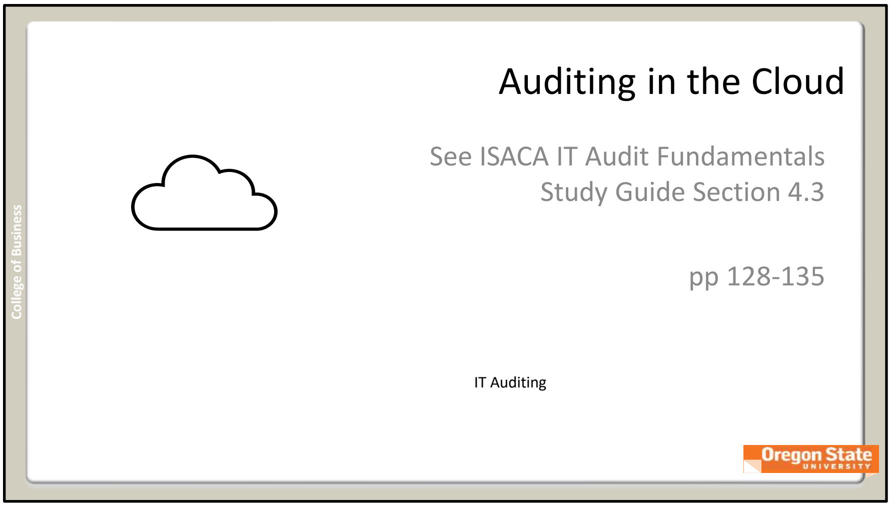


College of Business

Auditing in the Cloud

See ISACA IT Audit Fundamentals
Study Guide Section 4.3

pp 128-135

IT Auditing

Oregon State
UNIVERSITY

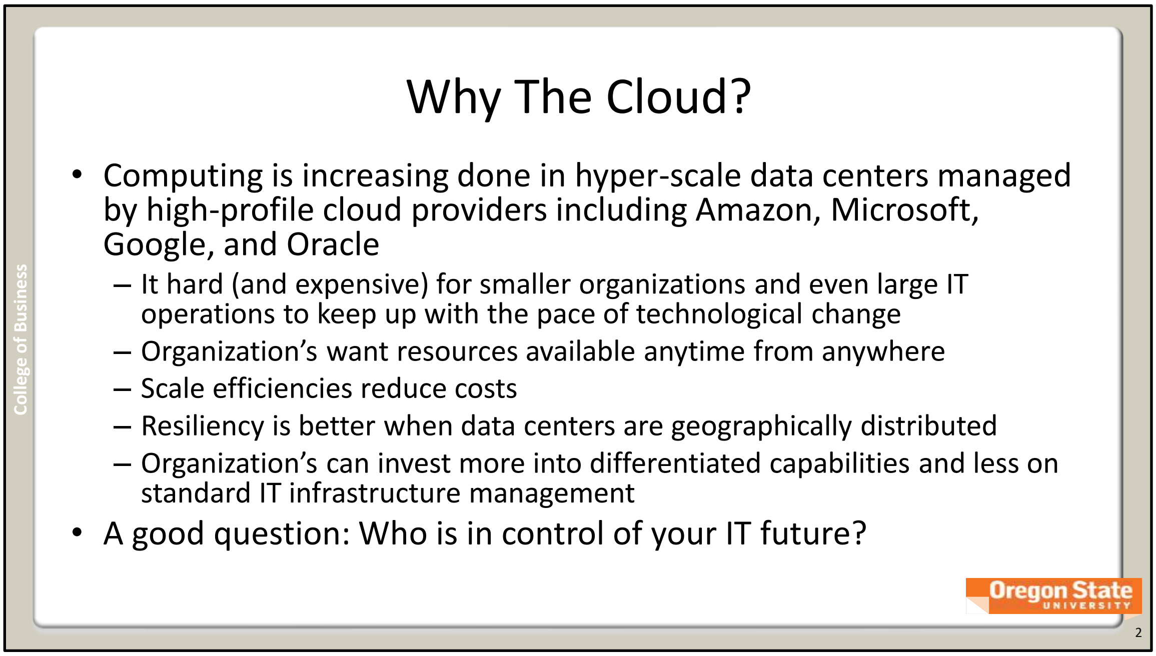
IT risk management guidance and IT audit norms have always emphasized appropriate planning for a disaster, but natural and other disasters have been largely and correctly considered low-probability events. As a result, controls for these risks have been frequently neglected in years past.

More recently, preparing for the worst has become more in fashion. And, applying risk assessment tools this makes sense.
When the only perceived threat that would crash entire systems was a natural disaster or war, most audited organizations would sensibly use a low likelihood in quantifying disaster risk. Even if the cost of rebuilding IT would be crippling, when the chance is very low, - far far less than 1% per year – exposure is also low making it hard to justify costly investments in protections that will never be needed. As a result, except in a few organizations – perhaps government, military, and finance – IT investments to improve operational capability made a lot more sense than investment in Business Continuity Disaster Recovery (BCDR) capability.

But that has changed in recent years. Perceived threats seem more likely as risk managers contemplate climate related factors such as floods or storms, cyber issues including ransomware, and increased threatening political/social events.
While this change of perspective may be speculative, it is a mathematical reality that, together, those possibilities pose a larger threat as compared to just the chance of an earthquake, flood, or fire.

Further, the rise of cloud services had radically changed – reduced – the cost of protecting against catastrophic failure.

In any case, there are many things organizations can, and probably should, do to cost effectively reduce residual risk through BCDR planning.



College of Business

Why The Cloud?

- Computing is increasing done in hyper-scale data centers managed by high-profile cloud providers including Amazon, Microsoft, Google, and Oracle
  - It hard (and expensive) for smaller organizations and even large IT operations to keep up with the pace of technological change
  - Organization's want resources available anytime from anywhere
  - Scale efficiencies reduce costs
  - Resiliency is better when data centers are geographically distributed
  - Organization's can invest more into differentiated capabilities and less on standard IT infrastructure management
- A good question: Who is in control of your IT future?

Oregon State UNIVERSITY

2

Cloud service providers – including Amazon, Microsoft, Google, and Oracle – compete to help organizations move IT to "the cloud."

High level decision makers are pitched with promises that costs will be lower, risks will be reduced, agility will be increased, recruiting IT talent will be less of an issue, and costs will be lower. Oh, did we mention cost twice?

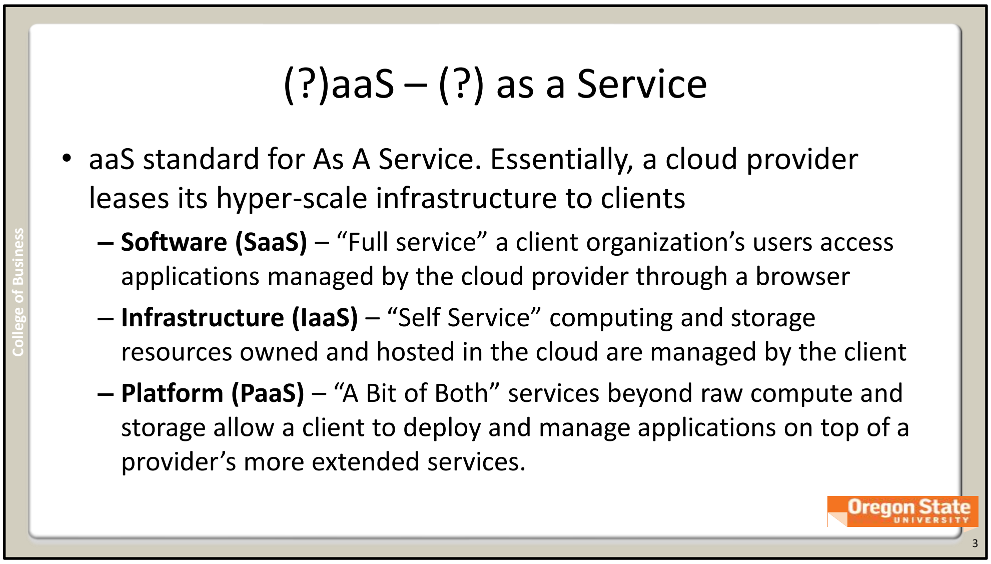
All of those things are probably true, but only if the organization establishes a strong architecture, develops effective control processes, and develops new skills to monitor and mitigate risks – including unexpected costs. Some organizations have done things almost well enough and experienced terrible consequences in terms of data loss, runaway costs, or other cyber consequences. IT auditors can help organizations identify potentially costly or damaging control weaknesses.

The forces driving organizations to the cloud are real. IT changes at a ferocious pace. An organization can spend years developing the skills and insights needed to effectively operate complex systems, only to see a component change in a way that reduces the value of hard won expertise. Organizations are hard pressed to keep up with the changes. It's hard to recruit and retain talent, and those people need constant (and expensive) training if they are to help the organization keep up with competitors and deal with growing threats. Essentially, a cloud strategy aims to allow an organization to invest in its own differentiated processes and leave more of the mundane "commodity" services to multi-billion dollar providers who can invest in current expertise and spread the costs across a huge number of clients.

The cybersecurity implications also influence cloud deployment decisions.

- If your major applications are in the cloud, a localized event – such as an earthquake, riot, or flood – will not knock out your systems. You might ask "but what if your cloud provider's data center is damaged?" First, a cloud provider's datacenters are likely to be better protected than yours. And also, building your own failover "hot site" is expensive. If you are in the cloud, you can (for a significant extra charge) create failover capabilities at multiple locations within a cloud provider's infrastructure.
- Cloud provider's have some of the most sophisticated cyber controls on earth: protection against denial of service, protection against compromise of cloud management accounts, and more. Of course, clients still need to configure things carefully.

On the cost side. If care is not taken, organizations may experience expensive, unexpected/unauthorized use. For example an attacker may perform unauthorized crypto-mining or unplanned AI tool usage can run up exorbitant bills. As with most strategies, a cloud strategy without strong tactical support will often fail.



College of Business

(?)aaS – (?) as a Service

- aaS standard for As A Service. Essentially, a cloud provider leases its hyper-scale infrastructure to clients
  - **Software (SaaS)** – "Full service" a client organization's users access applications managed by the cloud provider through a browser
  - **Infrastructure (IaaS)** – "Self Service" computing and storage resources owned and hosted in the cloud are managed by the client
  - **Platform (PaaS)** – "A Bit of Both" services beyond raw compute and storage allow a client to deploy and manage applications on top of a provider's more extended services.

The ISACA IT Audit Fundamentals Study guide (p 129) defines:
Software as a Service SaaS*: Offers the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). Provides a business application that is used by many individuals or enterprises concurrently.*

Platform as a Service (PaaS)*: Offers the capability to deploy onto the cloud infrastructure customer-created or –acquired applications that use programming languages and tools supported by the provider. Provides an application development sandbox in the cloud.*

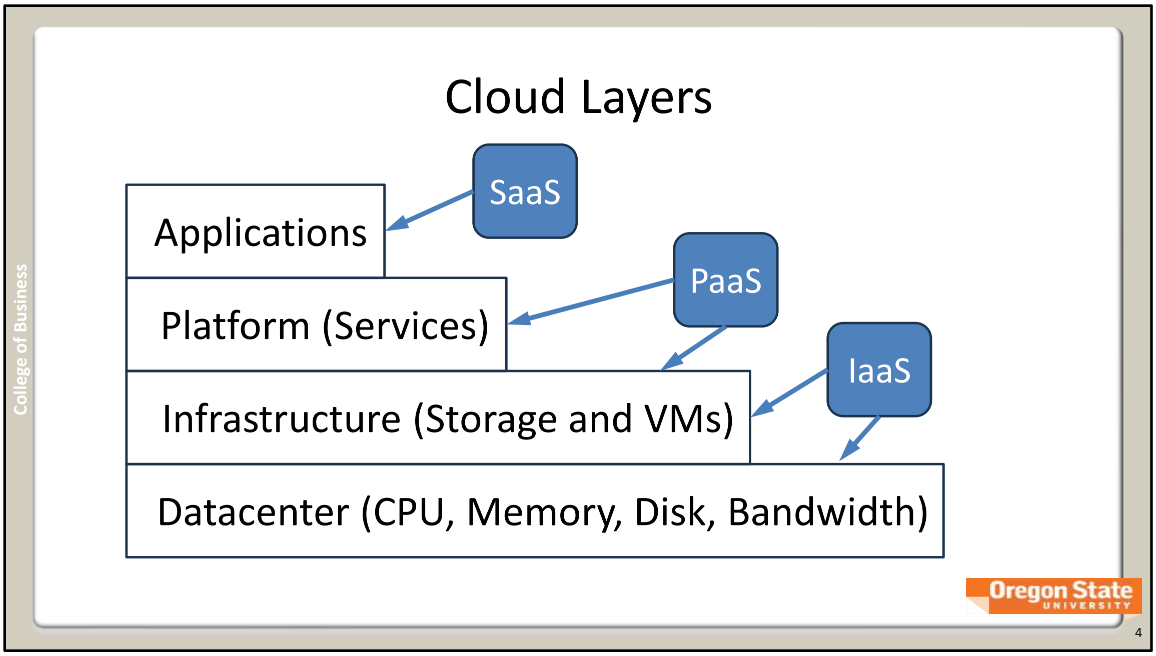
Infrastructure as a Service (IaaS)*: Offers the capability to provision processing, storage networks, and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems and applications. Provides online processing or data storage capacity.*

As is often true of products in the IT space, distinctions vary. For example, the difference between "programming languages and tools" in the PaaS definition and "fundamental computing resources" in the IaaS definition are less the completely clear.

From an IT audit perspective, we would want to think about these from a risk perspective.

- In IaaS, much more of the general IT risk mitigation burden falls to the customer. The cloud provider's IaaS service might provide virtual machine images to help keep up with patching and a configuration console for managing storage buckets, but a lot of ongoing maintenance work remains with the client. Change management risks are not very different in IaaS as compared to on premises deployments – seemingly innocuous configuration changes can be very disruptive.
- SaaS risk profiles are substantially different. Providers take on operating system risks and most application change management risks. The client pays more and needs to ensure that they deploy monitoring for application usage and configuration because they don't have the same operational visibility as they would have on prem or even in an IaaS or PaaS context.
- PaaS details are often negotiable. For example, database, analytic, and container service offerings allow clients to rely more on provider capabilities and less on local resources. As with SaaS, however, different client-side expertise has to be developed to make sure systems are properly supported. Sill, fewer resources (people) are needed, and those people can focus more on organization specific factors and less on rapidly changing yet common platform risks.

Categorization can be debatable. We would generally say that DBaaS is a PaaS service because the client has substantial control over the underlying system functionality and the database is likely to be only one part of a more complex deployment where the client's applications and middleware interact with the database. The client is using the database service as part of a "platform" on which it deploys systems. But, others might also reasonable label such a deployment SaaS if the client configure things at the database – rather then database server - level and didn't deploy related applications to access the database.



Cloud Layers

SaaS

PaaS

IaaS

Applications

Platform (Services)

Infrastructure (Storage and VMs)

Datacenter (CPU, Memory, Disk, Bandwidth)

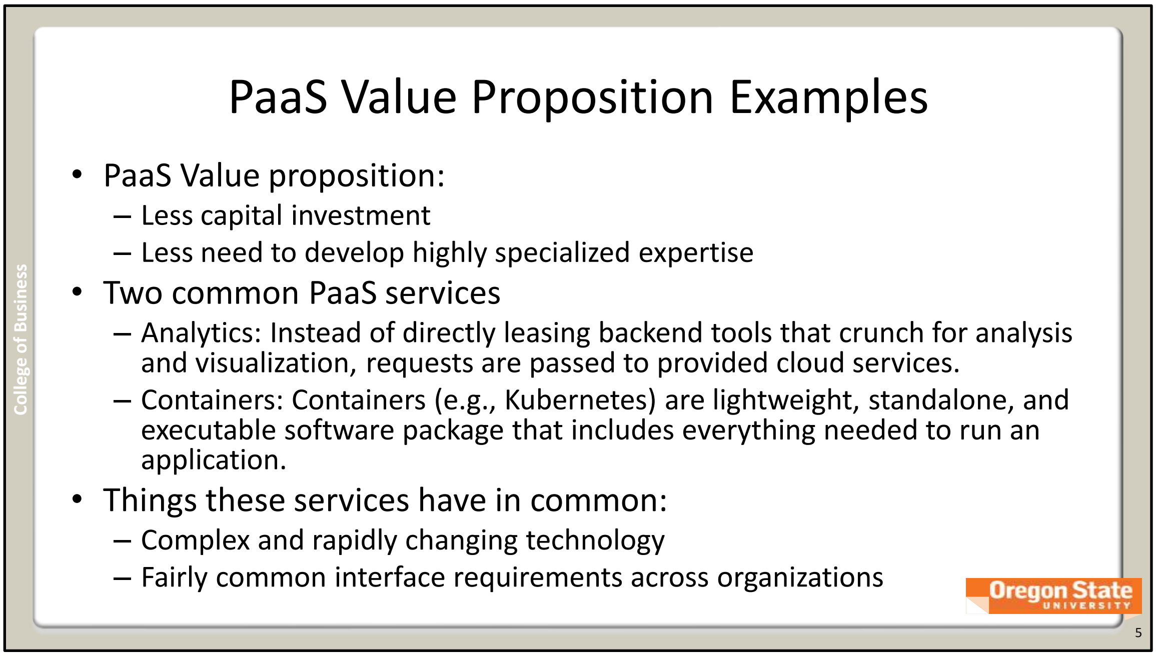
To understand the risks that are to be controlled, the auditor needs to understand what cloud components are used, how they are accessed, and what data or applications are deployed.

In a SaaS deployment, for example in an organization that users Salesforce, client's generally accesses services as web applications and services. Security rights, for example, are setting in the client's instance of the Salesforce application. Scripts and customizations are common, but they are configured using the Salesforce interface. How Salesforce delivers the configured services is in the cloud provider's hands. Platform elements such as database management, web server farms and more are largely invisible to the client organization, as are the VMs and storage components. Responsibility for installing OS patches to the Virtual machines that operate the salesforce software are done by salesforce, the client need not take a hand those processes.

Many organizations use some SaaS offerings such as email and identity, e.g., gmail or outlook and directory services, even if they deploy many applications in a PaaS context. Perhaps this is because security and reliability issues for such services are paramount and they are high value targets for sophisticated attackers. Google and Microsoft have immense investments in highly specialized tools for these specialized applications. It is unlikely an organization can provide matching security and reliability.

In IaaS deployments, clients manage the virtual machines on which their applications will run. The direct costs of managing hardware is a matter of concern for the cloud provider. The client interacts with provided virtual machines and storage in much the same they would if those elements were deployed in a local data center. Operating system patches, most security controls, and most network configuration settings are in the hands of the client. In addition, the client deploys application programs including webserver and database software and maintains those programs as well. In some cases, a cloud provider will even assign physical hardware, network connectivity, and other "bare metal" hardware to a specific client. The client doesn't have to manage the air conditioning or physical security, but they retain control over the hardware stack. That can be important for some organizations where the client prefers not to rely on the cloud vendor's management of, for example, highly sensitive data.

Value-add services such as advanced security management, databases, ML/analytics, middleware, and application hosting are often available in a PaaS deployment. A client will often contract for virtual machines as in IaaS, but they choose to let the provider manage the VMs and application software for other components of their computational stack. For example, a client may want to install its on instance of and ERP system on VMs it contracts for and manages. But they may want to use sophisticated machine learning (ML) tools or visualization tools. By contracting such services from a vendor, the expensive expertise required to maintain powerful backend tools can be provided at scale by the vendor and merely be consumed by the client.



PaaS Value Proposition Examples

- PaaS Value proposition:
  - Less capital investment
  - Less need to develop highly specialized expertise
- Two common PaaS services
  - Analytics: Instead of directly leasing backend tools that crunch for analysis and visualization, requests are passed to provided cloud services.
  - Containers: Containers (e.g., Kubernetes) are lightweight, standalone, and executable software package that includes everything needed to run an application.
- Things these services have in common:
  - Complex and rapidly changing technology
  - Fairly common interface requirements across organizations

College of Business

5

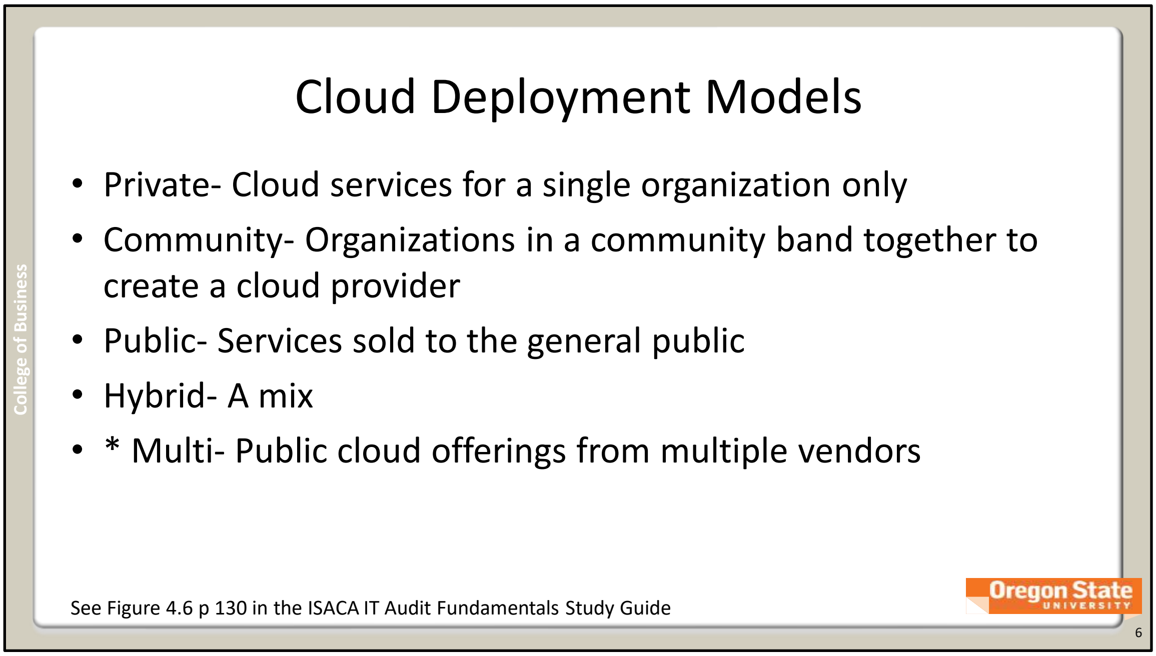
The value proposition for moving to the cloud instead of hosting your own systems comes down primarily to two things.

- Capital (e.g., hardware) investments in technology are hard to manage. With a cloud provider you "pay by the drink." If you use more, you pay more. But if you grow and need more you don't have to invest and wait. You can scale up (or down) quickly.
- Doing technology well takes a lot of expensive expertise. Teams that can effectively manage the base level servers and software tools in these examples need specialized knowledge but don't need to know much about how the organization uses them. An organization like Amazon Web Services (AWS), Azure (Microsoft), or Oracle can devote nearly unlimited resources to optimizing servers and software to provide such services.

Databases: Optimizing, managing, and securing large scale databases is both vital and complicated. Applications often separate logic from data. So, vendors (especially Oracle and Microsoft) can provide access to data services thereby allowing their clients to focus on the business functions. The experts at the cloud service can use their vast pool of knowledge to help organizations tune their deployments, avoid critical configuration mistakes, and facilitate other-wise very expensive features such as frequent backups, offsite storage of backups, and failover to secondary data centers. Also, especially for Microsoft (with SQL server) and Oracle (with Oracle database) vertical integration can provide a competitive advantage. Since they pay themselves for licenses to the expensive database software, they may be able to profitably offer Database as a Service (DBaaS) as part of a bundle with other cloud offerings.

Analytical and visualization tools including machine Learning (ML) benefit from expensive GPUs (Graphical Processing Units) and other hardware; and the tools are rapidly evolving. Spreading the cost of such investments across multiple customers make sense because each customer likely only uses that kind of computational power part of the time. Economies of scale apply.

Container services are a good way to host complex applications like ERP systems because they rely on a variety of underlying computational components including networks, middleware, web servers and more. Standing up separate devices for each function is expensive and difficult to manage. A "container" (e.g., Kubernetes) encapsulates all the components an application needs on a single virtual machine. Needed configurations to support component interactions are pre-configured in the container. IT administrators can then manage containers instead of managing individual devices and programs.
In some ways this helps with security because a lot of time and testing goes into the container setup. But containers will eventually be found to have vulnerabilities. So organizations still have to patch the software in the container.



College of Business

Cloud Deployment Models

- Private- Cloud services for a single organization only
- Community- Organizations in a community band together to create a cloud provider
- Public- Services sold to the general public
- Hybrid- A mix
- * Multi- Public cloud offerings from multiple vendors

See Figure 4.6 p 130 in the ISACA IT Audit Fundamentals Study Guide

Oregon State UNIVERSITY

6

The ISACA IT Audit Fundamentals Study Guide and other sources differentiate these four deployment models.

Just as S- P- and IaaS models entail different risk profiles, the risks and value propositions for different cloud deployment models vary.

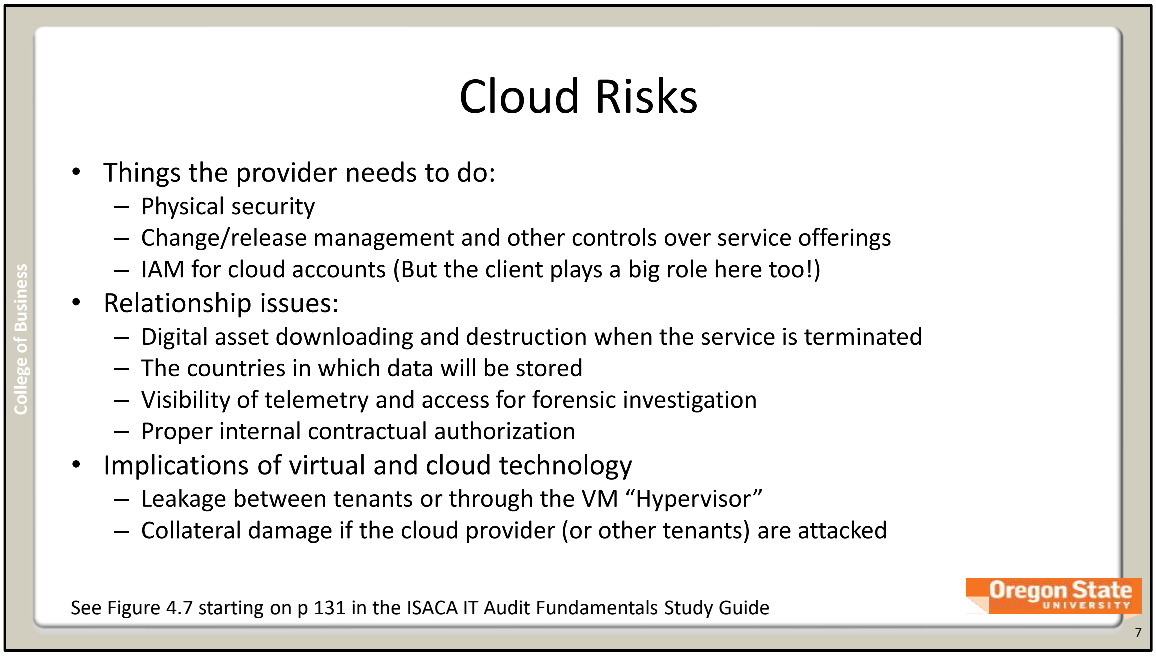
If an organization has a regulatory or strategic need to ensure that they retain near-complete control over their own systems, establishing some services similar to public cloud offerings but housed in a tightly controlled private environment may make sense. A deployment is most clearly a “private” cloud setup when a datacenter or dedicated facilities within a data center are used by only one client. Virtual Private Clouds mimic that model but use shared infrastructure. The differences between private and virtual private are not hard and fast and probably operate in a fluid legal environment. Public cloud vendors promise Virtual Private Cloud arrangements that very strictly segregate tenants, but hypervisor leakage, tenant isolation failures, physical access control issues, administrative access controls, and other features may still entail some chance of isolation failure.

It is not uncommon for organizations to set up some form of hybrid arrangement where some applications or services are private or local while some others use a public cloud provider.

Many organizations use cloud services from more than one vendor. That’s why we hear about “multi-cloud” environments. Deployment of a particular and important application may make more sense with one vendor or another. For example, a service that relies on an Oracle database MAY be more sensibly deployed to Oracle’s cloud infrastructure so that DBaaS can be a cost-effective and risk reducing feature. At the same time, other features, such as student lab environments, might well be deployed somewhere else, perhaps on Azure, to bundle services for cost negotiation, or to more simply support productivity tool integration, security operations, and/or identity infrastructure. The term “Multi-cloud” is not really a different category here as the “multi” clouds can be a mix of private, public, hybrid, and community cloud deployments.

A manager may prefer to try to move all cloud services to the same cloud provider to reduce costs, leverage developing expertise, or integrate connections. But “putting all your eggs in one basket”, as it were, can also be risky. Who knows if you will want to continue on with one provider after a number of years? Limiting exposure to a single provider can also be a smart move.

The point here for an auditor is that they need to understand how risk-laden components are deployed so that they can assess the likely effectiveness of the controls over those systems.



Cloud Risks

- Things the provider needs to do:
  - Physical security
  - Change/release management and other controls over service offerings
  - IAM for cloud accounts (But the client plays a big role here too!)
- Relationship issues:
  - Digital asset downloading and destruction when the service is terminated
  - The countries in which data will be stored
  - Visibility of telemetry and access for forensic investigation
  - Proper internal contractual authorization
- Implications of virtual and cloud technology
  - Leakage between tenants or through the VM “Hypervisor”
  - Collateral damage if the cloud provider (or other tenants) are attacked

See Figure 4.7 starting on p 131 in the ISACA IT Audit Fundamentals Study Guide

College of Business

7

The ISACA IT Audit Fundamentals Study Guide lists some important cloud risks and matches them up with useful controls. The text has good notes, we won’t repeat them here. Most of the listed risks are common to cloud and non-cloud deployments. But the controls need to operate differently when cloud services are involved. Issues can be framed into three risk areas:

Things providers must do that may need to be verified:
There are things the cloud provider must do to secure their operations. The client cannot see if these things are done right. Third-party assurance and other control reports allow client’s to understand the effectiveness of such safeguards. Trust, but verify. IAM responsibilities are shared between provider and client. Client administrative accounts for managing cloud resources are issued and audited by the client, but the provider handles authentication. Credentials for applications are mostly in the hands of clients.

Contracting concerns:

- Cloud contracts can be complicated. And while hope is high when relationships begin, the reality can be harsh if a client wants to break up an ongoing relationship with a cloud provider. It is important to have the cloud equivalent of pre-nuptial agreements so they can be sure proprietary data can reasonably be moved to some new platform in the future and not inappropriately disseminated once the contract has ended.
- Starting a new relationship with a cloud should be properly authorized. Individual units may be tempted to enter into relationships that are less than ideal or insecure. Vendor management and contract approval processes need to account for the details of cloud service offerings.
- In these days of international espionage and rivalry, many organizations are not allowed by law to have data stored in or transferred through countries that may pose interception risks. Government agencies and government contractors need to, by law, protect secrets. If data are physically housed in China, as an example, they are vulnerable to inspection by Chinese government actors. Major cloud providers offer geographically contained and otherwise protected services. But you have to ask for (and pay for) that extra layer of control.

Virtualization technology risks:
Finally, there are underlying risks associated with a shared virtual environment. At the administrative level, the provider could have flaws that result in leakage between its customers (called tenants) even though the intent is to block any such cross access. One important flavor of this is hypervisor attacks. At the base layer of every cloud service are large pools of hardware that run hypervisor software that supports large pools of virtual machines. If the hypervisor software become vulnerable, all the systems are at risk. Also, cloud providers are major targlets for bad actors. If a large scale denial-of-service attack is aimed at the provider or at another tenant, the effects can impact other users of the cloud service.