



Strategies for Secure Cloud Computing

An Introduction to Exploring the Cloud



There is a lot of buzz these days about cloud computing and how it's going to revolutionize the way we do business. While cloud computing isn't new--it has been around for over 10 years in various forms--it seems to be approaching critical mass. We understand it better today. In this paper, we will provide clear definitions for each cloud implementation, discuss vetting strategies for the selection of cloud services, and talk about ongoing management requirements for these services once they are deployed. Please note that this is not a comprehensive cloud deployment strategy paper, rather an introduction providing direction for further exploration into the cloud.

Definition of Terms

In order to properly begin a conversation on cloud computing, it's important to define the terms and use them when designing a cloud deployment strategy to meet your company's business needs. Listed below are the National Institute of Science and Technology's (NIST) definition of cloud computing and its underlying components. Please get familiar with them as they are imperative to understanding how your company can best leverage a cloud environment.

Cloud Computing Definition

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

Service Models

Cloud Software as a Service (SaaS): The capability provided to the consumer is 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). The consumer 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.

¹ Mell, Peter and Grance, Tim, "The NIST Definition of Cloud Computing", Version 15, October 7, 2009



Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer 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.

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems including storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, and policy and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or to a large industry group, and is owned by an organization selling cloud services.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

As you can see, the term “cloud computing” incorporates many types of service and deployment models. The use of the all-encompassing term “the cloud” is highly overused; it does not accurately describe what type of services are actually to be procured or how they are being deployed, so it is difficult to determine the risk associated with them. With our nomenclature in place, let’s move on to the next building block.

One Cloud Does Not Fit All: What Cloud Services Could Work for You

If a company is to understand what risks are associated with moving portions of their network into a cloud environment (I know of no fully deployed cloud network), they must first understand (map) their network, classify their information assets, identify which deployment models and services align with the company’s IT and security strategy, and then vet the solution providers to ensure they can meet the company’s particular requirements.

Step 1: Map Network

This is critical as your network topology should include all physical and virtual segments, so that the most efficient and secure design can be achieved. Note that network mapping should not just include the physical network; it should include the identification of all applications, databases and data flows, so that each component of the network can be properly aligned with corporate security policy.



Step 2: Classify Assets

Now that the network is properly mapped, the data flows should be reviewed to ensure that each of the information assets is properly classified. If you are not familiar with asset classification, I have attached a sample matrix (Table 1), so you may familiarize yourself with this process. Notice that the classification of an asset will drive who has access to the information, how it is transmitted and stored, and ultimately how it is destroyed. Asset classification is a cornerstone of your information security program and proper implementation of this control will greatly enhance your organization's ability to meet its legal and regulatory requirements relative to the safekeeping of consumer data.

Table 1 – ISO 2701 Information Classification Matrix²

INFORMATION CLASSIFICATION MATRIX AND HANDLING GUIDE							
CATEGORY	DESCRIPTION	Sample Documents/Records	MARKING	PHYS & ADMIN CONTROLS	REPRODUCTION	DISTRIBUTION	DESTRUCTION/ DISPOSAL
PUBLIC or open	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. The [PR Office/Marketing Dept./Information Security Management dept./etc.] must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization.	Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices	None	None	Unlimited	No restrictions	Recycling/trash
INTERNAL or proprietary	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient. Disclosure to anyone outside of [Company name] requires management authorization.	Most corporate information falls into this category. Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options, transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages	INTERNAL USE ONLY Apply to bottom left corner of each page	Author: responsible for proper markings. User: responsible for proper storage and document control	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement	Internal: use an internal mail envelope. External: use a sealed envelope. Electronic: use internal email system. Encryption is required for transmission to external email addresses. FAXing: take care over the FAX number!	Paper documents: shred. Electronic data: erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal
CONFIDENTIAL or restricted	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager	Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information	CONFIDENTIAL Apply to bottom left corner of each page	Originator: responsible for ensuring that confidential information is distributed on a strict need-to-know basis. Recipient: responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use.	Limited copies may be made only by permission of originator or his/her designates. A signed authorization slip will be presented	Internal: use a sealed envelop inside an internal mail envelope. Hand deliver if possible. External: use a plain sealed envelope. Hand deliver or send by registered mail, courier etc. Electronic: use internal email system only. Encrypt data. FAXing: requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt.	Paper documents: shred using an approved cross-cut shredder. Electronic data: erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal

This work is copyright © 2008, Richard D. Regalado and ISO27k implementers' forum, some rights reserved. It is licensed under the Creative Commons Attribution-NonCommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.ISO27001security.com, and (c) derivative works are shared under the same terms as this.

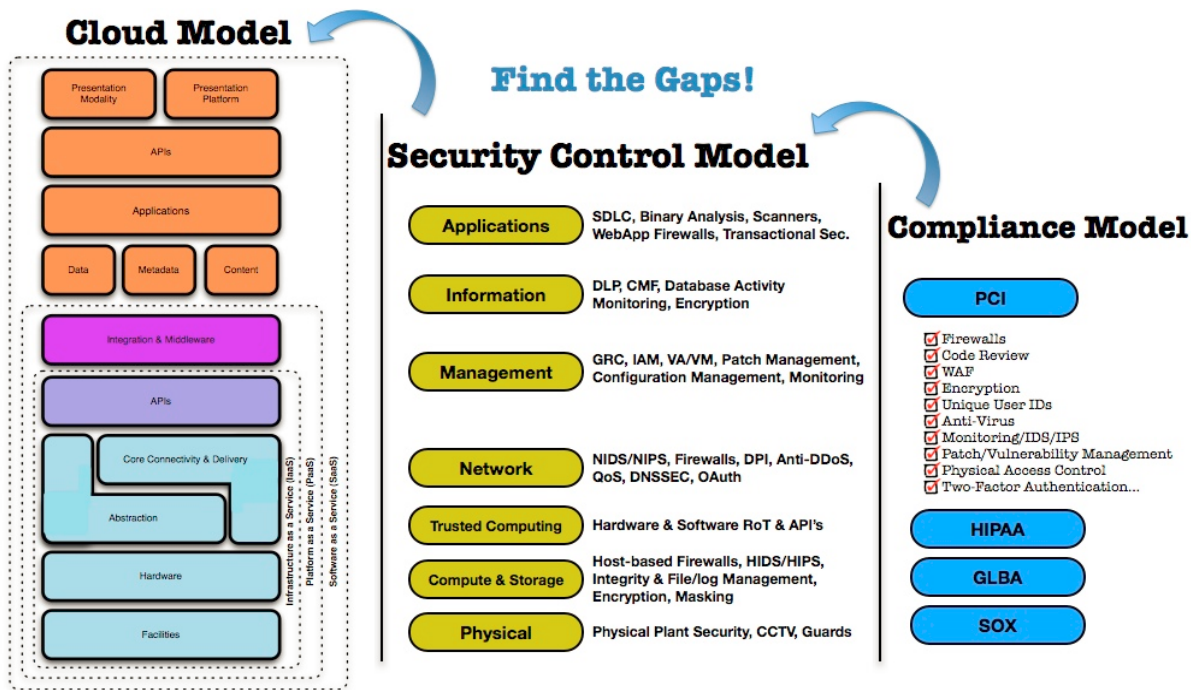
² Courtesy of the ISO27k implementers' forum www.ISO27001security.com



Step 3: Map Assets to Cloud Deployment Models

When information assets have been mapped and classified, you are in a position to identify which type of cloud model and may fit your organization’s needs. As you can see in Table 2 (below), the type of information resident on your system will drive your security needs and your security needs will, in turn, determine which cloud deployment model is right for your organization.

Table 2 - Mapping the Cloud Model to the Security Control & Compliance Model³



Step 4: Evaluate Potential Cloud Service Models and Providers

This step is a bit tricky and requires you to look at the solution to ensure that it meets both the requirements set forth by your IT department and information security policy. If the solution is deficient in either, then it is not a match. All SLA should contain language that covers you from both of these perspectives and provide the ability to independently validate the security of the solution. Furthermore, particular attention should be paid to the portability of the data from this solution or provider so that migration from the solution or provider can be achieved relatively easily. It is also important that a financial review of the cloud vendor be conducted prior the deployment as this their financial condition will have significant impact on their operations and your services.

After identifying potential solutions, the next building block on the cloud foundation is a deeper dive into the solutions security posture.

Basic Security Still Applies to the Cloud: You Can't Outsource Responsibility!

The title of this section should be self-evident, but I'll reiterate for the sake of clarity. Just because a section of the network isn't managed by your company doesn't mean that the data you put on this network isn't subject to your

³ Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

company's policies and procedures for the securing that data. Ensuring that the cloud vendor or solution you've selected meets or exceeds your company's policy for the securing of data (that will be stored or processed by that vendor or solution) is key to the implementation of a successful cloud deployment.

Note: This paper is just a cursory view of how we think about the cloud. Please visit the following resources for a more in-depth view of cloud security and vendor evaluation tools: Cloud Security Alliance at www.cloudsecurityalliance.org , and Jericho Forum at www.opengroup.org/jericho/ .

After the vendor or solution has been selected and reviewed to ensure it's in line with your organization's IT requirements and security policies, there is still one more step to completion.

Vigilance is the Price of the Cloud: Ongoing Monitoring is a Must

Ah, yes, the much maligned vendor management program. You've gone through the trouble of identifying a cloud solution that fits your organization's needs. However, it is imperative to have the right tools in place to ensure that the solution or vendor continues to live up to the obligations set forth in the contract/SLA. It is up to you to determine what is important to your organization (99% availability, compliance with the PCI DSS standard, etc.), but it must be in writing and you must have an independent way to validate that the solution or vendor is meeting your criteria (this would be transparency, another essential requirement of a cloud solution). If you have an internal audit team, this would be a good use of their time. If not, then ensure someone on your staff has the skill set to pull together and execute a vendor audit or monitoring program.

Network in the Cloud, Feet on the Ground: Pulling it All Together

The principles involved in cloud computing are not that complicated (but the technical details are!) and they aren't that new. As a matter of fact, many of them leverage the technologies and processes currently found in the mainframe environment. So don't let someone bamboozle you into thinking that it's this new-fangled thing. Using sound judgment and existing security techniques, you may find the portion of the cloud that's the right fit for your company's growing network needs.

Jim Bibles leads the Business and Product Development teams for ComplyGuard Networks. He is widely recognized as an expert in the development and implementation of risk-based compliance programs. His focus for the past 10 years has been in the payment space where he has implemented information security and merchant PCI DSS compliance programs for such companies as Visa Inc. and Wells Fargo Merchants Services. His current focus is developing merchant network vulnerability and risk management tools for small to medium-sized businesses and their service providers, so that they are in a better position to make intelligent, risk-based decisions on how they secure their network. Jim is a QSA and is an active thought leader within the payments community.

About ComplyGuard Networks

ComplyGuard Networks has more than 30 years of combined expertise in network security including vulnerability assessments, audit, penetration testing, and web application security. Our intellectual property portfolio positions ComplyGuard Networks uniquely in statutory and policy compliance. ComplyGuard Networks can provide any PCI or network security-related services businesses may require. For more information, contact us at 210-835-2000 or email info@complyguardnetworks.com. On the Web, visit www.complyguardnetworks.com.

