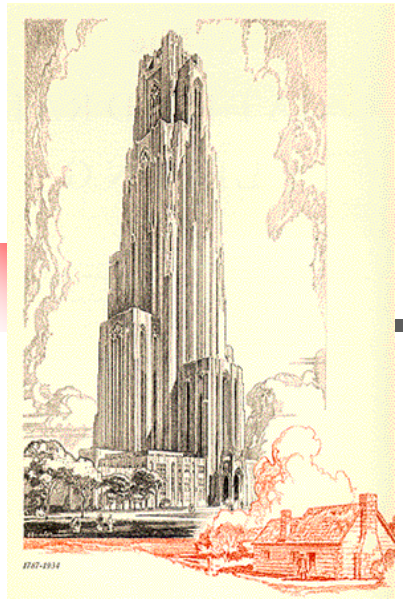
TEL2813/IS2621
Security Management

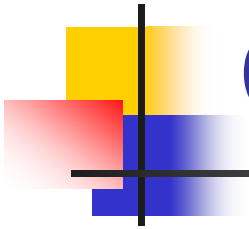


James Joshi
Associate Professor

Lecture 6

Feb 26, 2015

Cloud Computing – Security and Privacy Issues

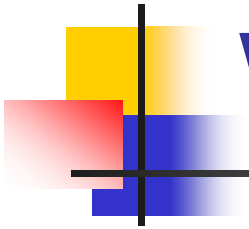


Objectives

- To understand Cloud Computing Issues
  - Foundational Elements of Cloud Computing
  - Security & Privacy
  - Cloud Migration Paths
  - Risks in Cloud

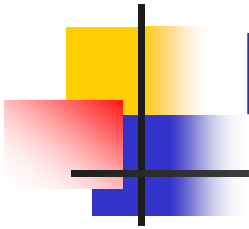
Acknowledgement:

- H. Takabi, J. Joshi, G-J Ahn, "Security and Privacy Challenges in Cloud Computing Environments" IEEE Security and Privacy, 2010
- NIST 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"
- Vivek Kundra, "Federal Cloud Computing Strategy," 2011
- Ernst&Young Report:"Cloud Computing Issues and Impacts"
- COSO report, "Enterprise Risk Management for Cloud Computing," 2012
- Peter Mell's NIST presentation: Effectively and Securely Using the Cloud Computing Paradigm



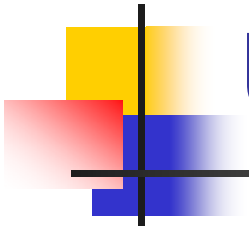
What is Cloud Computing

- NIST 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.
- Has
  - 5 Key characteristics
  - 3 service models
  - 4 deployment models



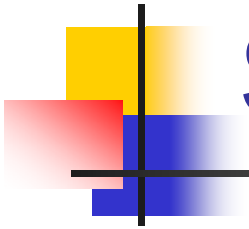
Key Characteristics

- On-demand self-service
  - Get computing capabilities as needed automatically
- Broad network access
  - Services availability over the net using desktop, laptop, PDA, mobile phone
- Resource pooling
  - Location independence
  - Resource pooling at provider resources to serve multiple clients
- Rapid elasticity
  - Ability to quickly add or remove services
- Measured service
  - Control, optimize services based on metering/measurements/metric



Unique Features

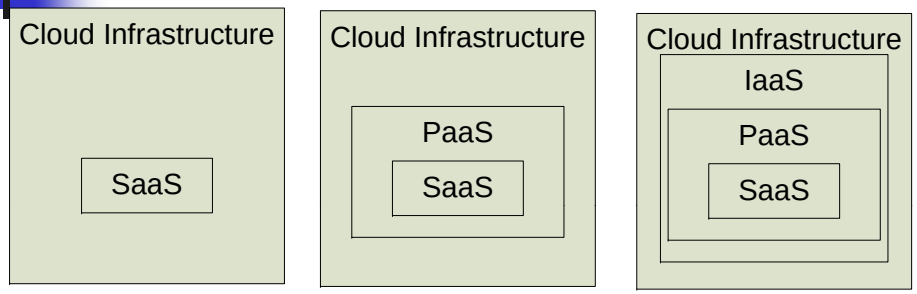
- Outsourcing Data and Applications
- Extensibility and Shared Responsibility
- Multi-tenancy
- Service-Level Agreements
- Virtualization and Hypervisors
- Heterogeneity
- Compliance and Regulations



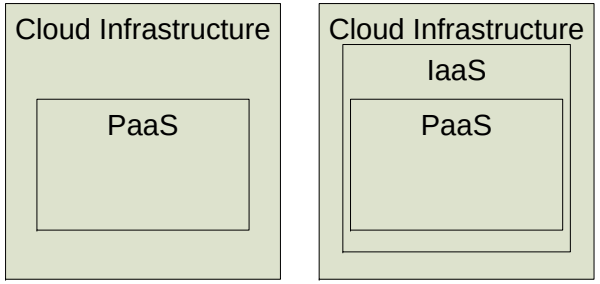
Service Models

- Cloud Software as a Service (SaaS)
  - Providers provide software applications over networks
  - Client doesn't manage or control the network, servers, OS, storage or applications
- Cloud Platform as a Service (PaaS)
  - Users deploy their own applications on a cloud
  - Users control their software/applications
  - Users don't manage servers, storage, etc.
- Cloud Infrastructure as a Service (IaaS)
  - Provider provides processing, storage, network, and other key computing resources
  - Clients get access to the infrastructure to deploy their platform/software
  - Client do not manage or control the infrastructure but do manage or control the OS, storage, apps, selected network components

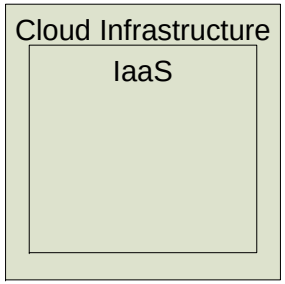
Service Model Architectures



Software as a Service (SaaS) Architectures

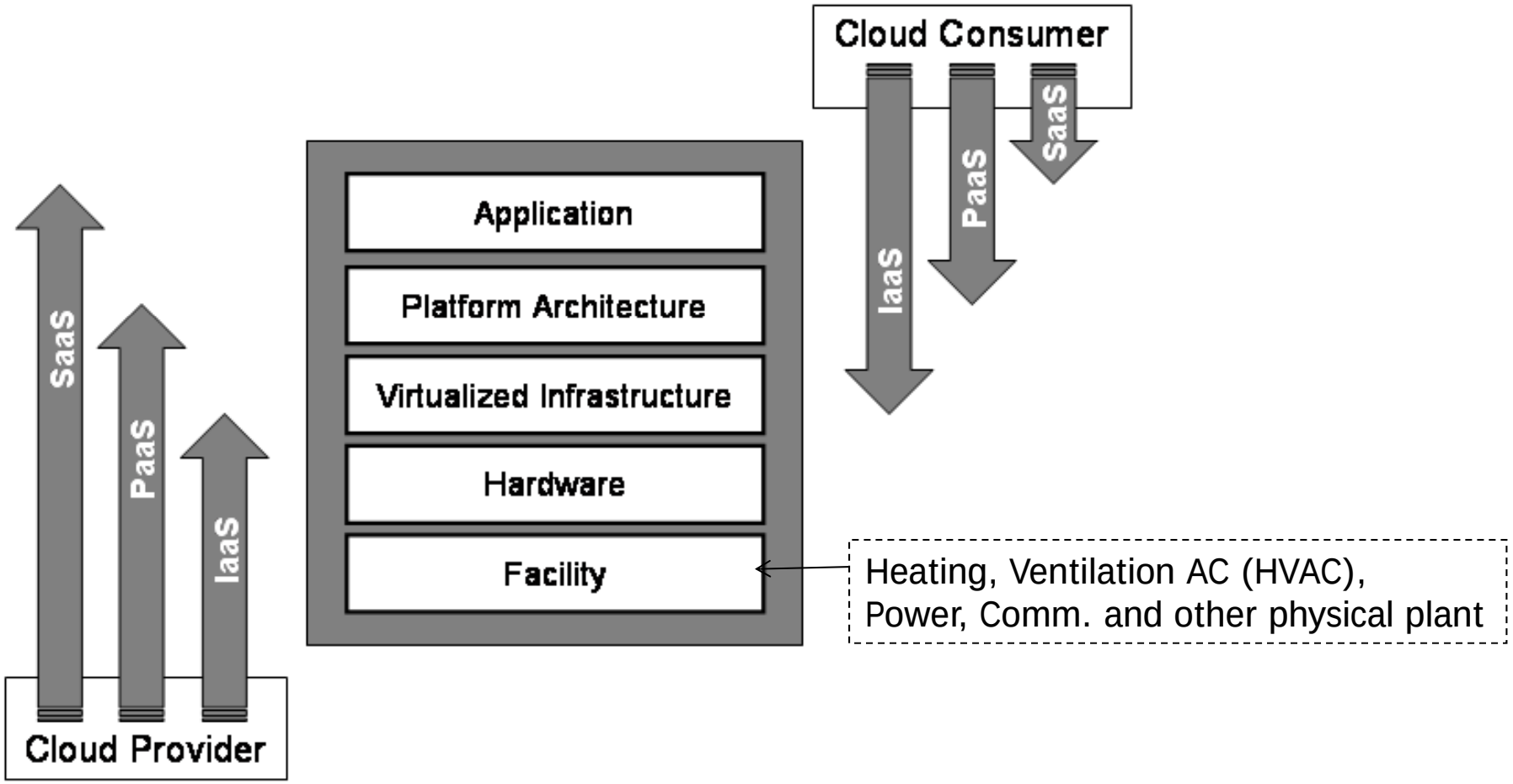


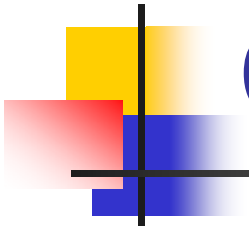
Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

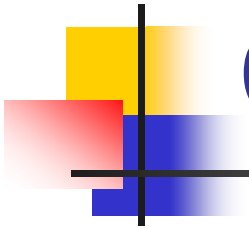
Scope and Control - differences





Cloud Deployment Models

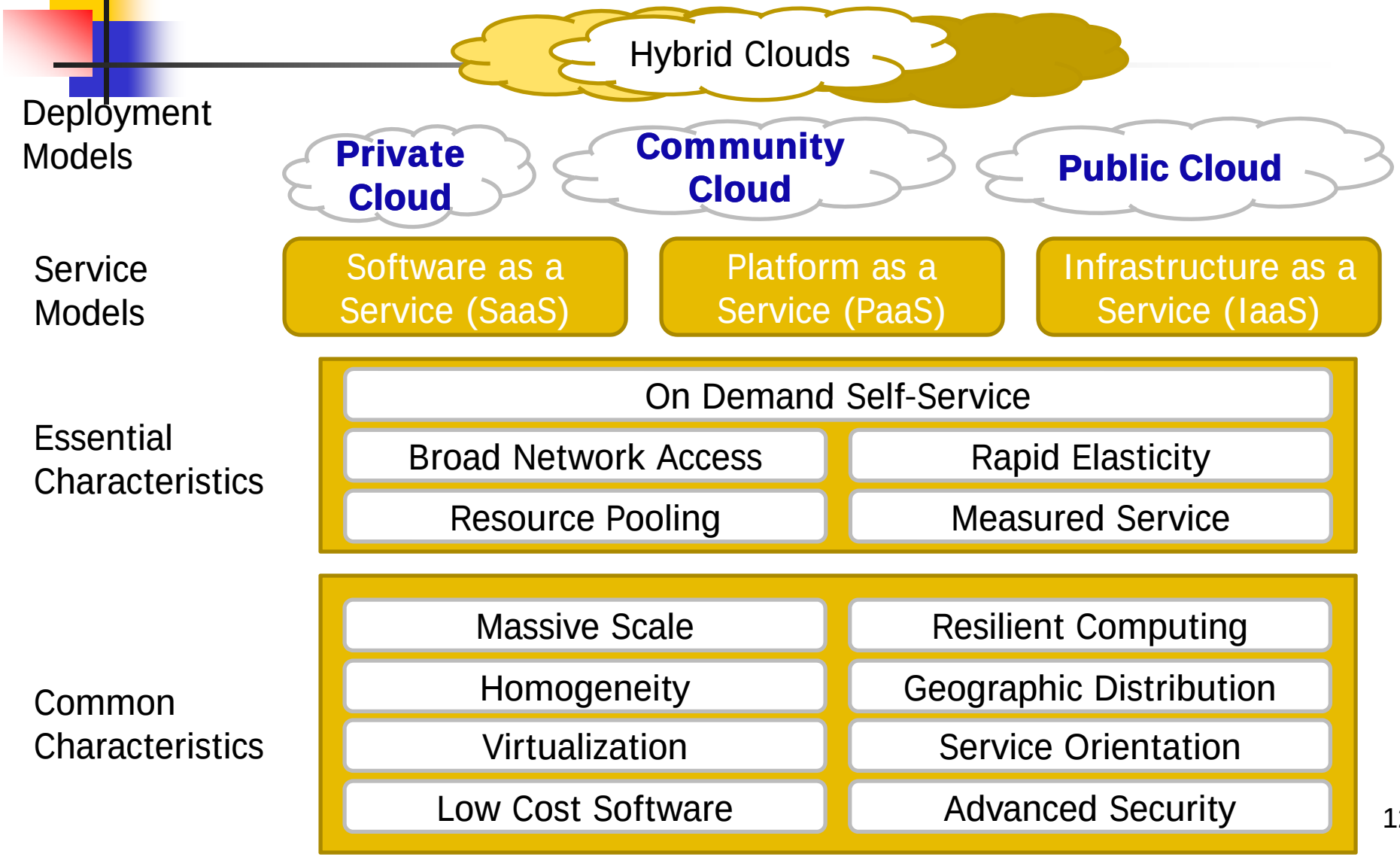
- Public cloud
  - Sold to the public, mega-scale infrastructure
  - available to the general public
- Private cloud
  - single org only; managed by the org or a 3rd party; on or off premise
- Community cloud
  - shared infrastructure for a specific community with shared concerns; managed by org or a 3rd party
- Hybrid cloud
  - composition of two or more clouds
  - bound by standard or proprietary technology

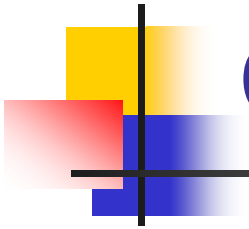


Common Cloud Characteristics

- Cloud computing often leverages:
  - Massive scale
  - Homogeneity
  - Virtualization
  - Resilient computing
  - Low cost software
  - Geographic distribution
  - Service orientation
  - Advanced security technologies

The NIST Cloud Definition Framework





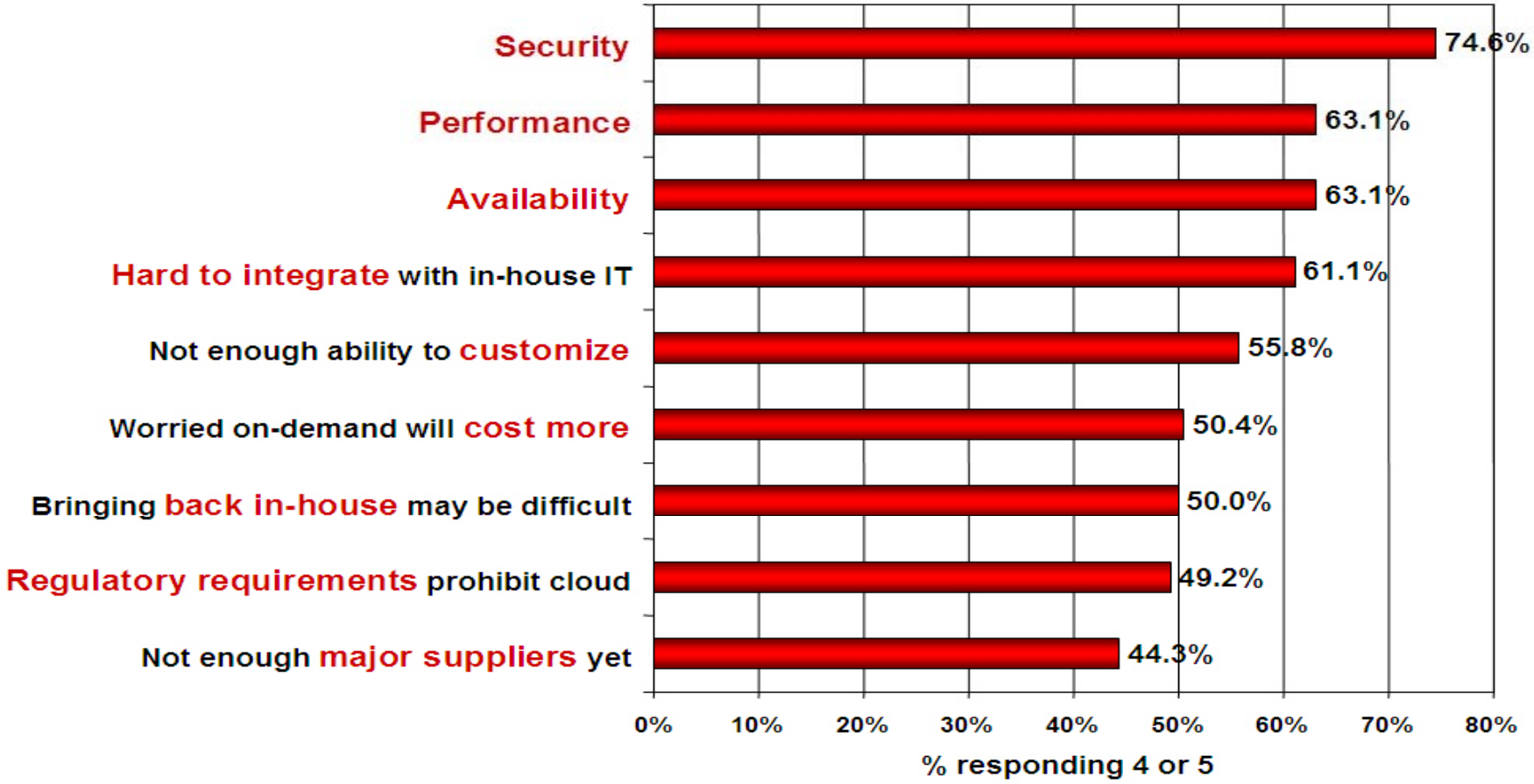
Outsourcing and Availability Issue

- Outsourcing parts of Org computing is a key thrust
- Security & privacy implications if the public cloud is used
- Cost and efficiency motivation for move
- Org is responsible for S&P of outsourced services
- Org should oversee and manage how the provider secures the environment

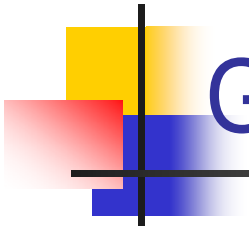
Major Issue?

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244



General Security Advantages

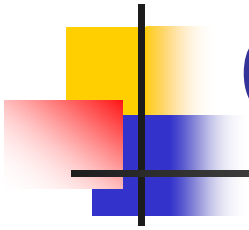
- Shifting public data to an external cloud
  - reduces the exposure of the internal sensitive data
- Cloud homogeneity
  - makes security auditing/testing simpler
- Clouds can enable automated security management
- Redundancy / Disaster Recovery

Cloud Security Advantages

- NIST 800-144 (Security Upside)
  - Staff Specialization (in Cloud Providers)
  - Platform Strength – greater homogeneity
  - Resource Availability – scalability help!
  - Backup and recovery – may be superior
  - Mobile Endpoints – heterogeneous devices
  - Data concentration- specifically for an org with mobile workforce

Cloud Security Advantages

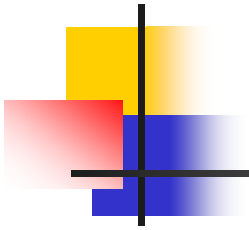
- Other
  - Data Fragmentation and Dispersal
  - Greater Investment in Security Infrastructure – hence availability
  - Fault Tolerance and Reliability; Greater Resiliency
  - Hypervisor Protection Against Network Attacks
  - Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)
  - Simplification of Compliance Analysis
  - Data Held by Unbiased Party (cloud vendor assertion)
  - Low-Cost Disaster Recovery and Data Storage Solutions
  - On-Demand Security Controls
  - Real-Time Detection of System Tampering
  - Rapid Re-Constitution of Services
  - Advanced Honeynet Capabilities



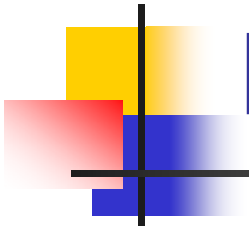
Cloud Security Downside

- NIST 800-144
  - System complexity –
    - e.g., public cloud is complex; attack surface increased
  - Shared Multi-tenancy
    - Logical separation instead of physical
  - Internet facing services
    - Exposure of admin/service interfaces
  - Loss of control – S&P are amplified!
    - On both physical/logical aspects; legal aspects

Security Relevant Cloud Components

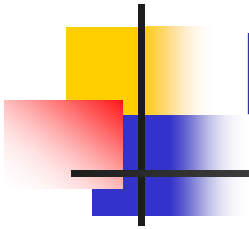


- Cloud Provisioning Services
- Cloud Data Storage Services
- Cloud Processing Infrastructure
- Cloud Support Services
- Cloud Network and Perimeter Security
- Elastic Elements: Storage, Processing, and Virtual Networks



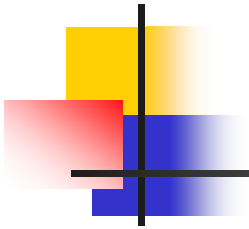
Provisioning Service

- Advantages
  - Rapid reconstitution of services
  - Enables availability
    - multiple data centers
    - multiple instances
  - Advanced honey net capabilities
- Challenges
  - Impact of compromising the provisioning service



Data Storage Services

- Advantages
  - Data fragmentation and dispersal
  - Automated replication
  - Provision of data zones (e.g., by country)
  - Encryption at rest and in transit
  - Automated data retention
- Challenges
  - Isolation management / data multi-tenancy
  - Storage controller
    - Single point of failure / compromise?
  - Exposure of data to foreign governments



Cloud Processing Infrastructure

- Advantages
  - Ability to secure masters and
  - Push out secure images
- Challenges
  - Application multi-tenancy
  - Reliance on hypervisors
  - Process isolation / Application sandboxes

Cloud Support Services

- Advantages
  - On demand security controls

    (e.g., authentication, logging, firewalls...)
- Challenges
  - Additional risk when integrated with customer applications
  - Needs certification and accreditation as a separate application
  - Code updates

Cloud Network and Perimeter Security

- Advantages
  - Distributed denial of service protection
  - VLAN capabilities
  - Perimeter security (IDS, firewall, authentication)
- Challenges
  - Virtual zoning with application mobility

Other issues

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
  - FISMA; HIPAA; SOX; PCI ; SAS 70 Audits

Obstacles & Opportunities

Table 6: Top 10 Obstacles to and Opportunities for Adoption and Growth of Cloud Computing.

	Obstacle	Opportunity
1	Availability of Service	Use Multiple Cloud Providers to provide Business Continuity; Use Elasticity to Defend Against DDOS attacks
2	Data Lock-In	Standardize APIs; Make compatible software available to enable Surge Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, and Firewalls; Accommodate National Laws via Geographical Data Storage
4	Data Transfer Bottlenecks	FedExing Disks; Data Backup/Archival; Lower WAN Router Costs; Higher Bandwidth LAN Switches
5	Performance Unpredictability	Improved Virtual Machine Support; Flash Memory; Gang Scheduling VMs for HPC apps
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large-Scale Distributed Systems	Invent Debugger that relies on Distributed VMs
8	Scaling Quickly	Invent Auto-Scaler that relies on Machine Learning; Snapshots to encourage Cloud Computing Conservationism
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses; Bulk use sales

Table 4: Examples of Cloud Computing vendors and how each provides virtualized resources (computation, storage, networking) and ensures scalability and high availability of the resources.

	Amazon Web Services	Microsoft Azure	Google AppEngine
Computation model (VM)	• x86 Instruction Set Architecture (ISA) via Xen VM • Computation elasticity allows scalability, but developer must build the machinery, or third party VAR such as RightScale must provide it	• Microsoft Common Language Runtime (CLR) VM; common intermediate form executed in managed environment • Machines are provisioned based on declarative descriptions (e.g. which "roles" can be replicated); automatic load balancing	• Predefined application structure and framework; programmer-provided "handlers" written in Python, all persistent state stored in MegaStore (outside Python code) • Automatic scaling up and down of computation and storage; network and server failover; all consistent with 3-tier Web app structure
Storage model	• Range of models from block store (EBS) to augmented key/blob store (SimpleDB) • Automatic scaling varies from no scaling or sharing (EBS) to fully automatic (SimpleDB, S3), depending on which model used • Consistency guarantees vary widely depending on which model used • APIs vary from standardized (EBS) to proprietary	• SQL Data Services (restricted view of SQL Server) • Azure storage service	•MegaStore/BigTable
Networking model	• Declarative specification of IP-level topology; internal placement details concealed • Security Groups enable restricting which nodes may communicate • Availability zones provide abstraction of independent network failure • Elastic IP addresses provide persistently routable network name	• Automatic based on programmer's declarative descriptions of app components (roles)	• Fixed topology to accommodate 3-tier Web app structure • Scaling up and down is automatic and programmer-invisible

Security Implications

TABLE I
SECURITY IMPLICATIONS OF CLOUD FEATURES

Feature	Security Implication
Outsourcing	Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customers' data in a way that has not been agreed upon in the past.
Extensibility and Shared Responsibility	There is a tradeoff between extensibility and security responsibility for customers in different delivery models.
Virtualization	There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.
Multi-tenancy	Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.
Service Level Agreement	The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time.
Heterogeneity	Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.

Security and Privacy Challenges (Takabi et al.)

- Authentication and Identity Management
  - interoperability
  - password-based: inherited limitation
  - How multi-tenancy can affect the privacy of identity information isn't yet well understood?
  - multi-jurisdiction issue
  - integrated with other security components.

Security and Privacy Challenges (cont.)

- Access Control and Accounting
  - Heterogeneity and diversity of services, as well as the domains' diverse access requirements
  - capture dynamic, context, or attribute- or credential-based access requirements
  - integrate privacy-protection requirements
  - interoperability
  - capture relevant aspects of SLAs

Security and Privacy Challenges (cont.)

- Trust Management and Policy Integration
  - compose multiple services to enable bigger application services
  - efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements
  - address challenges such as semantic heterogeneity, secure interoperability, and policy-evolution management.

Security and Privacy Challenges (cont.)

- Secure-Service Management
  - WSDL can’t fully meet the requirements of cloud computing services description
  - issues such as quality of service, price, and SLAs
  - automatic and systematic service provisioning and composition framework that considers security and privacy issues

Security and Privacy Challenges (cont.)

- Privacy and Data Protection
  - storing data and applications on systems that reside outside of on-premise datacenters
  - shared infrastructure, risk of potential unauthorized access and exposure.
  - Privacy-protection mechanisms must be embedded in all security solutions.
  - Provenance
    - Balancing between data provenance and privacy

Security and Privacy Challenges (cont.)

- Organizational Security Management
  - shared governance can become a significant issue if not properly addressed
  - Dependence on external entities
  - the possibility of an insider threat is significantly extended when outsourcing data and processes to clouds.

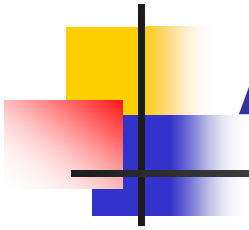
Security and Privacy Approaches (Takabi et al.)

- Authentication and Identity Management
  - User-centric IDM
  - users control their digital identities and takes away the complexity of IDM from the enterprises
  - federated IDM solutions
  - privacy-preserving protocols to verify various identity attributes by using, for example, zero-knowledge proof-based techniques

Security and Privacy Approaches (Takabi et al.)

- Access Control Needs
  - RBAC
  - policy-integration needs
    - Cross domain accesses
  - credential-based RBAC, GTRBAC, location-based RBAC

Security and Privacy Approaches (Takabi et al.)

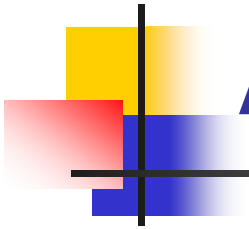


- Secure Interoperation
  - *Multi-domain*
  - centralized approaches
  - decentralized approaches
  - specification frameworks to ensure that the cross-domain accesses are properly specified, verified, and enforced
  - Policy engineering mechanisms

Security and Privacy Approaches (Takabi et al.)

- Secure-Service Provisioning and Composition
  - Open Services Gateway Initiative (OSGi)
  - Declarative OWL-based language can be used to provide a service definition manifest, including
    - a list of distinct component types that make up the service,
    - functional requirements,
    - component grouping and topology instructions

Security and Privacy Approaches (Takabi et al.)



- Trust Management Framework
  - trust-based policy integration
  - Delegation
  - must be incorporated in service composition framework

Security and Privacy Approaches (Takabi et al.)

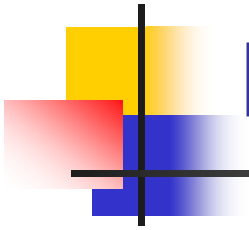
- Data-Centric Security and Privacy
  - shifts data protection from systems and applications
  - documents must be self-describing and defending regardless of their environments.

Security and Privacy Approaches (Takabi et al.)

- Managing Semantic Heterogeneity
  - semantic heterogeneity among policies
  - Use of an ontology is the most promising approach
  - policy framework and a policy enforcement architecture
  - inference engines

Key S&P Issues (NIST 800-144)

- Governance – amplifies this need!
  - Control and oversight challenging
  - Org programs should incorporate external entity
  - Role and responsibilities for risk mgmt
- Compliance
  - Law and regulations
  - Data location – in multiple physical locations? Disclosures? Cross border risks?
- Electronic Discovery
  - Does provider provide adequate e-discovery capabilities



Key S&P Issues (NIST 800-144)

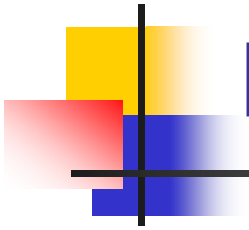
- Trust
  - Insider access
  - Data ownership – rights must be firmly established in SLA (e.g., controversy in SN related data ownership)
  - Composite Services
    - Composed through nesting and layering (e.g., SaaS, PaaS, etc.)
    - Compatibility, performance guarantees?
  - Visibility – of Provider's security measures
  - Ancillary data – accounts of consumers (payment info, client activity; access patterns; ..)!
  - Risk management

Key S&P Issues (NIST 800-144)

- Architecture
  - Attack surface – VM/hypervisor introduce new attack surface
  - Virtual network protection
    - Software-based switches and network configurations
    - Potential loss of separation of duty in admin roles
  - Virtual Machine images
    - Must be up-to-date with patches
  - Client Side Protection – do not overlook this!
    - Involves mobile devices

Key S&P Issues (NIST 800-144)

- Identity and Access Management
  - Org's IAM framework may not extend to public cloud
    - Maintaining two may not be scalable/workable
  - Some form of identity federation is needed – SAML, OpenID standards
  - Authentication - SAML Standard
  - Access Control – XACML standard
- Software Isolation



Key S&P Issues (NIST 800-144)

- Software Isolation - to support multitenancy!
  - Hypervisor complexity
  - Attack Vectors -- new ones? Malicious code breaking isolation?
- Data Protection - Data in cloud exist in shared env
  - Value concentration
  - Data isolation
  - Data sanitization
- Availability – accessible and usable
  - Temporary, Prolonged/Permanent Outages
  - Denial of Service attacks

Key S&P Issues (NIST 800-144)

- Incidence Response
  - Data availability
    - Clients may not see event logs and viln info under provider
      - Complex when several providers are involved; multi-tenancy
  - Incident analysis and resolution
    - Lack of detailed info regarding architecture/mechanisms
    - Forensic copies may be difficult to create – multitenant?
    - How to contain an attack?

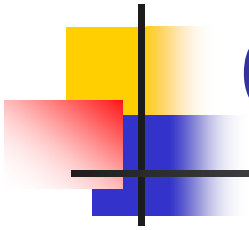
Summary of Recommendations

Architecture	Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

Summary of Recommendations

Availability	Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Outsourcing in Public Cloud - General Concerns



- Inadequate policies and practices
  - Undetected violations
  - Lack of sufficient data/configuration integrity
  - Loss of privacy – non-rigourous mechanisms?
- Weak confidentiality, Integrity, availability sureties
  - Need ways to establish assurances
- Other concerns
  - Principle-agent problem – need to make sure interest of the provider is consistent
- Attenuation of expertise
  - Organization may slowly lose expertise

Outsourcing in Public Cloud – Preliminary activities

- Specify requirements
  - Choice of deployment models; responsibilities
  - Exit strategy – as part of requirement analysis; relates to IR, DR, BC plans
  - Review common outsourcing provisions (standards, laws and regulations)
- Assess S&P risks
  - Emphasize flexible & adaptable risk mgmt program
  - Need Privacy Threshold analysis (PTA)
  - Need to understand underlying technologies by CSP

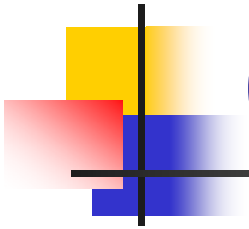
Outsourcing in Public Cloud – Preliminary activities

- Assess the competency of the CSP
  - CSP's ability, commitment
  - Evaluate levels of S&P provided
- Initiating and Coincident activities
  - Establish contractual activities (SLAs)
  - Assess Performance - continuous
- Concluding Activities (terminating)
  - Reaffirm contractual obligations
  - Eliminate Physical and electronic Access Rights
  - Recover Organizational resources and Data

- Experience and technical expertise of personnel
- The vetting process personnel undergo
- Quality and frequency of security and privacy awareness training provided to personnel
- Account management practices and accountability
- The type and effectiveness of the security services provided and underlying mechanisms used
- The adoption rate of new technologies
- Change management procedures and processes
- The cloud provider's track record
- The ability of the cloud provider to meet the organization's security and privacy policy, procedures, and regulatory compliance needs.

- A detailed description of the service environment, including facility locations and applicable security requirements
- Policies, procedures, and standards, including vetting and management of staff
- Predefined service levels and associated costs
- The process for assessing the cloud provider's compliance with the service level agreement, including independent audits and testing
- Specific remedies for harm caused or noncompliance by the cloud provider
- The period of performance and due dates for any deliverable
- The cloud provider's points of interface with the organization
- The organization's responsibilities for providing relevant information and resources to the cloud provider
- Procedures, protections, and restrictions for collocating or commingling organizational data and for handling sensitive data
- The cloud provider's obligations upon contract termination, such as the return and expunging of organizational data.

Cloud Accelerants (Ernst&Young)



- Elasticity
- Pay-as-you-go
- Cost savings
  - 25%-50 savings (Brookings report)
- Market Barrier reduction
  - Eases market entry!
- Infrastructure utilization
  - better efficiency; lower power consumption; global load balancing
- Public investment – worldwide
- Security as a service
- Standardization efforts
- Cloud brokers with expertise to help transition
- Risk of missing out

Drill-down discussion (E&Y)

- Pricing and business models
- Vendor Management and strategic sourcing – need to rethink; new skills!
  - Inner working not known; Sourcing parts – interdependencies & data S&P
  - Cloud brokers/aggregators; SLA standardization
- Availability and interoperability
  - Between yours and CSPs
- Security and privacy
- Standards and risk management
  - Cloud standards are in infancy
- Accounting and regulatory compliance
  - Can provide opportunities as well as challenges
- Cross border taxation and arrangements

Pricing and Business model considerations

Figure 1: Important cloud pricing and business model considerations

Issue	Implication
Maximizing asset utilization	Pricing programs must encourage customer behavior that helps smooth consumption peaks and valleys
Granularly detailed services pricing	Enables customers to optimize service cost via their software design, but could increase vendor lock-in
Capital expenditure	Corporate preference to use traditional return on investment (ROI) measures in making capital expenditure decisions could apply downward pressure to cloud pricing
SaaS customization	Because it requires non-standard, negotiated pricing, customization reduces the potential economic benefit of cloud models
Functionality "menu"	If providers make all functions available from a configuration menu, the possibility of differentiation via IT is diminished or eliminated
Funding innovation relevant to customer subsets	Given shared infrastructure, the economic model is unclear for innovation that benefits only a few customers; clearinghouses or application exchanges may evolve to fill the need
National regulation, particularly of data location, security and privacy	Creates obstacles to optimal asset utilization of cloud infrastructure

Source: Ernst & Young analysis.

Standards and Risk Mgmt

Figure 3: Cloud security "threat

1. Organizations shall develop a acceptable level.
2. Formal risk assessments sha intervals, determining the lik qualitative and quantitative i inherent and residual risk, co and vulnerability analysis, re
3. Risks shall be mitigated to ar established and documented
4. Risk assessment results shal administrative procedures, s relevant and effective.
5. Once access risks have been to minimize, monitor and me inappropriate access. Compe to provisioning access.

The risk guidelines above are described in a pragmatic tool to help CSPs address risk

Source: CSA Controls Matrix web page, http

Figure 4: Some possible future standards

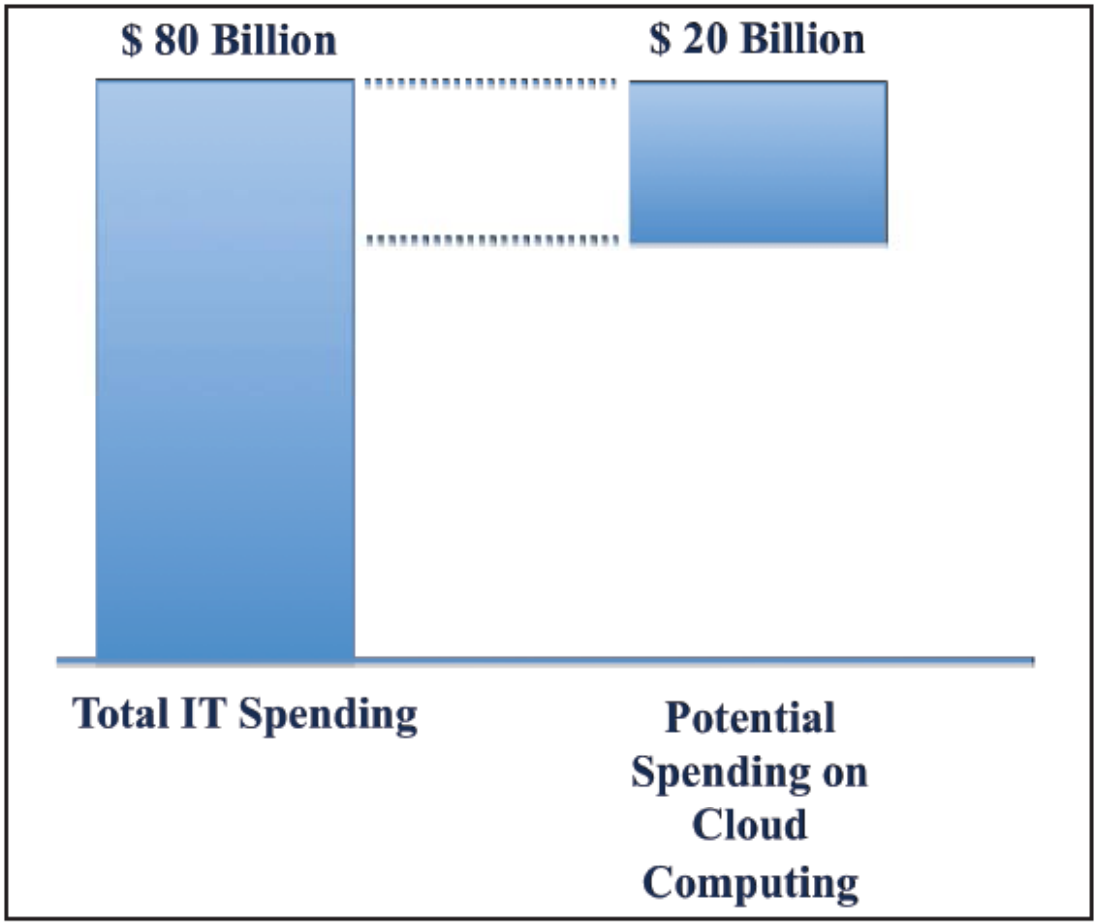
1. Federated security (e.g., identity) across clouds
2. Metadata and data exchanges among clouds
3. Standards for moving applications between cloud platforms
4. Standards for describing resource/performance capabilities and requirements
5. Standardized outputs for monitoring, auditing, billing, reports and notifications for cloud applications and services
6. Common representations (abstract, APIs, protocols) for interfacing cloud resources
7. Cloud-independent representation for policies and governance
8. Portable tools for developing, deploying and managing cloud applications and services
9. Orchestration and middleware tools for creating composite applications across clouds
10. Standards for machine-readable service level agreements (SLAs)

If all the cloud standards on this wish list were achieved, cloud users would fully realize the cloud's potential for IT flexibility and scalability that enables business agility. They are unlikely to be realized quickly, however, given that the wish list would limit CSP differentiation.

Source: Cloud Standards Overview, Object Management Group, July 2009, http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview

Federal Cloud Computing strategy

Figure 1: Estimated portion of Federal IT spend able to move to the cloud



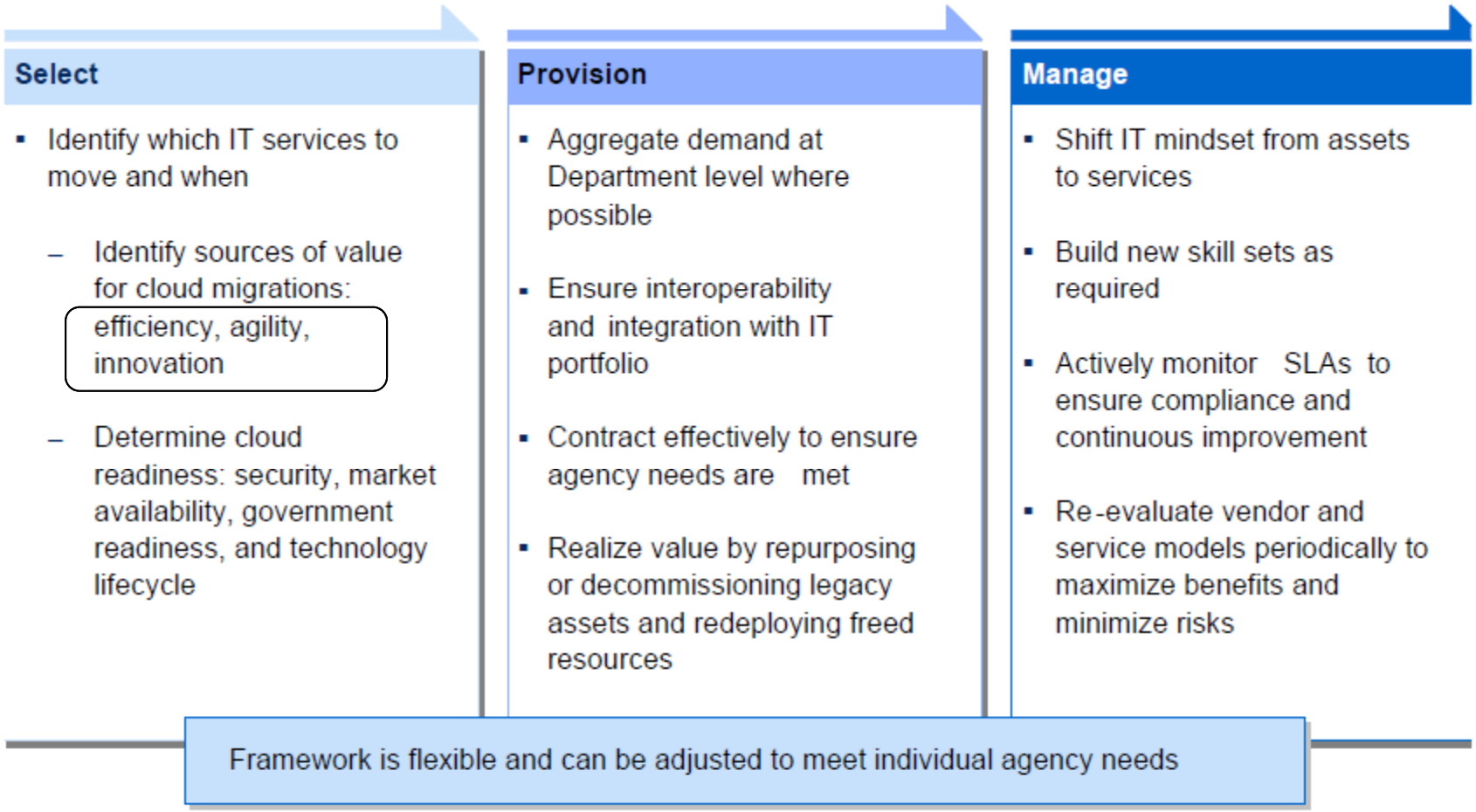
Benefits of CC

Figure 2: Cloud benefits: Efficiency, Agility, Innovation

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

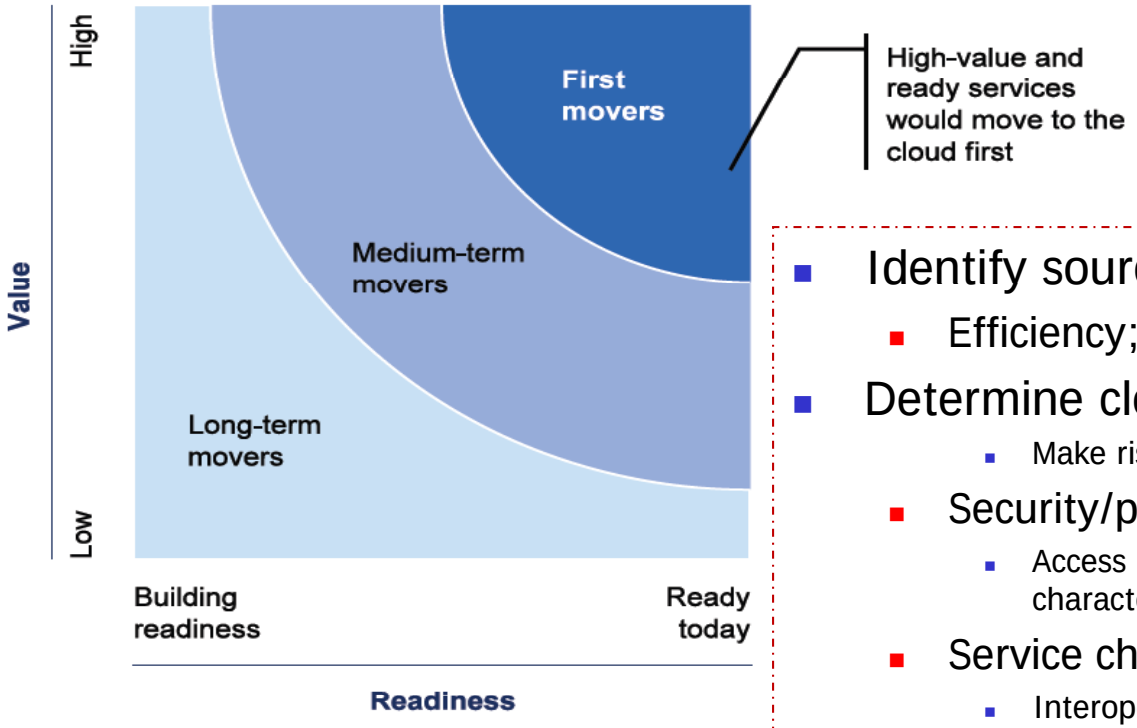
Framework for migration

Figure 3: Decision Framework for Cloud Migration



Value and readiness for migration

Figure 4: Selecting Services for Cloud Migration



- Identify source of value
  - Efficiency; Agility – in client's hand; Innovation
- Determine cloud readiness
  - Make risk based decisions
  - Security/privacy requirements(FISMA)
    - Access control policies; Statutory compliance; Data characteristics; Governance – transparency of CSPs
  - Service characteristics
    - Interoperability, performance, scalability, architecture compatibility
  - Market Characteristics
  - Infrastructure readiness – (mission criticality)
  - Government readiness and technology life cycle

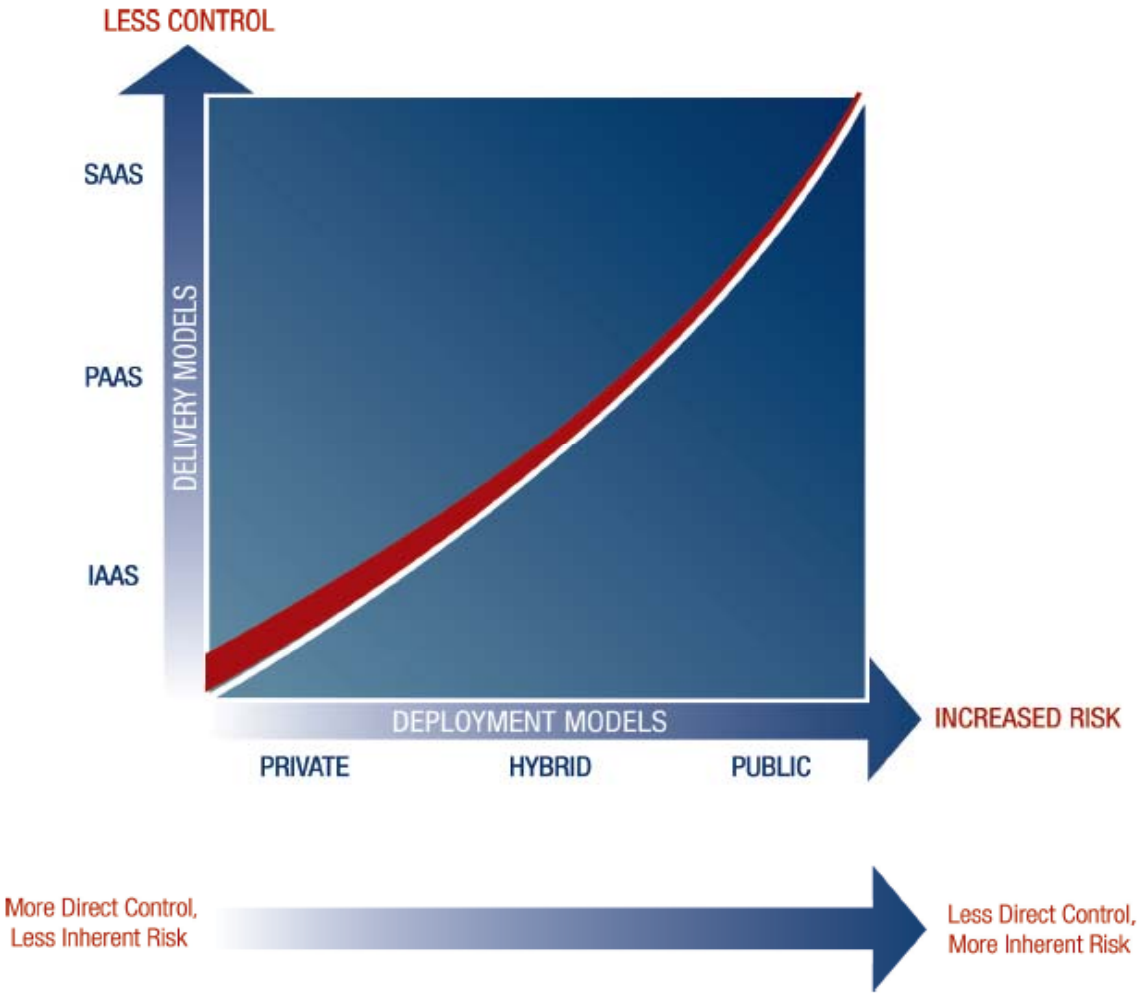
COSO's Risk Mgmt for Clouds

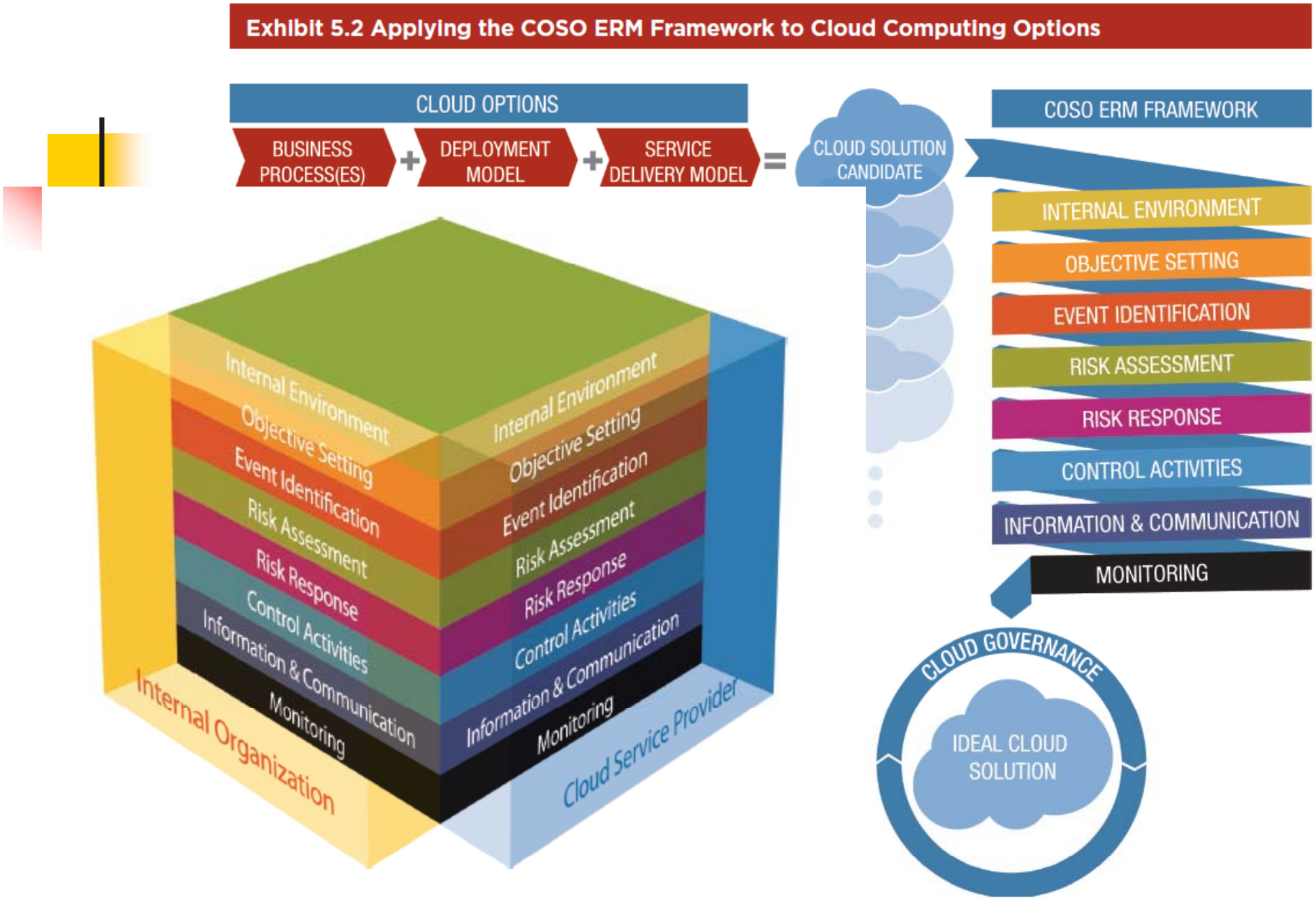
- Key risks associated with Cloud Computing
  - Disruptive force
    - Increased innovation could be risky for some org
    - Disrupt business models
  - CSPs and tenants create a risk ecosystem – for all
    - Liability; risk universe/escalation – different Orgs may have different risk mgmt programs
  - Lack of transparency
  - Reliability and transparency issues

COSO's Risk Mgmt for Clouds

- Key risks associated with Cloud Computing
  - Vendor lock-in and portability/interoperability issues
    - CSPs may provide proprietary tools
  - Security/Compliance issue
  - High value cyber attack targets
  - Risk of Data leakage
  - IT Organizational Changes
  - Cloud servicer provider viability
    - Their continuity may depend on evolving business models

Risk Relationship (source: COSO report)





(source: COSO report)

COSO Recommended Risk Responses

Risk	Response
Unauthorized cloud activities	Cloud policies & controls
Lack of transparency	Assessments of CSP control environment
Security, Compliance, Data leakage & data jurisdiction	Data classification policies and processes
Transparency and relinquishing direct control	Management oversight and operations monitoring controls
Reliability, performance, high-value cyber attack target	Incident management (should not completely rely on CSP's)
Non compliance with regulation	Monitoring of external environment
Vendor lock-in	Preparation for exist strategy
Non compliance with disclosure requirements	New disclosures in financial reporting (maybe required)

COSO CC Governance

Position	Responsibilities
Chief Information Officer	• Understand and monitor cloud computing's potential to support current business strategies and new business opportunities • Establish overall strategy for leveraging and aligning cloud solutions • Facilitate the integration of cloud solutions into the organization and with the current IT infrastructure • Assist with incorporating cloud governance into the organization's ERM program • Implement a data classification scheme in conjunction with data owners • Establish cloud processes for resource provisioning, user access management, and change management • Establish the organization's cloud incident management program • Monitor and enforce CSP service-level agreements • Monitor activities of the CSP and fellow cloud tenant customers
Chief Audit Executive or Internal Auditor	• Perform periodic audits to evaluate the design and effectiveness of the blended control environment in which controls and processes are shared with the CSP • Audit the CSP or review SOC reports to verify the effectiveness of CSP controls relied upon by the organization • Perform periodic compliance audits of data residing on external clouds to verify compliance with data classification polices • Audit CSP spend and contractual compliance • Evaluate cloud governance