The Cloud Standards Customer Council

THE Customer’s Voice for Cloud Standards!

- Provide customer-led guidance to multiple cloud standards-defining bodies
- Establishing criteria for open standards based cloud computing

2011/2012 Deliverables
- Practical Guide to Cloud Computing
- Establishing criteria for open standards based cloud computing
- Impact of Cloud on Healthcare

2013/2014 Deliverables
- Convergence of SoMoClo
- Analysis of Public Cloud SLAs
- Cloud Security Standards
- Migrating Apps to Public Cloud Services
- Social Business in the Cloud
- Big Data in the Cloud
- Practical Guide to Cloud Computing V2
- Migrating Apps: Performance Rqmmts
- Cloud Interoperability/Portability

2015 Deliverables
- Web App Hosting Architecture
- Mobile Cloud Architecture
- Big Data Cloud Architecture
- Security for Cloud Computing V2
- Practical Guide to Cloud SLAs V2
- Practical Guide to PaaS

2016 Projects
- Prac Guide to Hybrid Cloud Computing
- IoT Reference Architecture
- DevOps Cloud Reference Architecture
- More

550+ Organizations participating

http://cloud-council.org
What is Hybrid Cloud Computing?

Leveraging the capabilities and services of multiple cloud services, particular those from private on-premises and public off-premises, to address a business need in the quickest, most effective manner possible.
Why Hybrid Cloud is important to the business

1. **Enables a highly cost-effective, rapidly responsive and elastic IT, better aligned with the business needs in order to support two speed**

   - Hybrid cloud enables a more responsive and elastic IT that is able to quickly respond to the demands and needs of both steady speed *systems of record* (SoR) and new fast speed *systems of engagement* (SoE).

2. **Provides a portfolio of business and IT services that leverage the best capabilities of cloud service providers, enabling flexibility in what can be built and where it can be deployed.**

   - New tools and data for innovation. The business is no longer constrained by what they have available on premises.

3. **Enables the business to innovate faster while leveraging existing systems and capabilities**

   - The ability to compose services from both on premises and off premises (i.e. hybrid) is a key enabler to increase speed to market and to reduce costs.
# Key Considerations for Hybrid Cloud Computing

## Readiness Assessment

<table>
<thead>
<tr>
<th>Considerations</th>
<th>What to Assess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placement of solution components</td>
<td>What should go where and how should it be designed? Should a solution only include the usage of private dedicated or local cloud resources? How do you leverage available public cloud services?</td>
</tr>
<tr>
<td>Integration with existing enterprise systems</td>
<td>How can existing business applications along with existing management and monitoring systems be leveraged? How will the internetworking be accomplished?</td>
</tr>
<tr>
<td>Handing increased management complexity</td>
<td>How do I manage resources running in different cloud services, particularly public cloud services? The lifecycle of resources involved in supporting key business operations can be transient (short lived and/or move automatically).</td>
</tr>
<tr>
<td>Ensuring that security is considered in all aspects</td>
<td>How do I ensure that both on-premises AND off-premises cloud environments are secure? How about the data stored off-premises? How about the data in transit?</td>
</tr>
<tr>
<td>Rapidly evolving technologies</td>
<td>The speed of capabilities being deployed and or changed in a hybrid cloud changes at a different speed for fast speed resources vs steady speed. How does the organization support this?</td>
</tr>
<tr>
<td>Implementing common operational services</td>
<td>Given that there are multiple providers in play, how can the different backup/recovery solution and networking options enable a seamless environment that meets an organization’s SLAs?</td>
</tr>
<tr>
<td>Ensure regulatory compliance</td>
<td>How will you ensure data placement, data encryption, personal information protection, contractual management (e.g. software licensing) adheres to the appropriate regulations?</td>
</tr>
</tbody>
</table>
Guidance for successful implementation of Hybrid Cloud

Prescriptive guidance for customers to ensure successful implementation of hybrid cloud computing

**Guidance**

1. Determine cloud deployment model
2. Integrate with existing enterprise systems
3. Address connectivity requirements
4. Develop governance policies and service agreements
5. Assess security and privacy challenges
6. Manage the cloud environment

Determine the right deployment model is a key step in the hybrid cloud journey. The two speeds of IT – steady & fast – is a major consideration.

**Model Development**

1. Determine the resource model
2. Rationalize applications and data
3. Apply decision criteria to define the deployment model
4. Consider options for application placement in the hybrid cloud

**Deployment Decision Criteria**

- Flexibility
- Security
- Speed & Automation
- Cost
- Locality
- Service Levels
- System Interdependencies
Integrate with Existing Enterprise Systems

**Integration Actions**

- Insist CSP supports key open technologies
- Ensure on-prem apps leverage SOA design principles
- Determine if in-house systems can handle business aspects of using cloud services
- Consider implementing an Enterprise Service Bus (ESB)
- Leverage third party ID and Access Management
- Establish API Management capabilities to prevent unauthorized access to on-prem data
Address Connectivity Requirements

- Network links
- Network Virtualization
- Security -- VPNs
- Internet Infrastructure
- IP Address Plan
- Management
- DDoS Protection
- Service Continuity
Develop Governance Policies & Service Agreements

Include & Align

- Internal & External
- More Business Participants
- Multiple Vendors
- Escalation Responsibilities

Assess & Harmonize

- System & Service Touch points
- Service Provider Overlap
- Multiple governance types
- Multiple SLAs

Iterate & Sustain

- Change Management & Change Communications
- Measurement & Management Visibility
- Authoritative Source for Escalations

<table>
<thead>
<tr>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Process</td>
<td>Business Process</td>
<td>Business Process</td>
</tr>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>
Address and Resolve Security & Privacy Challenges

- Clarify significant risks
- Be realistic: Security may be *better* in the cloud!
- 10 steps proposed for the specific case of application migration

Also see the CSCC’s *Security for Cloud Computing: 10 Steps to Ensure Success*
http://www.cloud-council.org/resource-hub.htm#security-for-cloud-computing-10-steps-to-ensure-success

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Understand what data will migrate</td>
</tr>
<tr>
<td>2.</td>
<td>Map it to security classification</td>
</tr>
<tr>
<td>3.</td>
<td>Identify the privacy concerns</td>
</tr>
<tr>
<td>4.</td>
<td>Examine applicable regulations</td>
</tr>
<tr>
<td>5.</td>
<td>Apply a risk management method (probability, impact, mitigation)</td>
</tr>
<tr>
<td>6.</td>
<td>Review cloud provider’s measures</td>
</tr>
<tr>
<td>7.</td>
<td>Go/No-Go decision based on the above</td>
</tr>
<tr>
<td>8.</td>
<td>Protect data in transit and at rest</td>
</tr>
<tr>
<td>9.</td>
<td>Design authentication and authorization method (SSO, etc.)</td>
</tr>
<tr>
<td>10.</td>
<td>Put in place a rapid de-provisioning process</td>
</tr>
</tbody>
</table>
Critical Steps

1. Analyze management processes and use cases that need to be implemented
2. Analyze on-premises management tooling
3. Analyze CSP management functions and the service responsibility line

### Cloud Service provider vs. On-premises

<table>
<thead>
<tr>
<th>Cloud Service provider</th>
<th>On-premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customized ISM processes</td>
<td>Service Mgmt Environment (*)</td>
</tr>
<tr>
<td>Service Mgmt environment</td>
<td>Managed-workload</td>
</tr>
<tr>
<td>Managed-workload</td>
<td>Managed-workload</td>
</tr>
</tbody>
</table>

#### Integrated pattern
- Leverage both on-premises and built-in cloud ISM capabilities and tools
- Use APIs to get mgmt data from cloud and feed to on-prem mgmt tools and processes

#### On-premises pattern
- Extend on-premises management tools and agents to manage also workload on cloud
- Do not leverage built-in service mgmt capabilities from cloud provider

#### Dual pattern
- Use ISM tools and interfaces on-premises and provided by cloud service provider
- Integrate them manually or at process level documenting cross management best-practices and procedures
## Consider Backup, Archive, Disaster Recovery

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Details</th>
</tr>
</thead>
</table>
| **1. Choosing a hybrid cloud backup, archive and DR solution** | ▪ Highly available and fault tolerant. Global presence with built-in solutions for DR  
▪ Choose a DR performance model to accommodate solution: active-active, active-passive or passive  
▪ In public cloud, select CSP offerings for location and type of backup |
| **2. Hybrid cloud-based solution satisfies all your requirements** | ▪ Consider current IT patterns, business requirements, regulatory and compliance issues with respect to data  
▪ If data is in the public cloud, data is archived to locations supported by the cloud service provider (CSP)  
▪ Evaluate if the data replication available from the provider offers you control over replication and/or data consistency |
| **3. Create a Disaster Recovery (DR) Plan** | ▪ Prepare for disaster, ensure ability to access DR configuration information  
▪ Ability to restart operations in full compliance with expectations (RTO and RPO) |
| **4. The CSP will not provide DRaaS** | ▪ Hybrid cloud allows velocity for emergency business opportunities and supports hosting strategy  
▪ Necessary to secure resources internally to provide on-demand DR services  
▪ Explicitly defined SLA with details of DR service offerings |
Call to Action

- **Join the CSCC Now!**
  - To have an impact on customer use case based standards requirements
  - To learn about all Cloud Standards within one organization
  - To help define the CSCC’s future roadmap
  - Membership is free & easy: [http://www.cloud-council.org/become-a-member.htm](http://www.cloud-council.org/become-a-member.htm)

- **Get Involved!**
  - Join one or more of the CSCC Working Groups
    [http://www.cloud-council.org/workinggroups.htm](http://www.cloud-council.org/workinggroups.htm)

- **Leverage CSCC Collateral**
  - Visit [http://www.cloud-council.org/resource-hub.htm](http://www.cloud-council.org/resource-hub.htm)
Thank You