New Requirements for Security and Compliance Auditing in the Cloud

Cloud computing poses new challenges for IT security, compliance, and audit professionals who must protect corporate data and IT assets, and verify compliance of security controls. The cloud uproots predictability of traditional IT architectures, security controls, and audit procedures, and forces cloud service subscribers to cede two vital capabilities to cloud service providers: (1) control of data, programs, and actions and (2) visibility on status of data and program usage.

This paper presents how the world of IT security, audit and compliance must change in cloud environments. Beginning with a definition of cloud computing and its various models, this paper explains how cloud computing is changing assumptions about security, and provides guidelines for auditors who must verify the effectiveness of security controls used within a cloud computing system.

Table of Contents

QUALYS®

Overview of Cloud Computing

Establishing a clear definition for cloud computing is important because the term already enjoys wide use by the general public – despite considerable variation of meaning as understood by IT professionals. Both the European Network and Information Security Agency (ENISA) and the US National Institute of Standards and Technology (NIST) provide broadly similar definitions of what cloud computing is. According to NIST:

> ***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.***[1]

Characteristics defined by NIST include on demand self-service, which allows a cloud consumer to provision services without requiring human intervention by a service provider; broad network access by a variety of standard mechanisms and devices; resource pooling that enables providers to simultaneously service multiple consumers who themselves have no control or knowledge of individual technologies and resources operating "behind the curtain" of the cloud; rapid elasticity allowing consumers to quickly provision additional levels of service based on need; and measured service allowing usage to be monitored, controlled and reported.

The NIST definition goes on to identify five essential characteristics of cloud computing: on demand self-service, which allows a cloud consumer to provision services without requiring human intervention by a service provider; broad network access by a variety of standard mechanisms and devices; resource pooling that enables providers to simultaneously service multiple consumers who themselves have no control or knowledge of individual technologies and resources operating "behind the curtain" of the cloud; rapid elasticity allowing consumers to quickly provision additional levels of service based on need; and measured service allowing usage to be monitored, controlled, and reported.

Furthermore, consumers of cloud computing may choose from three kinds of cloud services, defined by NIST as:

- **Cloud Software-as-a-Service (SaaS)** – allowing a consumer to use a provider's applications that operate on the provider's infrastructure. For example, security and compliance offerings from Qualys are SaaS.

- **Cloud Platform-as-a-Service (PaaS)** – allowing a consumer to deploy applications it creates or acquires onto cloud infrastructure using the provider's programming languages and tools. With PaaS, the consumer controls the application but not the underlying infrastructure. An example is Windows Azure from Microsoft Corporation.

- **Cloud Infrastructure-as-a-Service (IaaS)** – allowing a consumer to run operating systems and applications on a cloud provider's infrastructure. IaaS is like renting an IT department owned and operated by a cloud provider. An example is Amazon Elastic Compute Cloud (EC2).

In addition, ENISA notes that cloud computing services are available in three main deployment models[2] . A private cloud operates according to cloud computing principles, but is accessible only within a private network . A partner cloud, also sometimes known as a community cloud, consists of cloud services offered by a provider to a limited and well-defined number of parties. A public cloud is available to any individual or organization who wants to rent its services (Qualys services are delivered by a public cloud). In addition, NIST identifies a fourth model, the hybrid cloud, which is any combination of the above; it is comprised of two or more clouds connected for data and application portability.

1 "The NIST Definition of Cloud Computing (Draft)," NIST Special Publication 800-145, p. 2 (Jan. 2011); http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

2 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Cloud Limits for Legacy Security Controls

There are many types of clouds, but all share a defining trait: subscribers must cede control and visibility to cloud service providers. NIST amplifies this notion:[3]

- **Control:** : the ability to decide, with high confidence, who and what is allowed to access subscriber data and programs, and the ability to perform actions (such as erasing data or disconnecting a network) with high confidence both that the actions have been taken and that no additional actions were taken that would subvert the subscriber's intent (e.g. a subscriber request to erase a data object should not be subverted by the silent generation of a copy).

- **Visibility:** : the ability to monitor, with high confidence, the status of a subscriber's data and programs and how subscriber data and programs are being accessed by others.

IT security, compliance, and audit professionals will acknowledge control and visibility as vital enablers of traditional security mechanisms used to protect data and programs, and to verify the effectiveness of those controls for compliance. With the legacy data center-centric model of computing, the issues of control and visibility were never in question. Security focused on a well-defined perimeter, which is why primary controls aimed to reinforce the data center from external attacks. Compliance laws such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act in the US and national laws in European countries flowing from the European Union's Data Privacy Directive also raised the bar for internal security and compliance. These requirements jump started the emergence of Governance, Risk Management & Compliance (GRC) tools for such activities as risk assessment, configuration management, and vulnerability management.

The issues of control and visibility affect responsibility for execution of security, audit and compliance. For example, for purposes of compliance with the Payment Card Industry Data Security Standard (PCI DSS), the globally implemented standard for securely processing credit and cards, the PCI Security Standards Council recommends entities consider how responsibility shifts based on the type of cloud service offering (see the Council's illustration): [4]

Example of how scope and responsibility may differ* by type of cloud service:

	Cloud customer responsibility
	Cloud service provider responsibility

	Type of Cloud Service		
Area of Responsibility	IAAS	PAAS	SAAS
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

* ***Note:*** *This is an example only. Cloud service offerings should be individually reviewed to determine how responsibilities* between *the cloud provider and cloud customer are assigned.*

Auditing Security of Mobile Devices

Mobile devices introduce new risks as sensitive data in the cloud may be accessed remotely, or is stored on the mobile endpoints. Here are a few key recommendations from security education and certification body ISACA [5]:

- Verify that any data labeled as sensitive are properly secured while in transit or at rest.
- Verify whether mobile device users are connecting to the enterprise network via a secure connection.
- Verify whether there is an asset management process in place for tracking mobile devices.
- Verify that data synchronization of mobile devices is not set to receive access to shared files or network drives with data prohibited for mobile use.

3 "DRAFT Cloud Computing Synopsis and Recommendations," NIST Special Publication 800-146, p. 4-3 (May 2011); http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

4 PCI Security Standards Council, "Information Supplement: PCI DSS Virtualization Guidelines," p. 23 (June 2011), https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

5 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx

Given the nature of shared responsibilities in cloud environments, it's important that service providers facilitate extension of audit and compliance tools into areas they directly manage. Enterprises need this collaboration because security regulations and newer laws are extending the compliance umbrella to assessment of third parties – like cloud service providers. It's an offshoot of data mobility stemming from outsourcing, offshoring, and the massive adoption of doing business "anytime, anywhere" with mobile devices.

Mobile Devices Pose New Audit Issues

In the past, security and audit professionals could assume data was always inside the protected perimeter. Now, it's a sure bet that that data can be virtually anywhere outside the traditional perimeter – especially with the adoption of cloud computing. Traditional agent-based monitoring and audit tools do not automatically extend into cloud systems. Moreover, sensitive data also is stored on smartphones, tablets, and other portable devices. Security and audit tools likewise do not automatically extend to mobile devices. Most of these devices do not use traditional operating systems, such as Windows, so they couldn't run traditional agent software if you wanted them to. For these reasons, it is important to identify new requirements for securing data in the cloud, and your ability to verify its security for compliance.

New Requirements for Cloud Security

The nature of cloud computing means your organization won't have a familiar degree of direct control over security of data and verification of its safety. That limitation is not stopping organizational adoption of cloud computing, however, so in a world of realpolitik, IT security, compliance, and audit professionals must pursue indirect solutions that achieve similar results to what they expect in traditional data center environments.

Many organizations use one or more frameworks to structure and prioritize choosing, deploying, and managing a myriad of security controls. In this paper, we have used the ISO27000 family of standards, which have been widely adopted by both public and private sector organisations within Europe. For organisations who must also comply with the US-based NIST standard, an appendix to NIST Special Publication 800-53: Recommended Controls for Federal Information Systems and Organizations provides a mapping between the two standards. [6]

ISO27002 divides security controls into eleven broad classes: these correspond to major sections of a typical security plan for an organization. For cloud environments, it is assumed the controls for the cloud are owned by external providers.

Cloud Security Hinges on Browser Security

Browsers are on the front line of the cloud. If they are insecure, the cloud is at risk. Follow these steps to ensure browser security:

- Update browser patches.Keep browser security patches up-to-date. According to research by Qualys, about 70% of installed browsers are vulnerable. Of those, 20% of the vulnerabilities are in the browser code or configuration.
- Update plug-ins. Browser plug-ins account for 80% of the vulnerabilities. Of these, most are in popular applications like Adobe Acrobat Reader, QuickTime, and especially Java.
- Regularly scan browsers. Scanning for browser and plug-in vulnerabilities is essential for security and audit. Repeat after remediation to ensure compliance.

Legacy Environments	Cloud Environments
A.5 Security Policy	
• Policies focus on processes affecting internal systems owned and operated by an enterprise.	• Policies focus on processes affecting external systems owned and operated by a provider.
A.6 Organization of information security	
• Internally managed procedures for risk assessment and vulnerability management.	• Provider must confirm execution of appropriate risk assessment and vulnerability management procedures.
• Enterprise completes appropriate security accreditations and assessments.	• Provider must confirm completion of appropriate security accreditations and assessments.
A.7 Asset Management	
• The enterprise must provide and maintain all physical and digital infrastructure. The focus is on internal systems owned and operated by an enterprise.	• Provider must provide and maintain physical and digital infrastructure. Focus is on external systems owned and operated by a provider.

6 See http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

A8. Human Resources Security	
• Focus on employees and contractors who work directly for an enterprise.	• Focus on employees and contractors who work directly for a provider.
• Personnel screening is by an enterprise.	• Provider must confirm effective personnel screening. This includes enforcement of screening standards in all international locations.
A9. Physical and Environmental Security	
• The enterprise must provide physical security including physical entry controls, as well as ensure appropriate siting of equipment and utilities, along with secure disposal of equipment.	• Provider must confirm effective controls for physical and environmental security at all its locations.
A10. Communications and operations management	
• Operations are solely the responsibility of the enterprise.	• If a provider goes out of business, it must provide assurance the subscriber will be able to take control of its applications and data prior to the provider's infrastructure going offline. Provider must provide assurance that the subscriber's applications and data will not become property of the provider's creditors upon bankruptcy.
• The enterprise is responsible for system and information integrity.	• Provider must confirm controls for system and information integrity.
A11. Access Control	
• Identification and authentication are handled internally.	• The subscriber's internal identification and authentication system ideally will work with the cloud provider's systems.
• Access controls are handled internally.	• Provider must confirm separation of duties and access are strictly enforced with its employees and contractors to prevent unapproved access to subscriber's data.
A12. Information systems acquisition, development and maintenance	
• Configuration management of new and existing equipment is controlled by an enterprise.	• Provider must confirm effective configuration management.
• System and communications controls are handled internally.	• Provider must confirm appropriate controls are in place for protecting systems and communications. This includes breaches that could occur from co-tenants on the cloud infrastructure as well as external vectors. Provider must ensure subscriber's service is not disrupted due to denial of service attacks on co-tenants.
A13. Information security incident management	
• Controls to identify and report on incidents and to respond to them are handled internally.	• Provider must confirm appropriate controls are in place to identify and report on incidents and to respond to them, and give subscribers independently auditable reports on all incidents.
A14. Business continuity management	
• The enterprise must provide contingencies for backup and disaster recovery.	• Provider must confirm backup and recovery contingencies for incidents, whether involving physical infrastructure or otherwise.
A15. Compliance	
• The enterprise is responsible for compliance with jurisdictional requirements, such as data protection laws in specific states or data privacy laws in specific countries. It alone interfaces with related law enforcement agencies.	• The provider must provide assurance of compliance for the subscriber. Provider must also assure subscriber that its service will not stop in order to satisfy legal cease-and-desist or other injunction affecting a co-tenant's service. Subscriber data must not be subject to search if law enforcement executes a search warrant against a co-tenant.
• Audit and accountability controls are handled internally or by independent auditors.	• Provider must give subscriber independently auditable evidence that all processes and SLAs are performing to contract specifications.

Industry Initiatives for Cloud Security

The IT industry is developing standard solutions for cloud computing. One high profile effort is by the Cloud Security Alliance (CSA), a consortium of more than a hundred vendors and solution providers, located across five continents, working to promote the use of best practices for providing security assurance in the cloud (see https://cloudsecurityalliance.org). An important sub-group in CSA is CloudAudit, which is developing an application programming interface to enable automation of audit, assertion, assessment, and assurance of data and applications in and between multiple clouds (see www.cloudaudit.org).

By building security and audit capabilities directly into cloud infrastructures, the industry believes it can amortize significant fixed costs that would otherwise be too expensive for individual user organizations. In a presentation at the Ninth Workshop on the Economics of Information Security held in June 2010, Dave Molnar and Stuart Schechter of Microsoft Research noted examples, such as "assembling a host and network security strategy, training staff on the full range of tasks required by the security strategy, keeping abreast of new threats and countermeasures, and developing a relationship with law enforcement [for compliance]."[7] They also note specific security and audit features that could be built into clouds, which would be similar to hosting tools such as Cpanel:

- Network and operating system auditing tools
- Tracking of all installed software, publishers, versions, and patch levels
- Credit card storage and fraud detection
- Public / private key generation, certificate generation, and storage
- Automatic authentication and protection of intra-tenant network communications
- Secure (append-only) logging of system events
- Spam filtering
- Password hashing and storage
- CAPTCHA generation and verification
- Software widgets such as password-strength meters

Over time, such vendor-driven efforts will ease the burden by subscribers of securing data in the cloud and verifying security of those data.

Checklists for Cloud Security & Audits

We conclude with two checklists addressing the main security and compliance challenges of cloud computing: securing data in a cloud environment and auditing security of that data. While these considerations are not exhaustive, they do present a path to stimulate preparation by IT security, compliance, and audit professionals as their responsibilities extend to the new world of cloud computing.

Industry Initiatives for Cloud Audit & Compliance

CSA cloud security alliance℠

CloudAudit

OPEN DATA CENTER ALLIANCE

Assessing Risks in Virtual Environments

Virtualization is the bedrock of cloud computing. It brings operational efficiencies and economies of scale – along with new challenges for audit and compliance. The PCI Security Standards Council, which sets globally implemented standards for securely processing credit and debit cards, recommends four elements when performing a risk assessment of virtual environments:

- **Define the environment.** You must identify every component, traffic flows and communication, physical location of components and data, functions and security levels of virtualized components, how segmentation is implemented, and many others.
- **Identify threats.** You must identify where potential attacks could affect the virtual environment. Consider virtual components such as the hypervisor, or unsecured out-of-band communications channels between shared components.
- **Identify vulnerabilities.** In addition to the usual vulnerabilities affecting physical resources, vulnerabilities may affect specific virtualization technologies and configurations. Traditional assessment tools do not have visibility into a virtual environment.
- **Evaluate and address risk.** The result will determine if you require additional controls to protect data in a virtualized environment.

7 David Molnar and Stuart Schechter, "Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud," p. 11 (Microsoft Research: 8 June 2010); http://weis2010.econinfosec.org/papers/session5/weis2010_schechter.pdf.

Securing Data in the Cloud

	Issue	Task
❑	Data Ownership	Do you have full rights and access to your data?
❑	Data Separation/ Segregation	Is your data isolated from other customers' data?
❑	Data Encryption	Is your data encrypted in transit and at rest?
❑	Data Backup/ Recovery	Is your data being backed up and available for recovery?
❑	Data Destruction	Is your data securely destroyed when no longer needed?
❑	Access Control	Who has access to your data?
❑	Activity/Log Management	Is access to your data logged and regularly monitored?
❑	Incident Response	Are there processes and notifications in place for incidents (including breaches) that impact your data?
❑	Security Controls	Are the appropriate security and configuration control in place to protect your data?
❑	Patch Management	Are the systems storing your data patched for the latest vulnerabilities and exploits?

Verifying Security of Data in the Cloud

	Issue	Task
❑	Right-to-Audit Clause	Do you have the ability to audit the provider?
❑	External Audit	Does the provider use an external auditor and provide those audit reports for review?
❑	Security Certifications	Does the provider have certification(s) to verify security controls?
❑	Security Monitoring	Do you have access to security tools to monitor the overall security of your data?
❑	Audit Process	What risks are applicable and what audit steps and tools will you use to audit those risks?

Learn More

Qualys SaaS solutions for security risk and compliance management are used by thousands of enterprises worldwide. Please visit qualys.com to learn more, see demos, or register for a free trial.

About Qualys

Qualys, Inc. is the leading provider of Software-as-a-Service (SaaS) IT security risk and compliance management solutions. Qualys solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures.

The QualysGuard® service is used today by more than 5,000 organizations in 85 countries, including 45 of the Fortune 100, and performs more than 500 million IP audits per year. Qualys has the largest vulnerability management deployment in the world at a leading global company, and has been recognized by leading industry analysts for its market leadership.
Qualys has established strategic agreements with leading managed service providers and consulting organizations including BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, Dell SecureWorks, Symantec, Tata Communications and TELUS. Qualys is a founding member of the Cloud Security Alliance (CSA).

For more information, please visit **www.qualys.com**.

QUALYS®
www.qualys.com

Qualys, Inc. - Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world. To find an office near you, visit
http://www.qualys.com

ON DEMAND SECURITY