

# 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*

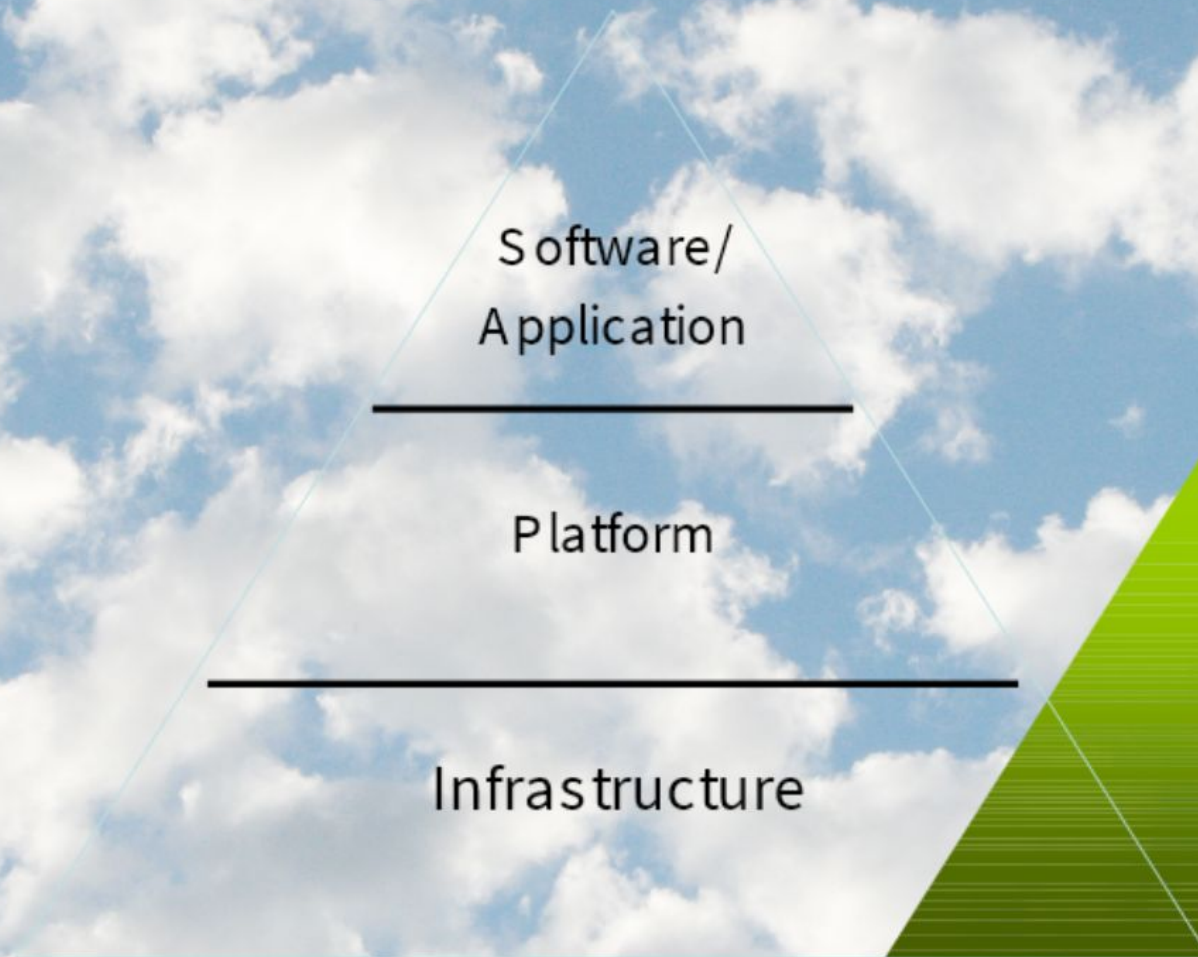
Customers are charged for the services they use and the amounts

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

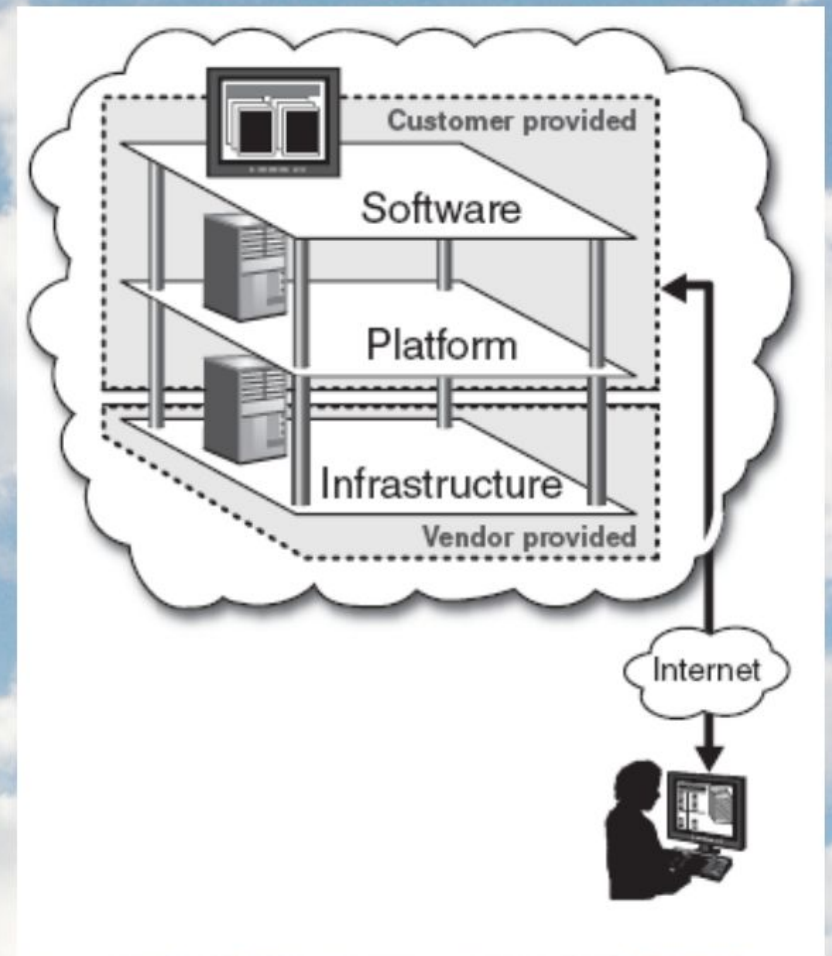




# Service Models

## 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.



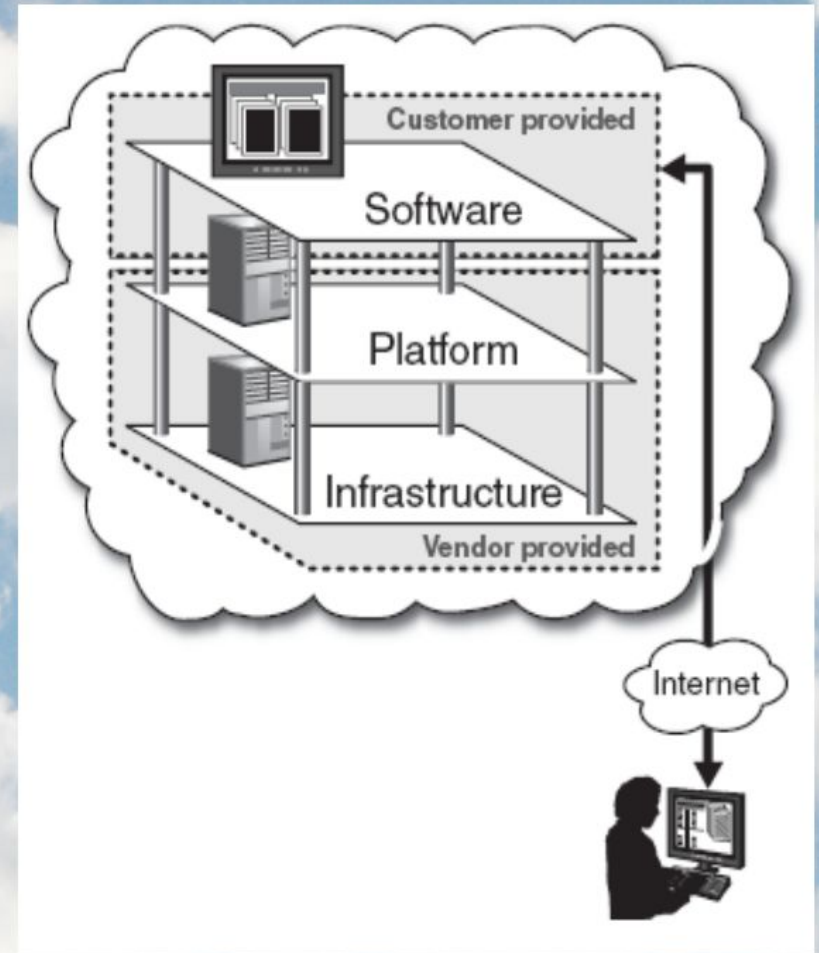
- **The customer uses their own platform (Windows, Unix) and applications**



# 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**

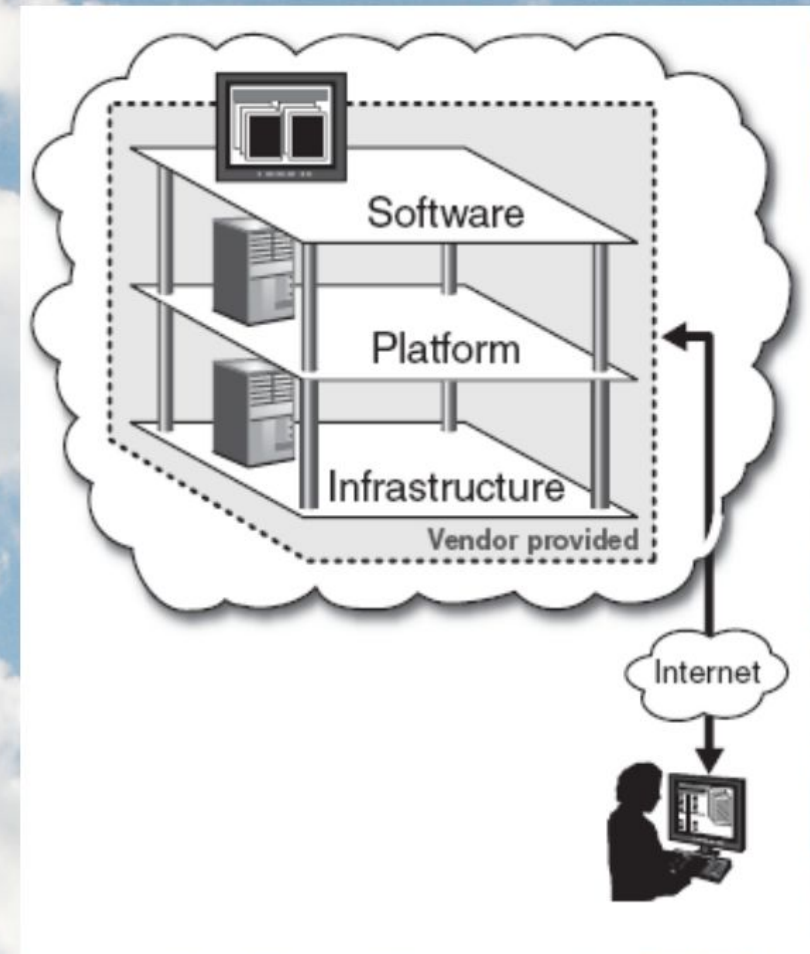




# Service Models

## 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 Guide

Load Computing

## What is Cloud Computing?

Cloud computing is where the organization outsources data processing to consumers owned by the provider. In other words, the provider takes responsibility for installing and maintaining the infrastructure, the application and the data. Consequently, they may include making the provider's responsibility for doing, backing up, monitoring and securing the data on the organization's side. The organization will need to have a robust security framework. However, they may or may not have ready access to the data or view the application or that processing data. In the current environment, the data or application may well come from mobile platforms (laptops or the M4C or even (mobile cars, smart phones, and so on).

Cloud computing much like outsourcing offers cost savings and the ability to share computing resources between businesses as part of the infrastructure costs, in turn enabling a variety of new and old networks and has the potential to provide information technology (IT) services more rapidly and at a lower cost. Cloud computing promises new services, based on pay-for-what-you-use and other models, to enable businesses to manage their information technology resources more effectively. To provide the services, providers are likely to rely on large computing resources, a decreased need to buy hardware or to build data centers, and more robust cloud storage capabilities.

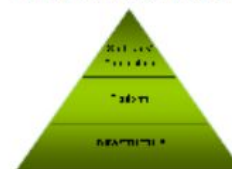
Examples of major computing in bulk: 30,000 of the same servers, and 100,000 of the new ones, are being replaced through Amazon's cloud services. Cloud computing can potentially deliver more benefit to individual servers owners, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robustness to labor or capacity limits. However, along with these benefits are the potential risks that, as the scale of computing increases, the long, unbroken chains of server-to-server connections from data centers, and from data centers to the cloud, may be difficult to troubleshoot and may be more difficult to secure.

For example, a user could have a mobile device that has a secure element, where the secure element is a hardware-based secure element, and the secure element is a component of the mobile device. The secure element could be a secure element that is a part of the mobile device, or the secure element could be a secure element that is a part of a separate device. Additionally, a user could use a vendor-provided infrastructure (computer, storage, backup) or use getting infrastructure services from a vendor or use a cloud computing.

An organization may choose to sell its software as either a public good, a private good, or a public good with a private market. A public good is a good that is nonrival and nonexcludable, applicable to many and often uncountable users. Information products are typically nonrival, but they are excludable, which makes them private goods. A private good must be sold to one user at a time, typically, customer by customer, and it is rival, so that one user's consumption of the good excludes other users from consuming it. A private good can be sold to a single customer or to many customers at once. In a private, controlled, local or "General" market, the customer has more control over the environment but also needs additional expertise to design and manage the software and requires careful planning to ensure that additional users can be accommodated.

### Head Dressing Model

There are general = three cloud computing models: infrastructure, platform, and software.



For an additional cost of \$600, Amazon ElasticSearch can be made available to support their business operations. Infrastructure may include storage, hardware, networking, and network components. These are located in the premises and customers use their own platform [Linux](#), [Windows](#), [enironment](#), and associated software. The service provider usually creates the environment and supports the forecasting, testing, and deployment of the environment regularly on a continuous basis.

In the **Infrastructure-as-a-Service (IaaS)** mode the vendor provides both the basic infrastructure and platform. Customers use their own software and applications and access them over the Internet. In fact, the **Infrastructure** is what is being rented. Customers are paying for hardware, network, the cloud and storage, operating system and security, but not the applications, databases and software (operating systems and other essential software) which the customers own themselves.

Many software-as-a-service (SaaS) model services are called "software or services," the vendor primarily is the software provider, and software/application (files, database, etc.). The customer accesses the application over the internet and pays depending on usage, on a term of a one year. Finally, results (v. 1).

### Elements affecting the reporting

Full text available at <http://www.sagepub.com>

The user who is not able to perform the same and apply call applications, will not have access to these over the Internet, users are able to access the same and apply call applications from their client and desktop, currently, we are not using desktops, we are using laptops, tablets or cell phones. We are not using a desktop, I would like to know if it is possible to store all the data in the cloud, so that the user can be able to access the same from anywhere, in physical or in a virtual location, for example, an auditor may update a record of meeting to document hand inspection of the room and it is relatively easy for the user, as the same is available for review or sharing to other team members who can access the same from their client or cell phone, I would like to know if it is possible to store all the data in the cloud, so that the user can be able to access the same from anywhere.

#### Use of web technologies

cloud services, such as data backup and recovery services, with the help of the Internet, are being increasingly implemented. These applications make use of sensitive knowledge. However, in order to access the cloud computing resources, these technologies support any level of security that might be required and allow sensitive data to be stored and retrieved based on the organization's requirements.

Example:  $\text{Ca}^{2+}$ ,  $\text{K}^{+}$ ,  $\text{Na}^{+}$ ,  $\text{H}^{+}$ ,  $\text{H}_2\text{O}$

When cloud computing an organization does not need to purchase computing resources to host its data. It uses the application, data, and service and application providers, and services are available to the companies anytime and anywhere by the cloud computing vendors. The system is required to be capable to be supported, maintained, backed up and transfer to another procedures. Additionally, the vendor is also responsible for ensuring access to the data and applications based on the requirements of the organization. The organization does have to provide to their users means to access the data and applications. There are typically three categories of cloud computing services offered today: (1) Infrastructure as a service (IaaS)



# Cloud Computing Guide

## **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).



# Cloud Computing Guide

## 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

## Whether on cloud computing

Cloud computing is a form of outsourcing where the organisation outsources data processing to computers owned by the vendor. Outsourcing may also include allowing the vendor's computers to store, backup, and provide online access to the organisation's data. The organisation 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 4G, mobile phones, smart phones, and tablets).

## Slide for the audited entity

When an agency chooses to use cloud computing, they need to be aware of the fact 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 provider's approach. As an auditor you will need to understand what the agency has done to mitigate the risks of cloud computing. When we as auditors are asked to provide whether an entity or organisation getting the benefit of cloud computing and 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 analyse whether the audit unit is a both aware of and is managing or mitigating the common risks of cloud computing the following matrix provides a way to look for certain documents and activities that will provide the info that the auditor can analyse.

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

Audit Issues	Criteria (basis of evaluation)	Information required <sup>1</sup>	Analysis Method	Audit Conclusion <sup>2</sup>
<b>Cloud Computing Policy</b> <b>Audit Objective:</b> To assess whether the organisation has a policy on cloud computing or has given it some thought prior to engaging in the activity.				
Does the organisation have a policy on whether they will utilize cloud computing?				
Is there an organizational policy that addresses the use of cloud computing? This may also be called a policy on outsourcing.		Organizational IT Policy or other which addresses cloud computing.	Interview and review of documents	Whether the organization has considered cloud computing as an option and whether they have decided what can and cannot be implemented on the cloud.
Who approved the policy?	Organizational policy on cloud computing or outsourcing.			
Does the policy set out under functions or services can be performed on a cloud computing platform which ones should be retained as existing IT infrastructure?				
How does the organization ensure that the policy is enforced?				

<sup>1</sup> If possible the source of info should be indicated.

<sup>2</sup> Audit conclusions could lead to possible action recommendations, I or further guidance see Chapter \_\_\_\_\_ (if necessary).



# Cloud Computing Handbook

Audit Issues	Criteria (Basis of evaluation)	Information required <sup>1</sup>	Analysis Method	Audit Conclusion <sup>2</sup>
<b>Cloud Computing Policy</b> <b>Audit Objective:</b> To assess whether the organization has a policy on cloud computing or has given it some thought prior to engaging in the activity.				
<p><b>Does the organization have a policy on whether they will utilize cloud computing?</b></p> <p>Is there an organizational policy that addresses the use of cloud computing? This may also be called a policy on outsourcing.</p> <p>Who approved the policy?</p> <p>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?</p> <p>How does the organization ensure that this policy is enforced?</p>	<p>Organizational policy on cloud computing or outsourcing</p>	<p>Organizational IT Policy or other which addresses cloud computing.</p>	<p>Interviews and review of documents</p>	<p>Whether the organization has considered cloud computing as an option and whether they have decided what can and cannot be implemented via the cloud.</p>



# Cloud Computing Handbook

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



# 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