**Cloud Security**

**Troy L Hutchison**

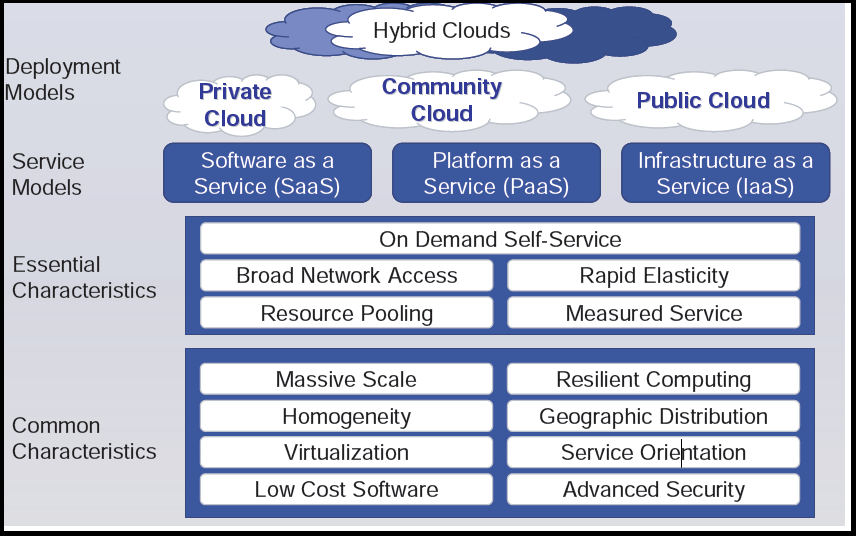
**CS591**

**Dr Chow**

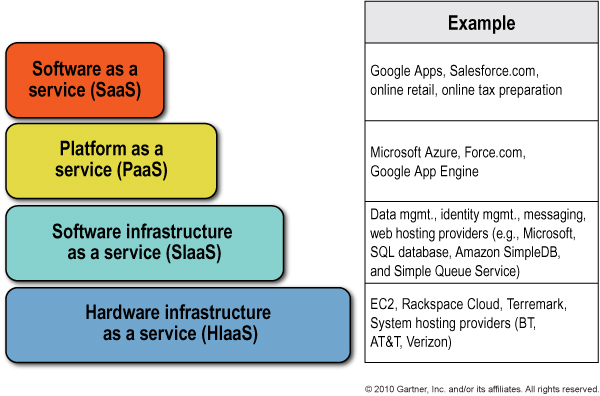
**Sunday, December 12, 2010**

# What is Cloud computing?

Cloud computing is 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.



The National Institute of Standard and Technology (NIST) definition of the Cloud is Software as a Service, Platform as a Service and Infrastructure as a Service. The Gartner group defines Infrastructure as a Service in greater detail separating into Software and Hardware Infrastructure components.



**Software as a Service (SaaS)**

Software as a Service (SaaS) is an application offered to a user as a service. SaaS is a complete, turnkey application solution (i.e., no IT organization built solution is required). Users access SaaS via a user-centric interface, such as a web browser or a rich Internet application (RIA) mechanism (e.g., media player plug-in). The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Examples include:

* Intuit Turbo Tax
* Intuit Quick books
* Mint.com
* Google Docs

**Platform as a Service (PaaS)**

Platform as a Service (PaaS) is an externally managed application platform for building and operating applications and services. PaaS provides the infrastructure needed to run applications over the Internet. It is delivered in the same way as a utility like electricity or water. Users simply “tap in” and take what they need without worrying about the complexity behind the scenes. Like any application platform, a PaaS environment supplies development and runtime frameworks to support presentation, business logic, data access, and communication capabilities. The PaaS environment must also supply supporting infrastructure capabilities, such as authentication, authorization, session management, transaction integrity, reliability, availability, and scalability. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Examples of PaaS Include:

* Google Apps
* Microsoft's Azure
* SalesForce.com

**Infrastructure as a Service**

**Software Infrastructure as a Service (SIaaS)**

Software Infrastructure as a Service (SIaaS) is a stand-alone cloud service that provides a specific application support capability, but not the entire application software platform service (otherwise, it would be PaaS). The intended consumers of SIaaS offerings are software developers who want to create an application that does not have dependencies on internal infrastructure components, which can be too expensive to license, slow to deploy, and difficult to maintain and support. SIaaS is not a user-consumable cloud service and, by definition, must be utilized by applications or higher-tier cloud services,

Examples of SIaaS include:

* Microsoft Structured Query Language (SQL) Data Services
* Google API
* Force.com
* Squarespace.com

**Hardware Infrastructure as a Service (HIaaS)**

Hardware Infrastructure as a Service (HIaaS) is a virtual or physical hardware platform offered as a service. The hardware platform is offered as a raw resource, so the consumer must install additional software or connect the resource to additional resources to create a complete solution. The system administrator manages the infrastructure platform using a web-based interface to provision, start, and stop individual platform instance.

Examples of HIaaS Include:

* Rackspace.com
* Amazon S3
* VMWare
* Amazon EC2

# Certification and Accreditation

To operate cloud based solutions, Cloud vendors must able to assure their customers that the information stored in the Cloud is safe and secure. To accomplish this many vendors have looked to outside agencies for certification and accreditation. Some of the more commonly used standards are AICPA Service Organization Controls Report (SOC), ISO 2700, and HIPPA.

AICPA Service Organization Controls Report (SOC), formerly known as a SAS 70 report. Service Organization Controls (SOC) reports are designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. Each type of SOC report is designed to help service organizations meet specific user needs:

## **There are three types of SOC reports**:

* **AICPA SOC 1:** Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting. These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) no. 16, *Reporting on Controls at a Service Organization*, are specifically intended to meet the needs of user entities’ management and their auditors, as they evaluate the effect of the controls at the service organization on the user entities’ financial statement assertions.
* **AICPA SOC 2:** Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy. These reports, prepared using the AICPA guide *Reports on Controls at a Service Organization over Security, Availability, Processing Integrity, Confidentiality, or Privacy* (currently under development), are intended for users that have a thorough understanding of the service organization and its internal controls. These reports can form an important part of the users’ oversight of the service organization; vendor management; and internal corporate governance and risk management.
* **AICPA SOC 3:** Trust Services Report (*Trust Services Principles, Criteria, and Illustrations*) (AICPA, *Technical Practice Aids*, vol. 1, (TPA sec. 100) commonly referred to as SysTrust reports). These reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not need the level of detail provided in a SOC 2 Report. These reports are general use reports and can be freely distributed or posted on a website as a seal.

**ISO 2700**

The ISO 27001 and ISO 27002 standards have gained attention for being a practical mechanism for both assessing and asserting good security practices. ISO 27002, in particular, helps companies build comprehensive and cost-effective enterprise security programs, ensuring that security resources are applied wisely and efforts are focused on activities that reduce real business risk. Investment in ISO 27002 compliance promises a high return because the requirements are largely a superset of other major regulations. Achieving ISO 27002 compliance positions most organizations to be well on their way to meeting the requirements of Sarbanes Oxley, Gramm-Leach-Bliley, HIPAA, and other relevant regulations.

**HIPPA**

Health Insurance Portability and Accountability Act (“HIPAA” and the “Act”). The purpose of HIPPA was to simplify and standardize the administrative functions of healthcare. The Administrative Simplification section of this law requires adaptation and implementation of standards for the security, privacy, and management of electronic healthcare transactions. The law applies to all healthcare organizations that choose to exchange data electronically.

#### HIPAA Hosting Solutions Include:

##### Web Application level protection

* Helps detect and contain undesirable traffic on public networks
* Helps prevent Malware invasions like Viruses, Worms, and Trojans
* Helps stop Hacker attempts like SQL injections and XSS (Cross-site scripting) attacks
* Customizable security rules ensure WAF is calibrated to protect your unique vulnerabilities

##### Application Level Monitoring and Intrusion Detection

* Alerts Administrators and Managers every time files, directories, or hardware are accessed and by whom
* Detects active hosts, bad logon attempts, and inappropriate content

##### Disaster Recovery with HIPAA Compliant Encryption

* Includes encrypted backup with fourteen day retention standard
* Capable of customized backup retention schedules
* Provides data encryption at rest in storage
* Requires a "key" to securely decrypt the data from backup

##### Virtualized, HIPAA Compliant Hosting Architecture

* Provides separate and privatized web application and database hosting environments
* Makes creating a development/beta testing environment affordable
* Runs on enterprise level hardware
* Forces password expiration
* Automates SSH & RTD timeouts

##### HIPAA Compliant System Architecture

* Separate web and database environment
* Exclusive environment for development, separate from production environment
* Password expiration
* Automatic SSH & RTD timeouts

##### Log Retention

* Provides a valuable, detailed audit trail during a forensic investigation

##### Managed Patching, Version Control, and Security Updates

* Upgrades hardware and OS automatically, and applications on request
* Provides support for Linux and Windows OS
* Alerts administrators when security vulnerabilities are detected

##### Physical and Logical Security

* Includes stringent data destruction policies
* Controls data movement inside and outside of our facilities
* Records any changes to the hosting environment
* Secures the datacenter environment with man-traps, surveillance, and controlled access

##### Vulnerability Scanning

* Tests HTTP services, virtual domains, Ports, and IP addresses for 10,000+ known vulnerabilities every day
* Delivers a detailed notification every time a vulnerability is found

**Vendor Solutions**

**SalesForce.com**

Salesforce.com represents one of the clearest examples of SaaS. Companies rent space on their customer relationship management system ([CRM](http://www.bestpricecomputers.co.uk/glossary/crm-software-solutions.htm)) and log onto the website without having to download or install any software. Everything is provided by the company and the only thing the customer organization has to do is load their data and configure their preferences.

Salesforce.com also sells a PaaS offering, Force.com. They remove the top layer of their CRM application and adding configuration tools Salesforce.com offers customers the ability to build their own business applications. These applications can access databases, use workflow concepts, have user interfaces and be built and deployed rapidly.

Sales Force .com has the following accreditations:

* ISO 2700

**Google Apps**

Google Apps consist of Gmail, Google Calendar, Google Docs, and other web based applications. These services, characterized by redundant computing environments and dynamic resource allocation, enable customers to access their data virtually anytime and anywhere from Internet-capable devices. This Cloud computing environment allows shared CPU, memory and storage resources utilized by many customers while also offering centralized managed security benefits.

Google Apps has the following accreditations:

* Federal Information Security Management Act (FISMA) certification & accreditation
* SAS 70 Type II

**Microsoft Azure**

Microsoft Azure is Microsoft’s entry into the Cloud computing arena. Windows Azure™ is a cloud services operating system that serves as the **development, service hosting and service management environment** for the Windows Azure platform. Windows Azure provides developers with on-demand compute and storage to host, scale, and manage web applications on the internet through Microsoft® datacenters.

Windows Azure is a flexible platform that supports multiple languages and integrates with your existing on-premises environment. To build applications and services on Windows Azure, developers can use their existing [**Microsoft Visual Studio®**](http://msdn.microsoft.com/en-us/vstudio/dd582936.aspx)expertise. In addition, Windows Azure supports popular standards, protocols and languages including SOAP, REST, XML, Java, PHP and Ruby.

**Amazon EC2**

Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, offering the flexibility to enable customers to build a wide range of applications. Amazon EC2 utilizes a custom version of XEN hypervisor.

Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host system, the virtual instance operating system or guest OS, a firewall, and signed API calls. Each of these items builds on the capabilities of the others. The goal is to ensure that data contained within Amazon EC2 cannot be intercepted by unauthorized systems or users and that Amazon EC2 instances themselves are as secure as possible without sacrificing the flexibility in configuration that customers demand.

**Pros**

* Improve availability through massive and redundant compute, storage, and backup facilities capable of handling bursts or spikes in utilization.
  + Service provide the ability to quickly
* Better security than some small to medium-size businesses (SMBs) could afford to deploy them.
* Relieve customers from the Security Management.
* Include outsourced security services, such as reputation, multiple engine malware scanning, and other offerings that have potential scale economies or that benefit from cost sharing across multiple customers.

**Cons**

* Multiple, conflicting “cloud” definitions
* Vendor hype
* Inadequate service level agreements
* Lack of interoperability
* Vendor lock-in
* Poor transparency on security from the vendors
* Inability to audit and assess

**Conclusion**

The responsibility of security in the Cloud does not rest solely with the Cloud service provider. It is a joint responsibility between the service provider and the service consumer. The service provider must provide safe and secure environment. The service level agreement should be understood be all parties. The roles and responsibilities must be will defined. The biggest challenge to today’s Cloud environment is consumer confidence. It is not an unreasonable fear even with the certification and accreditation process. The lack of legal enforce or penalties for failing to protect sensitive data. Until there are better guarantees in place to secure the data it would be wise to be very cautious on what information is shared in the Cloud.

References

Cloud Computing: What Accountants Need to Know By ALEXANDRA DEFELICE

OCTOBER 2010

ISO 2700X: A cornerstone of true security By Jonathan Gossels & Richard Mackey, Jr. ISSA Journal | April 2007

The NIST Definition of Cloud Computing , Authors: Peter Mell and Tim Grance Version 15, 10-7-09

Security Whitepaper: Google Apps Messaging and Collaboration Products, Google Inc 2010

Security Best Practices For Developing Windows Azure Applications

Andrew Marshall (Senior Security Program Manager, Security Engineering)  
Michael Howard (Principal Security Program Manager, Security Engineering)   
Grant Bugher (Lead Security Program Manager, OSSC)  
Brian Harden (Security Architect, OSSC)