Security for Cloud Computing: 10 Steps to Ensure Success Version 3.0
## Speakers

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracie Berardi</td>
<td>Program Manager&lt;br&gt;Cloud Standards Customer Council&lt;br&gt;Moderator</td>
</tr>
<tr>
<td>Claude Baudoin</td>
<td>Principal, cébé IT &amp; Knowledge Management&lt;br&gt;Cloud Standards Customer Council&lt;br&gt;Steering Committee member</td>
</tr>
<tr>
<td>Mike Edwards</td>
<td>Cloud Computing Standards expert&lt;br&gt;IBM Cloud PaaS Evangelist</td>
</tr>
<tr>
<td>Chris Dotson</td>
<td>Senior Technical Staff Member and Executive Architect, IBM Watson and Cloud Platform</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

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
- Security for Cloud Computing: 10 Steps to Ensure Success v3.0
- Interoperability and Portability for Cloud Computing: A Guide v2.0

2018 Projects
- Migrating Apps to Public Cloud Services: Roadmap for Success v2.0
- Cloud Customer Architecture for Artificial Intelligence
- And more!

700+ Organizations participating

http://cloud-council.org
Revision Highlights

- New worldwide privacy regulations taken into account
- New and updated cloud security standards added
- Data residency considerations added
- More emphasis given to security logging and monitoring
- Information governance framework highlighted more prominently
- Key management services to safeguard cryptographic keys added
- Security for continuous delivery and deployment explained
- Managing identity and access of services emphasized
- References to additional CSCC Security whitepapers added
Despite inherent loss of control implied by adoption of cloud computing, customers must take responsibility for impact on security and privacy for their business.
CSCC Security for Cloud Computing: 
10 Steps to Ensure Success

A reference to help enterprise IT & business decision makers as they analyze and consider the security implications of cloud computing on their business.

10 Steps to Manage Cloud Security

1. Ensure effective governance, risk & compliance
2. Audit operational & business processes
3. Manage people, roles & identities
4. Ensure proper protection of data & information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks & connections are secure
8. Evaluate security controls on physical infrastructure & facilities
9. Manage security terms in the cloud service agreement
10. Understand the security requirements of the exit process

“The CSCC has created a practical guide to help those with information security expertise as well as those that don’t have domain expertise. This work will help organizations step through ten areas to be cognizant of when evaluating cloud providers. The end effect is helping companies avoid decisions that put their data and service at risk.” Ryan Kean, Senior Director, Enterprise Architecture, The Kroger Company
Step 1: Ensure effective governance, risk and compliance

**GRC Requirements**

- Cloud computing presents different risks than traditional IT solutions
- A formal information governance framework establishes chains of responsibility, authority, and communication
- Customers must understand their risk tolerance and must focus on mitigating risks most crucial to the organization
- Customers must fully understand specific laws or regulations that apply to the services (data retention, privacy requirements, etc.)
- Customers should be notified if any breach occurs regardless if the customer is directly impacted
- Primary means to ensure application and data security is through Cloud Service Agreement

ISO 27018: Data Protection for Cloud Services
ISO 27017: Information Security Controls for Cloud Services
Step 2: Audit operational & business processes

Audit Requirements

- Security audit of cloud service providers is essential
- Security audits should be carried out by appropriately skilled staff
- Security audits should leverage an established standard for security controls
- Typically done as part of a formal certification process

Critical Focus Areas

- Understand the internal control environment of the provider
  - Ensure isolation in a multi-tenant environment
  - Provide protection of customer assets from provider’s staff
- Ensure appropriate access to provider’s events, logs and audit trail
- Self manage and monitor the usage of cloud hosted services

©2018 Cloud Standards Customer Council
Step 3: Manage people, roles & identities

Considerations

- **Key principle:** limit access to what each role requires
- Cloud service provider should support:
  - Federated identity management and/or single sign-on (see platforms at right)
  - Delegated user administration
  - Strong, multi-factor authentication
  - Role, entitlement and policy management
  - Identity and access auditing and reporting – needed by customers for assurance and regulatory compliance
  - Service identity & access management
- Monitoring and logging of access to the provider’s management platform
Step 4: Ensure proper protection of data & information

Considerations

- Data protection is a component of enterprise risk management
- It is about confidentiality, integrity, availability
- Applies to data at rest as well as data in motion
- Cloud deployment model (XaaS) affects who is responsible for handling security controls
- List of key controls for securing data in the cloud:
  - Create a data asset catalog (considering all forms of data)
  - Consider privacy requirements (see Step 5)
  - Require security logging and monitoring (particularly, data activity monitoring)
  - Require proactive notification of incidents

ISO 27017
Information Security Controls for Cloud Services
### Step 5: Enforce privacy policies

#### Considerations

- **Privacy is distinct from security.** It’s mostly about handling of *personally identifiable information (PII)*
  - Includes right to inspect and correct data, and in some cases to be forgotten

- **Evolving and gaining importance**
  - Multiple law and regulations (e.g., HIPAA)
  - EU’s GDPR (in force from 25 May 2018)

- **PII must be tagged correctly, stored securely** (e.g., encrypted, anonymized or obfuscated), and made available only to authorized users

- *Primary responsibility typically remains with the cloud customer*
  - In the Cloud Services Agreement, define clearly customer vs provider responsibilities

- Customers should monitor compliance
Step 6: Assess the security provisions for cloud applications

Considerations

- Organizations must apply same diligence to application security in the cloud as in a traditional IT environment.
- Split of responsibilities between customer and cloud provider depends on the deployment model:
  - **IaaS:**
    - Customer responsible for most security components
  - **Platform as a Service**
    - Provider responsible for secure operating system, middleware, network, etc.
    - Customer responsible for application security
  - **Software as a Service**
    - Provider provides application security
    - Customer must understand data encryption standards, audit capabilities, SLAs
- Incorporate security into a continuous delivery and deployment approach: DevOps → SecDevOps
Step 7: Ensure cloud networks & connections are secure

Considerations

- Customer should gain assurance on provider’s internal and external network security

- External network requirements
  - Traffic screening
  - Denial of service protection
  - Intrusion detection and prevention
  - Logging and notification

- Internal network requirements
  - Protect clients from each other
  - Allow for network segmentation
  - Protect the provider’s network
  - Monitor for intrusion attempts
Step 8: Evaluate security controls on physical infrastructure & facilities

Considerations

- Customer should gain assurance on provider’s physical security
  - Physical infrastructure & facilities should be in a secure area
  - Protection against external and environmental threats
  - Control of personnel in working areas
  - Equipment security controls
  - Controls on supporting utilities
  - Control security of cabling
  - Proper equipment maintenance
  - Control of removal and disposal of assets
  - Human resource security
  - DR and BC plans in place
Step 9: Manage security terms in the cloud service agreement (CSA)

- Security clauses in the CSA apply to cloud provider as well as any peer providers used to supply part of the service
- CSA should explicitly document that the provider must notify the customer of any breach in their system
- Establish metrics for performance and effectiveness of information security management
- Require data compliance reports to communicate the strengths and weaknesses of controls, services and mechanisms.
- Responsibilities will differ between IaaS, PaaS, and SaaS.
Step 10: Understand the security requirements of the exit process

Considerations

- Once termination process is complete, “the right to be forgotten” should be achieved
- No customer data should reside with provider after the exit process
- Require provider to cleanse log and audit data
  - Some jurisdictions may require retention of records of this type for specified periods by law
- Exit process must allow customer a smooth transition without loss or disclosure of data
Cloud computing can have a positive impact on security and privacy for customer organizations.

Cloud computing presents unique security and privacy challenges that need to be addressed.

Cloud security and privacy is a joint responsibility between customers and providers:
- Customers do not abdicate sole responsibility to their provider.

Responsibility split needs to be formalized in the Cloud Services Agreement.
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](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)
Additional CSCC Resources

- Data Residency Challenges

- Cloud Customer Architecture for Securing Workloads on Cloud Services
  - [http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-securing-workloads-on-cloud-services.htm](http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-securing-workloads-on-cloud-services.htm)

- Cloud Security Standards: What to Expect and What to Negotiate v2.0

- Practical Guide to Cloud Service Agreements v2.0

- Public Cloud Service Agreements: What to Expect and What to Negotiate v2.0

- Practical Guide to Cloud Computing v3.0

- Migrating Applications to Public Cloud Services: Roadmap for Success

- Practical Guide to Hybrid Cloud Computing

- Practical Guide to Platform-as-a-Service

- Practical Guide to Cloud Management Platforms
Thank You!

Join the conversation

www.cloud-council.org