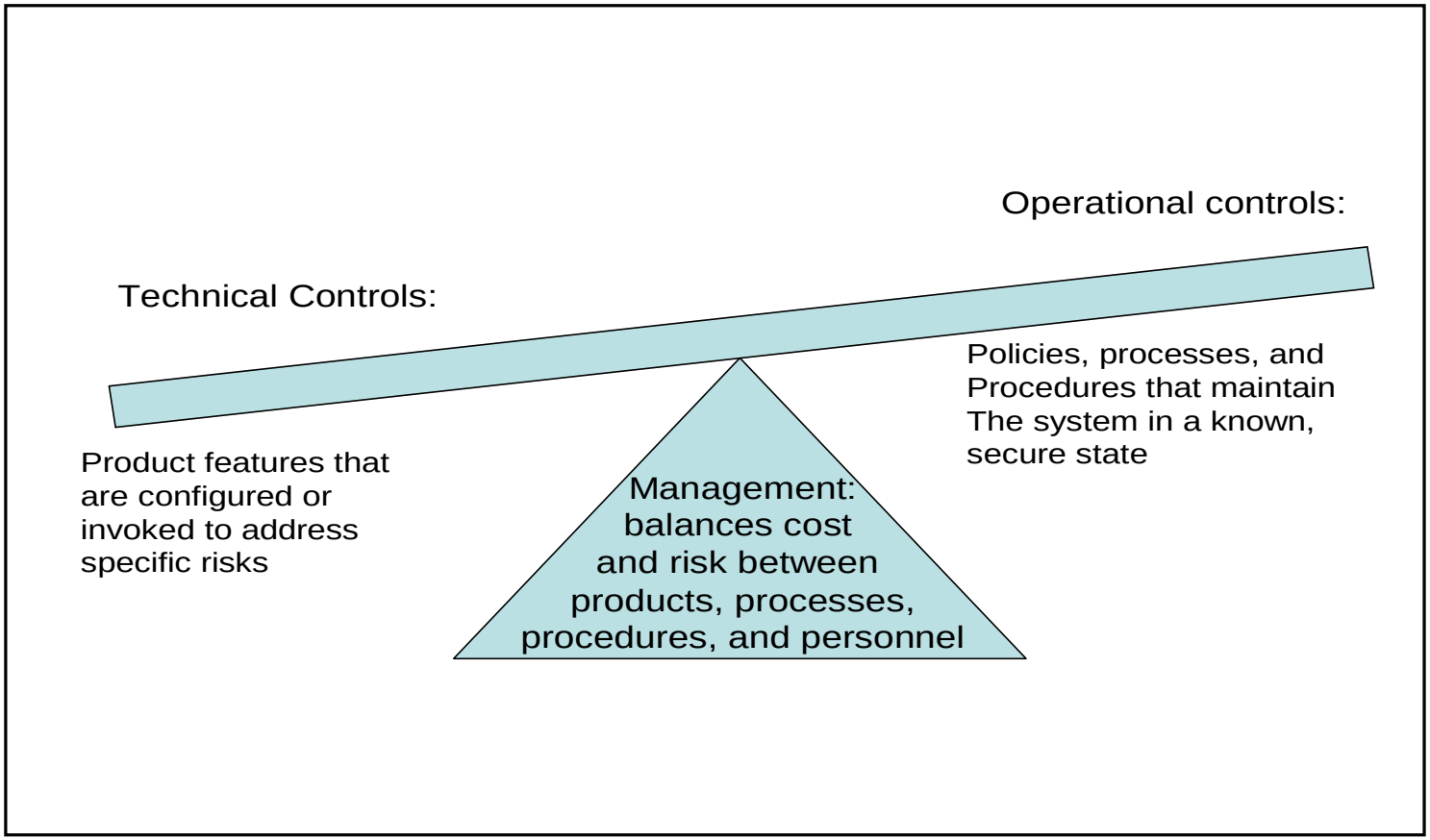
## Operational Controls

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



Controls are Complementary and rely on each other for fulfillment

# Relationship among controls



# Operational Controls

- People Oriented
  - Awareness and Training
  - Personnel Security
- Physically Oriented
  - Environmental Controls
  - Media Protection
  - System Integrity
  - Contingency Planning
- Device Oriented
  - Configuration Management
    - Software
    - Firmware
    - Hardware
  - Maintenance
    - Routine
    - Emergency
  - Incident Response
    - What is an incident?
    - Reactive v. Proactive actions
  - System & Information Integrity
    - Is the data corrupted?
    - Is the system image valid?
    - Are they current/accurate?

- Harder to address later in SDLC
- Frequently neglected in development
- Reason:
  - It's hard enough to get the system integrated and working, planning for later operations is left to the student.
- In reality:
  - Planning ahead is the best way to maintain a proactive assurance posture

# Security Objective of Device Controls

- Define and maintain a known, secure state
  - At delivery and ongoing
- Systems are integrated products
  - Each vendor has their own set of quality and security processes
  - Monthly patches, quarterly patches, emergency patches
  - Options are:
    - Working system with vulnerabilities
    - Semi-functioning system without testing
    - Cross your fingers and hope!
      - Everything works with the patch and no testing
      - Nobody tries to exploit the problems before you fix them

# In the Ideal World

Vendor patch released

- What is affected?
- What is the risk?

Command Assessment

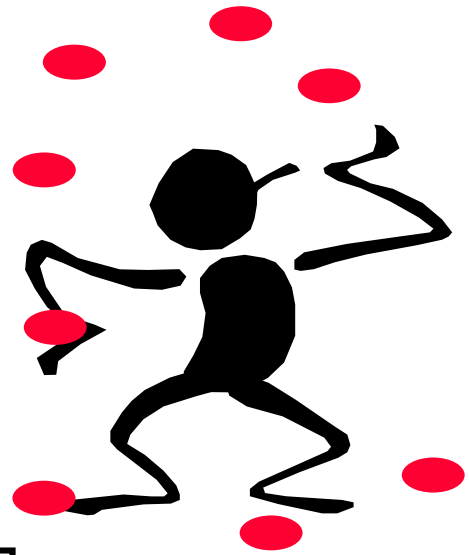
- Add to standard?
- Push changes out

Application Factory Triage

- Regression testing
- Impact assessment

Add to Baseline Configuration

- Update DM
- New standard

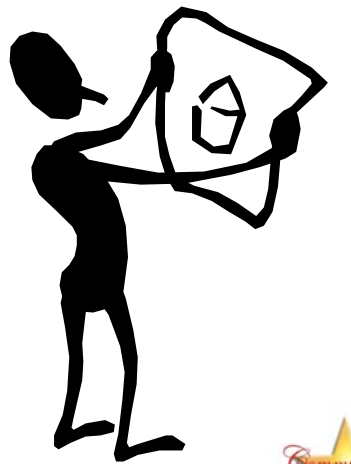


In reality:

N vendors per system
Different release schedules
N software applications
System may have over 100 products.

- CMMI processes already include configuration management and change management
- What they may not include is specific processes associated with security change management
- Risk must be addressed in the process

- System Security Engineering CMM
  - Add security relevant functions to standard CMMI activities
  - Incorporation in an organization's standard process framework is an incremental change
- A Caveat:
  - An incremental change that involves careful component management
  - Accounting at a more granular level
    - All the component software entities
    - Protocols, reference standards, etc.



# Mapping Goals, KPAs and FISMA:

**FISMA Control:**

Specifies what must be managed, what artifacts should be produced for the system. Control defines the compliance baseline.

Maps to CMMI KPA

CMMI KPA:
Basic process guidance & structure

Specific Guidance for Security Engineering

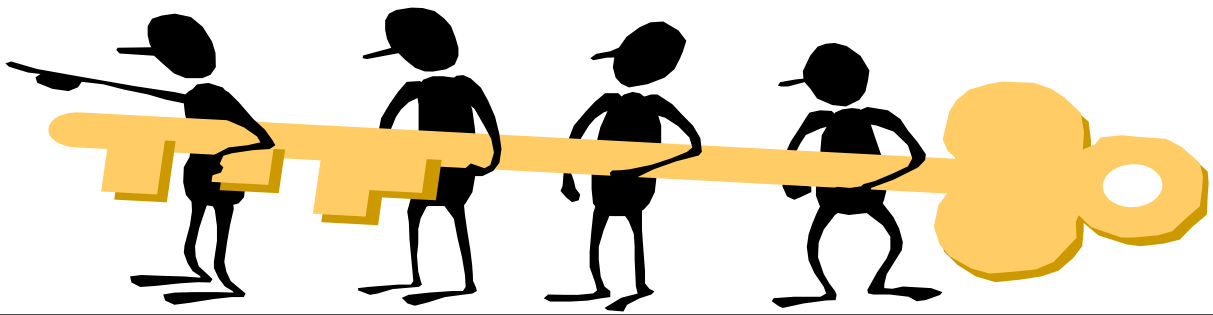
**SSE-CMM KPA:**

- Manage Configuration of Security Components.
- Assess security impact of change?
- Define change management process
- Assess risk associated with change?
- Document risk decisions

- Augmentation to existing process means higher probability of organizational acceptance
- Does not imply use of automated techniques: although they are easier with larger systems and global deployments
- Areas for automation:
  - Asset inventory
  - Baseline configuration tracking
  - Vendor notification and update service
  - Deployment tracking

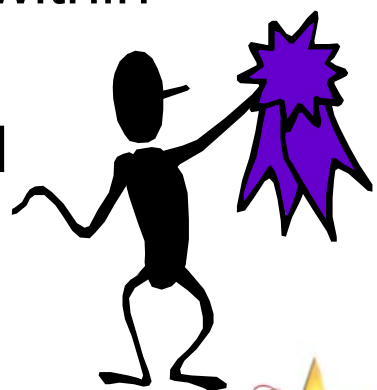
- Starting process management at authority to operate is too late.
- The baseline is established by then.
- May not have been monitored and upgraded throughout development.
  - It's hard to develop code on a moving target
  - Vulnerabilities may be inadvertently used as part of the system feature set
  - Compromises need to be documented

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

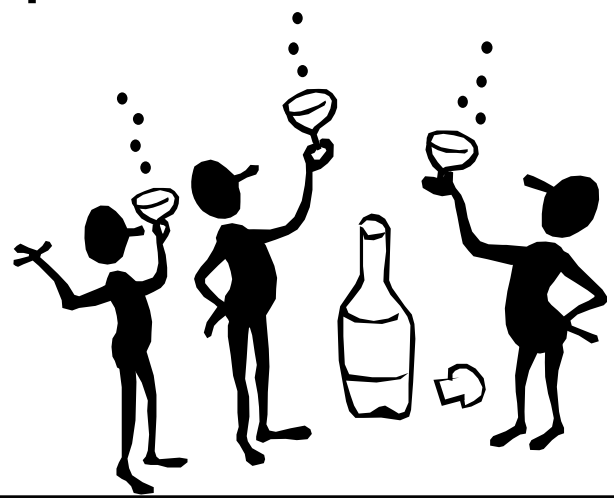


# *In Summary*

- 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



- Starting from a secure foundation is easier than trying to shore up an unsound one.
- Framework for security improvement is already there – but not applied.
- Process maturity dictates that we learn from our experiences and evolve.



# For More Information

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