Get Your Head in the Cloud
What Auditors Need to Know About Cloud Technologies

Jason Sechrist
Director of Audit Solutions
AuditBoard
Jason Sechrist
Director of Audit Solutions
AuditBoard
Why Are We Here?

• Level Set on What is “Cloud”
• Understand why risks are different in the Cloud
• What can Internal Audit do?
• Understand how a Service Organization Control (SOC) report maps back to your organization’s specific risks
• Identify requirements that Internal Auditors should be engaged with cloud service providers early in on their organization’s procurement/design phase
MY REPORT COMES TO THE CONCLUSION THAT CLOUD TECHNOLOGY IS OF NO USE TO THIS COMPANY. I’LL UPLOAD IT TO DROP BOX SO YOU CAN TAKE A LOOK AT IT.
Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as 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”

<table>
<thead>
<tr>
<th>IT capabilities provided by the Cloud are characterized by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Usually pay as you use – but can be a subscription</td>
</tr>
<tr>
<td>• Geographic independence</td>
</tr>
<tr>
<td>• Shared physical infrastructure not visible to the customer</td>
</tr>
<tr>
<td>• On demand allocation of resources</td>
</tr>
<tr>
<td>• Provided over the internet</td>
</tr>
<tr>
<td>• Highly Scalable</td>
</tr>
</tbody>
</table>
Service Models & Responsibilities

Traditional IT
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Visualization
- Servers
- Storage
- Networking

Infrastructure (as a Service)
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Platform (as a Service)
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Software (as a Service)
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking
## Service Models & Responsibilities

<table>
<thead>
<tr>
<th>Traditional IT</th>
<th>Infrastructure (as a Service)</th>
<th>Platform (as a Service)</th>
<th>Software (as a Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dining Table</td>
<td>Dining Table</td>
<td>Dining Table</td>
<td>Dining Table</td>
</tr>
<tr>
<td>Soda</td>
<td>Soda</td>
<td>Soda</td>
<td>Soda</td>
</tr>
<tr>
<td>Electric / Gas</td>
<td>Electric / Gas</td>
<td>Electric / Gas</td>
<td>Electric / Gas</td>
</tr>
<tr>
<td>Oven</td>
<td>Oven</td>
<td>Oven</td>
<td>Oven</td>
</tr>
<tr>
<td>Fire</td>
<td>Fire</td>
<td>Fire</td>
<td>Fire</td>
</tr>
<tr>
<td>Pizza Dough</td>
<td>Pizza Dough</td>
<td>Pizza Dough</td>
<td>Pizza Dough</td>
</tr>
<tr>
<td>Tomato Sauce</td>
<td>Tomato Sauce</td>
<td>Tomato Sauce</td>
<td>Tomato Sauce</td>
</tr>
<tr>
<td>Toppings</td>
<td>Toppings</td>
<td>Toppings</td>
<td>Toppings</td>
</tr>
<tr>
<td>Cheese</td>
<td>Cheese</td>
<td>Cheese</td>
<td>Cheese</td>
</tr>
</tbody>
</table>

**Made at Home**

**Take & Bake**

**Pizza Delivered**

**Dined Out**

---

Get Your Head in the Cloud
# Deployment Models & Uses

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Deployment Model</th>
</tr>
</thead>
</table>
| **Private Cloud**  | • Operated solely for an organization  
• May be managed by the organization or a third party  
• May exist on or off premise |
| **Public Cloud**   | • Made available to the general public  
• Owned by an organization selling cloud services |
| **Hybrid Cloud**   | • A composition of two or more clouds (private, community or public) that remain unique entities, but are bound together or by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). |
## Service Levels

<table>
<thead>
<tr>
<th>Service Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Unmanaged Cloud**| • Managed by the organization  
• Organization is responsible for the environment architecture, build, and ongoing operations  
• May be public or private cloud |
| **Managed Cloud**  | • Managed by a third party  
• Assists with the environment architecture and build  
• Manages ongoing operations such as configuration management and backups  
• May be public or private cloud |
Benefits to the Business

• Manage costs – utility model (pay as you go)
• Accelerated deployment
• Maximize performance
• Highly scalable
• Leverage external operational expertise
• Enables company to focus on core competencies
Is Your Organization on “The Cloud”?  

On average, companies are using **4.9 clouds** across both public and private. Respondents are already running applications in 3.4 clouds and experimenting with 1.5 more.

<table>
<thead>
<tr>
<th># of Public + Private Clouds Used</th>
<th>Average</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Using</td>
<td>3.4</td>
<td>3.0</td>
</tr>
<tr>
<td>Experimenting</td>
<td>1.5</td>
<td>1.0</td>
</tr>
<tr>
<td>Total</td>
<td>4.9</td>
<td>4.0</td>
</tr>
</tbody>
</table>
In your opinion, what is the top challenge to adopting cloud technologies?

A. Security
B. Governance/Compliance
C. Lack of Resources/Expertise
D. Performance
E. Managing Cloud Spending
# Top Challenges Facing Cloud Adoption

<table>
<thead>
<tr>
<th>Cloud Challenges – Enterprise</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Cloud Spend</td>
<td>84%</td>
</tr>
<tr>
<td>Governance</td>
<td>77%</td>
</tr>
<tr>
<td>Security</td>
<td>81%</td>
</tr>
<tr>
<td>Compliance</td>
<td>79%</td>
</tr>
<tr>
<td>Lack of Resources/Expertise</td>
<td>79%</td>
</tr>
<tr>
<td>Managing Multi-Cloud</td>
<td>68%</td>
</tr>
<tr>
<td>Cloud Migration</td>
<td>73%</td>
</tr>
</tbody>
</table>

*Not asked in 2018*

Source: RightScale 2019 State of the Cloud Report from Flexera
**Top Challenges for SaaS**

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Cost Implications of Software Licenses</td>
<td>52%</td>
</tr>
<tr>
<td>Complexity of License Rules in Public Cloud</td>
<td>42%</td>
</tr>
<tr>
<td>Ensuring We Follow License Rules</td>
<td>41%</td>
</tr>
<tr>
<td>Ensuring We Don’t Use Too Many Licenses</td>
<td>36%</td>
</tr>
<tr>
<td>Discovering What Software Is Used in Cloud</td>
<td>31%</td>
</tr>
<tr>
<td>Knowing When Licenses Are No Longer Used in Cloud</td>
<td>30%</td>
</tr>
</tbody>
</table>

*Source: RightScale 2019 State of the Cloud Report from Flexera*
Where Should Internal Audit Start?

Over 1/3 of Cloud Spend is WASTE!

% of Cloud Spend Wasted

27% Self-Estimated Wasted Spend
8% Additional Wasted Spend Measured by Flexera

Source: RightScale 2019 State of the Cloud Report from Flexera
Leverage Discounts

In addition, cloud users are not taking advantage of all the available discounts from cloud providers. Fewer than half of AWS users (47 percent) leverage Reserved Instances, and only 23 percent of Azure users do so.

<table>
<thead>
<tr>
<th>Discount Type</th>
<th>AWS</th>
<th>Azure</th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Reserved Instances – 47%</td>
<td></td>
<td>Enterprise Agreement – 30%</td>
<td>Committed Use Discounts – 10%</td>
</tr>
<tr>
<td>AWS EDP (Enterprise Discount) – 26%</td>
<td></td>
<td>Azure Reserved Instances – 23%</td>
<td>Ad Hoc Negotiated Discounts – 5%</td>
</tr>
<tr>
<td>AWS Spot Instances – 26%</td>
<td></td>
<td>Azure Hybrid Benefit – 15%</td>
<td></td>
</tr>
<tr>
<td>Ad Hoc Negotiated Discounts – 12%</td>
<td></td>
<td>Azure Low Priority VMs – 9%</td>
<td></td>
</tr>
</tbody>
</table>

Source: RightScale 2019 State of the Cloud Report from Flexera
Policies to Optimize Cloud Costs

% of Respondents

- Shutdown Workloads After Hours: 35% Automated, 36% Manual
- Rightsize Instances: 31% Automated, 49% Manual
- Required Tags: 32% Automated, 38% Manual
- Specify Expiration Dates: 29% Automated, 38% Manual
- Eliminate Inactive Storage: 24% Automated, 49% Manual
- Software License Compliance: 22% Automated, 53% Manual
- Allowed Instance Sizes/Types: 21% Automated, 50% Manual
- Underutilized Discounts: 21% Automated, 44% Manual
- User Lowest-Cost Cloud: 15% Automated, 42% Manual
- Use Lowest-Cost Regions: 15% Automated, 47% Manual

Source: RightScale 2019 State of the Cloud Report from Flexera
Security Concerns – Top Cloud Threats

- Data Breaches
- Weak Identity, Credential and Access Management
- Insecure APIs
- System and Application Vulnerabilities
- Account Hijacking
- Malicious Insiders

- Advanced Persistent Threats (APTs)
- Data Loss
- Insufficient Due Diligence
- Abuse and Nefarious Use of Cloud Computing
- Denial of Service
- Shared Technology Issues

Source: Cloud Security Alliance (CSA) – The Treacherous 12: Cloud Computing Threats
## Data Breach Costs – 2018 Ponemon Institute

### Global Study At a Glance

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost/Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Total Cost of a Data Breach:</td>
<td>$3.86 million</td>
</tr>
<tr>
<td>Average Cost Per Lost or Stolen Record:</td>
<td>$148</td>
</tr>
<tr>
<td>Likelihood of a Recurring Material Breach Over the Next Two Years:</td>
<td>27.9%</td>
</tr>
<tr>
<td>Average Total One-Year Cost Increase:</td>
<td>6.4%</td>
</tr>
<tr>
<td>One-Year Increase in Per Capita Cost:</td>
<td>4.8%</td>
</tr>
<tr>
<td>Average Cost Savings with an Incident Response Team:</td>
<td>$14 per record</td>
</tr>
</tbody>
</table>
Why Things are Different in the Cloud

Life Before the Cloud
- Access via managed devices/networks
- Layers of defense protecting internal apps
- Known security perimeter

Life With the Cloud
- Any user, any device access
- Users making decisions on sharing
- Clouds talking to other clouds
- Limited visibility/tools by cloud provider
How Cloud Threats are Different

- Infecting Devices: Local Network Backdoors, Multiple Layers of Security, On Private Cloud
- Versus
- Infecting Users: Cloud Application Backdoors, Immediate Access to Data, Cloud to Cloud Ecosystems
Identify/Discover

- Managed & Unmanaged Devices
- Users/Roles
- Device Posture
- IP Addresses

- What are the “sanctioned services” at your organization?
- How much insight do you have into “Shadow IT”?
Malicious Attack or Targets of Opportunity?

- Human Error: 27%
- System Glitch: 25%
- Malicious or Criminal Attack: 48%

Source: 2018 Ponemon Institute Study
Top Security Breaches of 2018

MyFitness Pal
What: 150 million usernames/passwords
How: “Unauthorized party gained access”

Quora
What: 100 million username/passwords and security questions
How: “Malicious third party accessed a system”

Cathay Pacific
What: 9.4 million passports, credit card and other personal data
How: “Passenger data was accessed with authorization”
Monitor and Response

Reduce the number of admin users*

- **4%**
  - Of an average company’s Google Apps users are admin

- **2%**
  - Of an average company’s Box users are admins

- **7%**
  - Of an average company’s Salesforce users are admins

**Monitor 3rd party apps** (cloud-to-cloud activities)

**Monitor Backdoors**
Incident response plan

**Monitor Admins**

Source: ISACA CSX presentation, Aug 18, 2015
Cloud Security Alliance – Controls Matrix

- Controls derived from guidance
- Applicable to SaaS/PaaS/IaaS
- Customer vs. CSP roles
- Mapped to familiar frameworks
- Helps bridge the “cloud gap” for IT & IT auditors
Taking the Initiative

- Internal Audit due diligence in the Procurement Process
- Validation of business case
- Right to Audit Clause and/or SSAE 18
- Impact of regulations on data security
- Contractual data protection responsibilities and related clauses
- SLAs (including security breach escalation protocol)
- Ask for CSP transparency to provide near real-time access that addresses auditing requirements
...applicable developer guides) as posted by us and updated by us from time to time on the AWS Site.
1.3. You will provide information or other materials related to Your Content (including copies of any client-side applications) as reasonably requested by us to verify your compliance with the Agreement.

We may monitor the external interfaces (e.g., ports) of Your Content to verify your compliance with the Agreement. You will not block or interfere with our monitoring, but you may use encryption technology or firewalls to help keep Your Content confidential. You will reasonably cooperate with us to identify the source of any problem with the Services that we reasonably believe may be attributable to Your Content or any end user materials that you control.
1.4. If we reasonably believe any of Your Content violates the law, infringes or misappropriates the rights of any third party or otherwise violates a material term of the Agreement (including the documentation...
Google Cloud Platform Service Terms

...the Services, as applicable. Google warrants that it will provide the Services in accordance with the applicable SLA (if any).

12. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS AGREEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GOOGLE AND ITS SUPPLIERS DO NOT MAKE ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE AND ITS SUPPLIERS ARE NOT RESPONSIBLE OR LIABLE FOR THE DELETION OR FAILURE TO STORE ANY CUSTOMER DATA AND OTHER COMMUNICATIONS MAINTAINED OR TRANSMITTED THROUGH USE OF THE SERVICES.

CUSTOMER IS SOLELY RESPONSIBLE FOR SECURING AND BACKING UP ITS APPLICATION, PROJECT, AND CUSTOMER DATA.

NEITHER GOOGLE NOR ITS SUPPLIERS, WARRANTS THAT THE OPERATION OF THE SOFTWARE OR THE SERVICES WILL BE ERROR-FREE OR UNINTERRUPTED. NEITHER THE SOFTWARE NOR THE SERVICES ARE DESIGNED, MANUFACTURED, OR INTENDED FOR HIGH RISK ACTIVITIES.

13. Limitation of Liability.

13.1 Limitation on Indirect Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY, NOR GOOGLE’S SUPPLIERS, WILL BE LIABLE UNDER THIS AGREEMENT FOR...
Get Your Head in the Cloud

Dropbox Service Terms

...minimum term you have paid us for, we’ll refund the portion of the fees you have pre-paid but haven’t received Services for.

Services “AS IS”
We strive to provide great Services, but there are certain things that we can’t guarantee. TO THE FULLEST EXTENT PERMITTED BY LAW, DROPBOX AND ITS AFFILIATES, SUPPLIERS AND DISTRIBUTORS MAKE NO WARRANTIES, EITHER EXPRESS OR IMPLIED, ABOUT THE SERVICES. THE SERVICES ARE PROVIDED "AS IS." WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some places don’t allow the disclaimers in this paragraph, so they may not apply to you.

Limitation of Liability
WE DON’T EXCLUDE OR LIMIT...
SOC Reports

Items to review in a SOC report

• Time period covered by SOC report (may need a bridge letter)
• Verify that the report is a type II report
• Review any testing exceptions and determine the impact to your assessment
• Consider the service auditor’s professional reputation
• Review complimentary User Entity Controls (UEC) and verify that these are inplace at your organization
• Does the script of the system include a subservience organization? Is the Inclusive or Carve Out method used?
SOC Reports

SOC reports do not eliminate Customer responsibilities

For Examples:

Service Provider control:
“Backup software is used to schedule and perform backups on customer servers.”

Customer Responsibilities:
• Identify data to backed up
• Provide backup schedule and update as necessary
• Ensure backup is rotated/sent off-site if desired
Summary

• Cloud service level and implementation types continue to evolve
• Benefits to the business can be leveraged when going to the cloud – but not one-size fits all
• Organizations may use multiple cloud environments or leverage a hybrid cloud setup (public/private)
• Service Organization Control (SOC) reports are not the whole solution when auditing outsourced services
• Internal Auditors should be engaging with cloud service providers early on in their organization’s procurement/design phase
• Leverage the Cloud Security Alliance (CSA) control framework to account for and mitigate risks
Q&A
Thank you!