Risk Management & Cloud Security

Setting & Enforcing Policy

experience BKD CPAs & Advisors

Agenda

- Define the cloud ecosystem
- Business use of cloud services
- Cloud service risks
- Governance of the cloud – critical policies, procedures & controls
- Third-party management considerations for the cloud

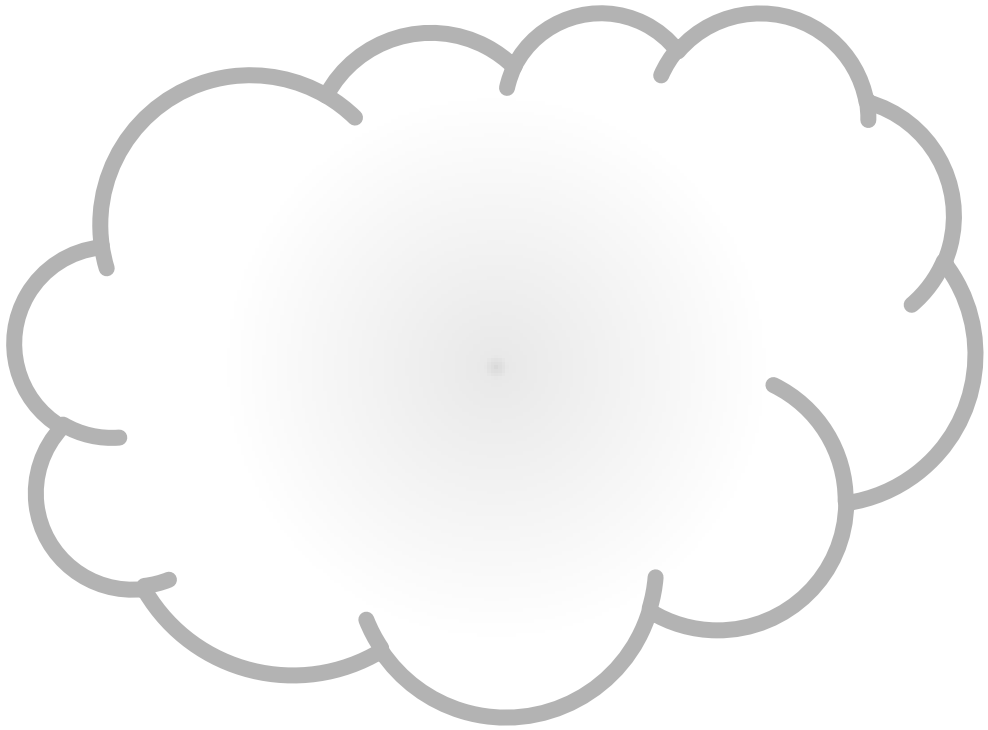
DEFINE THE CLOUD ECOSYSTEM

experience BKD CPAs & Advisors

Define the Cloud Ecosystem

- What is the cloud?
- Define the cloud
- Cloud service models
- Cloud deployment models

Define the Cloud Ecosystem



Define the Cloud Ecosystem

Cloud Computing: 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Source: NIST Special Publication 800-145 - The NIST Definition of Cloud Computing (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

)

Define the Cloud Ecosystem

Essential Characteristics

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Define the Cloud Ecosystem

Service Models

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

Define the Cloud Ecosystem

Software as a Service (SaaS)

Examples

- Sales Force CRM
- Google Apps
- Microsoft Office 365

Define the Cloud Ecosystem

Platform as a Service (PaaS)

Examples

- Microsoft Azure
- Google App Engine

Define the Cloud Ecosystem

Infrastructure as a Service (IaaS)

Examples

- Amazon Web Services (AWS)
- RackSpace
- GoGrid

Audience Question

Are you currently using Cloud Services and if so which service model are you using?

a) Yes – SaaS

b) Yes – PaaS

c) Yes – IaaS

d) Yes – A combination of service models

e) Have not adopted cloud computing at this time

Define the Cloud Ecosystem

Deployment Models

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

Define the Cloud Ecosystem

Private Cloud

- Provisioned for single organization
- May exist on or off site
- May be managed by organization or outsourced

Define the Cloud Ecosystem

Community Cloud

- Provisioned for exclusive use by a specific community
- May be managed by one or more of the community organizations
- May be managed by community organization or outsourced

Define the Cloud Ecosystem

Public Cloud

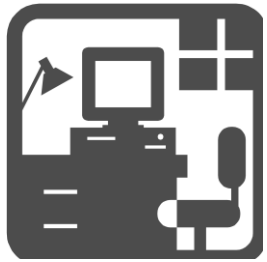
- Provisioned for general public
- Exists on the premise of the cloud provider
- May be owned, managed & operated by a business, academic or government organization or a combination

Define the Cloud Ecosystem

Hybrid Cloud

- Combination of two or more distinct cloud infrastructures
- Combines characteristics of private, public & community clouds

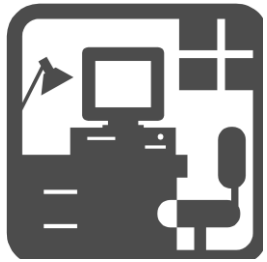
BUSINESS USE OF CLOUD SERVICES



experience BKD CPAs & Advisors

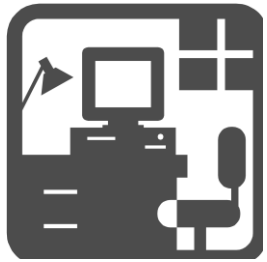
Business Use of Cloud Services

- Financial Savings
  - Equipment
  - Personnel
  - Infrastructure
  - Space & utilities
  - Reduced obsolescence
  - Reduced capital expenditures
  - Reduced implementation costs



Business Use of Cloud Services

- Increased Flexibility
  - Rapid deployment
  - Ability to add or reduce capacity
  - On-demand provisioning
  - Disaster recovery
  - Business expansion (across town or across the globe)



Business Use of Cloud Services

- Streamlined business development
  - Focus on innovation & research
  - Reduced effort on management, maintenance & support
  - Simplified entry into or exiting from business initiatives
  - Increased access to technical expertise

CLOUD SERVICE RISKS

Cloud Service Risks

- Security
  - Physical access to infrastructure, systems & data
  - Physical location of systems, data
  - Logical access to the network, OS, applications & databases
  - Network & data segregation

Cloud Service Risks

- Availability
  - Cloud provider service interruptions
  - Data location/availability for restoration
  - Network/connectivity interruptions
  - Failure of the provider to adhere to SLAs
  - Service provider disaster recovery

Cloud Service Risks

- Processing Integrity
  - Adherence to change management procedures
  - Incident management
  - Failure of the provider to adhere to SLAs
    - ✓Timeliness
    - ✓Accuracy
    - ✓Authorization
    - ✓Completeness

Cloud Service Risks

- Confidentiality
  - Comingling of data & other assets
  - Unauthorized access to sensitive or trade secret information

- Privacy
  - International laws affecting service provider location
  - Regulatory compliance/legal liability
  - Breach & incident management

Audience Question

Are the risks associated with cloud computing (e.g., data security, availability, long term viability, etc.) preventing you from adopting cloud services?

a) Yes

b) No

GOVERNANCE OF THE CLOUD

Critical Policies, Procedures & Controls

experience BKD CPAs & Advisors

Governance of the Cloud

- Governance
- Risk Management
- Tools

Governance of the Cloud

Governance

- Information Security
- Metrics
- Service-Level Agreements

Governance of the Cloud

Governance

- Information Security
  - Data life cycle
  - Data classification
  - Formal policies & procedures

Governance of the Cloud

Governance

- Metrics
  - Objectives
  - Define metrics
  - Periodic assessment & review

Governance of the Cloud

Governance

- Service-Level Agreements
  - Ensure SLAs & contracts give customer access to necessary performance & security data (*e.g.*, audit logs, usage, etc.)
  - Ensure SLAs contain appropriate controls
  - Ensure executive management, legal, IT & business process owners are involved in the SLA development process

Governance of the Cloud

Risk Management

- Data-flow analysis
- Managing risks associated with unique cloud computing components
- Audit & compliance

Governance of the Cloud

Risk Management

- Data-flow analysis
  - Understand the information life cycle
  - Develop data-flow schematics
  - Develop policies to periodically review & update data-flow documentation

Governance of the Cloud

Risk Management

- Managing Cloud Computing Risks
  - Maintain application & technology layer inventory
  - Develop inventory in conjunction with the data-flow analysis
  - Develop controls to address risks associated with each layer of the cloud “stack”

Governance of the Cloud

Risk Management

- Audit & compliance
  - Understanding cloud risks & regulatory implications
  - Leverage existing risk assessment tools & control frameworks
  - Assessing control maturity
  - Vendor management

Governance of the Cloud

Procedures/Tools

- Control frameworks (NIST, COBIT, CSA)
- Data-flow analysis
- The CIS Security Metrics v1.0.0
- Cloud Security Alliance
- NIST 800-146

Audience Question

If your organization is currently utilizing cloud services, have formal documented policies, procedures and controls been developed to address cloud computing specific risks?

a) Yes

b) No

Governance of the Cloud

Procedures/Tools Links

NIST Guidance

- http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

Cloud Security Alliance (CSA)

- https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- https://cloudsecurityalliance.org/research/ccm/

Information System Audit and Control Association (ISACA)

- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Management-Audit-Assurance-Program.aspx

The Center for Internet Security (CIS)

- https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

THIRD-PARTY MANAGEMENT

CONSIDERATIONS FOR THE CLOUD

experience BKD CPAs & Advisors

Third-Party Management

- Use of the cloud
  - Transfers risk
  - Reduces control
- Requires new control considerations
  - Service-level management
  - Third-party management

Third-Party Management

Define & Manage Service Levels

Control Objective - Controls provide reasonable assurance that service levels are defined & managed in a manner that satisfies financial reporting system requirements & provides a common understanding of performance levels with which the quality of services will be measured

Sample Control Activities

1) Service levels are defined & managed to support financial reporting system requirements
2) A framework is defined to establish key performance indicators to manage service level agreements, both internally & externally

Third-Party Management

Manage Third-party Services

Control Objective - Controls provide reasonable assurance that third-party services are secure, accurate & available, support processing integrity & defined appropriately in performance contracts

Sample Control Activities

1) A designated individual is responsible for regular monitoring & reporting on the achievement of the third-party service level performance criteria

2) Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy

Third-Party Management

Sample Control Activities (Continued)

3) IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service & a review of their financial viability

4) Third-party service contracts address risks, security controls & procedures for information systems & networks in the contract between the parties

5) Procedures exist & are followed to ensure that a formal contract is defined & agreed for all third-party services before work is initiated, including definition of internal control requirements & acceptance of the organization's policies & procedures

6) A regular review of security, availability & processing integrity is performed for service- level agreements & related contracts with third-party service providers

Service Organization Control Reports

	SOC 1	SOC 2	SOC 3
Purpose	Report on controls relevant to user entities ICFR [1]	Report on controls related to compliance & operations	Report on controls related to compliance & operations
Use of Report	Restricted [2]	Restricted [3]	General
Report Detail	Includes Testing Detail	Includes Testing Detail	No Testing Detail
AICPA Interpretive Guidance	SSAE 16 & AICPA Guide	AT 101, Trust Services Principles, & AICPA Guide	AT 101 & Trust Services Principles

[1]Internal Control Over Financial Reporting
[2]Service Organization Management, Users, Users Auditor
[3]Service Organization Management, Users, Knowledgeable Parties

SOC 1 – SSAE 16

- SSAE 16 – Focus is on controls relevant to a user entities' internal control over financial reporting (ICFR)

- Typical cloud organizations providing SOC 1 reports
  - SaaS – For processes/ applications impacting ICFR
    - ✓ Third-party administrators
    - ✓ Payroll providers
    - ✓ Tax management
    - ✓ Specialized A/P services
  - IaaS/PaaS – If deemed relevant to ICFR by user management

SOC 1 Content

- Auditor opinion
- Management assertion
- Narrative description of the system
- User considerations
- Control objectives, activities (description & results of testing for Type 2)
- Other relevant unaudited information

SOC 2 Reporting

- Governed by AT 101 – Attestation service
- SSAE 16 guidance also to be used
- Criteria for evaluation is Trust Services Principles (TSP) (not ICFR)
- Risk Basis for control objectives & activities
  - SOC 1/SSAE 16 – ICFR
  - SOC 2 - TSP

SOC 2 Reporting

- TSP Criteria
  - Security
  - Confidentiality of information processed
  - Availability
  - Processing Integrity of the system
  - Privacy of information processed

SOC 2 Reporting

- Limited Use report
  - Users generally user entity management not user auditors
  - Service organization
  - Knowledgeable parties
- Helps user entity management
  - Obtain information about service organization controls
  - Assess & address risks
  - Carry out its responsibility for monitoring

SOC 2 Reporting

- Auditor opinion
- Management assertion
- Narrative description of the system
- User considerations
- Control objectives, activities (description & results of testing for Type 2)
- TSP/control matrix to demonstrate support of selected TSPs
- Other relevant unaudited information

Audience Question

Have you formally inventoried and reviewed all cloud vendor contracts to ensure security controls have been appropriately addressed, measurable service-level agreements are in place and SOC audits have been performed, when required?

a) Yes

b) No

Questions?

experience BKD CPAs & Advisors

Thank You

Rod Walsh* | *Director

IT Risk Services

816.221.6300

rwalsh@bkd.com

experience BKD CPAs & Advisors