Federal Risk and Authorization Management Program

An Interagency Program

Pete Tseronis
Cloud Computing Advisory Council, Chair

Katie Lewin
GSA Cloud Computing PMO, Director

Kurt Garbars
GSA Senior Agency Information Security Officer

Peter Mell
NIST FedRAMP Technical Advisor
Cloud Computing Advisory Council, Vice Chair

NIST's Role in FedRAMP

- FedRAMP is a multiagency initiative
  - Conducted under the Federal CIO, the Cloud Computing Advisory Council's security working group, and the Federal Cloud Initiative

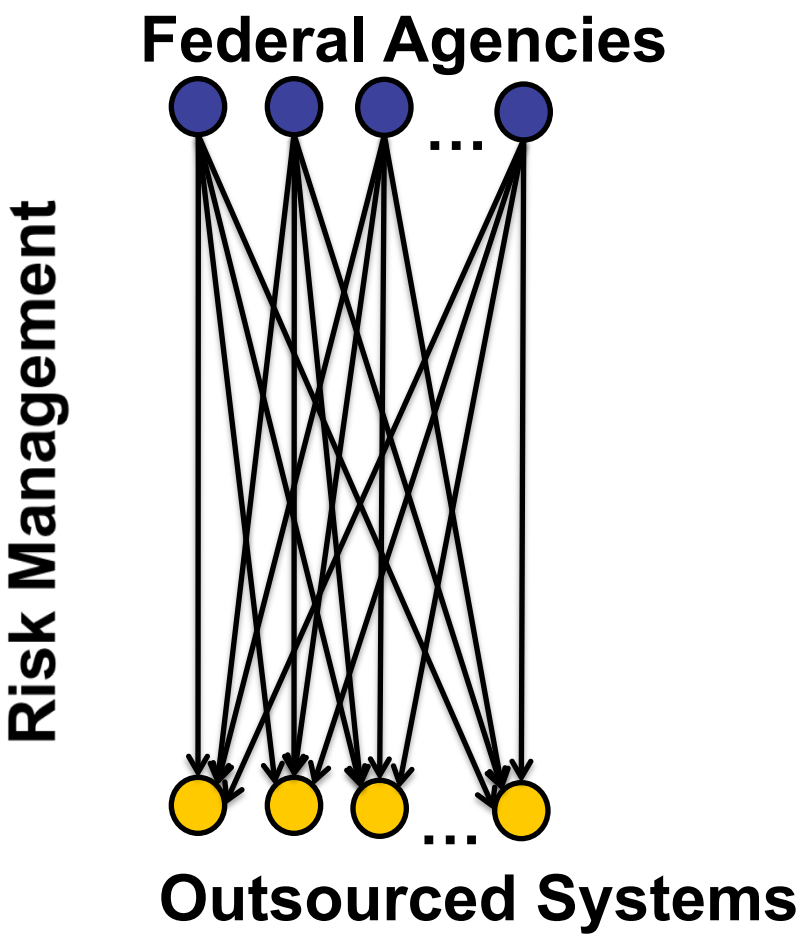
- NIST provides technical advice
- NIST led the definition of the FedRAMP process:
  - Risk management processes
  - Foundational guidance
  - Technical frameworks

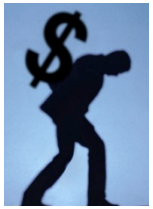
The Problem Statement

Problem: How do we best perform security authorization for large outsourced and multi-agency systems?

- Government is increasing its use of large shared and outsourced systems
  - Technical drivers: the move to cloud computing, virtualization, service orientation, and web 2.0
  - Cost savings: through datacenter and application consolidation
- Independent agency risk management of shared systems can create inefficiencies

The Problem: Independent Agency Risk Management of Shared Systems





: Duplicative risk management efforts

: Incompatible requirements

: Acquisition slowed by lengthy compliance processes

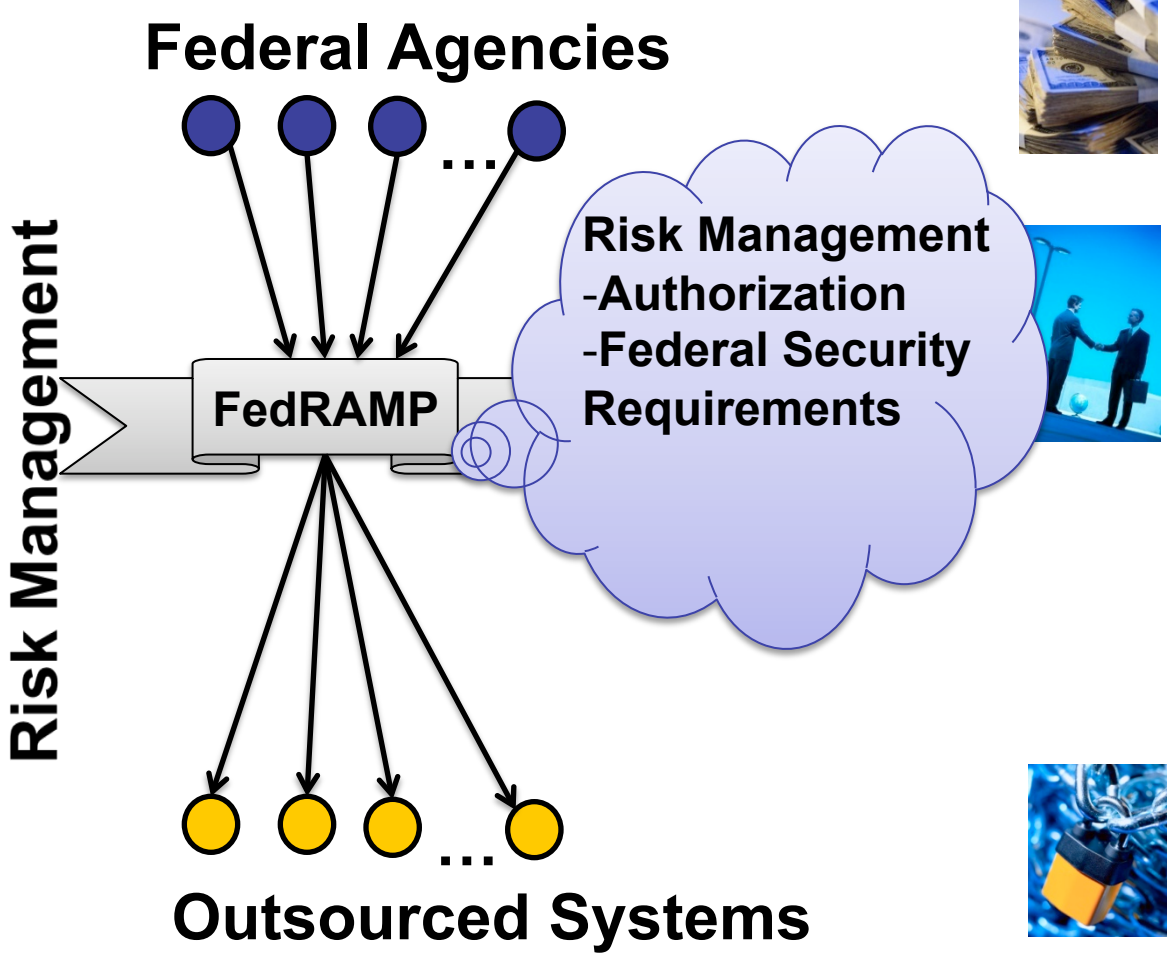
: Potential for inconsistent application of Federal security requirements

The Solution Concept: FedRAMP

Federal Risk and Authorization Management Program

- A government-wide initiative to provide joint authorization services
  - Unified government-wide risk management
  - Agencies would leverage FedRAMP authorizations (when applicable)
- Agencies **retain their responsibility and authority** to ensure use of systems that meet their security needs
- FedRAMP would provide an optional service to agencies

The Solution: Government-wide Risk Management of Shared Systems



: Risk management cost savings and increased effectiveness

: Interagency vetted approach

: Rapid acquisition through consolidated risk management

: Consistent application of Federal security requirements

FedRAMP: Federal Risk and Authorization Management Program

Agency Perspective

Independent Agency Effort

Security Control Selection
Security Implementation
Security Assessment
Authorization
Plan of Action and Milestones
Monitoring

Leveraged Authorization

Review security details
Leverage the existing authorization
Secure agency usage of system

Assurance strengthened through focused effort

: Slower acquisition

: Significant effort

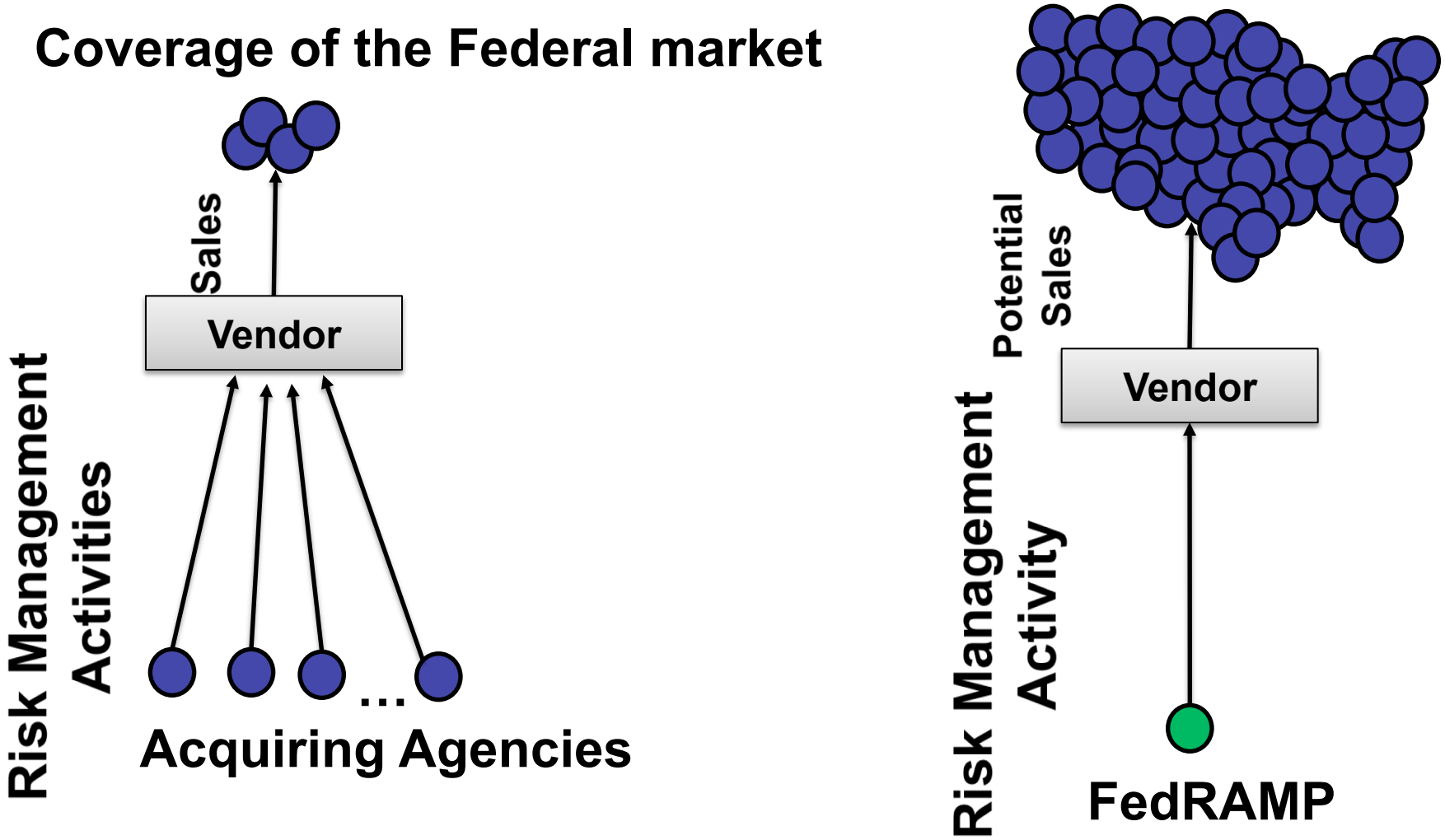
: Enables rapid acquisition

: Reduced effort

Agency Responsibilities

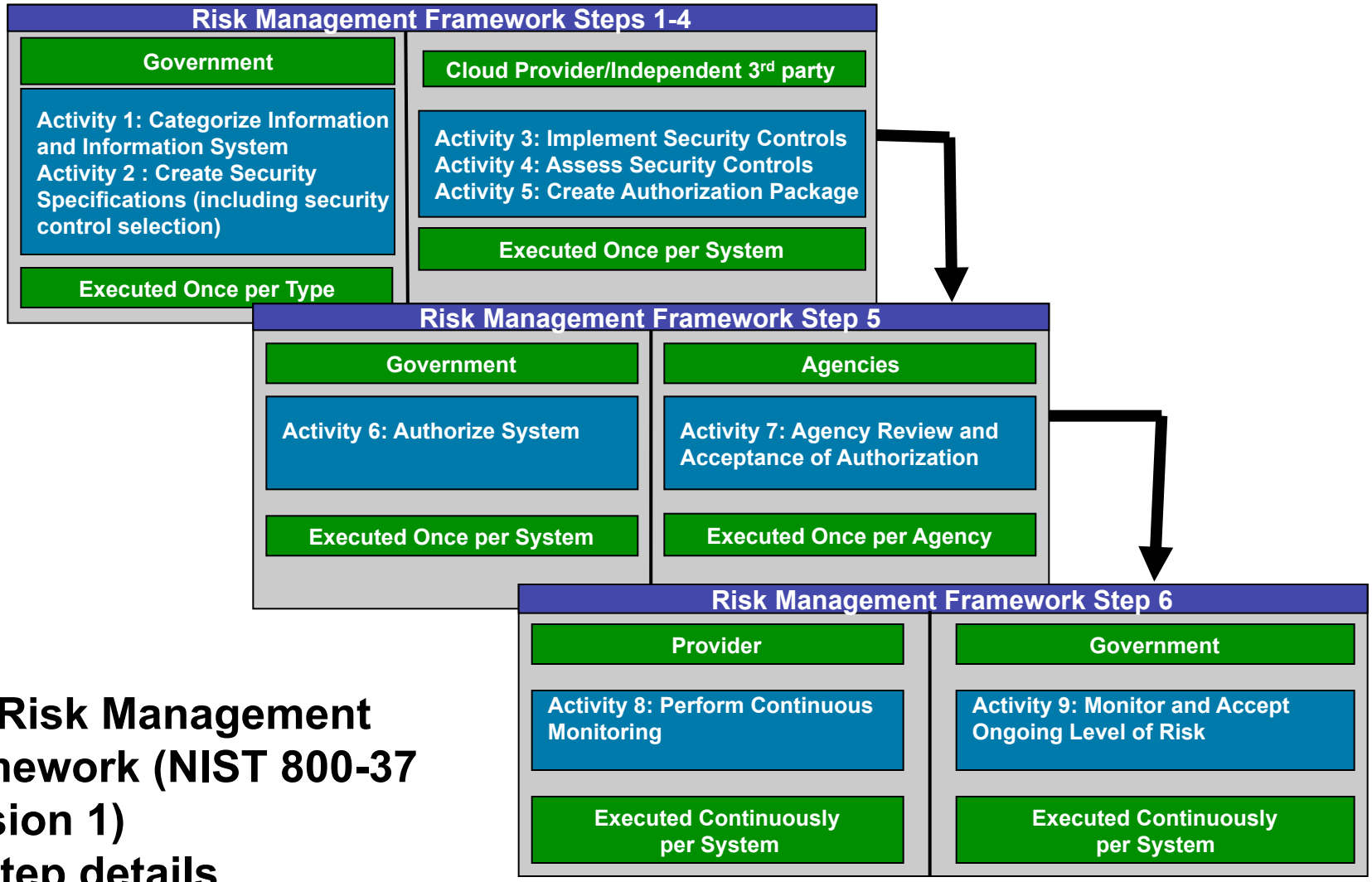
- Review FedRAMP authorization packages prior to making a decision to accept the risk
  - Determine suitability to agencies mission/risk posture
  - Determine if additional security work is needed
- Perform agency specific security activities
  - FedRAMP will publish a list of security controls that are the responsibility of the agency (can't be done government-wide)
  - Need for agency system security plans

Vendor Perspective



- Products publicly listed as FedRAMP authorized

Overview of FedRAMP Government-Wide Risk Management Process



See Risk Management Framework (NIST 800-37 revision 1) for step details

Expected FedRAMP Benefits: Security and Privacy Perspective

- **increases security** through focused risk management
- **reduces duplication** of effort
- **ensures security oversight** of outsourced systems
- provides **independent accountability** for government-developed systems used by multiple agencies
- ensures **integration with government-wide security** efforts

Expected FedRAMP Benefits: CIO Perspective

- **reduces costs** by eliminating duplication of effort
- **enables rapid acquisition** by leveraging pre-authorized solutions
- **provides transparency** through agency vetted security requirements and authorization packages
- **ameliorate technical hurdles** with multi-agency assessment and authorization of shared systems

Questions?

Presenter Name:

Peter Mell

NIST FedRAMP Technical Representative

Cloud Computing Advisory Council, Vice Chair

The NIST Cloud Definition

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- The full extended definition is available at:

http://csrc.nist.gov/groups/SNS/cloud-computing

The NIST Cloud Definition Framework