Background

2010  WGITA approved the cloud computing project with SAI USA as lead and Canada & India as members

2011  A status report was presented and comments solicited

2012  Final project description and common cloud computing risks were presented
       Members requested that this work be augmented with a cloud computing guide and audit handbook

2013  Guide & handbook completed for CC.

2013 Will be incorporated into the overall IT Audit Guide & Handbook in cooperation with IDI
What Is Cloud Computing?

• Generally speaking, cloud computing can be thought of as anything that involves delivering hosted services over the Internet.

• According to NIST Cloud computing is a model for enabling ubiquitous, 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. (Special Publication 800-145)
What It Provides

• Cloud computing provides shared services as opposed to local servers or storage resources
• Enables access to information from most web-enabled hardware
• Allows for cost savings – reduced facility, hardware/software investments, support
Essential Characteristics

• **On-demand self-service**
  A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

• **Broad network access**
  Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Source: NIST Special Publication 800-145
Characteristics

• **Resource pooling**
  The provider’s computing resources are pooled to serve multiple consumers
  Resources can be dynamically assigned and reassigned according to customer demand
  Customer generally may not care where the resources are physically located but should be aware of risks if they are located offshore

Source: NIST Special Publication 800-145
Characteristics

- **Rapid elasticity**
  Capabilities can be expanded or released automatically (i.e., more CPU power, or ability to handle additional users)

  To the customer this appears seamless, limitless, and responsive to their changing requirements

- **Measured service**
  Customers are charged for the services they use and the amounts
  There is a metering concept where customer resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service

Source: NIST Special Publication 800-145
Service Models

- Infrastructure
- Platform
- Software/Application
Service Models

Infrastructure-as-a-Service (IaaS)

- A service model that involves outsourcing the basic infrastructure used to support operations--including storage, hardware, servers, and networking components.

- The service provider owns the infrastructure equipment and is responsible for housing, running, and maintaining it. The customer typically pays on a per-use basis.

- The customer uses their own platform (Windows, Unix), and applications
Service Models

Platform-as-a-Service (PaaS)

• A service model that involves outsourcing the basic infrastructure and platform (Windows, Unix)

• PaaS facilitates deploying applications without the cost and complexity of buying and managing the underlying hardware and software where the applications are hosted.

• The customer uses their own applications
Service Models

Software-as-a-Service (SaaS)

• Also referred to as “software on demand,” this service model involves outsourcing the infrastructure, platform, and software/applications.

• Typically, these services are available to the customer for a fee, pay-as-you-go, or a no charge model.

• The customer accesses the applications over the internet.
Where Is My Data?

- Data resides on servers that the customer cannot physically access
- Vendors may store data anywhere at lowest cost if not restrained by agreement
Cloud Computing Guide

The guide is about a 10 page document that describes cloud computing and areas of risk

These risks should be managed by the IT organization that chooses to utilize cloud computing

For IT Auditors these risks are a roadmap which you can utilize to create your audit program
Cloud Computing

What is Cloud Computing?

Cloud computing involves the organization outsourcing data processing to computers owned by the vendor. In a private cloud, the vendor hosts the infrastructure and applications for a single customer. In the public cloud, the vendor can host the infrastructure and applications for multiple customers. The advantage of cloud computing is that it provides access to computing resources on demand, reducing costs for hardware and software.

Cloud Computing Models

There are three primary types of cloud computing models:

1. Infrastructure as a Service (IaaS): In this model, the cloud provider offers virtualized computing resources like servers, storage, network, and databases. The user manages the operating system and applications.
2. Platform as a Service (PaaS): In this model, the cloud provider offers a platform with pre-installed software and tools, allowing the user to develop and deploy applications.
3. Software as a Service (SaaS): In this model, the cloud provider offers complete applications, and the user accesses them via a web interface.

Examples of cloud computing include Web-based email applications and common business applications that are accessed online through a browser, instead of through a local computer. Cloud computing can potentially deliver several benefits for current systems, including better utilization of computing resources and more robust collaboration capabilities. However, with these benefits come the potential risks that any new form of computing services can bring, including information security breaches, infrastructure failure, and loss of data. Media reports have described security breaches of cloud infrastructure and attacks by others that have identified security as a major concern hindering federal agencies from adopting cloud computing services.

The benefits of cloud computing include:

1. Reduced costs: Cloud computing allows for scalable computing resources that can be increased or decreased as needed.
2. Increased efficiency: Cloud computing allows for faster access to applications and data.
3. Improved collaboration: Cloud computing allows for easier collaboration between different organizations.

The risks of cloud computing include:

1. Security risks: Cloud computing involves the sharing of data and applications, which can be vulnerable to security breaches.
2. Dependence on service providers: Cloud computing relies on third-party service providers, which can lead to service disruptions.
3. Legal and regulatory issues: Cloud computing can raise legal and regulatory issues, such as data sovereignty and intellectual property.

Cloud computing is becoming increasingly popular, with many organizations adopting it to reduce costs and increase efficiency. However, it is important to carefully consider the benefits and risks of cloud computing before making a decision.
What is Cloud Computing?

Cloud computing is where the organization outsources data processing to computers owned by the vendor. Primarily the vendor hosts the equipment while the audited entities still has control over the application and the data. Outsourcing may also include utilizing the vendor’s computers to store, backup, and provide online access to the organization data. The organization will need to have a robust access to the internet if they want their staff or users to have ready access to the data or even the application that process the data. In the current environment, the data or applications are also available from mobile platforms (laptops with Wi-Fi or cell/mobile cards, smart phones, and tablets).
Audit Concerns

When an organization chooses to utilize cloud computing, they need to be aware of risks that they may face with the service provider, the risk they face if they are unable to effectively oversee the service provider, and other risks related to management and security weaknesses in the service providers approach. As an auditor you will need to understand what the agency has done to mitigate the risks with cloud computing. When we as auditors are asked to appraise whether an entity or organization getting the benefits of cloud computing are managing the vendor to ensure that they get the required services we need to be aware of the risks that they may face.
Cloud Computing Guide

• Risk Areas
  – Service Provider Risks
  – Technical Risks
  – External (Overseas) Risks
  – Management/Oversight Risks
  – Security / Connectivity / Privacy Risks

These were discussed at the last meeting along with some mitigation strategies that the IT organization could use

The IT auditor would use those as a road map to frame audit questions
Cloud Computing Handbook

• The handbook provides the IT Auditor with some audit related questions that begin to explore whether the organization is managing the risks and the vendor
Cloud Computing Handbook

Refresher on cloud computing

Cloud computing is a form of outsourcing where the organization outsources data processing to computers owned by the vendor. Outsourcing may also include utilizing the vendor’s computers to store, backup, and provide online access to the organization data. The organization will need to have a robust access to the internet if they want their staff or users to have ready access to the data or even the application that process the data. In the current environment, the data or applications are also available from mobile platforms (laptops with Wi-Fi or cell/mobile cards, smart phones, and tablets).

Risks for the audited entity

When an agency chooses to utilize cloud computing, they need to be aware of risks that they may face with the service provider, the risks they face if they are unable to effectively oversee the service provider, and other risks related to management and security weaknesses in the service provider’s approach. As an auditor, you will need to understand what the agency has done to mitigate the risks with cloud computing. When we as auditors are asked whether an entity or organization getting the benefits of cloud computing are managing the vendor to ensure that they get the required services we need to be aware of the risks that they may face. In order to analyze whether the audit entity is both aware of and managing or mitigating the common risks with cloud computing the following matrix provides a way to look for certain documents and activities that will provide the data that the auditor can analyze.

A representative set of audit related questions is provided here in this guide. The auditor may augment these with other questions as appropriate. For example, managing cloud computing also requires project management discipline similar to those when managing any other contractor. However, since cloud computing does not typically entail development of new capability, the management activities are more specific to monitoring SLA requirements and taking action when the vendor is not performing to contractual requirements.

<table>
<thead>
<tr>
<th>Audit Issues</th>
<th>Criteria/Basis of evaluation</th>
<th>Information required</th>
<th>Analysis Method</th>
<th>Audit Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Computing Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Objective:</td>
<td>To assess whether the organization has a policy on cloud computing or has given it some thought prior to engaging in this activity.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the organization have a policy on whether they will utilize cloud computing?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there an organizational policy that addresses the use of cloud computing? This may also be called a policy on outsourcing.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who approved the policy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the policy lay out which functions or services can be performed utilizing cloud computing and which ones should be retained via existing IT infrastructure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How does the organization ensure that this policy is enforced?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational IT Policy or other which addresses cloud computing.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interviews and review of documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether the organization has considered cloud computing as an option and whether they have decided what can and cannot be implemented via the cloud.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 If possible the source of info should be indicated
2 Audit conclusions could lead to possible audit recommendations. For further guidance see Chapter (___ Reporting)
# Cloud Computing Policy

**Audit Objective:** To assess whether the organization has a policy on cloud computing or has given it some thought prior to engaging in the activity.

<table>
<thead>
<tr>
<th>Audit Issues</th>
<th>Criteria (Basis of evaluation)</th>
<th>Information required</th>
<th>Analysis Method</th>
<th>Audit Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the organization have a policy on whether they will utilize cloud computing?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there an organizational policy that addresses the use of cloud computing? This may also be called a policy on outsourcing.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who approved the policy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the policy lay out which functions or services can be performed utilizing cloud computing and which ones should be retained via existing IT infrastructure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How does the organization ensure that this policy is enforced?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization IT Policy or other which addresses cloud computing.</td>
<td>Interviews and review of documents</td>
<td>Whether the organization has considered cloud computing as an option and whether they have decided what can and cannot be implemented via the cloud.</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Computing Handbook

<table>
<thead>
<tr>
<th>Security</th>
<th>Security requirements, CSP Information security management policy and procedures</th>
<th>Agency adopted security standards.</th>
<th>Whether the agency has thought about security controls and standards and has required the CSP to follow the same.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit Objective:</strong> To assess whether the agency is periodically monitoring the vendor to ensure that security requirements are being met.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What are your security requirements and how are you ensuring that the CSP is meeting them?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What security standards are you requiring that the CSP follow?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What portions of your data requires encryption?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who is responsible for this encryption?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Next Steps

• As and when members conduct IT Audits that involve Cloud Computing we would like to receive your audit questions so we may update the guide

• Members may contact the Chair or SAI USA for additional information
Contacts

• SAI India
  Jagbans Singh
  ir@cag.gov.in

• SAI USA
  Madhav Panwar
  panwarm@gao.gov