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

Prepared by the
Cloud Security Alliance
December 2009

Introduction

The guidance provided herein is the second version of the Cloud Security Alliance document, **"Security Guidance for Critical Areas of Focus in Cloud Computing"**, which was originally released in April 2009. The permanent archive locations for these documents are:

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (this document)
http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf (version 1 guidance)

In a departure from the first version of our guidance, a decision was made to separate the key guidance from the core domain research. Each domain's core research is being released as its own white paper. These white papers and their release schedule are located at:

http://www.cloudsecurityalliance.org/guidance/domains/

In another change from the first version, **Domain 3: Legal** and **Domain 4: Electronic Discovery** were combined into a single domain. Additionally, **Domain 6: Information Lifecycle Management** and **Domain 14: Storage** were combined into a single domain, renamed Data Lifecycle Management. This has caused a renumbering of our (now 13) domains.

Table of Contents

Foreword

Welcome to the second version of the Cloud Security Alliance's "Security Guidance for Critical Areas of Focus in Cloud Computing". As the march of Cloud Computing continues, it brings both new opportunities and new security challenges. We humbly hope to provide you with both guidance and inspiration to support your business needs while managing new risks.

While the Cloud Security Alliance might be best known for this guidance, over the course of the next several months you will see a wide range of activities, including international chapters, partnerships, new research, and conference activities geared towards furthering our mission. You can follow our activities at www.cloudsecurityalliance.org.

The path to secure cloud computing is surely a long one, requiring the participation of a broad set of stakeholders on a global basis. However, we should happily recognize the progress we are seeing: new cloud security solutions are regularly appearing, enterprises are using our guidance to engage with cloud providers, and a healthy public dialogue over compliance and trust issues has erupted around the world. The most important victory we have achieved is that security professionals are vigorously engaged in securing the future, rather than simply protecting the present.

Please stay engaged on this topic, and continue to work with us to complete this important mission.

Best Regards,

Jerry Archer	Dave Cullinane	Nils Puhlmann
Alan Boehme	Paul Kurtz	Jim Reavis

The Cloud Security Alliance Board of Directors

Acknowledgments

Editors

Glenn Brunette
Rich Mogull

Contributors

Adrian Seccombe
Alex Hutton
Alexander Meisel
Alexander Windel
Anish Mohammed
Anthony Licciardi
Anton Chuvakin
Aradhna Chetal
Arthur J. Hedge III
Beau Monday
Beth Cohen
Bikram Barman
Brian O'Higgins
Carlo Espiritu
Christofer Hoff
Colin Watson
David Jackson
David Lingenfelter
David Mortman
David Sherry
David Tyson
Dennis Hurst
Don Blumenthal
Dov Yoran
Erick Dahan
Erik Peterson
Ernie Hayden
Francoise Gilbert
Geir Arild Engh-Hellesvik
Georg Hess
Gerhard Eschelbeck
Girish Bhat
Glenn Brunette
Greg Kane
Greg Tipps
Hadass Harel
James Tiller
Jean Pawluk
Jeff Reich
Jeff Spivey
Jeffrey Ritter
Jens Laundrup
Jesus Luna Garcia
Jim Arlen
Jim Hietala
Joe Cupano
Joe McDonald
Joe Stein
Joe Wallace
Joel Weise
John Arnold
Jon Callas
Joseph Stein
Justin Foster
Kathleen Lossau
Karen Worstell
Lee Newcombe
Luis Morales
M S Prasad
Michael Johnson
Michael Reiter
Michael Sutton
Mike Kavis
Nadeem Bukhari
Pam Fusco
Patrick Sullivan
Peter Gregory
Peter McLaughlin
Philip Cox
Ralph Broom
Randolph Barr
Rich Mogull
Richard Austin
Richard Zhao
Sarabjeet Chugh
Scott Giordano
Scott Matsumoto
Scott Morrison
Sean Catlett
Sergio Loureiro

Shail Khiyara
Shawn Chaput
Sitaraman Lakshminarayanan
Srijith K. Nair
Subra Kumaraswamy
Tajeshwar Singh
Tanya Forsheit
Vern Williams
Warren Axelrod
Wayne Pauley
Werner Streitberger
Wing Ko
Yvonne Wilson

Letter from the Editors

It is hard to believe that just seven short months ago, we pulled together a diverse group of individuals from all corners of the technology industry to publish the first "Security Guidance for Critical Areas in Cloud Computing." Since its launch, this seminal publication has continued to exceed our expectations for helping organizations around the world make informed decisions regarding if, when, and how they will adopt Cloud Computing services and technologies. But over those seven months our knowledge, and cloud computing technologies, have evolved at an astounding rate. This second version is designed to provide both new knowledge and greater depth to support these challenging decisions.

Adopting cloud computing is a complex decision involving many factors. It is our hope that the guidance contained in this work will help you better understand what questions to ask, the current recommended practices, and potential pitfalls to avoid. Through our focus on the central issues of Cloud Computing security, we have attempted to bring greater clarity to an otherwise complicated landscape, which is often filled with incomplete and oversimplified information. Our focus on the original 15 domains (now consolidated into 13) serves to bring context and specificity to the Cloud Computing security discussion: enabling us to go beyond gross generalizations to deliver more insightful and targeted recommendations.

On our journey, we have been joined by a growing list of industry organizations, corporations, and individuals who believe in our mission to develop and promote best practices for security assurance within Cloud Computing. Their perspectives and insights have been essential in creating a well-balanced, unbiased work that continues to serve as an excellent foundation upon which we can continue to build.

Cloud Computing is still a rapidly evolving landscape; and one that requires us to stay current or fall behind. In this release of version two of our guidance, we drew upon the collective experience and expertise of our large and diverse volunteer community to create a more complete work with greater detail and improved accuracy. Still, we must not be complacent. Just as security professionals have done for ages, we must continue to evolve our processes, methods, and techniques in light of the opportunities that Cloud Computing brings to our industries. This evolution is critical to our long-term success as we find new ways to improve the efficacy and efficiency of our security enforcement and monitoring capabilities.

Cloud Computing isn't necessarily more or less secure than your current environment. As with any new technology, it creates new risks and new opportunities. In some cases moving to the cloud provides an opportunity to re-architect older applications and infrastructure to meet or exceed modern security requirements. At other times the risk of moving sensitive data and applications to an emerging infrastructure might exceed your tolerance. Our goal in this Guidance isn't to tell you exactly what, where, or how to move into the cloud, but to provide you with practical recommendations and key questions to make that transition as securely as possible, on your own terms.

Finally, on behalf of the Cloud Security Alliance and the Editorial Working Group, we would like to thank each and every volunteer for all of their time and effort that was put into the development of this new guidance document. We were consistently inspired by the dedication of the teams to extend and improve their respective areas, and we believe that their efforts have

significantly added real value to this body of work. This document would not be what it is without their contributions.

As always, we are eager to hear your feedback regarding this updated guidance. If you found this guidance helpful or would like to see it improved, please consider joining the Cloud Security Alliance as a member or contributor.

Glenn Brunette
Rich Mogull
Editors

An Editorial Note on Risk: Deciding What, When, and How to Move to the Cloud

Throughout this Guidance we make extensive recommendations on reducing your risk when adopting cloud computing, but not all the recommendations are necessary or even realistic for all cloud deployments. As we compiled information from the different working groups during the editorial process, we quickly realized there simply wasn't enough space to provide fully nuanced recommendations for all possible risk scenarios. Just as a critical application might be too important to move to a public cloud provider, there might be little or no reason to apply extensive security controls to low-value data migrating to cloud-based storage.

With so many different cloud deployment options — including the SPI service models (SPI refers to **S**oftware as a Service, **P**latform as a Service, or **I**nfrastructure as a Service, explained in depth in Domain 1); public vs. private deployments, internal vs. external hosting, and various hybrid permutations — no list of security controls can cover all circumstances. As with any security area, organizations should adopt a risk-based approach to moving to the cloud and selecting security options. The following is a simple framework to help evaluate initial cloud risks and inform security decisions.

This process is **not** a full risk assessment framework, nor a methodology for determining all your security requirements. It's a quick method for evaluating your tolerance for moving an asset to various cloud computing models.

Identify the asset for the cloud deployment

At the simplest, assets supported by the cloud fall into two general buckets:

1. Data
2. Applications/Functions/Processes

We are either moving information into the cloud, or transactions/processing (from partial functions all the way up to full applications).

With cloud computing our data and applications don't need to reside in the same location, and we can even shift only parts of functions to the cloud. For example, we can host our application and data in our own data center, while still outsourcing a portion of its functionality to the cloud through a Platform as a Service.

The first step in evaluating risk for the cloud is to determine exactly what data or function is being considered for the cloud. This should include potential uses of the asset once it moves to the cloud to account for scope creep. Data and transaction volumes are often higher than expected.

Evaluate the asset

The next step is to determine how important the data or function is to the organization. You don't need to perform a detailed valuation exercise unless your organization has a process for that, but you do need at least a rough assessment of how sensitive an asset is, and how important an application/function/process is.

For each asset, ask the following questions:

1. How would we be harmed if the asset became widely public and widely distributed?
2. How would we be harmed if an employee of our cloud provider accessed the asset?
3. How would we be harmed if the process or function were manipulated by an outsider?
4. How would we be harmed if the process or function failed to provide expected results?
5. How would we be harmed if the information/data were unexpectedly changed?
6. How would we be harmed if the asset were unavailable for a period of time?

Essentially we are assessing confidentiality, integrity, and availability requirements for the asset; and how those are affected if all or part of the asset is handled in the cloud. It's very similar to assessing a potential outsourcing project, except that with cloud computing we have a wider array of deployment options, including internal models.

Map the asset to potential cloud deployment models

Now we should have an understanding of the asset's importance. Our next step is to determine which deployment models we are comfortable with. Before we start looking at potential providers, we should know if we can accept the risks implicit to the various deployment models: private, public, community, or hybrid; and hosting scenarios: internal, external, or combined.

For the asset, determine if you are willing to accept the following options:

1. Public.
2. Private, internal/on-premises.
3. Private, external (including dedicated or shared infrastructure).
4. Community; taking into account the hosting location, potential service provider, and identification of other community members.
5. Hybrid. To effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside.

At this stage you should have a good idea of your comfort level for transitioning to the cloud, and which deployment models and locations fit your security and risk requirements.

Evaluate potential cloud service models and providers

In this step focus on the degree of control you'll have at each SPI tier to implement any required risk management. If you are evaluating a specific offering, at this point you might switch to a fuller risk assessment.

Your focus will be on the degree of control you have to implement risk mitigations in the different SPI tiers. If you already have specific requirements (e.g., for handling of regulated data) you can include them in the evaluation.

Sketch the potential data flow

If you are evaluating a specific deployment option, map out the data flow between your organization, the cloud service, and any customers/other nodes. While most of these steps have been high-level, before making a final decision it's absolutely essential to understand whether, and *how*, data can move in and out of the cloud.

If you have yet to decide on a particular offering, you'll want to sketch out the rough data flow for any options on your acceptable list. This is to insure that as you make final decisions, you'll be able to identify risk exposure points.

Conclusions

You should now understand the importance of what you are considering moving to the cloud, your risk tolerance (at least at a high level), and which combinations of deployment and service models are acceptable. You'll also have a rough idea of potential exposure points for sensitive information and operations.

These together should give you sufficient context to evaluate any other security controls in this Guidance. For low-value assets you don't need the same level of security controls and can skip many of the recommendations — such as on-site inspections, discoverability, and complex encryption schemes. A high-value regulated asset might entail audit and data retention requirements. For another high-value asset not subject to regulatory restrictions, you might focus more on technical security controls.

Due to our limited space, as well as the depth and breadth of material to cover, this document contains extensive lists of security recommendations. Not all cloud deployments need every possible security and risk control. Spending a little time up front evaluating your risk tolerance and potential exposures will provide the context you need to pick and choose the best options for your organization and deployment.

Section I. Cloud Architecture

Domain 1: Cloud Computing Architectural Framework

This domain, the Cloud Computing Architectural Framework, provides a conceptual framework for the rest of the Cloud Security Alliance's guidance. The contents of this domain focus on a description of Cloud Computing that is specifically tailored to the unique perspective of IT network and security professionals. The following three sections define this perspective in terms of:

- The terminology used throughout the guidance, to provide a consistent lexicon.
- The architectural requirements and challenges for securing cloud applications and services.
- A reference model that describes a taxonomy of cloud services and architectures.

The final section of this domain provides a brief introduction to each of the other domains in the guidance.

Understanding the architectural framework described in this domain is an important first step in understanding the remainder of the Cloud Security Alliance guidance. The framework defines many of the concepts and terms used throughout the other domains.

What Is Cloud Computing?

Cloud computing ('cloud') is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them.

Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing.

More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption.

From an architectural perspective; there is much confusion surrounding how cloud is both similar to and different from existing models of computing; and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices.

There are many definitions today which attempt to address cloud from the perspective of academicians, architects, engineers, developers, managers, and consumers. This document focuses on a definition that is specifically tailored to the unique perspectives of IT network and security professionals.

The keys to understanding how cloud architecture impacts security architecture are a common and concise lexicon, coupled with a consistent taxonomy of offerings by which cloud services and architecture can be deconstructed, mapped to a model of compensating security and

operational controls, risk assessment and management frameworks, and in turn to compliance standards.

What Comprises Cloud Computing?

The earlier version of the Cloud Security Alliance's guidance featured definitions that were written prior to the published work of the scientists at the U.S. National Institute of Standards and Technology (NIST) and their efforts around defining cloud computing.

NIST's publication is generally well accepted, and we have chosen to align with the NIST Working Definition of cloud computing (version 15 as of this writing) to bring coherence and consensus around a common language so we can focus on use cases rather than semantic nuance.

It is important to note that this guide is intended to be broadly usable and applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted to suggest the exclusion of other points of view or geographies.

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in figure 1 and explained in detail below.

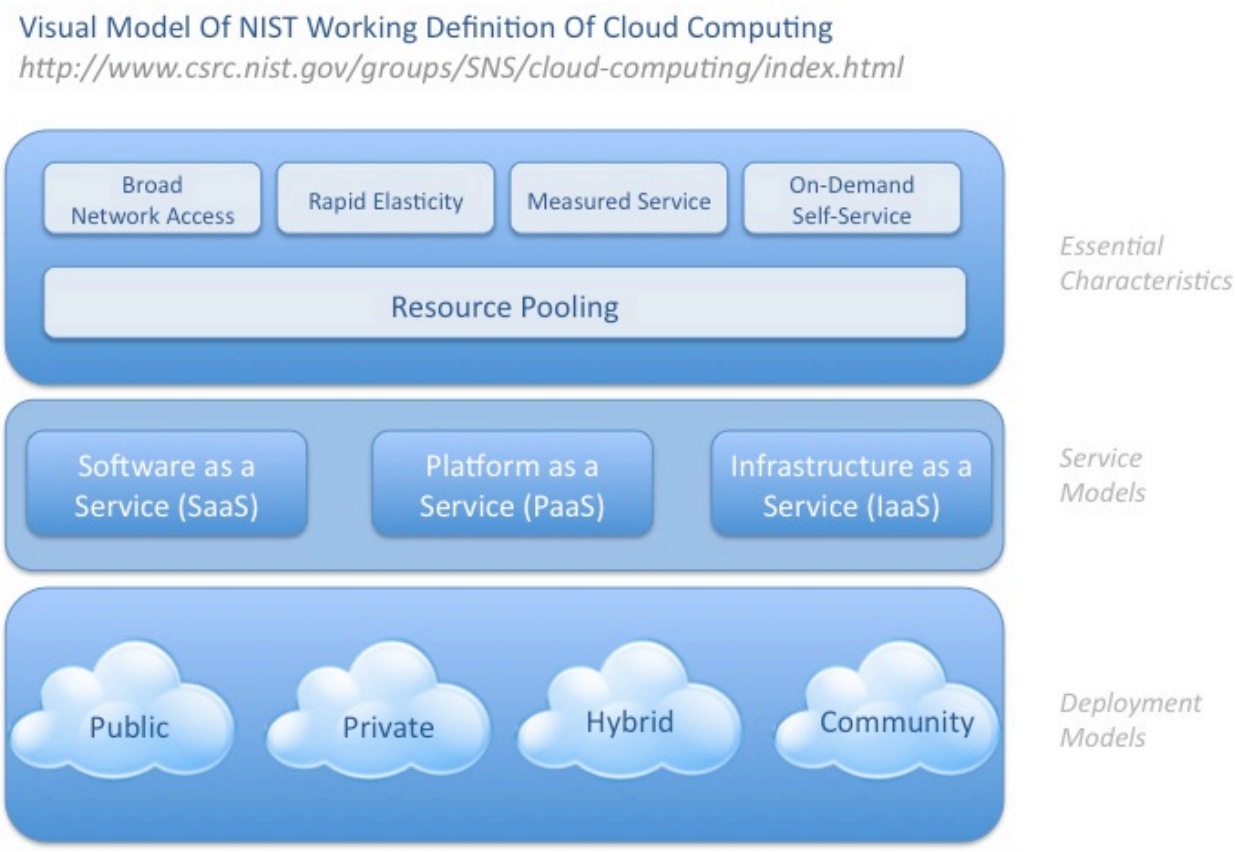


Figure 1 - NIST Visual Model of Cloud Computing Definition

Essential Characteristics of Cloud Computing

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

- **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 a 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, laptops, and PDAs) as well as other traditional or cloud-based software services.
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned — in some cases automatically — to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported — providing transparency for both the provider and consumer of the service.

It is important to recognize that cloud services are often but not always utilized in conjunction with, and enabled by, virtualization technologies. There is no requirement, however, that ties the abstraction of resources to virtualization technologies and in many offerings virtualization by hypervisor or operating system container is not utilized.

Further, it should be noted that multi-tenancy is not called out as an essential cloud characteristic by NIST but is often discussed as such. Please refer to the section on multi-tenancy featured after the cloud deployment model description below for further details.

Cloud Service Models

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model," where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively — defined thus:

- **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.

- **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, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

The NIST model and this document do not directly address the emerging service model definitions associated with cloud service brokers, those providers that offer intermediation, monitoring, transformation/portability, governance, provisioning, and integration services and negotiate relationships between various cloud providers and consumers.

In the short term, as innovation drives rapid solution development, consumers and providers of cloud services will enjoy varied methods of interacting with cloud services in the form of developing APIs and interfaces and so cloud service brokers will emerge as an important component in the overall cloud ecosystem.

Cloud service brokers will abstract these possibly incompatible capabilities and interfaces on behalf of consumers to provide proxy in advance of the arrival of common, open and standardized ways of solving the problem longer term with a semantic capability that allows fluidity and agility in a consumer being able to take advantage of the model that works best for their particular needs.

It is also important to note the emergence of many efforts centered around the development of both open and proprietary APIs which seek to enable things such as management, security and interoperability for cloud. Some of these efforts include the Open Cloud Computing Interface Working Group, Amazon EC2 API, VMware's DMTF-submitted vCloud API, Sun's Open Cloud API, Rackspace API, and GoGrid's API, to name just a few. Open, standard APIs will play a key role in cloud portability and interoperability as well as common container formats such as the DMTF's Open Virtualization Format (OVF.)

While there are many working groups, draft and published specifications under consideration at this time, it is natural that consolidation will take effect as market forces, consumer demand and economics pare down this landscape to a more manageable and interoperable set of players.

Cloud Deployment Models

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements:

- **Public Cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Private Cloud.** The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
- **Community Cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.
- **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).

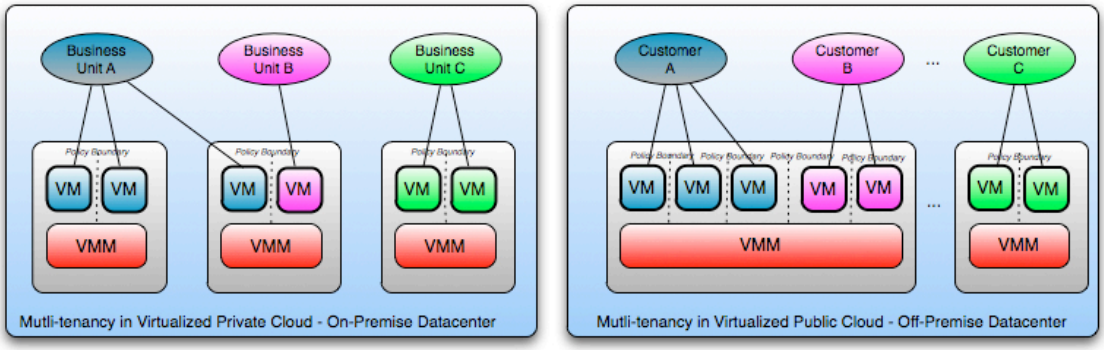
It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is virtual private clouds — a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers' datacenter, usually via virtual private network (VPN) connectivity.

The architectural mindset used when designing " solutions has clear implications on the future flexibility, security, and mobility of the resultant solution, as well as its collaborative capabilities. As a rule of thumb, perimeterized solutions are less effective than de-perimeterized solutions in each of the four areas. Careful consideration should also be given to the choice between proprietary and open solutions for similar reasons.

Multi-Tenancy

Although not an essential characteristic of Cloud Computing in NIST's model, CSA has identified multi-tenancy as an important element of cloud.

Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

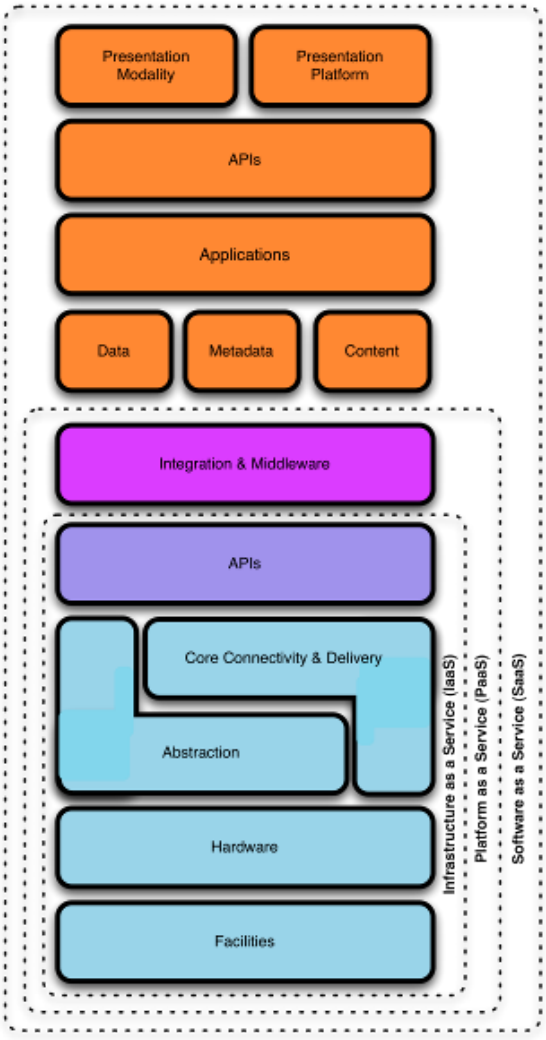


Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Figure 2 - Multi-Tenancy

From a provider's perspective, multi-tenancy suggests an architectural and design approach to enable economies of scale, availability, management, segmentation, isolation, and operational efficiency; leveraging shared infrastructure, data, metadata, services, and applications across many different consumers.



Multi-tenancy can also take on different definitions depending upon the cloud service model of the provider; inasmuch as it may entail enabling the capabilities described above at the infrastructure, database, or application levels. An example would be the difference between an IaaS and SaaS multi-tenant implementation.

Cloud deployment models place different importance on multi-tenancy. However, even in the case of a private cloud, a single organization may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. Thus multi-tenancy concerns should always be considered.

Cloud Reference Model

Understanding the relationships and dependencies between Cloud Computing models is critical to understanding Cloud Computing security risks. IaaS is the foundation of all cloud services, with PaaS building upon IaaS, and SaaS in turn building upon PaaS as described in the Cloud Reference Model diagram. In this way, just as capabilities are inherited, so are information security issues and risk. It is important to note that

commercial cloud providers may not neatly fit into the layered service models. Nevertheless, the reference model is important for relating real-world services to an architectural framework and understanding the resources and services requiring security analysis.

IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.

PaaS sits atop IaaS and adds an additional layer of integration with application development frameworks; middleware capabilities; and functions such as database, messaging, and queuing; which allow developers to build applications upon to the platform; and whose programming languages and tools are supported by the stack.

SaaS in turn is built upon the underlying IaaS and PaaS stacks; and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the application(s), and management capabilities.

It should therefore be clear that there are significant trade-offs to each model in terms of integrated features, complexity vs. openness (extensibility), and security. Trade-offs between the three cloud deployment models include:

- Generally, SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security (at least the provider bears a responsibility for security).
- PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.
- IaaS provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.

The key takeaway for security architecture is that the lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.

In the case of SaaS, this means that service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated; managed to; and enforced. In the case of PaaS or IaaS it is the responsibility of the consumer's system administrators to effectively manage the same, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. It should be clear in either case that one can assign/transfer responsibility but not necessarily accountability.

Narrowing the scope or specific capabilities and functionality within each of the cloud delivery models, or employing the functional coupling of services and capabilities across them, may yield derivative classifications. For example "Storage as a Service" is a specific sub-offering within the IaaS 'family'.

While a broader review of the growing set of cloud computing solutions is outside the scope of this document, the OpenCrowd Cloud Solutions taxonomy in the figure below provides an excellent starting point. The OpenCrowd taxonomy demonstrates the swelling ranks of solutions available today across each of the previously defined models.

It should be noted that the CSA does not specifically endorse any of the solutions or companies shown below, but provides the diagram to demonstrate the diversity of offerings available today.

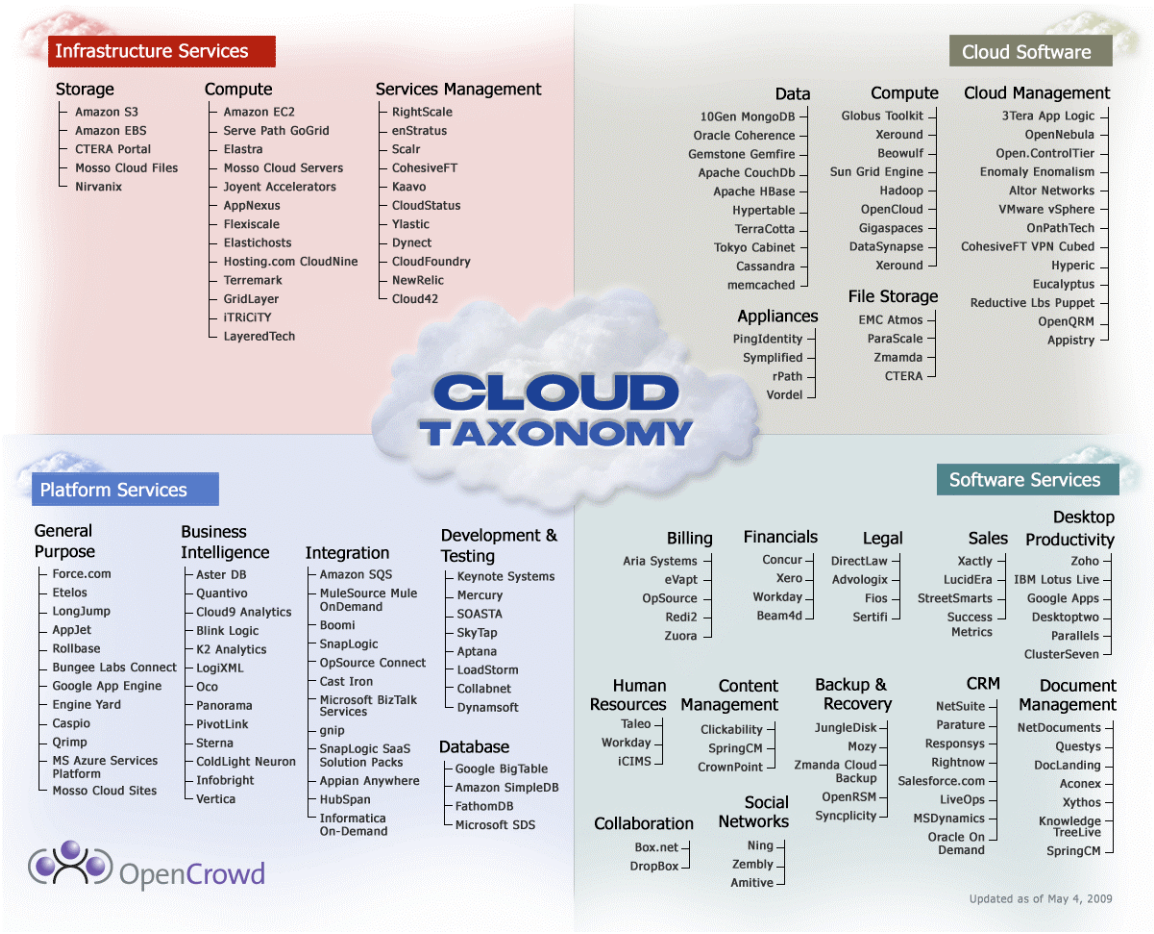


Figure 4 – OpenCrowd Taxonomy

For an excellent overview of the many cloud computing use cases, the Cloud Computing Use Case Group produced a collaborative work to describe and define common cases and demonstrate the benefits of cloud, with their goal being to "...bring together cloud consumers and cloud vendors to define common use cases for cloud computing...and highlight the capabilities and requirements that need to be standardized in a cloud environment to ensure interoperability, ease of integration, and portability."

Cloud Security Reference Model

The cloud security reference model addresses the relationships of these classes and places them in context with their relevant security controls and concerns. For organizations and individuals

grappling with cloud computing for the first time, it is important to note the following to avoid potential pitfalls and confusion:

1. The notion of *how* cloud services are deployed is often used interchangeably with *where* they are provided, which can lead to confusion. For example, public or private clouds may be described as external or internal clouds, which may or may not be accurate in all situations.
2. The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a firewall). While it *is* important to understand where security boundaries lie in terms of cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept.
3. The re-perimeterization and the erosion of trust boundaries already happening in the enterprise is amplified and accelerated by cloud computing. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of cloud services, all require new thinking with regard to cloud computing. The Jericho Forum has produced a considerable amount of material on the re-perimeterization of enterprise networks, including many case studies.

The deployment and consumption modalities of cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed by; and who is responsible for their governance, security, and compliance with policies and standards.

This is not to suggest that the on- or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do — but to underscore that risk also depends upon:

- The types of assets, resources, and information being managed
- Who manages them and how
- Which controls are selected and how they are integrated
- Compliance issues

For example a LAMP stack deployed on Amazon's AWS EC2 would be classified as a public, off-premise, third-party managed-IaaS solution; even if the instances and applications/data contained within them were managed by the consumer or a third party. A custom application stack serving multiple business units; deployed on Eucalyptus under a corporation's control, management, and ownership; could be described as a private, on-premise, self-managed SaaS solution. Both examples utilize the elastic scaling and self-service capabilities of cloud.

The following table summarizes these points:

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

Table - Cloud Computing Deployment Models

Another way of visualizing how combinations of cloud service models, deployment models, physical locations of resources, and attribution of management and ownership, is the Jericho Forum's (www.jerichoforum.org) Cloud Cube Model, shown in the figure below:

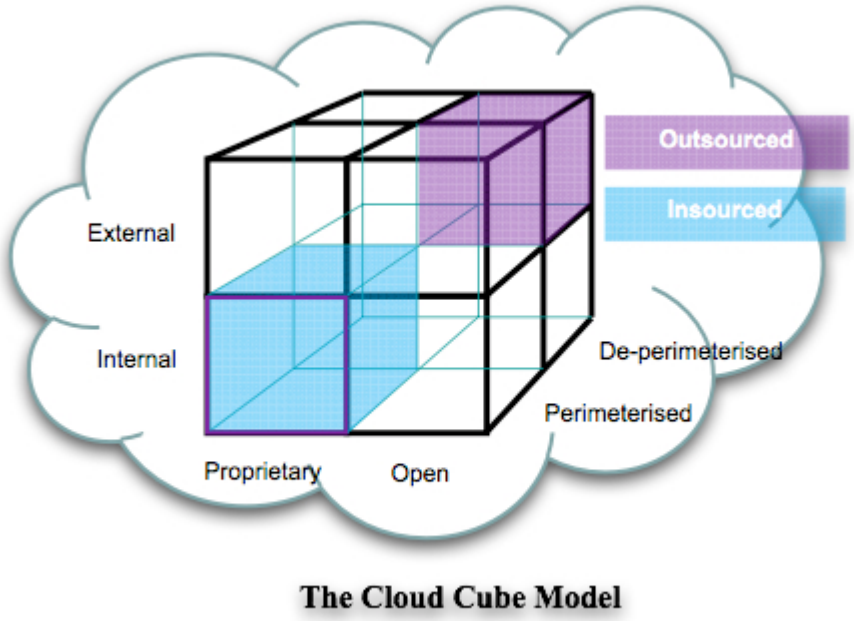


Figure 5 - Jericho Cloud Cube Model

The Cloud Cube Model illustrates the many permutations available in cloud offerings today and presents four criteria/dimensions in order to differentiate cloud 'formations' from one another and the manner of their provision, in order to understand how cloud computing affects the way in which security might be approached.

The Cloud Cube Model also highlights the challenges of understanding and mapping cloud models to control frameworks and standards such as ISO/IEC 27002, which provides "...a series of guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization."

The ISO/IEC 27002, section 6.2, "External Parties" control objective states: "…the security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services…"

As such, the differences in methods and responsibility for securing the three cloud service models mean that consumers of cloud services are faced with a challenging endeavor. Unless cloud providers can readily disclose their security controls and the extent to which they are implemented to the consumer, and the consumer knows which controls are needed to maintain the security of their information, there is tremendous potential for misguided decisions and detrimental outcomes.

This is critical. First one classifies a cloud service against the cloud architecture model. Then it is possible to map its security architecture; as well as business, regulatory, and other compliance requirements; against it as a gap-analysis exercise. The result determines the general "security" posture of a service and how it relates to an asset's assurance and protection requirements.

The figure below shows an example of how a cloud service mapping can be compared against a catalogue of compensating controls to determine which controls exist and which do not — as provided by the consumer, the cloud service provider, or a third party. This can in turn be compared to a compliance framework or set of requirements such as PCI DSS, as shown.

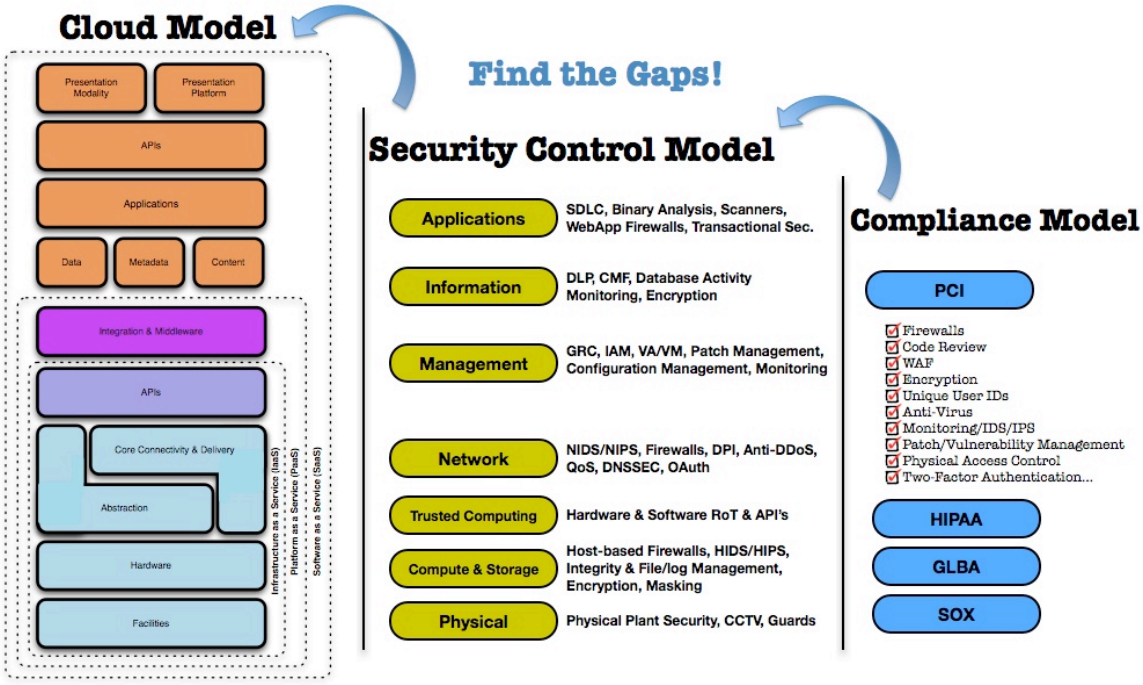


Figure 6 - Mapping the Cloud Model to the Security Control & Compliance Model

Once this gap analysis is complete, per the requirements of any regulatory or other compliance mandates, it becomes much easier to determine what needs to be done in order to feed back into a risk assessment framework; this, in turn, helps to determine how the gaps and ultimately risk should be addressed: accepted, transferred, or mitigated.

It is important to note that the use of cloud computing as an operational model does not inherently provide for or prevent achieving compliance. The ability to comply with any requirement is a direct result of the service and deployment model utilized and the design, deployment, and management of the resources in scope.

For an excellent overview of control frameworks which provides good illustrations of the generic control framework alluded to above, see the Open Security Architecture Group's 'landscape' of security architecture patterns documentation, or the always useful and recently updated NIST 800-53 revision 3 Recommended Security Controls for Federal Information Systems and Organizations security control catalogue.

What Is Security for Cloud Computing?

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), all the way to the information and applications (application security). Additionally controls are implemented at the people and process levels, such as separation of duties and change management, respectively.

As described earlier in this document, the security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon's AWS EC2 infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for security controls that relate to the IT system (instance) including the operating system, applications, and data.

The inverse is true for Salesforce.com's customer resource management (CRM) SaaS offering. Because the entire 'stack' is provided by Salesforce.com, the provider is not only responsible for the physical and environmental security controls, but it must also address the security controls on the infrastructure, the applications, and the data. This alleviates much of the consumer's direct operational responsibility.

One of the attractions of cloud computing is the cost efficiencies afforded by economies of scale, reuse, and standardization. To bring these efficiencies to bear, cloud providers have to provide services that are flexible enough to serve the largest customer base possible, maximizing their addressable market. Unfortunately, integrating security into these solutions is often perceived as making them more rigid.

This rigidity often manifests in the inability to gain parity in security control deployment in cloud environments compared to traditional IT. This stems mostly from the abstraction of infrastructure, and the lack of visibility and capability to integrate many familiar security controls — especially at the network layer.

The figure below illustrates these issues: in SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts. In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform itself falls onto the provider, but securing the applications developed against the platform and developing them securely, both belong to the consumer.

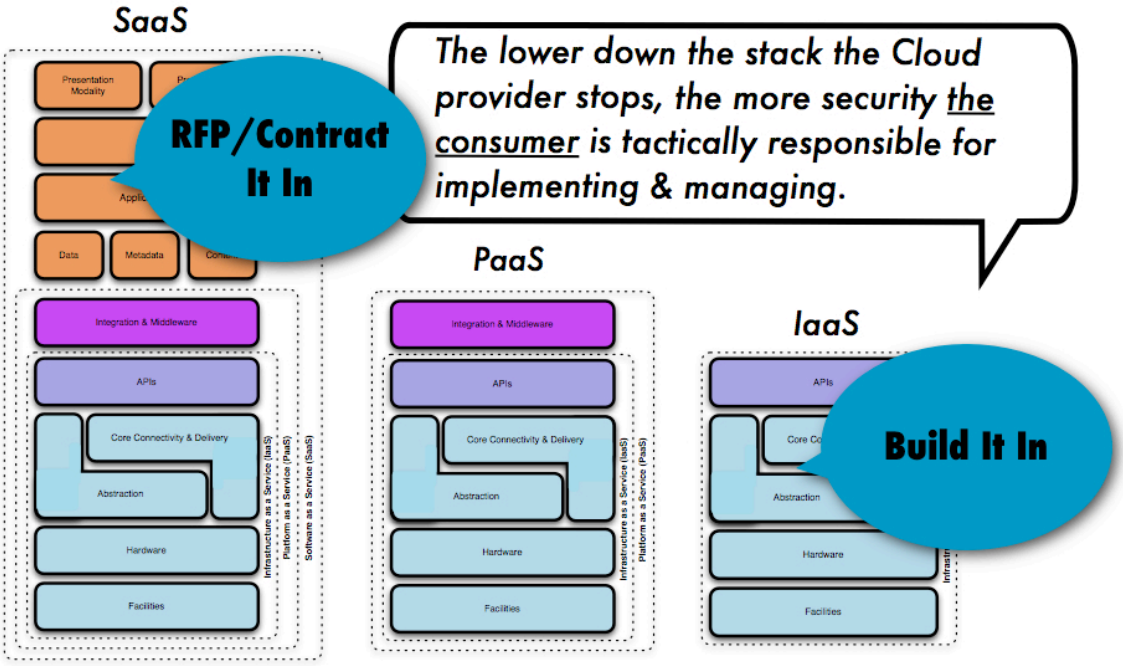


Figure 7 - How Security Gets Integrated

Understanding the impact of these differences between service models and how they are deployed is critical to managing the risk posture of an organization.

Beyond Architecture: The Areas Of Critical Focus

The twelve other domains which comprise the remainder of the CSA guidance highlight areas of concern for cloud computing and are tuned to address both the strategic and tactical security 'pain points' within a cloud environment, and can be applied to any combination of cloud service and deployment model.

The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

Governance Domains

Domain	Guidance dealing with ...
Governance and Enterprise Risk Management	The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues, are some of the items

	discussed.
Legal and Electronic Discovery	Potential legal issues when using Cloud Computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
Compliance and Audit	Maintaining and proving compliance when using Cloud Computing. Issues dealing with evaluating how Cloud Computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.
Information Lifecycle Management	Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls which can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.
Portability and Interoperability	The ability to move data/services from one provider to another, or bring it entirely back in-house. Issues surrounding interoperability between providers are also discussed.

Operational Domains

Traditional Security, Business Continuity and Disaster Recovery	How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas.
Data Center Operations	How to evaluate a provider's data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics

	that are fundamental to long-term stability.
Incident Response, Notification and Remediation	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident handling program.
Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS). Some specific security issues related to the cloud are also discussed.
Encryption and Key Management	Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational is discussing *why* they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
Identity and Access Management	Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity and Access Management (IAM).
Virtualization	The use of virtualization technology in Cloud Computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.

Summary

The keys to understanding how cloud architecture impacts security architecture are a common and concise lexicon; coupled with a consistent taxonomy of offerings by which cloud services and architecture can be deconstructed, mapped to a model of compensating security and

operational controls, risk assessment frameworks, and management frameworks; and in turn to compliance standards.

Understanding how architecture, technology, process, and human capital requirements change or remain the same when deploying Cloud Computing services is critical. Without a clear understanding of the higher-level architectural implications, it is impossible to address more detailed issues rationally.

This architectural overview, along with the twelve other areas of critical focus, will provide the reader with a solid foundation for assessing, operationalizing, managing, and governing security in Cloud Computing environments.

Contributors: Glenn Brunette, Phil Cox, Carlo Espiritu, Christofer Hoff, Mike Kavis, Sitaraman Lakshminarayanan, Kathleen Lossau, Erik Peterson, Scott Matsumoto, Adrian Seccombe, Vern Williams, Richard Zhou

Section II. Governing in the Cloud

Domain 2: Governance and Enterprise Risk Management

Effective governance and enterprise risk management in Cloud Computing environments follows from well-developed information security governance processes, as part of the organization's overall corporate governance obligations of due care. Well-developed information security governance processes should result in information security management programs that are scalable with the business, repeatable across the organization, measurable, sustainable, defensible, continually improving, and cost-effective on an ongoing basis.

The fundamental issues of governance and enterprise risk management in Cloud Computing concern the identification and implementation of the appropriate organizational structures, processes, and controls to maintain effective information security governance, risk management, and compliance. Organizations should also assure reasonable information security across the information supply chain, encompassing providers and customers of Cloud Computing services and their supporting third party vendors, in any cloud deployment model.

Governance Recommendations

√ A portion of the cost savings obtained by Cloud Computing services must be invested into increased scrutiny of the security capabilities of the provider, application of security controls, and ongoing detailed assessments and audits, to ensure requirements are continuously met.

√ Both Cloud Computing service customers and providers should develop robust information security governance, regardless of the service or deployment model. Information security governance should be a collaboration between customers and providers to achieve agreed-upon goals which support the business mission and information security program. The service model may adjust the defined roles and responsibilities in collaborative information security governance and risk management (based on the respective scope of control for user and provider), while the deployment model may define accountability and expectations (based on risk assessment).

√ User organizations should include review of specific information security governance structure and processes, as well as specific security controls, as part of their due diligence for prospective provider organizations. The provider's security governance processes and capabilities should be assessed for sufficiency, maturity, and consistency with the user's information security management processes. The provider's information security controls should be demonstrably risk-based and clearly support these management processes.

√ Collaborative governance structures and processes between customers and providers should be identified as necessary, both as part of the design and development of service delivery, and as service risk assessment and risk management protocols, and then incorporated into service agreements.

√ Security departments should be engaged during the establishment of Service Level Agreements and contractual obligations, to ensure that security requirements are contractually enforceable.

- √ Metrics and standards for measuring performance and effectiveness of information security management should be established prior to moving into the cloud. At a minimum, organizations should understand and document their current metrics and how they will change when operations are moved into the cloud, where a provider may use different (potentially incompatible) metrics.

- √ Wherever possible, security metrics and standards (particularly those relating to legal and compliance requirements) should be included in any Service Level Agreements and contracts. These standards and metrics should be documented and demonstrable (auditable).

Enterprise Risk Management Recommendations

As with any new business process, it's important to follow best practices for risk management. The practices should be proportionate to your particular usages of cloud services, which may range from innocuous and transient data processing up through mission critical business processes dealing with highly sensitive information. A full discussion of enterprise risk management and information risk management is beyond the scope of this guidance, but here are some cloud-specific recommendations you can incorporate into your existing risk management processes.

- √ Due to the lack of physical control over infrastructure in many Cloud Computing deployments; Service Level Agreements, contract requirements, and provider documentation play a larger role in risk management than with traditional, enterprise-owned infrastructure.

- √ Due to the on-demand provisioning and multi-tenant aspects of Cloud Computing, traditional forms of audit and assessment may not be available, or may be modified. For example, some providers restrict vulnerability assessments and penetration testing, while others limit availability of audit logs and activity monitoring. If these are required per your internal policies, you may need to seek alternative assessment options, specific contractual exceptions, or an alternative provider better aligned with your risk management requirements.

- √ Relating to the use of cloud services for functions critical to the organization, the risk management approach should include identification and valuation of assets, identification and analysis of threats and vulnerabilities and their potential impact on assets (risk and incident scenarios), analysis of the likelihoods of events/scenarios, management-approved risk acceptance levels and criteria, and the development of risk treatment plans with multiple options (control, avoid, transfer, accept). The outcomes of risk treatment plans should be incorporated into service agreements.

- √ Risk assessment approaches between provider and user should be consistent, with consistency in impact analysis criteria and definition of likelihood. The user and provider should jointly develop risk scenarios for the cloud service; this should be intrinsic to the provider's design of service for the user, and to the user's assessment of cloud service risk.

- √ Asset inventories should account for assets supporting cloud services and under the control of the provider. Asset classification and valuation schemes should be consistent between user and provider.

- √ The service, and not just the vendor, should be the subject of risk assessment. The use of cloud services, and the particular service and deployment models to be utilized, should be consistent with the risk management objectives of the organization, as well as with its business objectives.

- √ Where a provider cannot demonstrate comprehensive and effective risk management processes in association with its services, customers should carefully evaluate use of the vendor as well as the user's own abilities to compensate for the potential risk management gaps.

- √ Customers of cloud services should ask whether their own management has defined risk tolerances with respect to cloud services and accepted any residual risk of utilizing cloud services.

Information Risk Management Recommendations

Information Risk Management is the act of aligning exposure to risk and capability of managing it with the risk tolerance of the data owner. In this manner, it is the primary means of decision support for information technology resources designed to protect the confidentiality, integrity, and availability of information assets.

- √ Adopt a risk management framework model to evaluate IRM, and a maturity model to assess the effectiveness of your IRM model.

- √ Establish appropriate contractual requirements and technology controls to collect necessary data to inform information risk decisions (e.g., information usage, access controls, security controls, location, etc.).

- √ Adopt a process for determining risk exposure before developing requirements for a Cloud Computing project. Although the categories of information required to understand exposure and management capability are general, the actual evidential metrics gathered are specific to the nature of the cloud computing SPI model and what can be feasibly gathered in terms of the service.

- √ When utilizing SaaS, the overwhelming majority of information will have to be provided by the service provider. Organizations should structure analytical information gathering processes into contractual obligations of the SaaS service.

- √ When utilizing PaaS, build in information gathering as per SaaS above, but where possible include the ability to deploy and gather information from controls as well as creating contractual provisions to test the effectiveness of those controls.

- √ When utilizing an IaaS service provider, build information transparency into contract language for information required by risk analysis.

- √ Cloud service providers should include metrics and controls to assist customers in implementing their Information Risk Management requirements.

Third Party Management Recommendations

√ Customers should view cloud services and security as supply chain security issues. This means examining and assessing the provider's supply chain (service provider relationships and dependencies), to the extent possible. This also means examining the provider's own third party management.

√ Assessment of third party service providers should specifically target the provider's incident management, business continuity and disaster recovery policies, and processes and procedures; and should include review of co-location and back-up facilities. This should include review of the provider's internal assessments of conformance to its own policies and procedures, and assessment of the provider's metrics to provide reasonable information regarding the performance and effectiveness of its controls in these areas.

√ The user's business continuity and disaster recovery plan should include scenarios for loss of the provider's services, and for the provider's loss of third party services and third party-dependent capabilities. Testing of this part of the plan should be coordinated with the cloud provider.

√ The provider's information security governance, risk management, and compliance structures and processes should be comprehensively assessed:

- Request clear documentation on how the facility and services are assessed for risk and audited for control weaknesses, the frequency of assessments, and how control weaknesses are mitigated in a timely manner.
- Require definition of what the provider considers critical service and information security success factors, key performance indicators, and how these are measured relative to IT Service and Information Security Management.
- Review the provider's legal, regulatory, industry, and contractual requirements capture, assessment, and communication processes for comprehensiveness.
- Perform full contract or terms-of-use due diligence to determine roles, responsibilities, and accountability. Ensure legal review, including an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.
- Determine whether due diligence requirements encompass all material aspects of the cloud provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities, and use of subcontractors.

Contributors: Jim Arlen, Don Blumenthal, Nadeem Bukhari, Alex Hutton, Michael Johnson, M S Prasad, Patrick Sullivan

Domain 3: Legal and Electronic Discovery

Cloud Computing creates new dynamics in the relationship between an organization and its information, involving the presence of a third party: the cloud provider. This creates new challenges in understanding how laws apply to a wide variety of information management scenarios.

A complete analysis of Cloud Computing-related legal issues requires consideration of functional, jurisdictional, and contractual dimensions.

- The functional dimension involves determining which functions and services in Cloud Computing have legal implications for participants and stakeholders.
- The jurisdictional dimension involves the way in which governments administer laws and regulations impacting Cloud Computing services, the stakeholders, and the data assets involved.
- The contractual dimension involves the contract structures, terms and conditions, and enforcement mechanisms through which stakeholders in Cloud Computing environments can address and manage the legal and security issues.

Cloud Computing in general can be distinguished from traditional outsourcing in three ways: the time of service (on-demand and intermittent), the anonymity of identity of the service provider(s) and anonymity of the location of the server(s) involved. When considering IaaS and PaaS specifically, a great deal of orchestration, configuration, and software development is performed by the customer — so much of the responsibility cannot be transferred to the cloud provider.

Compliance with recent legislative and administrative requirements around the world forces stronger collaboration among lawyers and technology professionals. This is especially true in Cloud Computing, due to the potential for new areas of legal risk created by the distributed nature of the cloud, compared to traditional internal or outsourced infrastructure.

Numerous compliance laws and regulations in the United States and the European Union either impute liability to " subcontractors or require business entities to impose liability upon them via contract.

Courts now are realizing that information security management services are critical to making decisions as to whether digital information may be accepted as evidence. While this is an issue for traditional IT infrastructure, it is especially concerning in Cloud Computing due to the lack of established legal history with the cloud.

Recommendations

√ Customers and cloud providers must have a mutual understanding of each other's roles and responsibilities related to electronic discovery, including such activities as litigation hold, discovery searches, who provides expert testimony, etc.

√ Cloud providers are advised to assure their information security systems are responsive to customer requirements to preserve data as authentic and reliable, including both primary and secondary information such as metadata and log files.

- √ Data in the custody of cloud service providers must receive equivalent guardianship as in the hands of their original owner or custodian.

- √ Plan for both expected and unexpected termination of the relationship in the contract negotiations, and for an orderly return or secure disposal of assets.

- √ Pre-contract due diligence, contract term negotiation, post-contract monitoring, and contract termination, and the transition of data custodianship are components of the duty of care required of a cloud services client.

- √ Knowing where the cloud service provider will host the data is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data.

- √ As the custodian of the personal data of its employees or clients, and of the company's other intellectual property assets, a company that uses Cloud Computing services should ensure that it retains ownership of its data in its original and authenticable format.

- √ Numerous security issues, such as suspected data breaches, must be addressed in specific provisions of the service agreement that clarify the respective commitments of the cloud service provider and the client.

- √ The cloud service provider and the client should have a unified process for responding to subpoenas, service of process, and other legal requests.

- √ The cloud services agreement must allow the cloud services client or designated third party to monitor the service provider's performance and test for vulnerabilities in the system.

- √ The parties to a cloud services agreement should ensure that the agreement anticipates problems relating to recovery of the client's data after their contractual relationship terminates.

Contributors: Tanya Forsheit, Scott Giordano, Francoise Gilbert, David Jackson, Peter McLaughlin, Jean Pawluk, Jeffrey Ritter

Domain 4: Compliance and Audit

With Cloud Computing developing as a viable and cost effective means to outsource entire systems or even entire business processes, maintaining compliance with your security policy and the various regulatory and legislative requirements to which your organization is subject can become more difficult to achieve and even harder to demonstrate to auditors and assessors.

Of the many regulations touching upon information technology with which organizations must comply, few were written with Cloud Computing in mind. Auditors and assessors may not be familiar with Cloud Computing generally or with a given cloud service in particular. That being the case, it falls upon the cloud customer to understand:

- Regulatory applicability for the use of a given cloud service
- Division of compliance responsibilities between cloud provider and cloud customer
- Cloud provider's ability to produce evidence needed for compliance
- Cloud customer's role in bridging the gap between cloud provider and auditor/assessor

Recommendations

√ Involve Legal and Contracts Teams. The cloud provider's standard terms of service may not address your compliance needs; therefore it is beneficial to have both legal and contracts personnel involved early to ensure that cloud services contract provisions are adequate for compliance and audit obligations.

√ Right to Audit Clause. Customers will often need the ability to audit the cloud provider, given the dynamic natures of both the cloud and the regulatory environment. A right to audit contract clause should be obtained whenever possible, particularly when using the cloud provider for a service for which the customer has regulatory compliance responsibilities. Over time, the need for this right should be reduced and in many cases replaced by appropriate cloud provider certifications, related to our recommendation for ISO/IEC 27001 certification scoping later in this section.

√ Analyze Compliance Scope. Determining whether the compliance regulations which the organization is subject to will be impacted by the use of cloud services, for a given set of applications and data.

√ Analyze Impact of Regulations on Data Security. Potential end users of Cloud Computing services should consider which applications and data they are considering moving to cloud services, and the extent to which they are subject to compliance regulations.

√ Review Relevant Partners and Services Providers. This is general guidance for ensuring that service provider relationships do not negatively impact compliance. Assessing which service providers are processing data that is subject to compliance regulations, and then assessing the security controls provided by those service providers, is fundamental. Several compliance regulations have specific language about assessing and managing third party vendor risk. As with non-cloud IT and business services, organizations need to understand which of their cloud business partners are processing data subject to compliance regulations.

- √ Understand Contractual Data Protection Responsibilities and Related Contracts. The cloud service model to an extent dictates whether the customer or the cloud service provider is responsible for deploying security controls. In an IaaS deployment scenario, the customer has a greater degree of control and responsibility than in a SaaS scenario. From a security control standpoint, this means that IaaS customers will have to deploy many of the security controls for regulatory compliance. In a SaaS scenario, the cloud service provider must provide the necessary controls. From a contractual perspective, understanding the specific requirements, and ensuring that the cloud services contract and service level agreements adequately address them, are key.

- √ Analyze Impact of Regulations on Provider Infrastructure. In the area of infrastructure, moving to cloud services requires careful analysis as well. Some regulatory requirements specify controls that are difficult or impossible to achieve in certain cloud service types.

- √ Analyze Impact of Regulations on Policies and Procedures. Moving data and applications to cloud services will likely have an impact on policies and procedures. Customers should assess which policies and procedures related to regulations will have to change. Examples of impacted policies and procedures include activity reporting, logging, data retention, incident response, controls testing, and privacy policies.

- √ Prepare Evidence of How Each Requirement Is Being Met. Collecting evidence of compliance across the multitude of compliance regulations and requirements is a challenge. Customers of cloud services should develop processes to collect and store compliance evidence including audit logs and activity reports, copies of system configurations, change management reports, and other test procedure output. Depending on the cloud service model, the cloud provider may need to provide much of this information.

- √ Auditor Qualification and Selection. In many cases the organization has no say in selecting auditors or security assessors. If an organization does have selection input, it is highly advisable to pick a "cloud aware" auditor since many might not be familiar with cloud and virtualization challenges. Asking their familiarity with the IaaS, PaaS, and SaaS nomenclature is a good starting point.

- √ Cloud Provider's SAS 70 Type II. Providers should have this audit statement at a minimum, as it will provide a recognizable point of reference for auditors and assessors. Since a SAS 70 Type II audit only assures that controls are implemented as documented, it is equally important to understand the scope of the SAS 70 audit, and whether these controls meet your requirements.

- √ Cloud Provider's ISO/IEC 27001/27002 Roadmap. Cloud providers seeking to provide mission critical services should embrace the ISO/IEC 27001 standard for information security management systems. If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.

- √ ISO/IEC 27001/27002 Scoping. The Cloud Security Alliance is issuing an industry call to action to align cloud providers behind the ISO/IEC 27001 certification, to assure that scoping does not omit critical certification criteria.

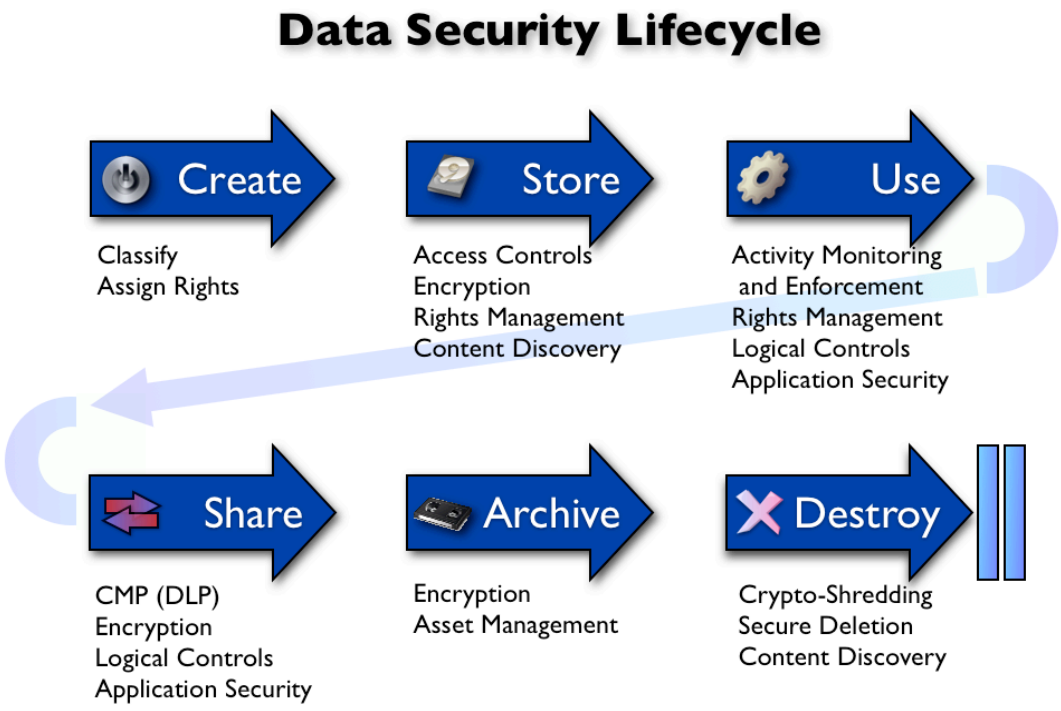
Contributors: Nadeem Bukhari, Anton Chuvakin, Peter Gregory, Jim Hietala, Greg Kane, Patrick Sullivan

Domain 5: Information Lifecycle Management

One of the primary goals of information security is to protect the fundamental data that powers our systems and applications. As we transition to Cloud Computing, our traditional methods of securing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies. With many cloud deployments we are also transferring data to external — or even public — environments, in ways that would have been unthinkable only a few years ago.

Information Lifecycle Management

The Data Security Lifecycle is different from Information Lifecycle Management, reflecting the different needs of the security audience. The Data Security Lifecycle consists of six phases:



Key challenges regarding data lifecycle security in the cloud include the following:

Data security. Confidentiality, Integrity, Availability, Authenticity, Authorization, Authentication, and Non-Repudiation.

Location of the data. There must be assurance that the data, including all of its copies and back-ups, is stored only in geographic locations permitted by contract, SLA, and/or regulation. For

instance, use of "compliant storage" as mandated by the European Union for storing electronic health records can be an added challenge to the data owner and cloud service provider.

Data remanance or persistence. Data must be effectively and completely removed to be deemed 'destroyed.' Therefore, techniques for completely and effectively locating data in the cloud, erasing/destroying data, and assuring the data has been completely removed or rendered unrecoverable must be available and used when required.

Commingling data with other cloud customers. Data – especially classified / sensitive data – must not be commingled with other customer data without compensating controls while in use, storage, or transit. Mixing or commingling the data will be a challenge when concerns are raised about data security and geo-location.

Data backup and recovery schemes for recovery and restoration. Data must be available and data backup and recovery schemes for the cloud must be in place and effective in order to prevent data loss, unwanted data overwrite, and destruction. Don't assume cloud-based data is backed up and recoverable.

Data discovery. As the legal system continues to focus on electronic discovery, cloud service providers and data owners will need to focus on discovering data and assuring legal and regulatory authorities that all data requested has been retrieved. In a cloud environment that question is extremely difficult to answer and will require administrative, technical and legal controls when required.

Data aggregation and inference. With data in the cloud, there are added concerns of data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information. Hence practices must be in play to assure the data owner and data stakeholders that the data is still protected from subtle "breach" when data is commingled and/or aggregated, thus revealing protected information (e.g., medical records containing names and medical information mixed with anonymous data but containing the same "crossover field").

Recommendations

- √ Understand how integrity is maintained and compromise of integrity is detected and reported to customers. The same recommendation applies to confidentiality when appropriate.

- √ The Cloud Computing provider must assure the data owner that they provide full disclosure (aka 'transparency') regarding security practices and procedures as stated in their SLAs.

- √ Ensure specific identification of all controls used during the data lifecycle. Ensure there specifications of to which entity is responsible for each control between the data owner and cloud services provider.

- √ Maintain a fundamental philosophy of knowing where your data is. Ensure your ability to know the geographical location of storage. Stipulate this in your SLAs and contracts. Ensure that appropriate controls regarding country location restrictions are defined and enforced.

- √ Understand circumstances under which storage can be seized by a third party or government entity. Ascertain that your SLA with the cloud provider includes advance notification to the data owner (if possible) that the data owner's information has been or will be seized.

- √ In some instances, a subpoena or e-discovery writ may be placed against the Cloud Computing services provider. In this case, when the provider has custody of customer data, the cloud services provider should be required to inform the data owner that the cloud services provider is compelled to disclose the data owner's data.

- √ A system of service penalties should be included in the contract between the data owner and the cloud service provider. Specifically, data that would be subject to state and international data breach laws (i.e., California Senate Bill 1386 or the new HIPAA data breach rules) should be protected by the cloud service provider.

- √ It is the data owner's responsibility to determine who should access the data, what their rights and privileges are, and under what conditions these access rights are provided. The data owner should maintain a "Default Deny All" policy for both data owner employees and the cloud service provider.

- √ Cloud services providers should offer contractual language that warrants the denial of access to data as a fundamental philosophy (i.e., "Default Deny All"). This specifically applies to cloud services employees and their customers other than the data owner's employees and authorized personnel.

- √ The data owner's responsibility is to define and identify the data classification. It is the cloud service provider's responsibility to enforce the data owner's access requirements based on data classification. Such responsibilities should be in the contract and enforced and audited for compliance.

- √ When a customer is compelled to disclose information, contamination of the data must not occur. Not only does the data owner need to ensure that all data requested for hold orders, subpoenas, e-discovery rulings, etc. are intact and disclosed properly; the data owner must ensure that no other data are affected.

- √ Encrypt data in the ". Encrypt data at rest and encrypt data in transit (Reference Domain 11, Encryption and Key Management.)

- √ Identify trust boundaries throughout the IT architecture and abstraction layers. Ensure subsystems only span trust boundaries as needed and with appropriate safeguards to prevent unauthorized disclosure, alteration, or destruction of data.

- √ Understand what compartmentalization techniques are employed by a provider to isolate its customers from one another. A provider may use a variety of methods depending upon the types and number of services offered.

- √ Understand the cloud provider's data search capabilities and limitations when attempting to view 'inside' the dataset for data discovery.

- √ Understand how encryption is managed on multi-tenant storage. Is there a single key for all data owners, one key per data owner, or multiple keys per data owner? Is there a system to prevent different data owners from having the same encryption keys?

- √ Data owners should require cloud service providers to ensure that their backed-up data is not commingled with other cloud service customer data.

- √ Understand cloud provider storage retirement processes. Data destruction is extremely difficult in a multi-tenant environment and the cloud provider should be using strong storage encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications, processes, and entities.

- √ Data retention and destruction schedules are the responsibility of the data owner. It is the cloud service provider's responsibility to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures and on media. The data owner should enforce and audit this practice if possible.

- √ Understand the logical segregation of information and protective controls implemented.

- √ Understand the privacy restrictions inherent in data entrusted to your company; you may have to designate your cloud provider as a particular kind of partner before entrusting them with this information.

- √ Understand cloud provider policies and processes for data retention and destruction and how they compare with internal organizational policy. Be aware that data retention assurance may be easier for the cloud provider to demonstrate, while data destruction may be very difficult.

- √ Negotiate penalties payable by the cloud provider for data breaches to ensure this is taken seriously. If practical, customers should seek to recover all breach costs as part of their provider contract. If impractical, customers should explore other risk transference vehicles such as insurance to recover breach costs.

- √ Perform regular backup and recovery tests to assure that logical segregation and controls are effective.

- √ Ensure that cloud provider personnel controls are in place to provide a logical segregation of duties.

- √ Understand how encryption is managed on multi-tenant storage. Is there a single key for all customers, one key per customer, or multiple keys per customer?

Data Security Recommendations by ILM Phase

Some of our general recommendations, as well as other specific controls, are listed within the context of each lifecycle phase. Please keep in mind that depending upon the cloud service model (SaaS, PaaS, or IaaS), some recommendations need to be implemented by the customer and others must be implemented by the cloud provider.

Create

- √ Identify available data labeling and classification capabilities.

√ Enterprise Digital Rights Management may be an option.

√ User tagging of data is becoming common in Web 2.0 environments and may be leveraged to help classify the data.

Store

√ Identify access controls available within the file system, DBMS, document management system, etc.

√ Encryption solutions, such as for email, network transport, database, files and filesystems.

√ Content discovery tools (often DLP, or Data Loss Prevention) can assist in identifying and auditing data which requires controls.

Use

√ Activity monitoring and enforcement, via logfiles and/or agent-based tools.

√ Application logic.

√ Object level controls within DBMS solutions.

Share

√ Activity monitoring and enforcement, via logfiles and/or agent-based tools.

√ Application logic.

√ Object level controls within DBMS solutions.

√ Identify access controls available within the file system, DBMS, and document management system.

√ Encryption, such as for email, network transport, database, files, and filesystems.

√ Data Loss Prevention for content-based data protection.

Archive

√ Encryption, such as for tape backup and other long term storage media.

√ Asset management and tracking.

Destroy

√ Crypto-shredding: the destruction of all key material related to encrypted data.

√ Secure deletion through disk wiping and related techniques.

√ Physical destruction, such as degaussing of physical media.

√ Content discovery to confirm destruction processes.

Contributors: Richard Austin, Ernie Hayden, Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna Garcia, Rich Mogull, Jeff Reich

Domain 6: Portability and Interoperability

Organizations must approach the cloud with the understanding that they may have to change providers in the future. Portability and interoperability must be considered up front as part of the risk management and security assurance of any cloud program.

Large cloud providers can offer geographic redundancy in the cloud, hopefully enabling high availability with a single provider. Nonetheless, it's advisable to do basic business continuity planning, to help minimize the impact of a worst-case scenario. Various companies will in the future suddenly find themselves with urgent needs to switch cloud providers for varying reasons, including:

- An unacceptable increase in cost at contract renewal time.
- A provider ceases business operations.
- A provider suddenly closes one or more services being used, without acceptable migration plans.
- Unacceptable decrease in service quality, such as a failure to meet key performance requirements or achieve service level agreements (SLAs).
- A business dispute between cloud customer and provider.

Some simple architectural considerations can help minimize the damage should these kinds of scenarios occur. However, the means to address these issues depend on the type of cloud service.

With Software as a Service (SaaS), the cloud customer will by definition be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration.

With Platform as a Service (PaaS), the expectation is that some degree of application modification will be necessary to achieve portability. The focus is minimizing the amount of application rewriting while preserving or enhancing security controls, along with achieving a successful data migration.

With Infrastructure as a Service (IaaS), the focus and expectation is that both the applications and data should be able to migrate to and run at a new cloud provider.

Due to a general lack of interoperability standards, and the lack of sufficient market pressure for these standards, transitioning between cloud providers may be a painful manual process. From a security perspective, our primary concerns is maintaining consistency of security controls while changing environments.

Recommendations

For All Cloud Solutions:

√ Substituting cloud providers is in virtually all cases a negative business transaction for at least one party, which can cause an unexpected negative reaction from the legacy cloud provider. This must be planned for in the contractual process as outlined in

Domain 3, in your Business Continuity Program as outlined in Domain 7, and as a part of your overall governance in Domain 2.

- √ Understand the size of data sets hosted at a cloud provider. The sheer size of data may cause an interruption of service during a transition, or a longer transition period than anticipated. Many customers have found that using a courier to ship hard drives is faster than electronic transmission for large data sets.

- √ Document the security architecture and configuration of individual component security controls so they can be used to support internal audits, as well as to facilitate migration to new providers.

For IaaS Cloud Solutions:

- √ Understand how virtual machine images can be captured and ported to new cloud providers, who may use different virtualization technologies.

- √ Identify and eliminate (or at least document) any provider-specific extensions to the virtual machine environment.

- √ Understand what practices are in place to make sure appropriate deprovisioning of VM images occurs after an application is ported from the cloud provider.

- √ Understand the practices used for decommissioning of disks and storage devices.

- √ Understand hardware/platform based dependencies that need to be identified before migration of the application/data.

- √ Ask for access to system logs, traces, and access and billing records from the legacy cloud provider.

- √ Identify options to resume or extend service with the legacy cloud provider in part or in whole if new service proves to be inferior.

- √ Determine if there are any management-level functions, interfaces, or APIs being used that are incompatible with or unimplemented by the new provider.

For PaaS Cloud Solutions:

- √ When possible, use platform components with a standard syntax, open APIs, and open standards.

- √ Understand what tools are available for secure data transfer, backup, and restore.

- √ Understand and document application components and modules specific to the PaaS provider, and develop an application architecture with layers of abstraction to minimize direct access to proprietary modules.

- √ Understand how base services like monitoring, logging, and auditing would transfer over to a new vendor.

- √ Understand control functions provided by the legacy cloud provider and how they would translate to the new provider.

- √ When migrating to a new platform, understand the impacts on performance and availability of the application, and how these impacts will be measured.

- √ Understand how testing will be completed prior to and after migration, to verify that the services or applications are operating correctly. Ensure that both provider and user responsibilities for testing are well known and documented.

For SaaS Solutions:

- √ Perform regular data extractions and backups to a format that is usable without the SaaS provider.

- √ Understand whether metadata can be preserved and migrated.

- √ Understand that any custom tools being implemented will have to be redeveloped, or the new vendor must provide those tools.

- √ Assure consistency of control effectiveness across old and new providers.

- √ Assure the possibility of migration of backups and other copies of logs, access records, and any other pertinent information which may be required for legal and compliance reasons.

- √ Understand management, monitoring, and reporting interfaces and their integration between environments.

- √ Is there a provision for the new vendor to test and evaluate the applications before migration?

Contributors: Warren Axelrod, Aradhna Chetal, Arthur Hedge, Dennis Hurst, Sam Johnston, Scott Morrison, Adam Munter, Michael Sutton, Joe Wallace

Section III. Operating in the Cloud

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery

The body of knowledge accrued within traditional physical security, business continuity planning and disaster recovery remains quite relevant to Cloud Computing. The rapid pace of change and lack of transparency within Cloud Computing requires that traditional security, Business Continuity Planning (BCP) and Disaster Recovery (DR) professionals be continuously engaged in vetting and monitoring your chosen cloud providers.

Our challenge is to collaborate on risk identification, recognize interdependencies, integrate, and leverage resources in a dynamic and forceful way. Cloud Computing and its accompanying infrastructure assist to diminish certain security issues, but may increase others and can never eliminate the need for security. While major shifts in business and technology continue, traditional security principles remain.

Recommendations

- √ Keep in mind that centralization of data means the risk of insider abuse from within the cloud provider is a significant concern.
- √ Cloud providers should consider adopting as a security baseline the most stringent requirements of any customer. To the extent these security practices do not negatively impact the customer experience, stringent security practices should prove to be cost effective in the long run by reducing risk as well as customer-driven scrutiny in several areas of concern.
- √ Providers should have robust compartmentalization of job duties, perform background checks, require/enforce non-disclosure agreements for employees, and limit employee knowledge of customers to that which is absolutely needed to perform job duties.
- √ Customers should perform onsite inspections of cloud provider facilities whenever possible.
- √ Customers should inspect cloud provider disaster recovery and business continuity plans.
- √ Customers should identify physical interdependencies in provider infrastructure.
- √ Ensure there is an authoritative taxonomy stated in contracts to clearly define contractual obligations related to security, recovery, and access to data.
- √ Customers should ask for documentation of the provider's internal and external security controls, and adherence to any industry standards.
- √ Ensure customer Recovery Time Objectives (RTOs) are fully understood and defined in contractual relationships and baked into the technology planning process. Ensure technology roadmaps, policies, and operational capabilities can satisfy these requirements.

- √ Customers need to confirm that the provider has an existing BCP Policy approved by the provider's board of directors.

- √ Customers should look for evidence of active management support and periodic review of the BC Program to ensure that the BC Program is active.

- √ Customer should check whether the BC Program is certified and/or mapped to internationally recognized standards such as BS 25999.

- √ Customers should ascertain whether the provider has any online resource dedicated to security and BCP, where the program's overview and fact sheets are available for reference.

- √ Ensure cloud suppliers are vetted via the company Vendor Security Process (VSP) so there is a clear understanding of what data is to be shared and what controls are to be utilized. The VSP determination should feed the decision-making process and assessment of whether the risk is acceptable.

- √ The dynamic nature of Cloud Computing and its relative youth justify more frequent cycles of all the above activities to uncover changes not communicated to customers.

Contributors: Randolph Barr, Luis Morales, Jeff Spivey, David Tyson

Domain 8: Data Center Operations

The number of Cloud Computing providers continues to increase as business and consumer IT services move to the cloud. There has been similar growth in data centers to fuel Cloud Computing service offerings. Cloud providers of all types and sizes, including well known technology leaders and thousands of startups and emerging growth companies, are making major investments in this promising new approach to IT service delivery.

Sharing IT resources to create efficiencies and economies of scale is not a new concept. However the cloud business model works best if the traditionally enormous investments in data center operations are spread over a larger pool of consumers. Historically data center architectures have been deliberately oversized to exceed periodic peak loads, which means during normal or low demand periods, data center resources are often idle or underutilized for long stretches of time. Cloud service providers, on the other hand, seek to optimize resource usage, both human and technological, to gain competitive advantage and maximize operating profit margins.

The challenge for consumers of cloud services is how to best evaluate the provider's capabilities to deliver appropriate and cost-effective services, while at the same time protecting the customer's own data and interests. Do not assume that the provider has the best interests of their customers as their top priority. With the common carrier model of service delivery, which Cloud Computing is a form of, the service provider normally has little or no access to or control over the customers' data or systems beyond the contracted level of management. Certainly this is the correct approach to take, but some cloud architectures might take liberties with customers' data integrity and security that the customer would not be comfortable with if they became aware. The consumer must educate themselves about the services they are considering by asking appropriate questions and becoming familiar with the basic architectures and potential areas for security vulnerabilities.

When making a decision to move all or part of IT operations to the cloud, it first helps to understand how a cloud provider has implemented Domain 1's "Five Principal Characteristics of Cloud Computing", and how that technology architecture and infrastructure impacts its ability to meet service level agreements and address security concerns. The provider's specific technology architecture could be a combination of IT products and other cloud services, such as taking advantage of another provider's IaaS storage service.

The technology architecture and infrastructure of cloud providers may differ; but to meet security requirements they must all be able to demonstrate comprehensive compartmentalization of systems, data, networks, management, provisioning, and personnel. The controls segregating each layer of the infrastructure need to be properly integrated so they do not interfere with each other. For example, investigate whether the storage compartmentalization can easily be bypassed by management tools or poor key management.

Lastly, understand how the cloud provider handles resource democratization and dynamism to best predict proper levels of system availability and performance through normal business fluctuations. Remember, Cloud Computing theory still somewhat exceeds its practice: many customers make incorrect assumptions about the level of automation actually involved. As provisioned resource capacity is reached, the provider is responsible for ensuring that additional resources are delivered seamlessly to the customer.

Recommendations

It is imperative that an organization considering purchasing cloud services, of whatever kind, be fully aware of exactly what services are being contracted for and what is not included. Below is a summary of information that needs to be reviewed as part of the vendor selection process, and additional questions to help qualify providers and better match their services against organizational requirements.

- √ Regardless of which certifications cloud providers maintain, it is important to obtain a commitment or permission to conduct customer or external third-party audits.

- √ Cloud customers should understand how cloud providers implement Domain 1's "Five Principal Characteristics of Cloud Computing", and how that technology architecture and infrastructure impact their ability to meet service level agreements.

- √ While the technology architectures of cloud providers differ, they must all be able to demonstrate comprehensive compartmentalization of systems, networks, management, provisioning, and personnel.

- √ Understand how resource democratization occurs within your cloud providers to best predict system availability and performance during your business fluctuations. If feasible, discover the cloud providers' other clients to assess the impact their business fluctuations may have on your customer experience with the cloud provider. However this is no substitute for ensuring the service level agreements are clearly defined, measurable, enforceable, and adequate for your requirements.

- √ Cloud customers should understand their cloud providers' patch management policies and procedures and how these may impact their environments. This understanding should be reflected in contract language.

- √ Continual improvement is particularly important in a cloud environment because any improvement in policies, processes, procedures, or tools for a single customer could result in service improvement for all customers. Look for cloud providers with standard continual improvement processes in place.

- √ Technical support or the service desk is often a customer's window into the provider's operations. To achieve a smooth and uniform customer support experience for your end users, it is essential to ensure that the provider's customer support processes, procedures, tools, and support hours are compatible with yours.

- √ As in Domain 7, review business continuity and disaster recovery plans from an IT perspective, and how they relate to people and processes. A cloud provider's technology architecture may use new and unproven methods for failover, for example. Customers' own business continuity plans should also address impacts and limitations of cloud computing.

Contributors: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Alexander Windel, Richard Zhao

Domain 9: Incident Response, Notification, and Remediation

The nature of Cloud Computing makes it more difficult to determine who to contact in case of a security incident, data breach, or other event that requires investigation and reaction. Standard security incident response mechanisms can be used with modifications to accommodate the changes required by shared reporting responsibilities. This domain provides guidance on how to handle these incidents.

The problem for the cloud customer is that applications deployed to cloud fabrics are not always designed with data integrity and security in mind. This may result in vulnerable applications being deployed into cloud environments, triggering security incidents. Additionally, flaws in infrastructure architecture, mistakes made during hardening procedures, and simple oversights present significant risks to cloud operations. Of course, similar vulnerabilities also endanger traditional data center operations.

Technical expertise is obviously required in incident handling, but privacy and legal experts have much to contribute to cloud security. They also play a role in incident response regarding notification, remediation, and possible subsequent legal action. An organization considering using cloud services needs to review what mechanisms have been implemented to address questions about employee data access that is not governed by user agreements and privacy policies. Application data not managed by a cloud provider's own applications, such as in IaaS and PaaS architectures, generally has different controls than data managed by a SaaS provider's application.

The complexities of large cloud providers delivering SaaS, PaaS, and IaaS capabilities create significant incident response issues that potential customers must assess for acceptable levels of service. When evaluating providers it is important to be aware that the provider may be hosting hundreds of thousands of application instances. From an incident monitoring perspective, any foreign applications widen the responsibility of the security operations center (SOC). Normally a SOC monitors alerts and other incident indicators, such as those produced by intrusion detection systems and firewalls, but the number of sources that must be monitored and the volume of notifications can increase exponentially in an open cloud environment, as the SOC may need to monitor activity between customers as well as external incidents.

An organization will need to understand the incident response strategy for their chosen cloud provider. This strategy must address identification and notification, as well as options for remediation of unauthorized access to application data. To make matters more complicated, application data management and access have different meanings and regulatory requirements depending on the data location. For example, an incident may occur involving data in Germany, whereas if the same data had been stored in the US it might not have been considered an issue. This complication makes incident identification particularly challenging.

Recommendations

- √ Cloud customers need to clearly define and communicate to cloud providers what they consider incidents (such as data breaches) versus mere events (such as suspicious intrusion detection alerts) before service deployment.

- √ Cloud customers may have very limited involvement with the providers' incident response activities. Therefore it is critical for customers to understand the prearranged communication paths to the provider's incident response team.

- √ Cloud customers should investigate what incident detection and analysis tools providers use to make sure they are compatible with their own systems. A provider's proprietary or unusual log formats could be major roadblocks in joint investigations, particularly those that involve legal discovery or government intervention.

- √ Poorly designed and protected applications and systems can easily overwhelm everyone's incident response capabilities. Conducting proper risk management on the systems and utilizing defense-in-depth practices are essential to reduce the chance of a security incident in the first place.

- √ Security Operation Centers (SOC) often assume a single governance model related to incident response, which is inappropriate for multi-tenant cloud providers. A robust and well maintained Security Information and Event Management (SIEM) process that identifies available data sources (application logs, firewall logs, IDS logs, etc) and merges these into a common analysis and alerting platform can assist the SOC in detecting incidents within the cloud computing platform.

- √ To greatly facilitate detailed offline analyses, look for cloud providers with the ability to deliver snapshots of the customer's entire virtual environment – firewalls, network (switches), systems, applications, and data.

- √ Containment is a race between damage control and evidence gathering. Containment approaches that focus on the confidentiality-integrity-availability (CIA) triad can be effective.

- √ Remediation highlights the importance of being able to restore systems to earlier states, and even a need to go back six to twelve months for a known-good configuration. Keeping legal options and requirements in mind, remediation may also need to support forensic recording of incident data.

- √ Any data classified as private for data breach regulations should always be encrypted to reduce the consequences of a breach incident. Customers should stipulate encryption requirements contractually, per Domain 11.

- √ Some cloud providers may host a significant number of customers with unique applications. These cloud providers should consider application layer logging frameworks to provide granular narrowing of incidents to a specific customer. These cloud providers should also construct a registry of application owners by application interface (URL, SOA service, etc.)

- √ Application-level firewalls, proxies, and other application logging tools are key capabilities currently available to assist in responding to incidents in multi-tenant environments.

Contributors: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Alexander Windel, Richard Zhao

Domain 10: Application Security

Cloud environments — by virtue of their flexibility, openness, and often public availability — challenge many fundamental assumptions about application security. Some of these assumptions are well understood; however many are not. This section is intended to document how Cloud Computing influences security over the lifetime of an application — from design to operations to ultimate decommissioning. This guidance is for all stakeholders — including application designers, security professionals, operations personnel, and technical management — on how to best mitigate risk and manage assurance within Cloud Computing applications.

Cloud Computing is a particular challenge for applications across the layers of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud-based software applications require a design rigor similar to applications residing in a classic DMZ. This includes a deep up-front analysis covering all the traditional aspects of managing information confidentiality, integrity, and availability.

Applications in cloud environments will both impact and be impacted by the following major aspects:

- **Application Security Architecture** – Consideration must be given to the reality that most applications have dependencies on various other systems. With Cloud Computing, application dependencies can be highly dynamic, even to the point where each dependency represents a discrete third party service provider. Cloud characteristics make configuration management and ongoing provisioning significantly more complex than with traditional application deployment. The environment drives the need for architectural modifications to assure application security.

- **Software Development Life Cycle (SDLC)** – Cloud computing affects all aspects of SDLC, spanning application architecture, design, development, quality assurance, documentation, deployment, management, maintenance, and decommissioning.

- **Compliance** – Compliance clearly affects data, but it also influences applications (for example, regulating how a program implements a particular cryptographic function), platforms (perhaps by prescribing operating system controls and settings) and processes (such as reporting requirements for security incidents).

- **Tools and Services** – Cloud computing introduces a number of new challenges around the tools and services required to build and maintain running applications. These include development and test tools, application management utilities, the coupling to external services, and dependencies on libraries and operating system services, which may originate from cloud providers. Understanding the ramifications of who provides, owns, operates, and assumes responsibility for each of these is fundamental.

- **Vulnerabilities** – These include not only the well-documented—and continuously evolving—vulnerabilities associated with web apps, but also vulnerabilities associated with machine-to-machine Service-Oriented Architecture (SOA) applications, which are increasingly being deployed into the cloud.

Recommendations

- √ Software Development Lifecycle (SDLC) security is important, and should at a high level address these three main areas of differentiation with cloud-based development: 1) updated threat and trust models, 2) application assessment tools updated for cloud environments, and 3) SDLC processes and quality checkpoints to account for application security architectural changes.

- √ IaaS, PaaS, and SaaS create different trust boundaries for the software development lifecycle; which must be accounted for during the development, testing, and production deployment of applications.

- √ For IaaS, a key success factor is the presence of trusted virtual machine images. The best alternative is the ability to provide your own virtual machine image conforming to internal policies.

- √ The best practices available to harden host systems within DMZs should be applied to virtual machines. Limiting services available to only those needed to support the application stack is appropriate.

- √ Securing inter-host communications must be the rule; there can be no assumption of a secure channel between hosts, whether in a common data center or even on the same hardware device.

- √ Managing and protecting application credentials and key material are critical.

- √ Extra care should be undertaken with the management of files used for application logging and debugging, as the locations of these files may be remote or unknown and the information could be sensitive.

- √ Account for external administration and multi-tenancy in the application's threat model.

- √ Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as WS-Security. The ability to segment ESBs is not available in PaaS environments.

- √ Metrics should be applied to assess effectiveness of application security programs. Among the direct application security-specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Indirect data handling metrics, such as the percentage of data encrypted, can indicate that responsible decisions are being made from an application architecture perspective.

- √ Cloud providers must support dynamic analysis web application security tools against applications hosted in their environments.

- √ Attention should be paid to how malicious actors will react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in the user

context. They are likely to attack infrastructure and perform extensive black box testing.

√ Customers should obtain contractual permission to perform remote vulnerability assessments, including traditional (network/host), and application vulnerability assessments. Many cloud providers restrict vulnerability assessments due to the provider's inability to distinguish such tests from actual attacks, and to avoid potential impact upon other customers.

Contributors: John Arnold, Warren Axelrod, Aradhna Chetal, Justin Foster, Arthur J. Hedge III, Georg Hess, Dennis Hurst, Jesus Luna Garcia, Scott Matsumoto, Alexander Meisel, Anish Mohammed, Scott Morrison, Joe Stein, Michael Sutton, James Tiller, Joe Wallace, Colin Watson

Domain 11: Encryption and Key Management

Cloud customers and providers need to guard against data loss and theft. Today, encryption of personal and enterprise data is strongly recommended, and in some cases mandated by laws and regulations around the world. Cloud customers want their providers to encrypt their data to ensure that it is protected no matter where the data is physically located. Likewise, the cloud provider needs to protect its customers' sensitive data.

Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.

Encryption for Confidentiality and Integrity

Cloud environments are shared with many tenants, and service providers have privileged access to the data in those environments. Thus confidential data hosted in a cloud must be protected using a combination of access control (see Domain 12), contractual liability (see Domains 2, 3, and 4), and encryption, which we describe in this section. Of these, encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failures.

Encrypting data in transit over networks. There is the utmost need to encrypt multi-use credentials, such as credit card numbers, passwords, and private keys, in transit over the Internet. Although cloud provider networks may be more secure than the open Internet, they are by their very architecture made up of many disparate components, and disparate organizations share the cloud. Therefore it is important to protect this sensitive and regulated information in transit even within the cloud provider's network. Typically this can be implemented with equal ease in SaaS, PaaS, and IaaS environments.

Encrypting data at rest. Encrypting data on disk or in a live production database has value, as it can protect against a malicious cloud service provider or a malicious co-tenant as well as against some types of application abuse. For long-term archival storage, some customers encrypt their own data and then send it as ciphertext to a cloud data storage vendor. The customer then controls and holds the cryptographic keys and decrypts the data, if necessary, back on their own premises. Encrypting data at rest is common within IaaS environments, using a variety of provider and third party tools. Encrypting data at rest within PaaS environments is generally more complex, requiring instrumentation of provider offerings or special customization. Encrypting data at rest within SaaS environments is a feature cloud customers cannot implement directly, and need to request from their providers.

Encrypting data on backup media. This can protect against misuse of lost or stolen media. Ideally, the cloud service provider implements it transparently. However, as a customer and provider of data, it is your responsibility to verify that such encryption takes place. One consideration for the encryption infrastructure is dealing with the longevity of the data.

Beyond these common uses of encryption, the possibly of exotic attacks against cloud providers also warrants further exploration of means for encrypting dynamic data, including data residing in memory.

Key Management

Existing cloud service providers may provide basic encryption key schemes to secure cloud based application development and services, or they may leave all such protective measures up to their customers. While cloud service providers are progressing towards supporting robust key management schemes, more work is needed to overcome barriers to adoption. Emerging standards should solve this problem in the near future, but work is still in progress. There are several key management issues and challenges within Cloud Computing:

Secure key stores. Key stores must themselves be protected, just as any other sensitive data. They must be protected in storage, in transit, and in backup. Improper key storage could lead to the compromise of all encrypted data.

Access to key stores. Access to key stores must be limited to the entities that specifically need the individual keys. There should also be policies governing the key stores, which use separation of roles to help control access; an entity that uses a given key should not be the entity that stores that key.

Key backup and recoverability. Loss of keys inevitably means loss of the data that those keys protect. While this is an effective way to destroy data, accidental loss of keys protecting mission-critical data would be devastating to a business, so secure backup and recovery solutions must be implemented.

There are a number of standards and guidelines applicable to key management in the cloud. The OASIS Key Management Interoperability Protocol (KMIP) is an emerging standard for interoperable key management in the cloud. The IEEE 1619.3 standards cover storage encryption and key management, especially as they pertain to storage IaaS.

Recommendations

- √ Use encryption to separate data holding from data usage.
- √ Segregate the key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflicts when compelled to provide data due to a legal mandate.
- √ When stipulating encryption in contract language, assure that the encryption adheres to existing industry and government standards, as applicable.
- √ Understand whether and how cloud provider facilities provide role management and separation of duties.
- √ In cases where the cloud provider must perform key management, understand whether the provider has defined processes for a key management lifecycle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.

- √ Assure regulated and/or sensitive customer data is encrypted in transit over the cloud provider's internal network, in addition to being encrypted at rest. This will be up to the cloud customer to implement in IaaS environments, a shared responsibility between customer and provider in PaaS environments, and the cloud provider's responsibility in SaaS environments.

- √ In IaaS environments, understand how sensitive information and key material otherwise protected by traditional encryption may be exposed during usage. For example, virtual machine swap files and other temporary data storage locations may also need to be encrypted.

Contributors: John Arnold, Girish Bhat, Jon Callas, Sergio Loureiro, Jean Pawluk, Michael Reiter, Joel Weise

Domain 12: Identity and Access Management

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several Cloud Computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary precursor towards strategic use of on-demand computing services. Supporting today's aggressive adoption of an admittedly immature cloud ecosystem requires an honest assessment of an organization's readiness to conduct cloud-based Identity and Access Management (IAM), as well as understanding the capabilities of that organization's Cloud Computing providers.

We will discuss the following major IAM functions that are essential for successful and effective management of identities in the cloud:

- Identity provisioning/deprovisioning
- Authentication
- Federation
- Authorization & user profile management

Compliance is a key consideration throughout.

Identity Provisioning: One of the major challenges for organizations adopting Cloud Computing services is the secure and timely management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. Furthermore, enterprises that have invested in user management processes within an enterprise will seek to extend those processes and practice to cloud services.

Authentication: When organizations start to utilize cloud services, authenticating users in a trustworthy and manageable manner is a vital requirement. Organizations must address authentication-related challenges such as credential management, strong authentication (typically defined as multi-factor authentication), delegated authentication, and managing trust across all types of cloud services.

Federation: In a Cloud Computing environment, Federated Identity Management plays a vital role in enabling organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP). In that context, exchanging identity attributes between the service provider (SP) and the IdP in a secure way is also an important requirement. Organizations considering federated identity management in the cloud should understand the various challenges and possible solutions to address those challenges with respect to identity lifecycle management, available authentication methods to protect confidentiality, and integrity; while supporting non-repudiation.

Authorization & user profile management: The requirements for user profiles and access control policy vary depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organization (such as an employer, university, hospital, or other enterprise). The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.

Identity Provisioning – Recommendations

- √ Capabilities offered by cloud providers are not currently adequate to meet enterprise requirements. Customers should avoid proprietary solutions such as creating custom connectors unique to cloud providers, as these exacerbate management complexity.

- √ Customers should leverage standard connectors provided by cloud providers to the extent practical, preferably built on SPML schema. If your cloud provider does not currently offer SPML, you should request it.

- √ Cloud customers should modify or extend their authoritative repositories of identity data so that it encompasses applications and processes in the cloud.

Authentication – Recommendations

Both the cloud provider and the customer enterprises should consider the challenges associated with credential management and strong authentication, and implement cost effective solutions that reduce the risk appropriately.

SaaS and PaaS providers typically provide the options of either built-in authentication services to their applications or platforms, or delegating authentication to the enterprise.
Customers have the following options:

- √ Authentication for enterprises. Enterprises should consider authenticating users via their Identity Provider (IdP) and establishing trust with the SaaS vendor by federation.

- √ Authentication for individual users acting on their own behalf. Enterprises should consider using user-centric authentication such as Google, Yahoo, OpenID, Live ID, etc., to enable use of a single set of credentials valid at multiple sites.

- √ Any SaaS provider that requires proprietary methods to delegate authentication (e.g., handling trust by means of a shared encrypted cookie or other means) should be thoroughly evaluated with a proper security evaluation, before continuing. The general preference should be for the use of open standards.

For IaaS, authentication strategies can leverage existing enterprise capabilities.

- √ For IT personnel, establishing a dedicated VPN will be a better option, as they can leverage existing systems and processes.

- √ Some possible solutions include creating a dedicated VPN tunnel to the corporate network or federation. A dedicated VPN tunnel works better when the application leverages existing identity management systems (such as a SSO solution or LDAP based authentication that provides an authoritative source of identity data).

- √ In cases where a dedicated VPN tunnel is not feasible, applications should be designed to accept authentication assertions in various formats (SAML, WS-Federation, etc), in combination with standard network encryption such as SSL. This approach enables the organizations to deploy federated SSO not only within an enterprise, but also to cloud applications.

- √ OpenID is another option when the application is targeted beyond enterprise users. However, because control of OpenID credentials is outside the enterprise, the access privileges extended to such users should be limited appropriately.

- √ Any local authentication service implemented by the cloud provider should be OATH compliant. With an OATH-compliant solution, companies can avoid becoming locked into one vendor's authentication credentials.

- √ In order to enable strong authentication (regardless of technology), cloud applications should support the capability to delegate authentication to the enterprise that is consuming the services, such as through SAML.

- √ Cloud providers should consider supporting various strong authentication options such as One-Time Passwords, biometrics, digital certificates, and Kerberos. This will provide another option for enterprises to use their existing infrastructure.

Federation Recommendations

In a Cloud Computing environment, federation of identity is key for enabling allied enterprises to authenticate, provide single or reduced Sign-On (SSO), and exchange identity attributes between the Service Provider (SP) and the Identity Provider (IdP). Organizations considering federated identity management in the cloud should understand the various challenges and possible solutions to address them with respect to identity lifecycle management, authentication methods, token formats, and non-repudiation.

- √ Enterprises looking for a cloud provider should verify that the provider supports at least one of the prominent standards (SAML and WS-Federation). SAML is emerging as a widely supported federation standard and is supported by major SaaS and PaaS cloud providers. Support for multiple standards enables a greater degree of flexibility.

- √ Cloud providers should have flexibility to accept the standard federation formats from different identity providers. However most cloud providers as of this writing support a single standard, e.g., SAML 1.1 or SAML 2.0. Cloud providers desiring to support multiple federation token formats should consider implementing some type of federation gateway.

- √ Organizations may wish to evaluate Federated Public SSO versus Federated Private SSO. Federated Public SSO is based on standards such as SAML and WS-Federation with the cloud provider, while Federated Private SSO leverages the existing SSO architecture over VPN. In the long run Federated Public SSO will be ideal, however an organization with a mature SSO architecture and limited number of cloud deployments may gain short-term cost benefits with a Federated Private SSO.

- √ Organizations may wish to opt for federation gateways in order to externalize their federation implementation, in order to manage the issuance and verification of tokens. Using this method, organizations delegate issuing various token types to the federation gateway, which then handles translating tokens from one format to another.

Access Control Recommendations

Selecting or reviewing the adequacy of access control solutions for cloud services has many aspects, and entails consideration of the following:

- √ Review appropriateness of the access control model for the type of service or data.
- √ Identify authoritative sources of policy and user profile information.
- √ Assess support for necessary privacy policies for the data.
- √ Select a format in which to specify policy and user information.
- √ Determine the mechanism to transmit policy from a Policy Administration Point (PAP) to a Policy Decision Point (PDP).
- √ Determine the mechanism to transmit user information from a Policy Information Point (PIP) to a Policy Decision Point (PDP).
- √ Request a policy decision from a Policy Decision Point (PDP).
- √ Enforce the policy decision at the Policy Enforcement Point (PEP).
- √ Log information necessary for audits.

IDaaS Recommendations

Identity as a Service should follow the same best practices that an internal IAM implementation does, along with added considerations for privacy, integrity, and auditability.

- √ For internal enterprise users, custodians must review the cloud provider's options to provide secured access to the cloud, either through a direct VPN or through an industry standard such as SAML and strong authentication. The reduction of cost from using the cloud needs to be balanced against risk mitigation measures to address the privacy considerations inherent in having employee information stored externally.
- √ For external users such as partners, the information owners need to incorporate interactions with IAM providers into their SDLC, as well as into their threat assessments. Application security – the interactions of the various components with each other, and the vulnerabilities created thereby (such as SQL Injection and Cross Site Scripting, among many others) – must also be considered and protected against.
- √ PaaS customers should research the extent to which IDaaS vendors support industry standards for provisioning, authentication, communication about access control policy, and audit information.
- √ Proprietary solutions present a significant risk for components of IAM environments in the cloud, because of the lack of transparency into the proprietary components. Proprietary network protocols, encryption algorithms, and data communication are often less secure, less robust, and less interoperable. It is important to use open standards for the components of IAM that you are externalizing.

- √ For IaaS customers, third-party images used for launching virtual servers need to be verified for user and image authenticity. A review of the support provided for life cycle management of the image must verify the same principles as with software installed on your internal network.

Contributors: Subra Kumaraswamy, Sitaraman Lakshminarayanan, Michael Reiter, Joseph Stein, Yvonne Wilson

Domain 13: Virtualization

The ability to provide multi-tenant cloud services at the infrastructure, platform, or software level is often underpinned by the ability to provide some form of virtualization to create economic scale. However, use of these technologies brings additional security concerns. This domain looks at these security issues. While there are several forms of virtualization, by far the most common is the virtualized operating system, and this is the focus in this version of our guidance. If Virtual Machine (VM) technology is being used in the infrastructure of the cloud services, then we must be concerned about compartmentalization and hardening of those VM systems.

The reality of current practices related to management of virtual operating systems is that many of the processes that provide security-by-default are missing, and special attention must be paid to replacing them. The core virtualization technology itself introduces new attack surfaces in the hypervisor and other management components, but more important is the severe impact virtualization has on network security. Virtual machines now communicate over a hardware backplane, rather than a network. As a result, standard network security controls are blind to this traffic and cannot perform monitoring or in-line blocking. These controls need to take a new form to function in the virtual environment.

Commingling of data in centralized services and repositories is another concern. A centralized database as provided by a Cloud Computing service should in theory improve security over data distributed over a vast number and mixture of endpoints. However this is also centralizing risk, increasing the consequences of a breach.

Another concern is the commingling of VMs of different sensitivities and security. In Cloud Computing environments, the lowest common denominator of security will be shared by all tenants in the multi-tenant virtual environment unless a new security architecture can be achieved that does not "wire in" any network dependency for protection.

Recommendations

- √ Identify which types of virtualization your cloud provider uses, if any.
- √ Virtualized operating systems should be augmented by third party security technology to provide layered security controls and reduce dependency on the platform provider alone.
- √ Understand which security controls are in place internal to the VMs other than the built-in hypervisor isolation — such as intrusion detection, anti-virus, vulnerability scanning, etc. Secure by default configuration must be assured by following or exceeding available industry baselines.
- √ Understand which security controls are in place external to the VMs to protect administrative interfaces (web-based, APIs, etc.) exposed to the customers.
- √ Validate the pedigree and integrity of any VM image or template originating from the cloud provider before using.

- √ VM-specific security mechanisms embedded in hypervisor APIs must be utilized to provide granular monitoring of traffic crossing VM backplanes, which will be opaque to traditional network security controls.

- √ Administrative access and control of virtualized operating systems is crucial, and should include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.

- √ Explore the efficacy and feasibility of segregating VMs and creating security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data on separate physical hardware components such as servers, storage, etc.

- √ Have a reporting mechanism in place that provides evidence of isolation and raises alerts if there is a breach of isolation.

- √ Be aware of multi-tenancy situations with your VMs where regulatory concerns may warrant segregation.

Contributors: Bikram Barman, Girish Bhat, Sarabjeet Chugh, Philip Cox, Joe Cupano, Srijith K. Nair, Lee Newcombe, Brian O'Higgins

References

A guide to security metrics. SANS Institute, June 2006. http://www.sans.org

Amazon EC2 API - http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/

Amazon Elastic Compute Cloud Developer Guide,
http://docs.amazonwebservices.com/AWSEC2/2009-03-01/DeveloperGuide/

Amazon Simple Queue Service Developer Guide,
http://docs.amazonwebservices.com/AWSSimpleQueueService/2008-01-01/SQSDeveloperGuide/

Amazon Simple Storage Service Developer Guide,
http://docs.amazonwebservices.com/AmazonS3/2006-03-01/

Amazon SimpleDB Developer Guide,
http://docs.amazonwebservices.com/AmazonSimpleDB/2007-11-07/DeveloperGuide/

Amazon web services blog: Introducing amazon virtual private cloud (vpc), Amazon, August 2009. http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html

Amazon Web Services: Overview of Security Processes, September 2008

An Innovative Policy-based Cross Certification methodology for Public Key Infrastructures. Casola V., Mazzeo A., Mazzocca N., Rak M. 2nd EuroPKI Workshop. Springer-Verlag LNCS 35. Editors: D. Chadwick, G. Zhao. 2005.

Auditing the Cloud, Grid Gurus, http://gridgurus.typepad.com/grid_gurus/2008/10/auditing-the-cl.html, October 20, 2008

Azure Services Platform, http://msdn.microsoft.com/en-us/library/dd163896.aspx

Balanced Scorecard for Information Security Introduction", Published: March 06, 2007, http://technet.microsoft.com/en-us/library/bb821240.aspx

BITS Kalculator and BITS Financial Services Shared Assessments Program (third party provider assessment methodology)

Building Security In Maturity Model, http://www.bsi-mm.com/

Business case for a comprehensive approach to identity and access management, May 2009 https://wiki.caudit.edu.au/confluence/display/CTSCIdMWG/Business+case

Business Roundtable, Principles of Corporate Governance, 2005

Business Roundtable, Statement on Corporate Governance, 1997.

Business Software Alliance, Information Security Governance: Towards a Framework for Action Centers for Medicare and Medicaid Services Information Security Risk Assessment Methodology

Cloud Computing and Compliance: Be Careful Up There, Wood, Lamont, ITWorld, January 30, 2009

Cloud computing definition, by P. Mell and T. Grance, NIST June 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Cloud Computing is on the Up, but what are the Security Issues?, Mather, Tim, Secure Computing Magazine (UK), March 2, 2009.

Cloud Computing Use Case Group Whitepaper -http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing vocabulary (cloud computing wiki) http://sites.google.com/site/cloudcomputingwiki/Home/cloud-computing-vocabulary

Cloud Computing: Bill of Rights, http://wiki.cloudcomputing.org/wiki/CloudComputing:Bill_of_Rights

Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum, V 1.0, April 2009

Cloud Security and Privacy – An Enterprise perspective on Risks and Compliance from O'Reilly - http://oreilly.com/catalog/9780596802776/ -

Cloud Standards Organization - http://cloud-standards.org/

Cloud Storage Strategy, Steve Lesem, July 19, 2009, http://www.cloudstoragestrategy.com/2009/07/cloud-storage-and-the-innovators-dilemma.html

Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (DRAFT), 2009. http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf

Contracting for Certified Information Security: Model Contract Terms and Analysis (published by the Internet Security Alliance and available at www.cqdiscovery.com)

Contracting for Information Security: Model Contract Terms (published by the Internet Security Alliance and available at www.cqdiscovery.com)

CPMC ClearPoint Metric Catalog, 2009 Online Available: http://www.clearpointmetrics.com/newdev_v3/catalog/MetricApplicationPackage.aspx

CVSS A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007 Online Available: http://www.first.org/cvss/cvss-guide.html

Data Lifecycle Management Model Shows Risks and Integrated Data Flow, by Ernie Hayden, Information Security Magazine, July 2009
http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321704_mem1,00.html

Data Privacy Clarification Could Lead to Greater Confidence in Cloud Computing, Raywood, Dan, Secure Computing Magazine (UK), March 9, 2009.

Defending Electronic Mail as Evidence—The Critical E-Discovery Questions, Jeffrey Ritter, (available at www.cqdiscovery.com)

Does Every Cloud Have a Silver Compliance Lining?, Tom McHale, July 21, 2009 Online Available: http://blog.ca-grc.com/2009/07/does-every-cloud-have-a-silver-compliance-lining/

Encryption of Data At-Rest: Step-by-step Checklist", a whitepaper prepared by the Security Technical Working Group of the Storage Network Industry Association (SNIA).

ENISA - http://www.enisa.europa.eu/

Fedora Infrastructure Metrics, 2008. http://fedoraproject.org/wiki/Infrastructure/Metrics

Few Good Information Security Metrics, By Scott Berinato, July 2005 Online Available: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Force.com Web Services API Developer's Guide,
http://www.salesforce.com/us/developer/docs/api/index.htm

Global Privacy & Security, Francoise Gilbert, (Aspen Publishing 2009).

GoGrid API - http://wiki.gogrid.com/wiki/index.php/API

GSA to launch online storefront for cloud computing services, August 2009.
http://www.nextgov.com/nextgov/ng_20090715_3532.php

Guidelines for Media Sanitization," NIST's Special Publication 800-88

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, T. Ristenpart, et al,

http://blog.odysen.com/2009/06/security-and-identity-as-service-idaas.html

http://blogs.forrester.com/srm/2007/08/two-faces-of-id.html

http://blogs.intel.com/research/2008/10/httpseverywhere_encrypting_the.php

http://code.google.com/apis/accounts/docs/AuthForWebApps.html

http://code.google.com/apis/accounts/docs/OpenID.html

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

http://csrc.nist.gov/publications/PubsSPs.html

http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

http://www.aspeninstitute.org/publications/identity-age-cloud-computing-next-generation-internets-impact-business-governance-socia

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

http://www.sas70.com

https://siswg.net/index.php?option=com_docman&task=cat_view&gid=21&Itemid=99999999

Information Security Governance: A Call to Action, National Cyber Security Summit Task Force, Corporate Governance Task Force Report, April 2004.

Information Security Law: Emerging Standard for Corporate Compliance, Thomas Smedinghoff, (ITGP 2008).

ISACA, IT Governance Institute, Control Objectives for Information and related Technology (CobiT), 4.1

ISO/IEC 19011:2002 Guidelines for quality and/or environmental management systems auditing

ISO/IEC 20000-1:2005 Information technology—service management—Part 1: Specification

ISO/IEC 20000-1:2005 Information technology—service management—Part 2: Code of practice

ISO/IEC 21827:2008 Information technology—Systems Security Engineering—Capability Maturity Model (SSE-CMM®)

ISO/IEC 27000:2009 Information technology—Security techniques—Information security management systems—Overview and vocabulary

ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements.

ISO/IEC 27002:2005 Information technology—Security techniques—Code of practice for information security management

ISO/IEC 27005:2008 Information technology—Information security techniques—Information security risk management

ISO/IEC 27006:2007 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 28000:2007 Specification for security management systems for the supply chain

ISO/IEC 38500:2008 Corporate governance of information technology

IT Governance Institute, Board Briefing on Governance, 2nd Edition, 2003

IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006

ITGI Enterprise Risk: Identify Govern and Manage IT Risk—The Risk IT Framework, Exposure Draft version 0.1 February 2009.

Jericho Forum - http://www.opengroup.org/jericho/ and the Jericho Cloud Cube model http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Justify Identity Management Investment with Metrics, by Roberta J. Witty, Kris Brittain and Ant Allan, 23 Feb 2004. Gartner Research ID number TG-22-1617.

Managing Assurance, Security and Trust for Services. Online. Available: http://www.master-fp7.eu/

National Association for Information Destruction Inc - http://www.naidonline.org/forms/cert/cert_program_us.pdf

NIST Guidelines for Media Sanitization (800-88) - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

NIST Recommended Security Controls for Federal Information Systems (SP800-53)

NIST SP 800-30 Risk Management Guide for Information Technology Systems

OATH- http://www.openauthentication.org

OCEG, Foundation Guidelines Red Book, v1 10/27/2008

OCTAVE-S Implementation Guide, Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody, Version 1, 2005

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Open Cloud Computing Interface Working Group - http://www.occi-wg.org/doku.php

Open Security Architecture Group - http://www.opensecurityarchitecture.org

OpenCrowd - http://www.opencrowd.com/views/cloud.php

OpenID – http://openid.net

OpenID attribute exchange http://openid.net/specs/openid-attribute-exchange-1_0.htmlOAuth (created by a small group of individuals) http://OAuth.net/

OpenSocial – sharing social networking information http://www.opensocial.org/

ORCM Overcoming Risk And Compliance Myopia, August 2006 Online Available: http://logic.stanford.edu/POEM/externalpapers/grcdoc.pdf

OSAG Security Landscape - http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape

OWASP Top Ten Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Princeton Startup Lawyer, "Company Formation-Fiduciary Duties (the basics)", June 17, 2009, http://princetonstartuplawyer.wordpress.com/2009/06/17/company-formation-fiduciary-duties-the-basics/

Python Runtime Environment, http://code.google.com/appengine/docs/

Rackspace API - http://www.rackspacecloud.com/cloud_hosting_products/servers/api

Sailing in Dangerous Waters: A Director's Guide to Data Governance, E. Michael Power & Roland L. Trope, (American Bar Association, 2005).

SAML- http://www.oasis-open.org/specs/index.php#saml

Security Guidance for Critical Areas of Focus in Cloud Computing, Version 1, by Cloud Security Alliance, April 2009

Service Level Agreements: Managing Cost and Quality in Service Relationships, Hiles, A. (1993), London:Chapman & Hall
SNIA Encryption of Data At Rest: A Step-by-Step Checklist
http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/ssif/knowledge_center/white_papers/Encryption-Steps-Checklist_v3.060830.pdf

SNIA Introduction to Storage Security
http://www.snia.org/forums/ssif/knowledge_center/white_papers/Storage-Security-Intro1.051014.pdf

SNIA Storage Security Best Current Practices
http://www.snia.org/forums/ssif/forums/ssif/programs/best_practices/

Storage Security Best Current Practices (BCPs)" by the Security Technical Working Group of SNIA

Sun Project Kenai API - http://kenai.com/projects/suncloudapis

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management—Integrated Framework (2004).

The Darker Side of Cloud Computing, by Matthew D. Sarrel, PC Mag.com, February 1, 2009

The Force.com Workbook, http://wiki.developerforce.com/index.php/Forcedotcomworkbook

The Institute of Internal Auditors, Critical Infrastructure Assurance Project, "Information Security Governance: What Directors Need to Know", 2001

The International Grid Trust Federation (IGTF). http://www.igtf.net

United States General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, 1999.

United States Sentencing Commission, Guidelines Manual

vCloud API - http://www.vmware.com/solutions/cloud-computing/vcloud-api.html

Where We're Headed: New Developments and Trends in the Law of Information Security, Thomas J. Smedinghoff, Privacy and Data Security Law Journal, January 2007, pps. 103-138

Windows Azure SDK, http://msdn.microsoft.com/en-us/library/dd179367.aspx

Windows Cardspace - http://msdn.microsoft.com/en-us/library/aa480189.aspx

WS-Federation : http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

