## Speakers

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracie Berardi</td>
<td>Program Manager, Cloud Standards Customer Council, Moderator</td>
</tr>
<tr>
<td>Claude Baudoin</td>
<td>Principal, cébé IT &amp; Knowledge Management, Steering Committee member, Cloud Standards Customer Council</td>
</tr>
<tr>
<td>Ash Heda</td>
<td>Cloud Architect, Wipro</td>
</tr>
<tr>
<td>Srinivasa Reddy Karri</td>
<td>IT Security Manager, Schlumberger</td>
</tr>
</tbody>
</table>
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

700+ Organizations participating

2018 Projects

• Migrating Apps to Public Cloud Services: Roadmap for Success v2.0
• Best Practices for Developing and Growing a Cloud-Enabled Workforce
• Cloud Customer Architecture for Artificial Intelligence
• And more!

2017 Deliverables

• Cloud Customer Architecture for Hybrid Integration
• Impact of Cloud Computing on Healthcare v2.0
• Cloud Customer Architecture for API Management
• Data Residency Challenges
• Cloud Customer Architecture for Blockchain
• Cloud Customer Architecture for Big Data and Analytics v2.0
• Hybrid Cloud Considerations for Big Data and Analytics
• Practical Guide to Cloud Management Platforms
• Practical Guide to Cloud Computing v3.0
• Interoperability and Portability for Cloud Computing: A Guide v2.0
• Security for Cloud Computing: 10 Steps to Ensure Success v3.0

http://cloud-council.org
Migrating Applications to Public Cloud Services: Roadmap to Success V2.0

Recommended steps end users should take to ensure successful migration of existing applications to cloud computing

Initially published Dec. 2013
V2.0 published Feb. 2018

6 Steps to Ensure Successful Migration

1. Assess your applications and workloads
2. Build the business case
3. Develop the technical approach
4. Adopt a flexible integration model
5. Address security, privacy and data residency req't's
6. Manage the migration

Conclusion, Appendices, References

What’s New in Version 2.0?

- Strengthened the motivation section
- Explained the difference between applications and workloads, and strengthened Appendix A which explores this in further detail
- Improved the “costs and savings” section of Step 1
- Expanded the technical approach (Step 3) to include containers-as-a-service (CaaS) and function-as-a service (FaaS) models, and added patterns
- Expanded the integration and migration models (Step 4) to explain options such as redesigning for microservices
- Added data residency issues to Step 5 on security and privacy (restructured, mentioned the GDPR impact)
- Revised and strengthened the migration procedure (Step 6 + Appendix B)
- Added new references (and moved all to Appendix C)
## Step 1: Assess Your Applications and Workloads

### Readiness Assessment

<table>
<thead>
<tr>
<th>Considerations</th>
<th>What to Assess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>• Organization readiness, impact on the business, risk tolerance level, innovation culture, need to reach new client-oriented KPIs</td>
</tr>
<tr>
<td>Application Lifecycle</td>
<td>• New, up for refresh, approaching retirement?</td>
</tr>
<tr>
<td></td>
<td>• Ease of redesigning for cloud computing</td>
</tr>
<tr>
<td>Architecture</td>
<td>• Web-based? SOA? N-tier? APIs?</td>
</tr>
<tr>
<td></td>
<td>• Suitable for microservices?</td>
</tr>
<tr>
<td>Data</td>
<td>• Assess the integrity, privacy, residency and compliance requirements of the data</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>• Account for performance, resiliency, high availability and disaster recovery</td>
</tr>
<tr>
<td>Security</td>
<td>• Identify significant risks, ensure proper treatment, and clearly define responsibilities</td>
</tr>
<tr>
<td>Integration</td>
<td>• Understand control, data and presentation integration requirements</td>
</tr>
</tbody>
</table>
**Business Impact**
- Revenue impact
- Customer acquisition or engagement impact
- User satisfaction
- Time to market improvements

**Service Levels**
- Application availability
- Application performance
- Application security
- Privacy
- Regulatory compliance

**Savings Analysis**
- Move from CAPEX to OPEX
- Savings on handling of peak loads
- Contract duration flexibility
- Staff reduction or reassignment

**Cost Analysis**
- On-going cloud service costs
- Service management
- Security Management
- License management
- Application re-designs
- Data and application integration
- Application deployment and testing
- Application maintenance and administration
- Human resources, training and talent management
Step 3: Develop the Technical Approach

- Most substantial step in the paper (5 pages)
- Adds new information about the CaaS and FaaS service models
• Technical considerations for migration
  • Skills: Do your employees have cloud services skills?
  • Security: Ensure adequate security – with integration
  • Integration: Data and applications, between cloud service & on-premises
  • Monitoring and management: How will migrated app be handled?
  • Scalability: Can migrated app take advantage of cloud service scalability?
  • Availability and backup: How will these be achieved?

• Impact on DevOps / Continuous Delivery

• Consider the use of *Patterns*
  • Standard architectural organization for specific application requirements
  • Ranges of patterns are documented and available
**Step 4: Adapt a Flexible Integration Model**

### Needs, Scope and Types

- **Needs**
  - End-to-end workflows
  - Master data management
  - Single sign-on
  - Remote monitoring
  - API management

- **Scope**
  - Cloud to cloud
  - Cloud to on-premises

- **Types of integration**
  - Control (mutual invocation)
  - Data (access to same databases)
  - Presentation (mashup on user interface)

### Principles

- Flexibility
- Standards
- Opportunity for modernization
- “T-shirt sizing” (S/M/L/XL) of effort per integration point

### Integration Patterns

- One-by-one redesign
- Move entangled of apps at one time
- Caching & synchronization
- Microservices
- Enterprise Service Bus (ESB) extending to the cloud
- Special cloud integration solutions
### Step 5: Address Security, Privacy, and Data Residency Requirements

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


<table>
<thead>
<tr>
<th>Step</th>
<th>Description</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 during bulk migration, in transit, at rest, and during use</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>
## Step 6: Manage the Migration

<table>
<thead>
<tr>
<th>Migration Procedure</th>
<th>Migration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Deploy the Cloud Environment</strong></td>
<td>▪ Storage, servers, network, security resources</td>
</tr>
<tr>
<td><strong>2. Implement monitoring &amp; management services</strong></td>
<td>▪ Organization, responsibility matrix, processes and procedures (e.g., ITIL-based), toolchains</td>
</tr>
</tbody>
</table>
| **3. Install & configure the applications & middleware** | ▪ Applications and supporting middleware  
▪ Often done by providers through automated templates  
▪ Perform integrations                                  |
| **4. Harden the Production Environment**                 | ▪ Additional utilities for business continuity and security  
▪ If part of the cloud service offering, test them                                           |
| **5. Mock Migration**                                   | ▪ Trial run of the migration project plan  
▪ Purpose: uncover issues  
▪ Allow time between the mock migration and the final cutover to fix problems              |
| **6. Operational readiness testing**                     | ▪ Test incident readiness, backup/DR, failure modes  
▪ Review coverage of all migration responsibilities                                               |
| **7. Cutover to Production Cloud**                       | ▪ Serious issues found? Go back to previous steps  
▪ No serious issues: plan real migration, execute, follow up                                    |
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: [www.cloud-council.org/become-a-member](http://www.cloud-council.org/become-a-member)

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

- **Leverage CSCC Collateral**
  - Visit [http://www.cloud-council.org/resource-hub](http://www.cloud-council.org/resource-hub)
Some Additional Resources

- **Interoperability and Portability for Cloud Computing: A Guide V2.0**

- **Migrating Applications to the Cloud: Assessing Performance and Response Time Requirements**

- **Practical Guide to Cloud Computing Version 3.0**

- **Security for Cloud Computing: 10 Steps to Ensure Success Version 3.0**

- **Practical Guide to Cloud Service Agreements Version 2.0**

- **Practical Guide to Cloud Management Platforms**
Thank You