Crowe Horwath

The Unique Alternative to the Big Four®

Enterprise Risk Management and Cloud Governance

June 18, 2013

Audit | Tax | Advisory | Risk | Performance

Agenda

- What Is Cloud Computing?
- The Opportunities
- The Risks
- Changes in the Business Operating Environment With Cloud Computing
- Approaching ERM in the Cloud Computing Paradigm
- Cloud Governance
- Recommended Risk Responses for Cloud Computing

What Is Cloud Computing?

- Definition from the National Institute of Standards and Technology (NIST) (emphasis added):
  - "Cloud computing is a model for enabling ubiquitous, 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."

- Cloud Jargon:
  - Characteristics: on-demand, access via network, resource pooling, elasticity, measured
  - Service delivery models: SaaS, PaaS, IaaS
  - Deployment models: private, public, hybrid
  - CSP (cloud service provider)
  - Multi-tenant

Opportunities

- **Cost savings** – Customers pay for only the computing resources used. There are no physical space requirements or utility costs. All dollars are expensed (that is, receive a U.S. tax benefit).
- **Speed of deployment** – The time to fulfill requests for computing power and applications can change from months to weeks, weeks to days, and days to hours.
- **Scalability and better alignment of technology resources** – Companies can scale up or down their capacity without capital expenditures.
- **Decreased effort in managing technology** – Cloud computing provides the organization more time to focus on core purpose and goals; more consistent technology upgrades; and expedited fulfillment of IT resource requests.
- **Environmental benefits** – Significant adoption of cloud computing should yield less overall power consumption, carbon emissions, and physical land use.

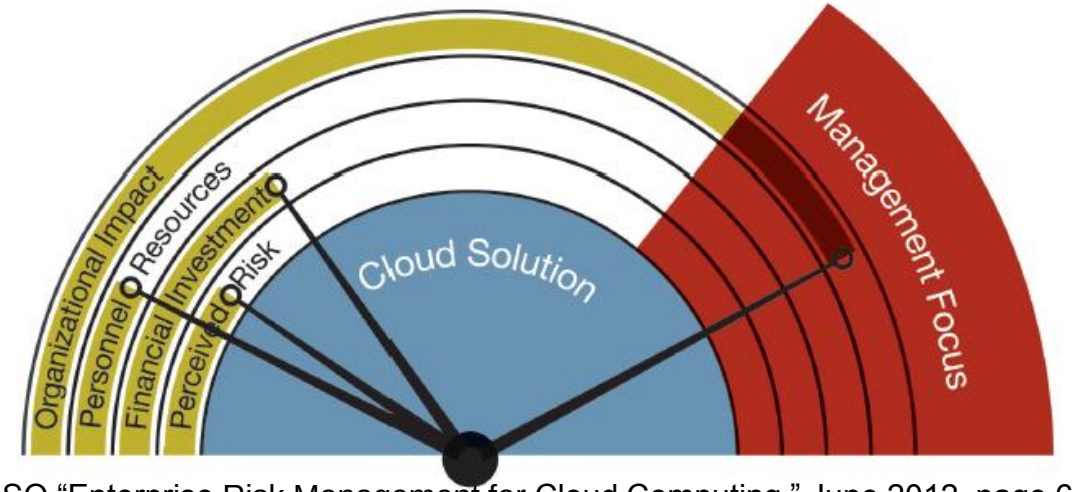
Risks

- Some of the typical risks associated with cloud computing are:
  - Disruptive force
  - Residing in the same risk ecosystem as the cloud service provider (CSP) and other tenants of the cloud
  - Lack of transparency
  - Reliability and performance issues
  - Vendor lock-in and lack of application portability and interoperability
  - Security and compliance concerns
  - Creation of high-value cyber-attack targets
  - Risk of data leakage
  - IT organizational changes
  - Viability of the CSP

Changes in the Operating Environment With Cloud Computing

- Risks and other cloud computing effects should be incorporated in ERM programs.
  - Organizations can engage cloud computing solutions while bypassing normal management oversight controls.
  - Cloud computing solutions are: a) easily adopted within a short period of time, b) require a small monetary investment, and c) involve very few personnel.

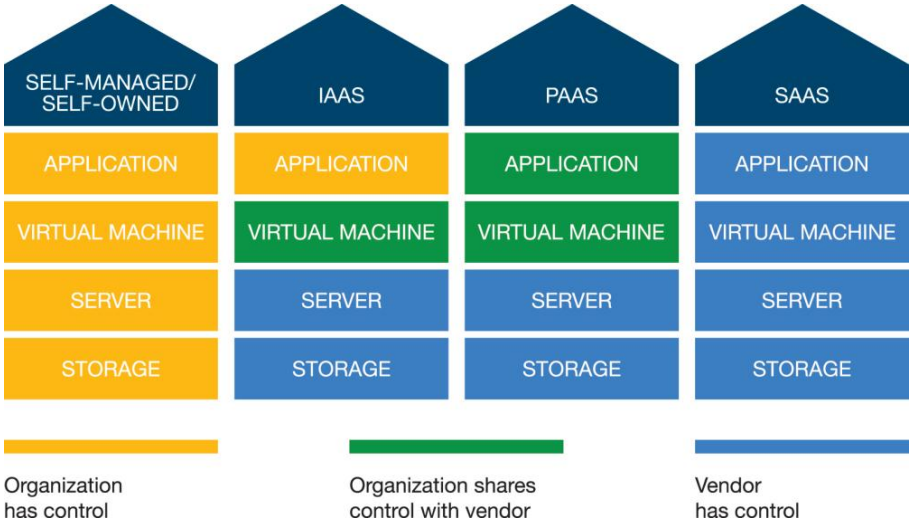
Exhibit 4.1 Cloud Solutions Can Be Adopted While Eluding Management Oversight

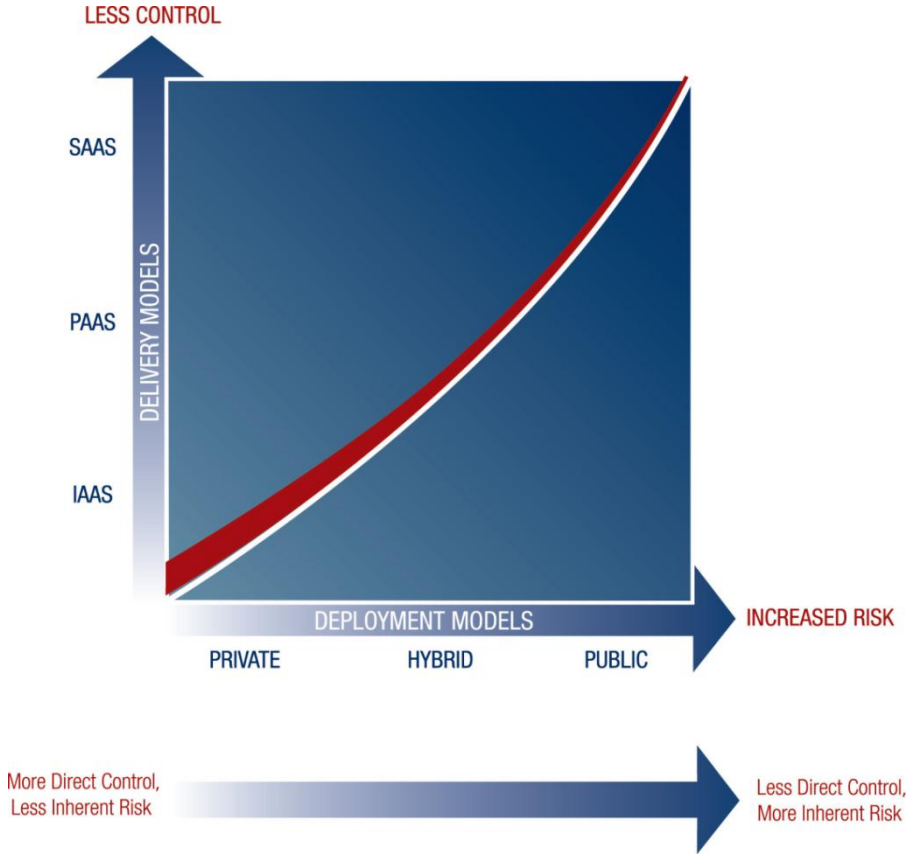


COSO "Enterprise Risk Management for Cloud Computing," June 2012, page 6

Changes in the Operating Environment With Cloud Computing

- Inherent Risk Relationship With Cloud Service Delivery and Deployment Models
  - With most cloud solutions, the organization has less direct control of the solution and consequently a higher level of inherent risk.





COSO “Enterprise Risk Management for Cloud Computing,” June 2012, pages 7, 19

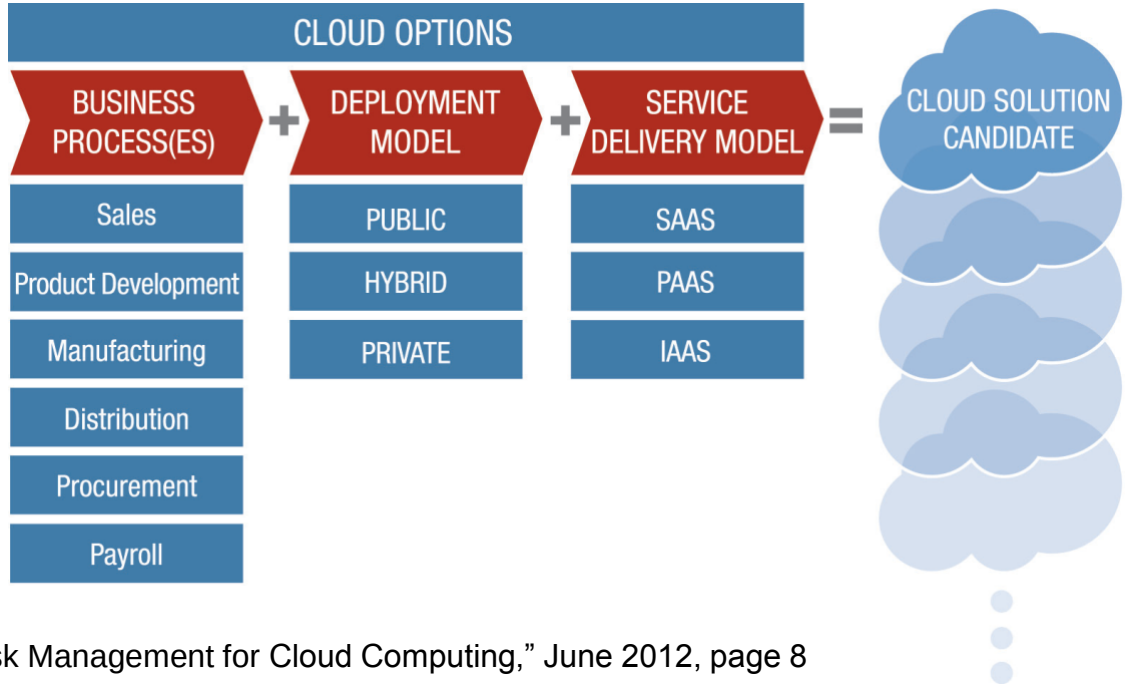
Approaching ERM in the Cloud Computing Paradigm

- Cloud computing's impact on an operating environment should be assessed and included in the enterprise risk management program.
  - Create a well-developed plan – clearly defining objectives and courses of actions in advance.
    - Strong governance model
    - Sound reporting structure
    - Accurate understanding of internal IT skills and abilities
    - Defined risk appetite

- Best Practice: Incorporate cloud governance in the initial stages before a cloud solution is adopted.
  - It is prudent to perform a risk assessment and establish cloud governance where an organization has already implemented a cloud solution(s).

Approaching ERM in the Cloud Computing Paradigm (continued)

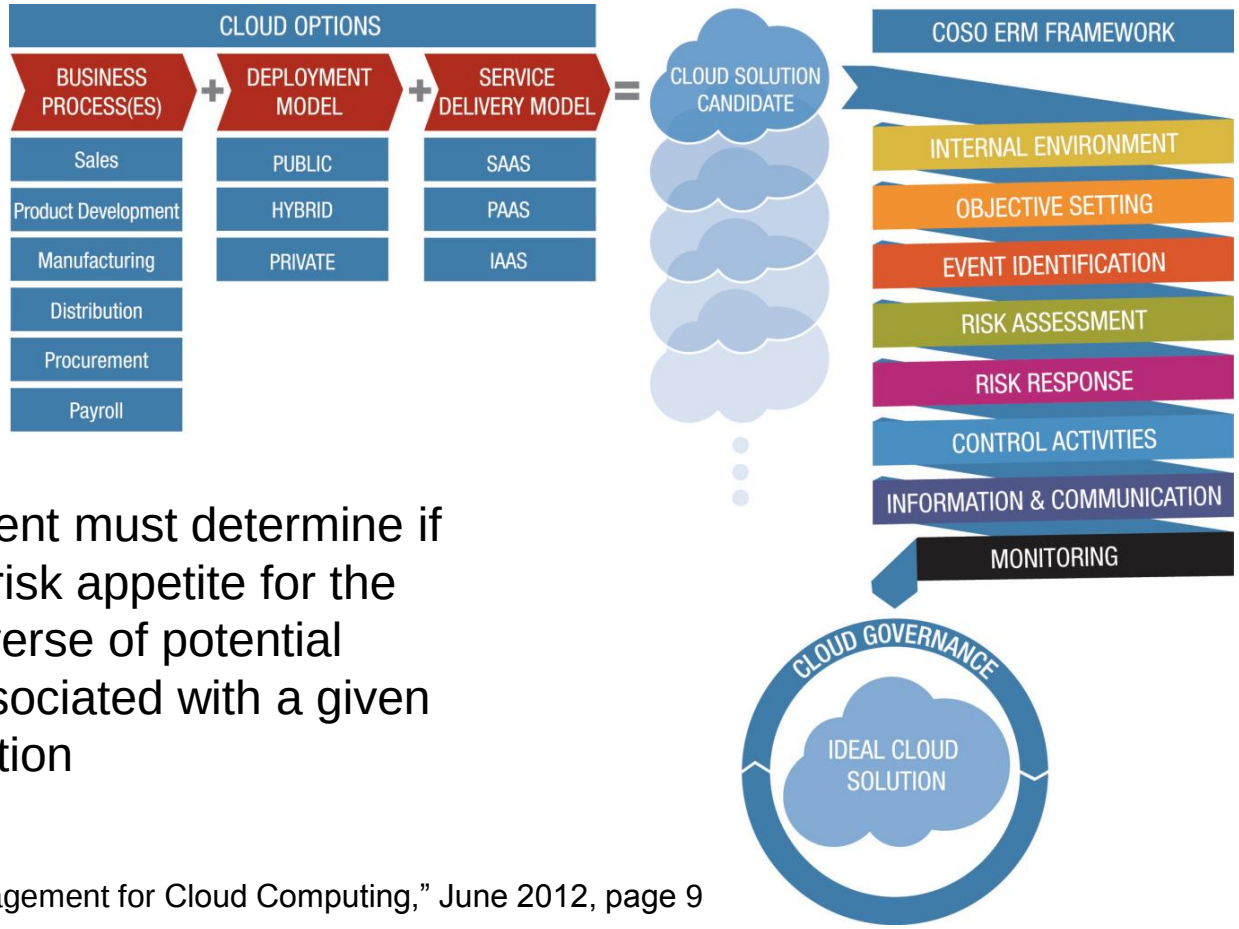
- The degree of adjustment required to an organization's existing ERM program in a cloud computing paradigm depends on:
  - Business processes the cloud supports
  - Cloud deployment delivery model
  - Service delivery model



COSO "Enterprise Risk Management for Cloud Computing," June 2012, page 8

Approaching ERM in the Cloud Computing Paradigm (continued)

- Applying the COSO ERM framework to effectively assess and manage the related risks



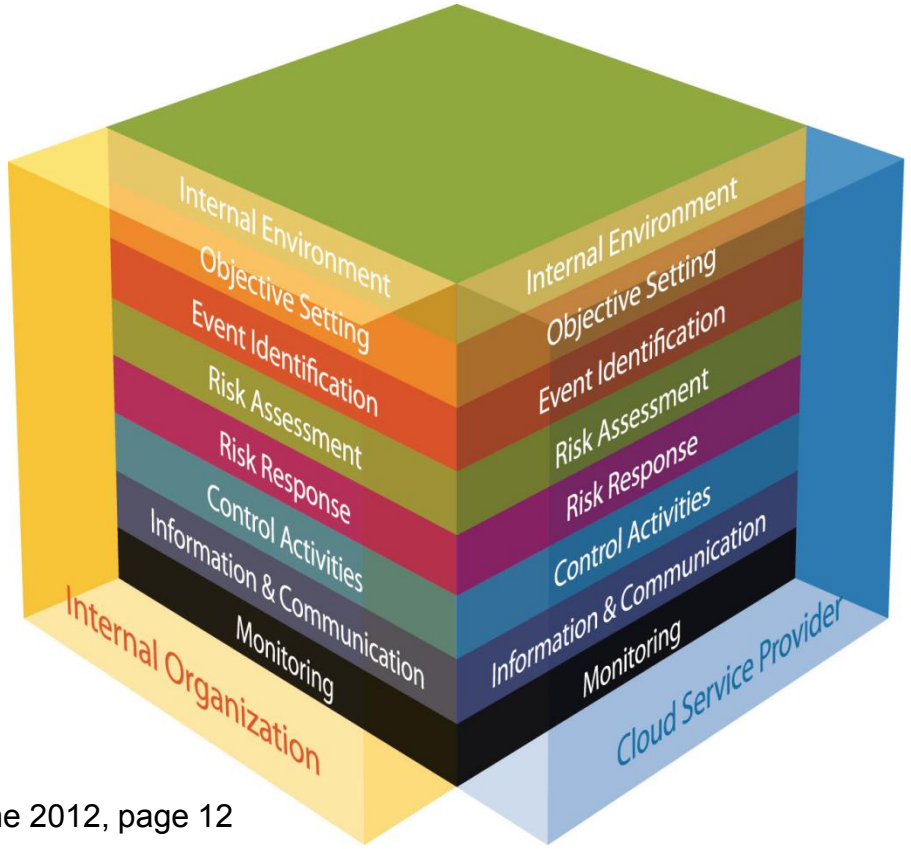
  - Management must determine if it has the risk appetite for the entire universe of potential events associated with a given cloud solution

COSO "Enterprise Risk Management for Cloud Computing," June 2012, page 9

Approaching ERM in the Cloud Computing Paradigm (continued)

- Risk Profile Impact of CSPs and fellow cloud tenants
  - Using cloud computing converts an organization's internal environment into a combination of its own internal environment and the internal environment of the contracted CSP.

- Why Both?
  - Data and processes are hosted in a shared environment with other cloud tenants.
  - Behavior and events of the CSP and fellow tenants could have a direct impact on the organization.



COSO "Enterprise Risk Management for Cloud Computing," June 2012, page 12

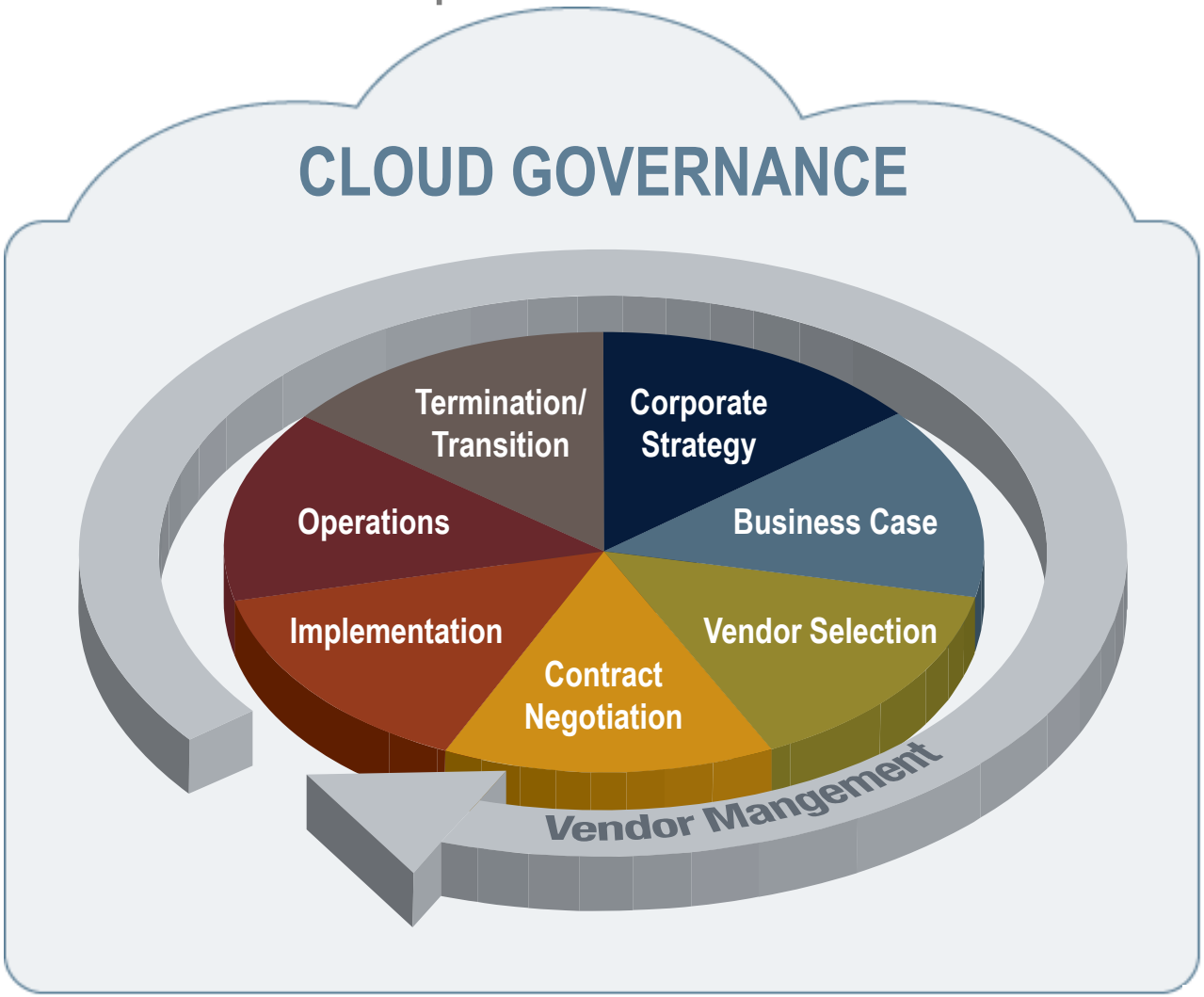
Cloud Governance

- "Cloud governance" refers to the controls and processes in place for cloud planning and strategy, vendor selection, contract negotiation, implementation, operation, and possible termination and transition of cloud services.

- A well-designed cloud governance model anticipates planned and unplanned events in each phase of the cloud life cycle to help confirm processes occur as expected. Prepared responses to anticipated events may include executing a series of actions or taking no action at all.

- Should an event occur, having thought through the occurrence of potential events facilitates the setup of alerts for timely notification.

Cloud Governance Components – Consumer

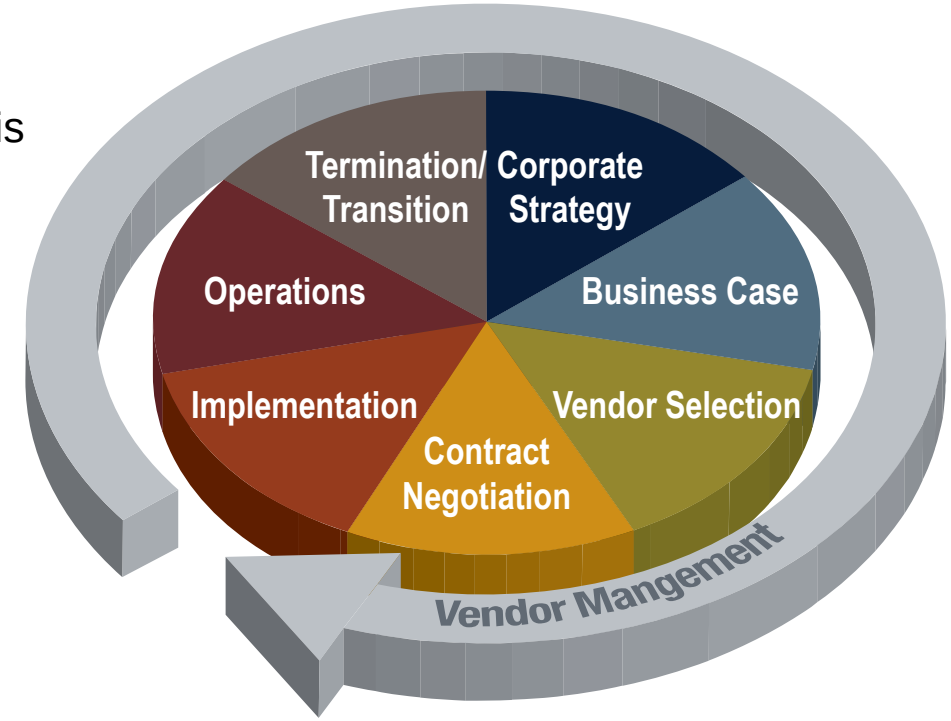


Cloud Governance Program – Sample Risk Responses

- **Corporate strategy –** Verify that your cloud strategy aligns with your corporate and IT vision.
- **Business case creation –** Define requirements and criteria for moving business processes to the cloud.
- **Vendor selection –** Thoroughly assess vendors against defined criteria to verify that they meet business requirements.
- **Contract negotiation –** Set SLAs; review contracts to allow for SSAE 16 or the right to audit, and the right to access data in the event of termination.
- **Implementation –** Perform testing and migration with business process owners.
- **Operations –** Enforce SLAs with vendors, review independent auditor reports, monitor incident response, and perform periodic security assessments.
- **Termination and transition –** Establish predefined exit and transition strategy.
- **Vendor management –** Enforce SLAs with vendors, assess vendor continued financial viability, and confirm that vendor strategic direction continues to align with the organization's.

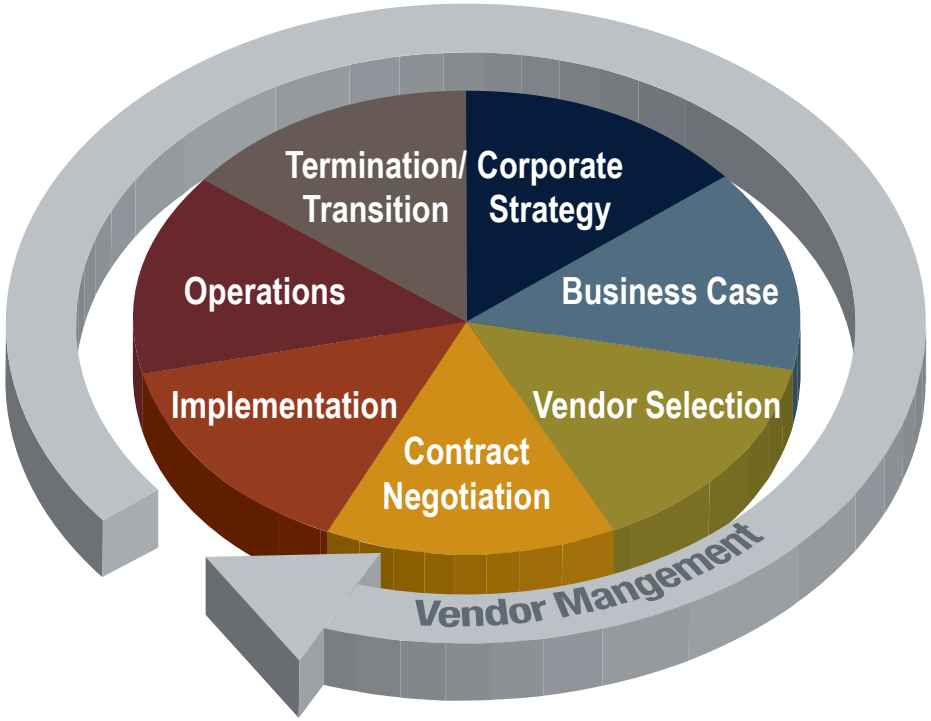
Cloud Governance (continued)

- **Corporate Strategy**
  - IT direction and alignment to corporate strategy
- **Business Case Creation**
  - Business/organizational impact analysis
  - Risk assessment
  - Business requirements
  - Compliance/tax requirements and evaluation
- **Vendor Selection**
  - NDA
  - Vendor lists
  - Requirements and evaluation criteria
  - Terms and conditions
  - Demo and test drive
  - Due diligence



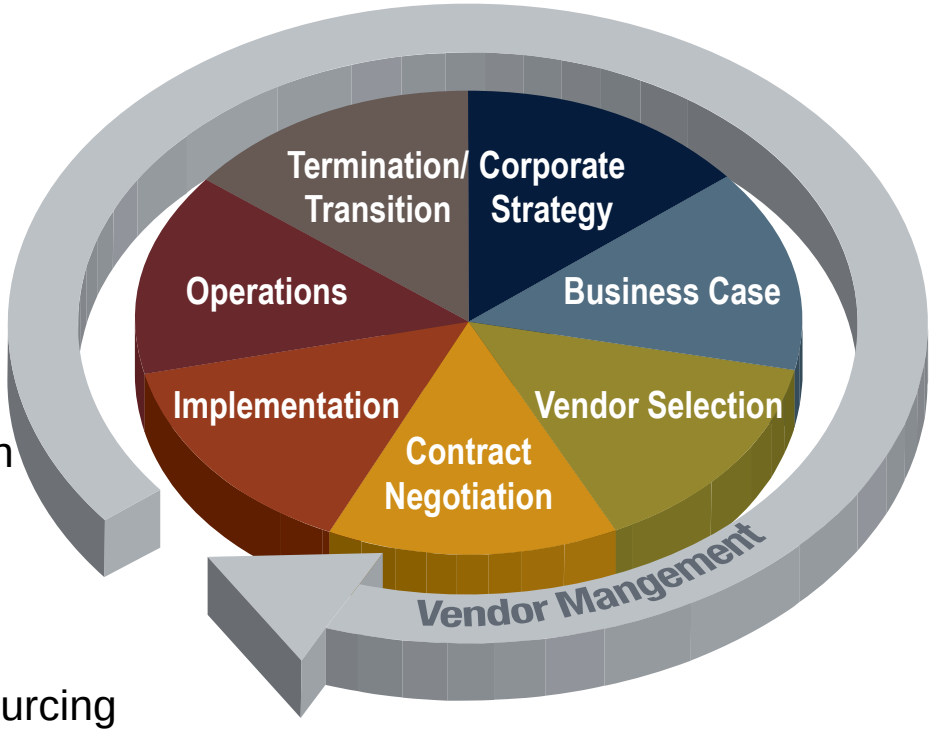
Cloud Governance (continued)

- **Contract Negotiation**
  - Fees and renewals
  - Timeline
  - Contractual terms
  - SLAs and liability for noncompliance
  - Data availability and disaster recovery
  - Termination and data archival
  - SSAE 16 and right to audit
  - Roles and responsibilities
- **Implementation**
  - Trial run
  - Organization change management
  - Configuration
  - Customization
  - Data migration
  - Pilot



Cloud Governance (continued)

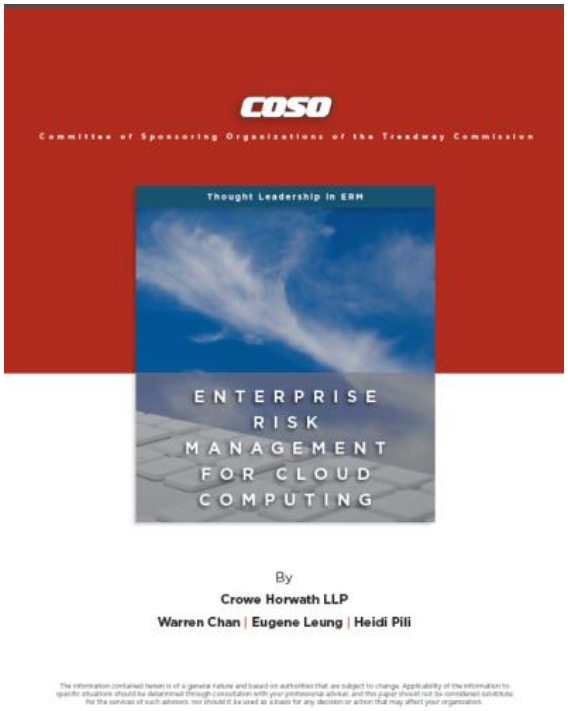
- **Operations**
  - Vendor management
  - User provisioning and administration
  - Benchmark and trend analysis
  - Cost/benefit analysis and ROI follow-up
- **Termination/Transition**
  - Timeline
  - Removal of all data (including backups)
  - Data retrieval
  - New solution identification and transition
- **Vendor Management**
  - Policies and procedures
  - Approved vendor list
  - Approved business processes for outsourcing
  - Approved data classification
  - Data confidentiality



Questions?

Works Cited

- Warren Chan, Eugene Leung, and Heidi Pili, "Enterprise Risk Management for Cloud Computing," Committee of Sponsoring Organizations of the Treadway Commission, June 20, 2012.



For more information, contact:

Warren Chan
630.586.5135
Warren.Chan@crowehorwath.com

Vicky Cheng
630.990.4432
Vicky.Cheng@crowehorwath.com

Christeen Russell
212.750.4195
Christeen.Russell@crowehorwath.com