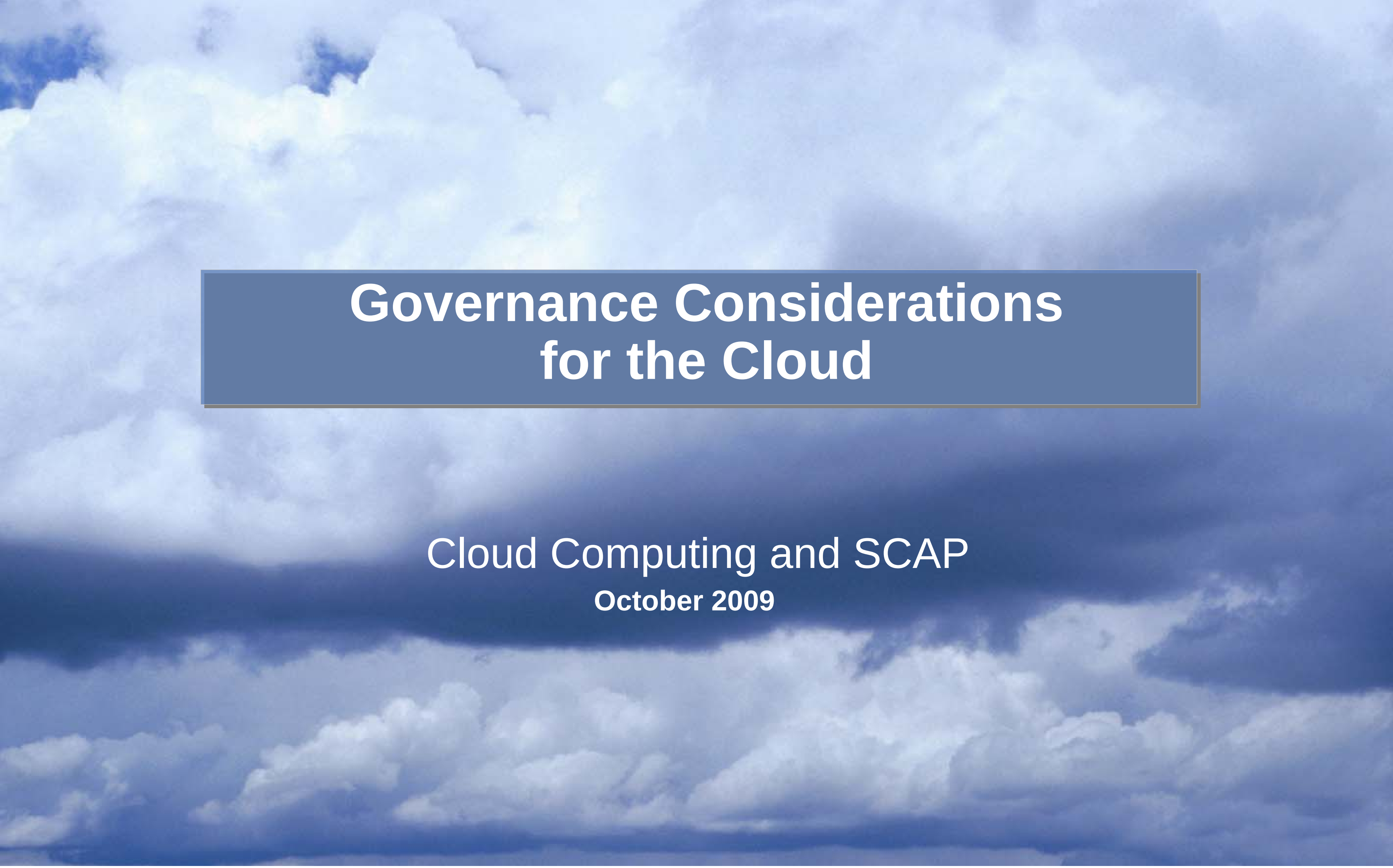


Governance Considerations for the Cloud

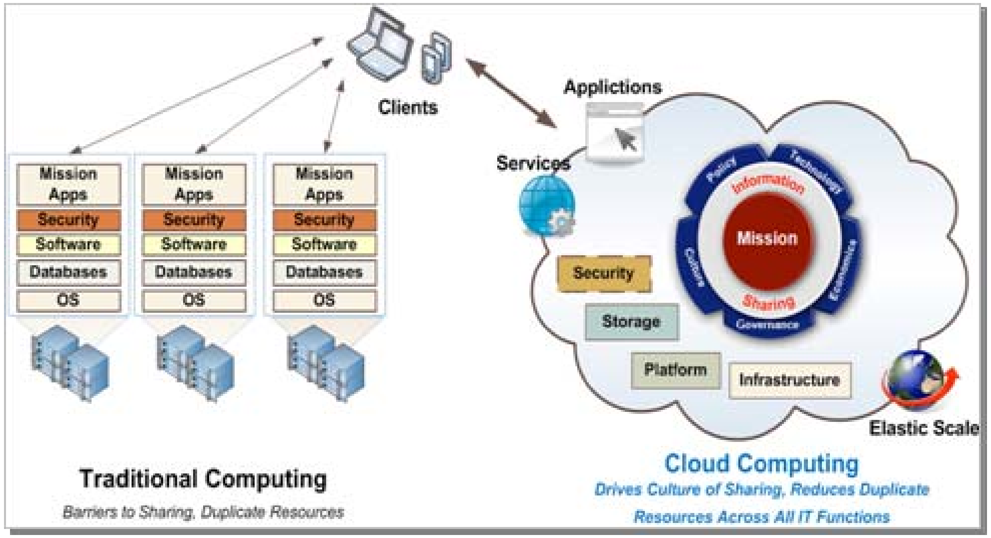
Cloud Computing and SCAP

October 2009

Booz | Allen | Hamilton

What is Cloud Computing?

Cloud Computing 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.**

5 Key Characteristics

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Rapid elasticity
- Pay per use

3 Delivery Models (What's being offered)

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

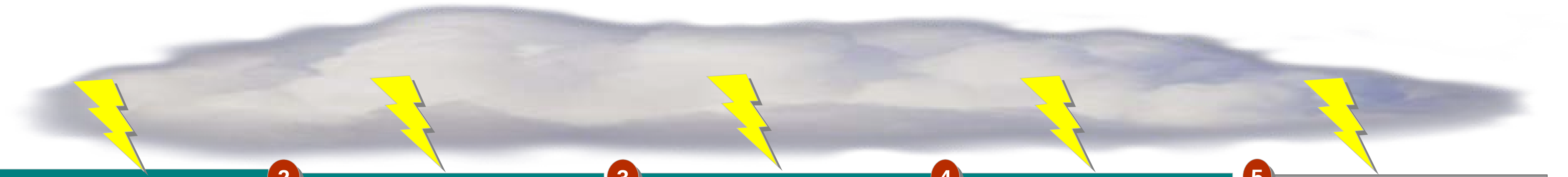
4 Deployment Models (How is it being offered)

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

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

There are specific security challenges that organizations face when moving to a Cloud

Cloud Security Major Challenges



1 Data Protection

- Where do data physically reside, and does data's location have legal ramifications?
- Are data safely protected while stationary or in motion within and across a Cloud?
- How is availability of data assured in the Cloud?

2 Security Control

- What security controls need to be implemented by a Cloud provider and how are they implemented?
- How are assurance levels effectively and efficiently managed and assessed in Cloud?

3 Compliance

- Is my Cloud complying with the necessary guidance?
- Can the Cloud provider substantiate claims that security controls are implemented sufficiently?

4 Multi-Tenancy

- Are my assets vulnerable if another customer is exploited by an attack?
- How does the cloud provider keep different customers' data separated and inaccessible by other customers?

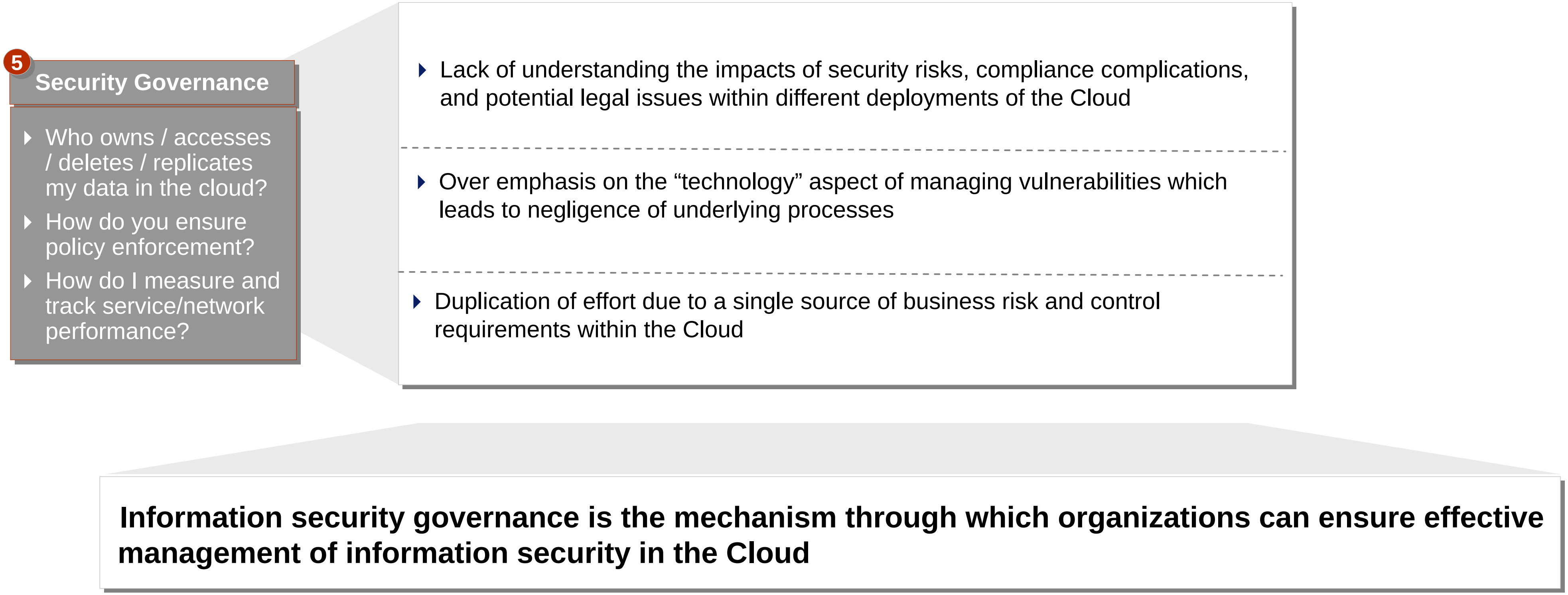
5 Security Governance

- Who owns / accesses / deletes / replicates my data in the cloud?
- How do you ensure policy enforcement?
- How do I measure and track service/network performance?

To Resolve These Issues, Clients Must First Focus On Addressing Underlying Strategic Considerations. These questions identify the key fundamental issues that agencies (working with cloud providers) must address in order to resolve the overall security hurdles. In some cases, these strategic considerations represent the root cause of each challenge

However, one of the key challenges that is not always addressed is governance

Key Questions and Challenges



5 **Security Governance**

- Who owns / accesses / deletes / replicates my data in the cloud?
- How do you ensure policy enforcement?
- How do I measure and track service/network performance?

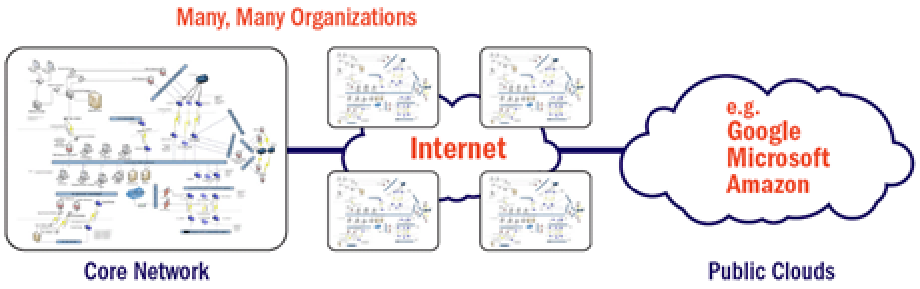
- Lack of understanding the impacts of security risks, compliance complications, and potential legal issues within different deployments of the Cloud
- Over emphasis on the “technology” aspect of managing vulnerabilities which leads to negligence of underlying processes
- Duplication of effort due to a single source of business risk and control requirements within the Cloud

Information security governance is the mechanism through which organizations can ensure effective management of information security in the Cloud

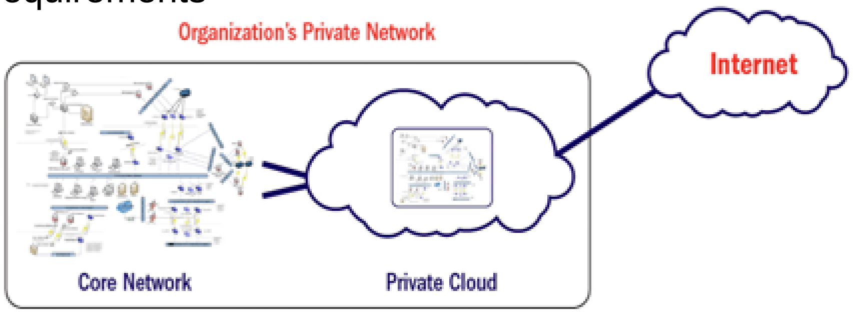
To address governance, the level of risk and complexity of each cloud deployment must be taken into consideration

Cloud Deployment Models

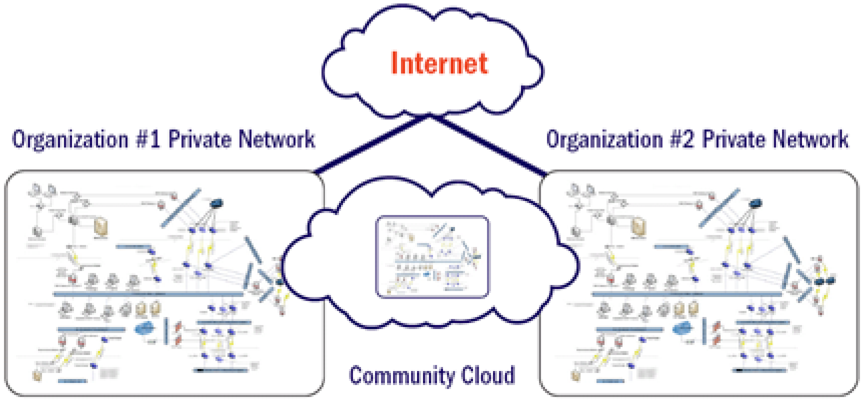
- **PUBLIC CLOUD:** <u>Highest risk</u> due to lack of security control, multi-tenancy, data management, limited SLA and lack of common regulatory controls



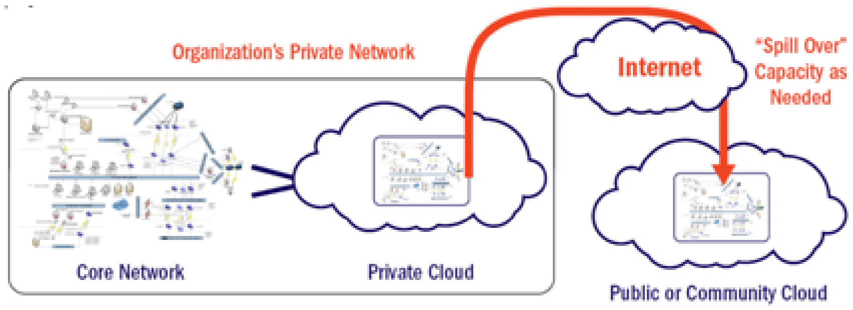
- **PRIVATE CLOUD:** <u>Least risk</u> due to single ownership and strong shared mission goals and legal/regulatory requirements



- **COMMUNITY CLOUD:** <u>Moderate risk</u> due to multi-tenancy, however less risk than public cloud due to shared legal/regulatory compliance issues


Internet
Organization #1 Private Network
Organization #2 Private Network
Community Cloud

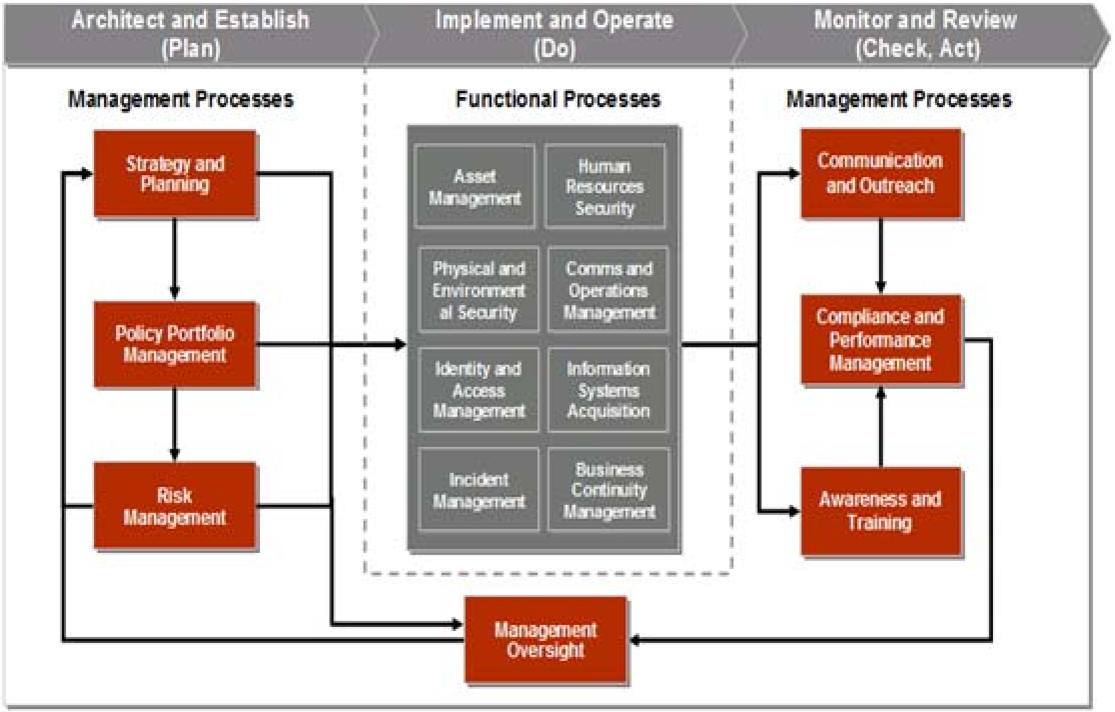
- **HYBRID CLOUD:** <u>Risk dependent upon combined models</u>. Combination of private/community is lowest risk, while combination of public is greatest risk


Organization's Private Network
Internet
"Spill Over" Capacity as Needed
Core Network
Private Cloud
Public or Community Cloud

Here is an example of an Information Security Governance Framework that can be applied to govern the Cloud

Information Security Governance Framework

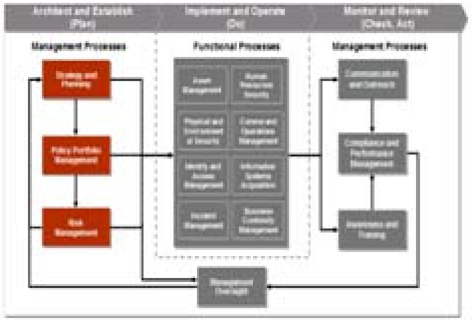
- This information security governance framework follows the standard quality management (or Plan, Do, Check, Act) cycle of continuous improvement and is comprised of seven management processes
- Four outcomes of implementing an effective security governance framework:
  - Strategic Alignment
  - Value Delivery
  - Risk Management
  - Performance Measurement
- The management processes govern the implementation and operation of the functional processes, which vary based on the Cloud environment
- The three phases to implement this security governance framework are:
  - Architect and Establish (Plan)
  - Implement and Operate (Do)
  - Monitor and Review (Check, Act)



Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Functional Processes
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Communication and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Booz | Allen | Hamilton

The Architect and Establish phase is necessary to establish strategy, policy, and risk management of the Cloud

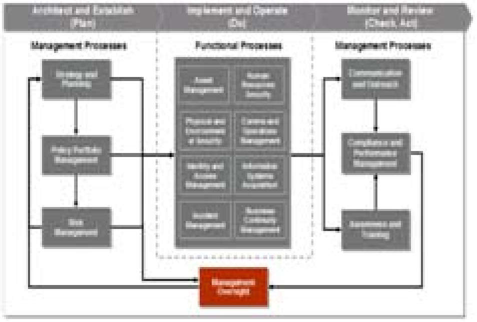

Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Functional Processes
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Management Processes
Communication and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Architect and Establish Phase

- **Strategy & Planning:**
  - Establish information security program direction and guide activities
  - Ensure alignment of the information security program with mission goals and objectives
  - Define the information security program vision, goals, requirements, and scope
- **Policy Portfolio Management:**
  - Define and communicate management expectations of information security
  - Translate goals and requirements into actionable mandates
  - Establish clearly defined roles and responsibilities for information security
  - Facilitate efficient and consistent implementations with supporting standards, guidelines, and procedures
- **Risk Management:**
  - Enable information asset-based protection and mitigation planning
  - Enhance the organization’s ability to select and apply protection based on the specific risks and threats affecting an asset
  - Ensure consistent information security risk assessment methodologies
  - Enable better optimization of security expenditures, resources, and activities
  - Inform security priorities and planning
  - Provide basis for measuring information security program efficiency and effectiveness

The Architect and Establish phase is critical to developing a Cloud vision, strategy and deployment plan that is effective to the organization’s goals and objectives

The Implement and Operate phase is focused on the oversight management of security operations of the Cloud

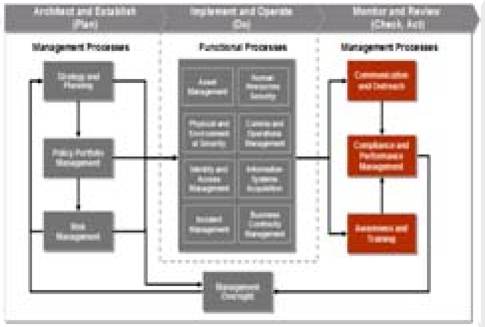

Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Functional Processes
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Asset Management
Human Resources Security
Physical and Environmental Security
Comms and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Communication and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Implement and Operate Phase

- **Management Oversight**:
  - Ensure ongoing management involvement in program direction and priorities
  - Establish enterprise information security governance
  - Ensure the information security program supports mission goals and objectives
  - Reinforce the importance of information security throughout the organization
  - Oversee risk management to balance mission goals and information security costs
  - Track and optimize information security resource allocation
  - Authorize improvements to the information security program on a continuing basis
- **Functional Processes:**
  - *Outside the scope of the information security governance framework*
  - The implementation and operation of information security controls is contained in each of these functional processes area will vary with the deployment and service model of the Cloud

The Implement and Operate phase is largely dependent upon the Cloud and type of deployment model. SLAs and MOUs provide more flexibility to the end user for the management oversight

The Monitor and Review phase is focused on communications, awareness & training, and compliance for the Cloud



Architect and Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check, Act)
Management Processes
Functional Processes
Management Processes
Strategy and Planning
Policy Portfolio Management
Risk Management
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Identity and Access Management
Information Systems Acquisition
Incident Management
Business Continuity Management
Communication and Outreach
Compliance and Performance Management
Awareness and Training
Management Oversight

Monitor and Review Phase

- **Communications and Outreach:**
  - Consistently communicate the importance of the information security throughout the organization
  - Clarify roles and responsibilities
  - Drive the ongoing competency of information security staff
- **Awareness and Training***:*
  - Educate staff on required actions related to changes in regulatory, legislative, and other mandates
  - Broaden and deepen the security awareness of the organization
  - Enhance compliance through better understanding and knowledge
- **Compliance and Performance Management:**
  - Create regular measurement and reporting of progress and issues
  - Inform and prioritize program improvements
  - Record progress toward achieving strategic goals and compliance with requirements
  - Drive continuous improvement of the information security program
  - Minimize potential for recurrence of systemic issues
  - Optimize consistency and efficiency of security implementations
  - Inform modifications to risk analyses and risk mitigations

Compliance checking can be automated through the use of tools, such as the SCAP validation program sponsored through NIST

SCAP scanning is a tool that can help determine compliance of security requirements implemented in Cloud provider OS images

SCAP Scanning Tool

- OS images obtained from Cloud providers may introduce risks to Cloud users and their organizations
- For example, risks were identified at the BlackHat and DefCon2009 that
  - Clouds could be "pre-owned virtual machines" where OS images are uploaded with built in trojan horses, and
  - The use of cloud services could be turned into botnet-in-a-box or spam servers
- The SCAP Validation Program enables consumers and providers to gain confidence in the level of SCAP functionality implemented in computing infrastructure
- In the case of a Cloud, SCAP validated scanners provide consumers with the ability to check the security policy compliance and vulnerabilities of the Cloud provider’s OS images and measure the deviation from required settings
- Additionally, consumers of the Cloud are able to obtain measurable data that maps to high level requirements (e.g., NIST SP 800-53) and develop their own customizable metrics from security configuration parameters of a hardened OS or common vulnerability language outputs

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-117 (Draft)

Guide to Adopting and Using the Security Content Automation Protocol (SCAP) (Draft)

Recommendations of the National Institute of Standards and Technology

Matthew Barrett
Chris Johnson
Peter Mell
Stephen Quinn
Karen Scarfone

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126 (Draft)

The Technical Specification for the Security Content Automation Protocol (SCAP)

Recommendations of the National Institute of Standards and Technology

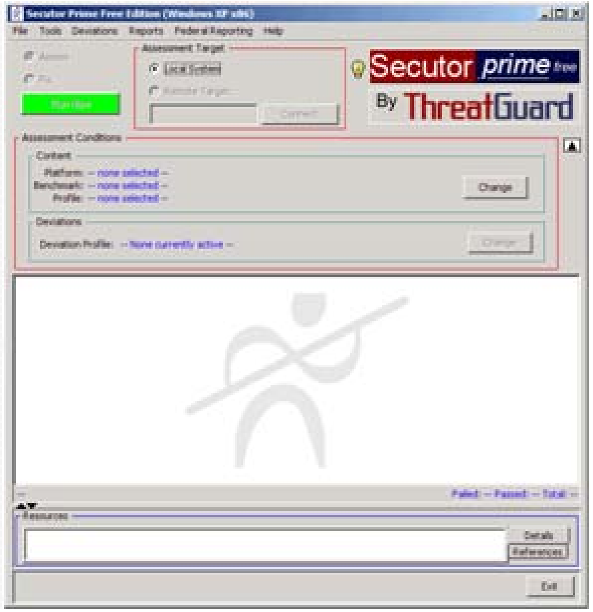
Christopher Johnson
Stephen Quinn
Karen Scarfone
David Waltermire

DRAFT

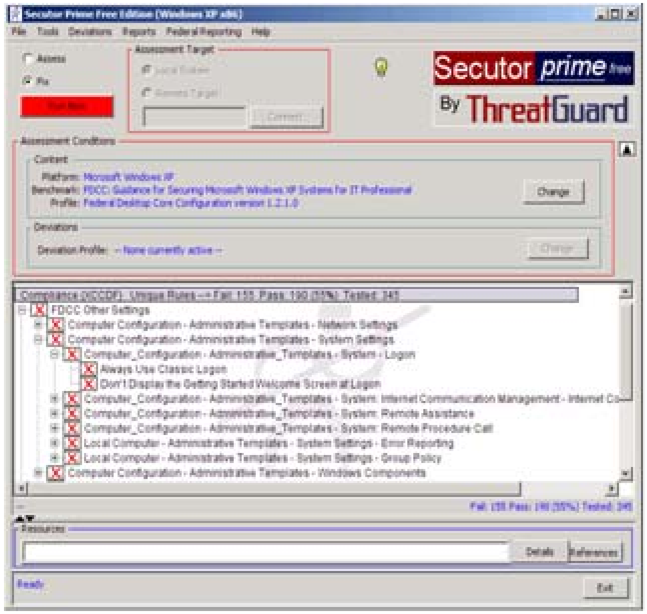
As a demonstration, let’s use a SCAP-validated scanner to check security compliance of a Cloud provider’s OS image

SCAP Scanning Tool Demo

- The objective is to run the SCAP-validated scanner against the provider’s OS images and determine the compliance of configuration settings, which in this demonstration pertains to the Federal Desktop Core Configuration (FDDC)
- The Cloud is a public cloud offering an Infrastructure as a Service (IaaS)
- The SCAP-validated scanner is free for use:
  - SCAP Secutor Prime found here at: http://www.threatguard.com/downloads.htm



Platform: -- none selected --
Benchmark: -- none selected --
Profile: -- none selected --
Deviation Profile: -- None currently active --



Platform: Microsoft Windows XP
Benchmark: FDCC: Guidance for Securing Microsoft Windows XP Systems for IT Professional
Profile: Federal Desktop Core Configuration version 1.2.1.0
Deviation Profile: -- None currently active --

Compliance (XCCDF) Unique Rules --> Fail: 155 Pass: 190 (55%) Tested: 345

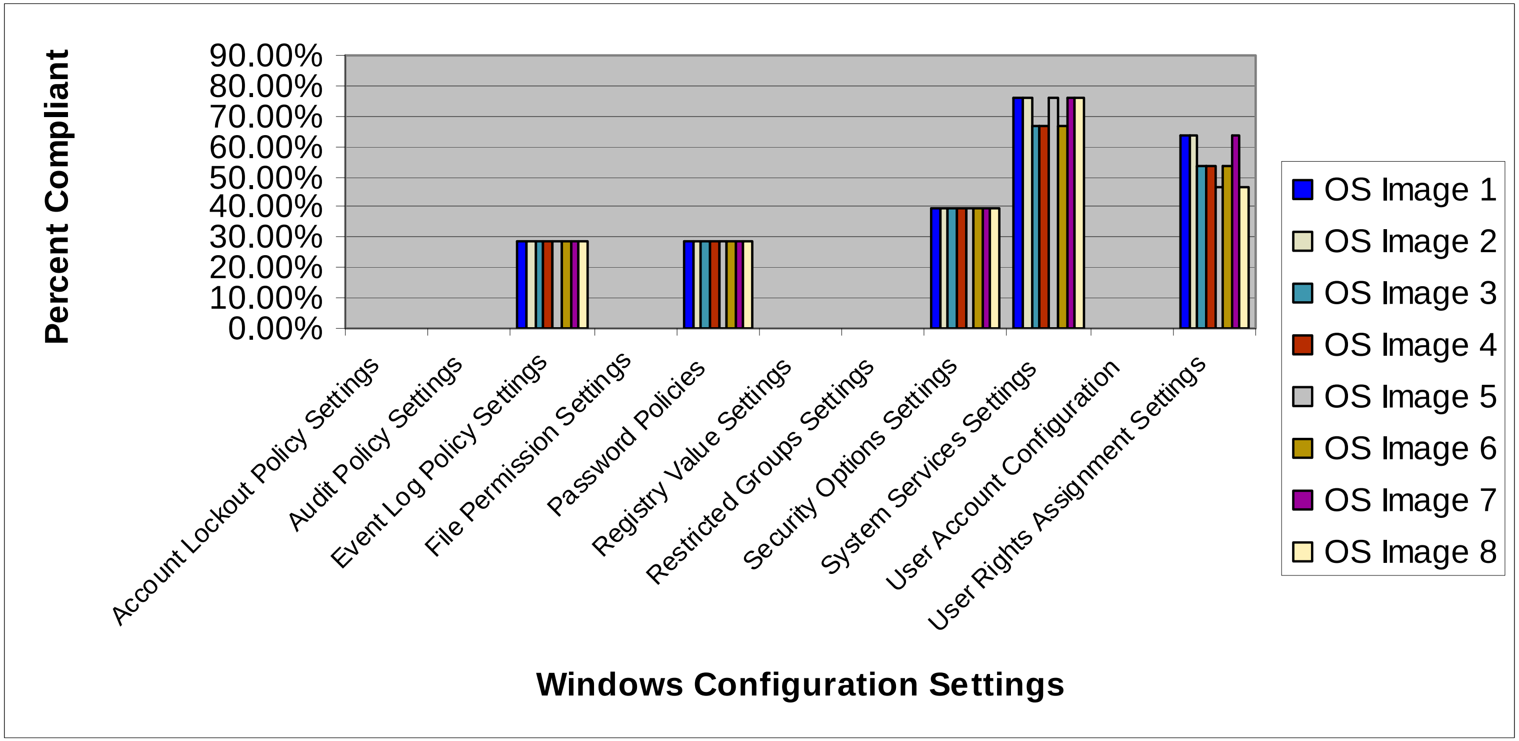
```
☒ FDCC Other Settings
  ☒ Computer Configuration - Administrative Templates - Network Settings
  ☒ Computer Configuration - Administrative Templates - System Settings
    ☒ Computer_Configuration - Administrative_Templates - System - Logon
      ☒ Always Use Classic Logon
      ☒ Don't Display the Getting Started Welcome Screen at Logon
    ☒ Computer_Configuration - Administrative_Templates - System: Internet Communication Management - Internet Co
    ☒ Computer_Configuration - Administrative_Templates - System: Remote Assistance
    ☒ Computer_Configuration - Administrative_Templates - System: Remote Procedure Call
    ☒ Local Computer - Administrative Templates - System Settings - Error Reporting
    ☒ Local Computer - Administrative Templates - System Settings - Group Policy
  ☒ Computer Configuration - Administrative Templates - Windows Components
```

Fail: 155 Pass: 190 (55%) Tested: 345

SCAP provides end users with the ability to see how secure configuration settings are on OS images provided

SCAP Scanning Tool Results

- 8 OS images were scanned from one public cloud provider to determine the compliance of security configuration settings
- On average, there was a consistent ~95% for patching compliance and ~30% windows settings configured correctly
- A breakdown of the windows configuration settings across all images is provided below:



- Results show that images created by another end user and released into a public cloud are not securely configured and could potentially contain malicious software

This identifies a mutual obligation between providers and end users to ensure compliance is in place within the Cloud

SCAP Tool Benefits

- Providers have an obligation to ensure compliance in their Clouds
  - Pertaining to our SCAP demonstration, virtual machine images must be updated regularly to maintain compliance
- End users need to be cognizant that compliance ‘as stated’ may not always be the case at ‘all times’ and that some responsibility falls under the due diligence to ensure compliance is maintained
  - To this effect, Agencies should verify configuration settings of procured OS settings
  - When possible, it is recommended that Agencies create their own image and upload for use
  - In addition, tools such as SCAP can be used to minimize the risk of vulnerabilities on purchased products in the Cloud and ensure procured OS images are configured securely for use
- Looking forward:
  - Agencies could see IAVAs applied in operating environments upon notification and have that compliance status reported
  - Cloud providers could offer an SCAP-based scanning service to consumers to validate compliance of VMIs procured by the Agency's staff

Do you have questions?

Additional Information/Resources

- For more detailed information, please contact:

Ron Ritchey, PhD
Principal

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
8283 Greensboro Drive
McLean, VA 22102, USA
Tel (703) 337- 6704
Ritchey_Ronald@bah.com