

**Navigating Thunderstorms:
Managing Risks in the Cloud**

Daren Kinser – Auditor, UCSD
Jennifer McDonald – Auditor, UCSD

Agenda

- Cloud Computing Overview
- Cloud Related Applications
- Interactive Risk Assessment Exercise

Cloud Computing – What Is It?

- National Institute of Standards and Technology (NIST): “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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”¹

1. Mell, Peter and Tim Grance. “The NIST Definition of Cloud Computing” The National Institute of Standards and Technology, September 2011. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

Five Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Three Service Models

- Software as a Service (SaaS) - Applications hosted by an outside party and accessed via the internet. Avoids the need for complex in-house software installation and management. Examples: Salesforce.com
- Infrastructure as a Service (IaaS) - Resources owned by an outside party and used on a contractual basis.(storage, servers, etc.) Examples: Amazon Elastic Cloud (EC2), Amazon Simple Storage Service (S3), and Rackspace.
- Platform as a Service (PaaS) - Platforms provided by an outside party used for building/running applications. Overlaps with SaaS. Example: Google App Engine

Other “Service Models”

- Network as a Service (NaaS)
- Storage as a Service (SaaS)
- Security as a Service (SECaaS)
- Data Base as a Service (DBaaS)
- Data as a Service (DaaS)

Three Deployment Models

- **Public** - Services offered to anyone regardless of affiliation. All users share the same resources.
- **Private** - Services and resources are supplied by and/or to only a select group like a private company, University, etc.
- **Hybrid** - Using a public cloud provider to build a private cloud. This may also include connections from the cloud resources to the local or other remote resources. Some companies may desire a private cloud but prefer that it's hosted off site.

Advantages

- Elasticity of Computing Resources
- Economy
- Easy Collaboration
- Levels Playing Field
- Reliability
- Disaster Recovery

Disadvantages / Concerns/ (Risks?)

- Security and Privacy
- Availability/Reliability
- Data Ownership
- Performance
- Data Leakage To Public Clouds

Why Now?

- Bandwidth Increases
- Virtualization
- Mobile Devices: Smart Phones, Tablets
- HTML 5

Patchy Clouds With a Chance of Rain

- Governance
 - Contracts and Service Level Agreements are in place
 - Compliance with Regulatory Standards
- Vendor Management
 - Risk Assessment
 - Details specified in contract and Service Level Agreements
- Business Process – Financial and Operational
- Technical – Security and Privacy

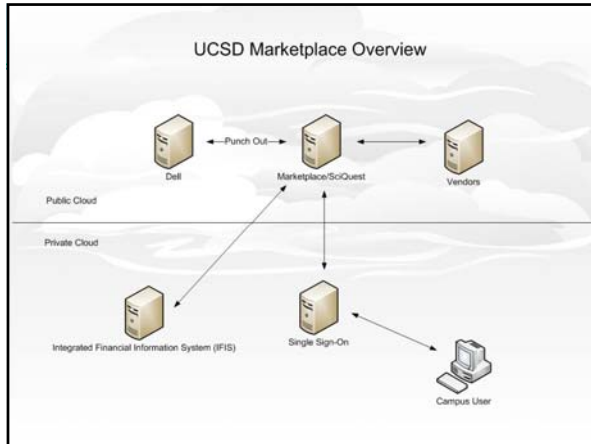
Campus Cloud Related Applications

Private Cloud Activity

- Storage – San Diego Super Computer (SDSC)
- Integrated Financial Information System (IFIS)
- Personnel Payroll System (PPS)
- Electronic Certification of Effort Reporting (ECERT)

Public Cloud Activity (Hosted Solutions)

- Campus Asset Management System (CAMS)
- Marketplace/SciQuest



Business Process Considerations

- Access Controls
- Purchasing Requirements
- Workflow Approval Processes
- Reporting Functions

Risk Assessment – Audit Scoping

- Independent Review – Internal Audit
 - Understand Scope of Services Provided
 - Include Business Process Assessment and Information Flow (Integrated Audit approach)
 - Business Process Residual Risk
 - Evaluating third party assurance reports
 - On-site Visits

