Cloud
Standards
Customer
Council

Security for Cloud Computing
10 Steps to Ensure Success

August, 2012

Contents

Acknowledgements

The *Security for Cloud Computing: 10 Steps to Ensure Success* document is a collaborative effort that brings together diverse customer-focused experiences and perspectives into a single guide for IT and business leaders who are considering adopting cloud computing. The following participants have provided their expertise and time to this effort.

Workgroup Leaders

Ryan Kean (The Kroger Co.) – Workgroup chair; Application Section Leader

David Harris (Boeing) – Workgroup chair; Cloud Security Assessment Section Leader

John Meegan (IBM) – Lead Technical Editor; Introduction and SLA Section Leader

Barry Pardee (Tailwind Associates) – Current Landscape Section Leader

Yves Le Roux (CA Technologies) – GRC Section Leader

Chris Dotson (IBM) – Network & Connections Section Leader

Eric Cohen (PricewaterhouseCoopers) – Auditing Section Leader

Mike Edwards (IBM) – Data Section leader; Infrastructure Section Leader; Exit Process Section Leader

Jonathan Gershater (Trend Micro) – People, Roles & Identity Section Leader

Key Contributors

The workgroup leaders wish to recognize the following individuals for their outstanding efforts to provide content, share their expertise and ensure completeness of the white paper: Matt Rutkowski (IBM), Shamun Mahmud (DLT Solutions).

Reviewers

The following reviewers provided feedback on the white paper: Keith Trippie (Department of Homeland Security), Michael Chen (Cluster Technology Limited), Jeffery Finke (The MITRE Corporation), Dave Russell (IBM), Andrew Low (IBM).

Introduction

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers as they analyze and consider the security implications of cloud computing on their business. The paper includes a list of steps, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings in key areas from different cloud providers.

When considering a move to use cloud computing, consumers must have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as each model brings different security requirements and responsibilities. Additionally, this paper highlights the role that standards play to improve cloud security and also identifies areas where future standardization could be effective.

The section titled "Current Cloud Security Landscape" provides an overview of the security and privacy challenges pertinent to cloud computing and points out considerations that organizations should weigh when outsourcing data, applications, and infrastructure to a cloud computing environment.

The section titled "Cloud Security Guidance" is the heart of the guide and includes the steps that can be used as a basis for evaluation of cloud provider security. It discusses the threats, technology risks, and safeguards for cloud computing environments, and provides the insight needed to make informed IT decisions on their treatment. Although guidance is provided, each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the cloud services that can best fulfill those needs.

The section titled "Cloud Security Assessment" provides consumers with an efficient method of assessing the security capabilities of cloud providers and assessing their individual risk. A questionnaire for consumers to conduct their own assessment across each of the critical security domains is provided.

A related document, the *Practical Guide to Cloud Service Level Agreements*[1], released by the Cloud Standards Customer Council (CSCC) in April 2012, provides additional guidance on evaluating security criteria in cloud SLAs.

Cloud Security Landscape

While security and privacy concerns when using cloud computing services are similar to those of traditional non-cloud services, concerns are amplified by external control over organizational assets and the potential for mismanagement of those assets. Transitioning to public cloud computing involves a transfer of responsibility and control to the cloud provider over information as well as system

[1] See http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

components that were previously under the organization's direct control. The transition is usually accompanied by loss of direct control over the management of operations and also a loss of influence over decisions made about the computing environment.

Despite this inherent loss of control, the cloud service consumer still needs to take responsibility for their use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. The consumer achieves this by ensuring that the contract with the provider and its associated service level agreement (SLA) has appropriate provisions for security and privacy. In particular, the SLA must help maintain legal protections for privacy relating to data stored on the provider's systems. The consumer must also ensure appropriate integration of the cloud computing services with their own systems for managing security and privacy.

Cloud computing represents a very dynamic area at the present time, with new suppliers and new offerings arriving all the time. There are a number of security risks associated with cloud computing that must be adequately addressed: [2]

- **Loss of governance.** For public cloud deployments, consumers necessarily cede control to the cloud provider over a number of issues that may affect security. At the same time, cloud service level agreements (SLA) may not offer a commitment to provide such capabilities on the part of the cloud provider, thus leaving gaps in security defenses.
- **Responsibility ambiguity**. Given that use of cloud computing services spans across the consumer and the provider organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly. The split of responsibilities between consumer and provider organizations is likely to vary depending on the model being used for cloud computing (e.g. Iaas versus SaaS).
- **Isolation failure.** Multi-tenancy and shared resources are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).
- **Vendor lock-in**. Dependency on proprietary services of a particular cloud provider could lead to the consumer being tied to that provider. Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.
- **Compliance and legal risks.** Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to use cloud computing if the cloud provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud consumer. It is the responsibility of the cloud consumer to check that the cloud provider has appropriate certifications in place, but it is also necessary for the cloud consumer to be clear about the division of security responsibilities between the consumer and the provider and to ensure that the consumer's responsibilities are handled appropriately when using cloud computing services.

[2] Credit to European Network and Information Security Agency (ENISA). Visit http://www.enisa.europa.eu/ for more information.

- **Handling of security incidents**. The detection, reporting and subsequent management of security breaches is a concern for consumers, who are relying on providers to handle these matters.
- **Management interface vulnerability.** Consumer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than traditional hosting providers and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
- **Data protection.** Cloud computing poses several data protection risks for cloud consumers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud consumer (in the role of data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated cloud services.
- **Malicious behavior of insiders**. Damage caused by the malicious actions of insiders working within an organization can be substantial, given the access and authorizations they may have. This is compounded in the cloud computing environment since such activity might occur within either or both the consumer organization and the provider organization.
- **Business failure of the provider**. Such failures could render data and applications essential to the consumer's business unavailable.
- **Service unavailability**. This could be caused by a host of factors, from equipment or software failures in the provider's data center, through failures of the communications between the consumer systems and the provider services.
- **Insecure or incomplete data deletion.** Requests to delete cloud resources, for example, when a consumer terminates service with a provider, may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a consumer perspective), either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other clients. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the consumer than is the case with dedicated hardware.

While the above security risks need to be addressed, use of cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of many organizations. Cloud service providers should be able to offer advanced facilities for supporting security and privacy due to their economies of scale and automation capabilities - potentially a boon to all consumer organizations, especially those who have limited numbers of personnel with advanced security skills.

Cloud Security Guidance

As consumers transition their applications and data to use cloud computing, it is critically important that the level of security provided in the cloud environment be equal to or better than the security provided by their traditional IT environment. Failure to ensure appropriate security protection could ultimately result in higher costs and potential loss of business thus eliminating any of the potential benefits of cloud computing.

This section provides a prescriptive series of steps that should be taken by cloud consumers to evaluate and manage the security of their cloud environment with the goal of mitigating risk and delivering an appropriate level of support. The following steps are discussed in detail:

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities
9. Manage security terms in the cloud SLA
10. Understand the security requirements of the exit process

Requirements and best practices are highlighted for each step. In addition, each step takes into account the realities of today's cloud computing landscape and postulates how this space is likely to evolve in the future, including the important role that standards will play to improve interoperability and comparability across providers.

Step 1: Ensure effective governance, risk and compliance processes exist

Most organizations have established security and compliance policies and procedures that are used to protect their intellectual property and corporate assets especially in the IT space. These policies and procedures are developed based upon risk analyses to the organization considering the impact of having these assets compromised. A framework of controls and further procedures are established to mitigate risk and serve as a benchmark for the execution and validation of compliance. These principles and policies, the enterprise security plan, and the surrounding quality improvement process represent the enterprise security governance, risk management, and compliance model.

Security controls in cloud computing are similar to those in traditional IT environments. However, because of the cloud service and operational models employed with the implied organizational division of responsibilities and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. As part of the transition to cloud computing, it is critical that consumers understand their level of risk tolerance and focus on mitigating the risks that the organization cannot afford to neglect.

The primary means a consumer of cloud service has to ensure their cloud hosted applications and data will be secured in accordance with its security and compliance policies is to verify that the contract between the consumer and the provider, along with an associated service level agreement (SLA), contain all their requirements. It is vital for a consumer to understand all the terms related to security and to ensure that those terms meet the needs of the consumer. If a suitable contract and SLA is not available, then it is inadvisable for an organization to proceed with the use of cloud services.

Often it is not understood that the type of service model being offered by the provider (i.e. IaaS, PaaS or SaaS) has significant impact on the assumed "split of responsibilities" between the consumer and the provider to manage security and associated risks. For IaaS, the provider is supplying (and responsible for securing) basic IT resources such as machines, disks and networks. The consumer is responsible for the operating system and the entire software stack necessary to run applications, plus the data placed into the cloud computing environment. As a result, most of the responsibility for securing the applications themselves and the data they use falls onto the consumer. In contrast, for SaaS, the infrastructure, software and data are primarily the responsibility of the provider, since the consumer has little control over any of these features of the service. These aspects need appropriate handling in the contract and SLA.

From a general governance perspective, cloud providers should notify consumers about the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur. Due to the high financial and reputational costs resulting from a breach, consumers may want the provider to indemnify them if the breach was their fault.

A fundamental design premise in cloud computing is that, as a consumer, your data can be stored by, processed on and transmitted to any of the servers or devices the cloud service provider operates. In some instances, servers hosting consumer data may be located in multiple datacenters within different jurisdictions, either because the service provider has multi-jurisdictional operations or has subcontracted services to providers that operate in other jurisdictions. This means that it may be difficult at any particular point in time to know where your data actually resides, which regulators have jurisdiction and what regulations apply. This matters since some regulations restrict the allowable locations for data.

The jurisdictional issue directly influences the protection of personally identifiable information (PII) and the law enforcement access to this data.[3] There is divergence across countries in the laws on investigation and enforcement, including access to encrypted data and investigation of extraterritorial

[3] The Business Software Alliance (BSA) Global Cloud Computing Scorecard provides an assessment of security and privacy policies that countries are implementing for cloud computing. Refer to http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf for details.

offences. A court can only hear a matter if it has jurisdiction over the parties and the subject matter of the action, while law enforcement agencies can only exercise their powers within their authorized jurisdictions.

Before migrating services to a cloud computing environment, it is important to understand precisely the specific laws or regulations that apply to the services and what are the relevant duties or obligations imposed (e.g. data retention, data protection, interoperability, medical file management, disclosure to authorities). This allows consumers to identify the legal issues and the related legal risks, and consequently the impact these will have on the services being migrated to cloud computing.

One useful approach to the security challenges of cloud computing is for a cloud provider to demonstrate that they are compliant with an established set of security controls. Certification of the provider gives more confidence in that provider to prospective consumers. There are a number of different certifications which can be useful for cloud computing services - which one is most appropriate depends to some extent on the cloud service model (IaaS, PaaS, SaaS) and also depends on your regional and industry requirements.

The most widely recognized international standard for information security compliance is ISO/IEC 27001[4] which includes national variants and well developed certification regimes. ISO is currently developing new standards, ISO/IEC 27017[5] "Security in Cloud Computing" and ISO/IEC 27018[6] "Privacy in Cloud Computing", which will specifically address cloud security and privacy considerations that build upon ISO/IEC 27001.

Some organizations provide frameworks and certifications for evaluating IT security which can be applied to cloud service providers, including the American Institute of Certified Public Accountants (AICPA) and Information Systems Audit and Control Association (ISACA) which provide the SSAE 16[7] and CoBIT 5[8] frameworks respectively. Other organizations provide specialized frameworks for specific services or industries such as the Payment Card Industry (PCI) Data Security Standard (DSS). [9]

Groups such as the Cloud Security Alliance (CSA) provide guidance which includes a Cloud Controls Matrix (CCM), a provider self assessment program, Consensus Assessment Initiative (CAI), Certificate of Cloud Security Knowledge (CCSK), and a registry to publish the self evaluation results (STARS).[10]

[4] See http://www.iso.org/iso/catalogue_detail?csnumber=42103 for details.

[5] See http://www.iso27001security.com/html/27017.html for details.

[6] See http://www.iso27001security.com/html/27018.html for details.

[7] See http://ssae16.com/SSAE16_overview.html for details.

[8] See http://www.isaca.org/COBIT/Pages/default.aspx for details.

[9] See https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf for details.

[10] Refer to https://cloudsecurityalliance.org/ for details on the CSA programs.

Step 2: Audit operational & business processes

Companies understand the importance of auditing the compliance of IT systems, which host their applications and data, to assess effectiveness in enforcing their corporate, industry or government requirements and policies.

As a baseline, consumers should expect to see a report of the cloud provider's operations by independent auditors. Unfettered access to essential audit information is a key consideration of contracts and SLA terms with any cloud provider. As part of any terms, cloud providers should offer timely access to and self management of audit event, log and report information relevant to a consumer's specific data or applications.

Security compliance tends to be a significant element of any compliance framework. There are three significant areas where the consideration of security methods for cloud computing are of particular interest to cloud consumers and to auditors:

1. Understanding the internal control environment of a cloud provider, including risks, controls and other governance issues when that environment touches the provision of cloud services.
2. Access to the corporate audit trail, including workflow and authorization, when the audit trail spans cloud services.
3. Assurance of the facilities for management and control of cloud services made available to cloud consumers by cloud providers and how such facilities are secured.

Understanding the internal control environment of a cloud provider

Using the services of cloud providers creates the need for appropriate auditing of the activities of persons that may be employed by the cloud provider or consumer (along with any consumer customers and partners) to ensure that the security controls meet the requirements of the consumers. Consumers should expect to see audit information relating to any cloud provider they plan to use. There are alternative standards that can be used as the basis for auditing a service provider, such as the ISO 27000 series. These standards aim to provide the basis for assuring consumers about the nature of the controls environment in place at the cloud provider's organization.

Key controls that relate to cloud computing services include those which

- ensure isolation of consumer applications and data in shared, multi-tenant environments
- provide protection of consumer assets from unauthorized access by the provider's staff

Auditors may be employed by the consumer or they may be employed by the provider - but the key element is that they should be *independent*. Auditors require access to information about the policies and procedures of a cloud provider which relate to security controls. Auditors also require access to logs and records which show whether the policies and procedures are being followed correctly - and in some cases, the auditors may require specific testing to take place to demonstrate compliance with the prescribed policies and procedures.

Security and authentication technologies, allied to event logging, in the cloud computing environment can help auditors as they deal with issues related to workflow - were those who entered, approved, changed or otherwise touched data authorized to do so, on an individual, group or role-related basis? Was that authorization appropriate on a one-time, periodic or ongoing basis?

Access to the corporate audit trail

It is vital for cloud service consumers to have appropriate audit access to cloud provider events, logs and audit trails to prove enforcement of provider security controls. Auditors need to assure cloud consumers that all the necessary information is being logged and stored appropriately by cloud providers, including authentication, authorization and management information relating to the use of particular applications and data against all security and compliance policies established by the provider or consumer.

For complete insight into security controls, as they relate to the consumer's applications and data, mechanisms for the routine flow of audit information from the provider to the consumer is recommended. This flow may include secure logs and reports against an agreed upon schedule. There should be more timely notification of any exceptional security alerts, events or incidents - and incident management processes should be documented and audited. Any audit data should have the necessary associated information to enable forensic analysis to understand how any particular incident occurred, what assets were compromised and what policies, procedures and technologies need to be changed to prevent recurrence, along with any additional security controls that need to be established.[11]

Ideally, there should be automated, standards-based, programmatic access to all of these audit facilities, to ensure timely availability of required data and to remove cost burdens associated with human processing of requests for information.

Assurance of the facilities for management and control of cloud services

In addition to controls which apply to cloud services themselves, there is also a need for providers to enable consumers to self manage and more closely monitor the usage of their cloud hosted applications and services. These facilities may include: service catalogs, subscription services, payment processes, the provision of streams of operational event data and logs, usage metering data, facilities for configuring services including adding and removing user identities and the configuration of authorizations.

These facilities are often more sensitive in security terms than the services and applications to which they apply, since the potential for abuse and damage may be higher. A security audit must extend to these facilities as well as to the main services of the provider.

[11] The emerging DMTF Cloud Audit Data Federation (CADF) Workgroup is planning to develop an audit event data model and a compatible interaction model that is able to describe interactions between IT resources suitable for cloud deployment models. Refer to dmtf.org/sites/default/files/CADFWG_Charter_05-02-2011.pdf for details on the workgroup's charter.

Auditing is essential

The security audit of cloud service providers is an essential aspect of the security considerations for cloud consumers. Audits should be carried out by appropriately skilled staff, either belonging to the consumer or to an independent auditing organization. Security audits should be carried out on the basis of one of the established standards for security controls. Consumers need to check that the sets of controls in place meet their security requirements.

There is also a need to ensure proper integration of the cloud provider's reporting and logging facilities with the consumer's systems, so that appropriate operational and business data flows on a timely basis to enable consumers to manage their use of provider services.

Step 3: Manage people, roles and identities

Consumers must ensure that their cloud provider has processes and functionality that governs who has access to the consumer's data and applications. This ensures access to their cloud environments is controlled and managed.

Organizations manage dozens to thousands of employees and users who access their cloud applications and services, each with varying roles and entitlements. Cloud providers must allow the cloud consumer to assign and manage the roles and associated levels of authorization for each of their users in accordance with their security policies. These roles and authorization rights are applied on a per resource, service or application basis. For example, a cloud consumer, in accordance with its security policies, may have an employee whose role permits them to generate a purchase request, but a different role and authorization rights is granted to another employee responsible for approving the request.

The cloud provider must have a secure system for provisioning and managing unique identities for their users and services. This Identity Management functionality must support simple resource accesses and robust consumer application and service workflows. A key requirement for moving a consumer application to the cloud is assessing the provider's ability to allow the consumer to assign their user identities into access groups and roles that reflect their operational and business security policies.

Any user access or interaction with the provider's management platform, regardless of role or entitlement, should be monitored and logged to provide auditing of all access to consumer data and applications.

Table 1 highlights the key features a cloud provider should support in order for a consumer to effectively manage people, roles and identities in the cloud:

Table 1. Cloud provider support for people, roles and identities

Provider Supports	Consumer Considerations and Questions
Federated Identity Management (FIM), External Identity Providers (EIP)	• Enterprises that are cloud consumers, in many cases, already have an existing database of users, most likely stored in an enterprise directory, and they wish to leverage this user

	database without recreating user identities. • Question to cloud provider: Can I integrate my current user store (internal database or directory of users) without recreating all my users within your cloud environment?
Identity Provisioning and Delegation	• Consumer organizations need to administer their own users; the cloud provider should support delegated administration. • Question to cloud provider: What provisioning tools do you provide for on-boarding and off-boarding users? • Question to cloud provider: Does your platform offer delegated administration for my organization to administer users?
Single Sign-On (SSO), Single Sign-Off	• Consumer organizations may wish to federate identity across applications to provide single-sign-on (SSO) along with single sign-off to assure user sessions get terminated properly. For example, an organization using separate SaaS applications for CRM and ERP would like single-sign-on and sign-off across these applications (e.g. using standards such as SAML[12], WS-Federation[13] and OAuth[14]). • Question to cloud provider: Do you offer single-sign-on for access across multiple applications you offer or trusted federated single-sign-on across applications with other vendors?
Identity and Access Audit	• Consumers need auditing and logging reports relating to service usage for their own assurance as well as compliance with regulations. • Question to cloud provider: What auditing logs, reports, alerts and notifications do you provide in order to monitor user access both for my needs and for the needs of my auditor?
Robust Authentication	• For access to high value assets hosted in the cloud, cloud

[12] Refer to https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security for details.

[13] Refer to https://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed for details.

[14] Refer to http://oauth.net/ for details.

	consumers may require that their provider support strong, multi-factor, mutual and/or even biometric authentication. • Question to cloud provider: If required, does your platform support strong, multi-factor or mutual authentication?
Role, Entitlement and Policy Management	• Cloud consumers need to be able to describe and enforce their security policies, user roles, groups and entitlements to their business and operational applications and assets, with due consideration for any industry, regional or corporate requirements. • Question to cloud provider: Does your platform offer fine-grained access control so that my users can have different roles that do not create conflicts or violate compliance guidelines?

Cloud providers should have formalized processes for managing their own employee access to any hardware or software used to store, transmit or execute consumer data and applications, which they should disclose and demonstrate to the consumer

Step 4: Ensure proper protection of data and information

Data are at the core of IT security concerns for any organization, whatever the form of infrastructure that is used. Cloud computing does not change this, but cloud computing does bring an added focus because of the distributed nature of the cloud computing infrastructure and the shared responsibilities that it involves. Security considerations apply both to *data at rest* (held on some form of storage system) and also to d*ata in motion* (being transferred over some form of communication link), both of which may need particular consideration when using cloud computing services.

Essentially, the questions relating to data for cloud computing are about various forms of risk: risk of theft or unauthorized disclosure of data, risk of tampering or unauthorized modification of data, risk of loss or of unavailability of data. It is also worth remembering that in the case of cloud computing, "data assets" may well include things such as application programs or machine images, which can have the same risk considerations as the contents of databases or data files.

The general approaches to the security of data are well described in specifications such as the ISO 27002 standard - and these control-oriented approaches apply to the use of cloud computing services, with some additional cloud-specific considerations as described in the ISO 27017 standard (currently under development). Security controls as described in ISO 27002 highlight the general features that need to be addressed, to which specific techniques and technologies can then be applied.

The type of cloud service is very likely to affect the key question of who is responsible for handling particular security controls. For IaaS, more responsibility is likely to be with the consumer (e.g. for encrypting data stored on a cloud storage device); for SaaS, more responsibility is likely to be with the provider, since both the stored data and the application code is not directly visible or controllable by the consumer.

Table 2 highlights the key steps consumers should take to ensure that data involved in cloud computing activities is properly secure.

Table 2. Controls for securing data in cloud computing

Controls	Description
Create a data asset catalog	• A key aspect of data security is the creation of a data asset catalog, identifying all data assets, classifying those data assets in terms of criticality to the business (which can involve financial and legal considerations, including compliance requirements), specifying ownership and responsibility for the data and describing the location(s) and acceptable use of the assets. • Relationships between data assets also need to be cataloged. • An associated aspect is the description of responsible parties and roles, which in the case of cloud computing must span the cloud service consumer organization and the cloud service provider organization.
Consider all forms of data	• Organizations are increasing the amount of unstructured data held on IT systems, which can include items such as images of scanned documents and pictures of various kinds. • Unstructured data can be sensitive and require specific treatment - for example redaction or masking of personal information such as signatures, addresses, license plates. • For structured data, in a multi-tenancy cloud environment, data held in databases needs consideration. Database segmentation can be offered in a couple of varieties: shared or isolated data schema. o In a shared data schema, each customer’s data is intermixed within the same database. This means that customer A's data may reside in row 1 while customer B's data resides in row 2. o In an isolated architecture, the consumers' data is segregated into its own database instance. While this may provide additional isolation, it also impacts the providers' economies of scale and could, potentially, increase the

	cost to the consumer. o In either scenario, database encryption should be employed to protect all data at rest.
Consider privacy requirements	• Data privacy often involves laws and regulations relating to the acquisition, storage and use of personally identifiable information (PII). • Typically, privacy implies limitations on the use and accessibility of PII, with associated requirements to tag the data appropriately, store it securely and to permit access only by appropriately authorized users. • This requires appropriate controls to be in place, particularly when the data is stored within a cloud provider's infrastructure. The ISO 27018 standard (in preparation) addresses the controls required for PII. These controls may restrict the geographical location in which the data is stored, for example, which runs counter to one aspect of cloud computing which is that cloud computing resources can be distributed in multiple locations.
Apply confidentiality, integrity and availability	• The key security principles of *confidentiality, integrity and availability* are applied to the handling of the data, through the application of a set of policies and procedures, which should reflect the classification of the data. • Sensitive data should be encrypted, both when it is stored on some medium and also when the data is in transit across a network - for example, between storage and processing, or between the provider's system and a consumer user's system. o An extra consideration when using cloud computing concerns the handling of encryption keys - where are the keys stored and how are they made available to application code that needs to decrypt the data for processing? It is not advisable to store the keys alongside the encrypted data, for example. • Integrity of data can be validated using techniques such as message digests or secure hash algorithms, allied to data duplication, redundancy and backups. • Availability can be addressed through backups and/or redundant storage and resilient systems, and techniques related to the handling of denial-of-service attacks. There is also a need for a failover strategy, either by using a service provider who offers this as part of their service offering, or if the provider does not offer resiliency as a feature of their services the consumer may consider self provision of failover by having equivalent services on standby with another provider.

Apply identity and access management	• Identity and access management is a vital aspect of securing data (refer to “Step 3: Manage people, roles and identities” on page 13) with appropriate authorization being required before any user is permitted to access sensitive data in any way. • Related to this is the requirement for logging and security event management (e.g. the reporting of any security breaches) relating to the activities taking place in the cloud service provider environment. • Following from this is the need for a clear set of procedures relating to data forensics in the event of a security incident. Note that the logs and reporting mechanisms are also in need of appropriate security treatment, to prevent a wrongdoer from being able to cover their tracks.

Most of the security techniques and technologies involved are not new, although cloud computing can create new considerations. For example, if encryption is used on some data, how are the encryption keys managed and used? In addition, the way in which security is applied will most likely depend on the nature of the cloud service being offered. For IaaS, much of the security responsibility is likely to lie with the consumer. For SaaS, much more responsibility is likely to be placed onto the provider, especially since the data storage facilities may be opaque as far as the consumer is concerned.

Step 5: Enforce privacy policies

Privacy is gaining in importance across the globe, often involving laws and regulations, relating to the acquisition, storage and use of personally identifiable information (PII). Typically, privacy implies limitations on the use and accessibility of PII, with associated requirements to tag the data appropriately, store it securely and to permit access only by appropriately authorized users. This requires appropriate controls to be in place, particularly when the data is stored within a cloud provider’s infrastructure. The ISO 27018 standard (in preparation) addresses the controls required for PII.

In many countries, numerous laws, regulations and other mandates require public and private organizations to protect the privacy of personal data and the security of information and computer systems. Appendix A on page 31 provides an overview of the worldwide privacy regulations that currently exist.

When data is transferred to a cloud computing environment, the responsibility for protecting and securing the data typically remains with the consumer (the *data controller* in EU terminology[15]), even if in some circumstances, this responsibility may be shared with others. When an organization relies on a

[15] The European Union provides a Glossary of terms associated with Data Protection here: http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary

third party to host or process its data, the data controller remains liable for any loss, damage, or misuse of the data. It is prudent, and may be legally required, that the data controller and the cloud provider enter into a written (legal) agreement that clearly defines the roles, expectations of the parties, and allocates between them the many responsibilities that are attached to the data at stake.

It is critical that privacy issues are adequately addressed in the cloud contract and service level agreement (SLA). If not, the cloud consumer should consider alternate means of achieving their goals including seeking a different provider, or not putting sensitive data into the cloud computing environment. For example, if the consumer wishes to place HIPAA-covered information into a cloud computing environment, the consumer must find a cloud service provider that will sign a HIPAA business associate agreement or else not put that data into the cloud computing environment.

Enterprises are responsible for defining policies to address privacy concerns and raise awareness of data protection within their organization. They are also responsible for ensuring that their cloud providers adhere to the defined privacy policies. Consumers have an ongoing obligation to monitor their provider's compliance with its policies. This includes an audit program covering all aspects of the privacy policies including methods of ensuring that corrective actions will take place.

Step 6: Assess the security provisions for cloud applications

Organizations need to proactively protect their business-critical applications from external and internal threats throughout their entire life cycle, from design to implementation to production. Clearly defined security policies and processes are critical to ensure the application is enabling the business rather than introducing additional risk.

Application security poses specific challenges to the cloud provider and consumer. Organizations must apply the same diligence to application security as they do for physical and infrastructure security. If an application is compromised, it can present liability and perception issues to both the cloud provider and the consumer, especially if the ultimate end users of the application are customers of the consumer rather than employees.

In order to protect an application from various types of breaches, it is important to understand the application security policy considerations based on the different cloud deployment models. Table 3 highlights the impact of cloud deployment on application security. All of these considerations are in addition to those outlined in this whitepaper (facilities, network, data, etc).

Table 3. Deployment model impact on application security

Deployment Type	Application Security Policy Considerations
Infrastructure as a Service	• The consumer has responsibility for deployment of the complete software stack - operating system, middleware and application - and for all aspects of security that relate to this stack. • The application security policy should closely mimic the policy of applications hosted internally by the consumer. • The consumer should focus on network, physical environment, auditing, authorization, and authentication considerations as outlined in this document.

	• The consumer is typically responsible for patching of operating system, middleware and application. • Appropriate data encryption standards should be applied.
Platform as a Service	• The consumer has responsibility for application deployment and for securing access to the application itself. • The provider has responsibility for properly securing the infrastructure, operating system and middleware. • The consumer should focus on audit, authorization, and authentication considerations as outlined in this document. • Appropriate data encryption standards .should be applied. • In a PaaS model, the consumer may or may not have knowledge of the format and location of their data. It is important that they are knowledgeable of how their data may be accessed by individuals with administrative access.
Software as a Service	• Application tier security policy constraints are mostly the responsibility of the provider and are dependent upon terms in the contract and SLA. The consumer must ensure that these terms meet their confidentiality, integrity and availability requirements. • Important to understand provider's patching schedule, controls of malware, and release cycle. • Threshold policies help to identify unexpected spikes and reduction of user load on the application. Thresholds are based on resources, users and data requests. • Typically, the consumer is only able to modify parameters of the application that have been exposed by the provider. These parameters are likely independent of application security configurations, however, the consumer should ensure that their configuration changes augment; not inhibit the provider's security model. • The consumer should have knowledge of how their data is protected against administrative access by the provider. In a SaaS model, the consumer will likely not be aware of the location and format of the data storage. • The consumer must understand the data encryption standards which are applied to data at rest and in motion.

It should be noted that there is a cost to the consumer to ensure that these considerations are applied. The costs are typically built into technology, resources, interventions, and audits. However, these costs will, likely, pale in comparison to the potential liability damages and loss of reputation from an application security breach.

When developing and deploying applications in a cloud environment it is critical that consumers realize that they may be forfeiting some control and have to design their cloud applications with that consideration in mind. In addition, it is critical that consumers developing software use a structured methodology to engineer security into their cloud applications from the ground up.

Step 7: Ensure cloud networks and connections are secure

A cloud service provider must attempt to allow legitimate network traffic and drop malicious network traffic, just as any other Internet-connected organization does. However, unlike many other organizations, a cloud service provider will not necessarily know what network traffic its consumers plan to send and receive. Nevertheless, consumers should expect certain external network perimeter safety measures from their cloud providers.

To use the analogy of a hotel, we expect the hotel to provide some limited amount of perimeter security – not allowing anyone into the building without a key card during certain times of night, for example, or challenging obviously dangerous persons – even though we should not expect the hotel to deny access to every dangerous person.

With this in mind, it is recommended that consumers evaluate the external network controls of a cloud provider based on the areas highlighted in Table 4.

Table 4. External network requirements

Provider Responsibility	Description / Guidance
Traffic screening	• Certain traffic is almost never legitimate – for example, traffic to known malware ports. The provider should block this traffic on behalf of the consumers. • Traffic screening is generally performed by firewall devices or software. Some firewall considerations: o Does the provider publish a standard perimeter block list that aligns with the terms of service for the offering? Consumers should request a copy of the block list; a reasonable block list can provide a consumer with both assurance of a thoughtful network protection plan as well as some functional guidelines on what is allowed. There may be some cause for concern if the block list is not in line with the terms of service. o Does the provider's firewall block all IPv6 access, or protect against both IPv4 and IPv6 attacks? More and more devices are IPv6 capable, and some providers forget to limit IPv6 access – which can allow an attacker an easy way around the IPv4 firewall. o Is the traffic screening able to withstand and adapt to attacks such as Distributed Denial-of-Service attacks? DDOS attacks are more and more commonly used for extortion purposes by organized crime, and the ability of a cloud service provider and its Internet service provider to assist in blocking the unwanted traffic can be crucial to withstanding an attack.
Intrusion	• Some traffic may look legitimate, but deeper inspection indicates that it is carrying malicious payload such as spam, viruses, or known attacks. The

detection/prevention	provider should block or at least notify consumers about this traffic. • Intrusion detection and/or prevention systems (IDS/IPS) may be software or devices. Whereas a firewall usually only makes decisions based on source/destination, ports, and existing connections, an IDS/IPS looks at both overall traffic patterns as well as the actual contents of the messages. Many firewalls now include IDS/IPS capabilities. • Although technically not IDS/IPS devices, application-level proxies (such as e-mail gateways/relays) will often perform similar functions for certain types of network traffic and are considered here as well. • An IDS will typically only flag potential problems for human review; an IPS will take action to block the offending traffic automatically. Some IDS/IPS considerations: o IDS/IPS content matching can detect or block known malware attacks, virus signatures, and spam signatures, but are also subject to false positives. Does the cloud provider have a documented exception process for allowing legitimate traffic that has content similar to malware attacks or spam? o Similarly, IDS/IPS traffic pattern analysis can often detect or block attacks such as a denial-of-service attack or a network scan. However, in some cases this is perfectly legitimate traffic (such as using cloud infrastructure for load testing or security testing). Does the cloud provider have a documented exception process for allowing legitimate traffic that the IDS/IPS flags as an attack pattern?
Logging and notification	• For assurance purposes and troubleshooting, it's important that consumers have some visibility into the network health. • Incident reporting and incident handling procedures must be clear and the consumer should look for visibility into the handling process. Note that if any PII is stored in the cloud computing environment, there may be legal requirements associated with any incident. • Some network logging information is of a sensitive nature and may reveal information about other clients, so a cloud provider may not allow direct access to this information. However, it is recommended that consumers ask certain questions about logging and notification policies: o What is the network logging and retention policy? In the event of a successful attack, the consumer may want to perform forensic analysis, and the network logs can be very helpful. o What are the notification policies? As a cloud consumer, you should be notified in timely manner if your machines are attacked or compromised and are attacking someone else. o Are historical statistics available on the number of attacks detected and blocked? These statistics can help a consumer understand how effective the provider's detection and blocking capabilities actually are.

Cloud computing includes a number of resources that are not shared in a traditional data center. One of these resources is the cloud provider's internal network infrastructure, such as the access switches and routers used to connect cloud virtual machines to the provider's backbone network.

Internal network security differs from external network security in that we postulate that any attackers have already made it through the external defenses, either via an attack or, more commonly, because the attackers are legitimately authorized for a different part of the network. After a user is allowed access to a portion of the cloud service provider's network, the provider has a number of additional responsibilities with respect to internal network security.

The primary categories of internal network attacks that consumers should be concerned with include:

1. Confidentiality breaches (disclosure of confidential data)
2. Integrity breaches (unauthorized modification of data)
3. Availability breaches (denial of service, either intentional or unintentional)

Consumers must evaluate the cloud service provider's internal network controls with respect to their requirements and any existing security policies the consumer may have. Each consumer's requirements will be different, but it is recommended that consumers evaluate the internal network controls of a service provider based on the areas highlighted in Table 5.

Table 5. Internal network requirements

Provider Responsibility	Description / Guidance
Protect clients from one another	Cloud providers are responsible for separating their clients in multi-tenant situations. Most cloud service providers will use one or more of the following technologies for this purpose: 1. Dedicated virtual LANs, or VLANs, are a technology that makes a collection of ports on a physical Ethernet switch appear to be a separate switch. In theory, network traffic on one VLAN cannot be seen on a different VLAN any more than network traffic on one physical Ethernet switch can be seen on a different, non-connected Ethernet switch. VLAN separation technology is often a primary control for cloud providers and is generally very effective. However, there are documented “VLAN hopping” attacks that allow unauthorized traffic between VLANs, such as “double-tagging” and “switch spoofing”. Many cloud providers offer dedicated VLANs for consumers that no other consumers should be able to access. It is recommended that consumers verify that the provider's VLAN controls address the known VLAN hopping attacks. 2. Virtual Private Networks (VPNs, and also sometimes referred to simply as “tunnels”) can be used to connect a consumer's dedicated cloud VLAN back to the consumer's network; this configuration is commonly known as a “site-to-site” VPN.

	VPNs can also be used to allow roaming users anywhere on the Internet to securely access the consumer's VLAN; this configuration is commonly called “client-to-site”. In both cases, there are multiple technologies (such as SSL and IPSec) with different security implementations (such as certificate/credential based or endpoint authentication). It is recommended that consumers decide whether VPNs are required, and if so ensure that the cloud provider supports the required operating mode (client-to-site or site-to-site) and security implementation. 3. Per-instance software firewalls are one of the “last lines of defense” and allow consumers to regulate what traffic comes into their instances by configuring the software firewall on the instance itself. If using a cloud provider's images, consumers should ensure that the images contain proper software firewall capabilities and that the rules are simple to deploy and modify. Per-instance software firewalls are particularly important when sharing a VLAN with other consumers. 4. “Private VLAN” (PVLAN) is a term that has two meanings. One meaning is a VLAN that is dedicated to a particular consumer, which is defined simply as “Dedicated VLAN” above. The second more technical use of the term is a VLAN that prohibits all traffic between hosts on the private VLAN by default. With Private VLAN technology, consumer A and consumer B could be on the same VLAN, but still be unable to communicate with one another – they may only be allowed to talk to the router that allows internet access. Private VLAN technology is effective as long as the router, which is permitted to talk to all stations on the network, is not configured to relay traffic originating in the VLAN back in to the VLAN, thereby bypassing the switch's controls. Private VLAN technology provides good isolation but can lead to functional problems, as cloud instances often need to talk to other cloud instances in addition to systems out on the Internet. For this reason, per-instance firewalls are more commonly used for instance separation on the same VLAN. If PVLAN technology is needed, it is recommended that the consumer test to ensure that the router is properly configured and that traffic between cloud instances on the same VLAN is blocked. 5. Hypervisor based filters, such as *ebtables* on Linux, are functionally similar to private VLANs in that they can prohibit or allow communications at the “virtual switch” level. However, these can also be used to prevent attacks such as IP and MAC address spoofing. If dedicated VLANs are not used, it is recommended that the consumer ask what protections are in place to prevent another consumer's instance from masquerading as one of your instances.
Protect the provider's network	• Separate the provider's network from all clients. If the provider's network is breached, it could lead to almost undetectable data loss. • The client separation strategies above are worthless if the provider's control network is not properly protected. An attacker who gains access to the provider's control network may be able to perform attacks on other consumers from the control network.

	• Consumers should ask what security controls are in place for the cloud infrastructure itself. While many cloud providers will not give out in-depth details of their security measures due to valid security concerns, there should be a stated security policy and some assurance (e.g. via audit and certification) that it is followed.
Monitor for intrusion attempts	• Activity auditing and logging are an important part of preventive security measures as well as incident response and forensics. Audit information and logs should be subject to appropriate security controls to prevent unauthorized access, destruction or tampering. • Cloud consumers should ask what types of internal network security incidents have been reported and if there are any published statistics or metrics. • Consumers should also ask for the provider's processes for alerting consumers about both successful and unsuccessful internal network attacks.

Step 8: Evaluate security controls on physical infrastructure and facilities

An important consideration for security of any IT system concerns the security of physical infrastructure and facilities. In the case of cloud computing, these considerations apply, but it will often be the case that the infrastructure and facilities will be owned and controlled by the cloud service provider and it is the responsibility of the cloud consumer to get assurance from the provider that appropriate security controls are in place.

Assurance may be provided by means of audit and assessment reports, demonstrating compliance to such security standards as ISO 27002.

A brief description of the security controls that should apply to the physical infrastructure and facilities of a cloud provider includes:

- *Physical Infrastructure and facilities should be held in secure areas*. A physical security perimeter should be in place to prevent unauthorized access, allied to physical entry controls to ensure that only authorized personnel have access to areas containing sensitive infrastructure. Appropriate physical security should be in place for all offices, rooms and facilities which contain physical infrastructure relevant to the provision of cloud services.

- *Protection against external and environmental threats*. Protection should be provided against things like fire, floods, earthquakes, civil unrest or other potential threats which could disrupt cloud services.

- *Control of personnel working in secure areas.* Such controls should be applied to prevent malicious actions.

- *Equipment security controls.* Should be in place to prevent loss, theft, damage or compromise of assets.

- *Supporting utilities such as electricity supply, gas supply, and water supply should have controls in place.* Required to prevent disruption either by failure of service or by malfunction (e.g. water leakage). This may require multiple routes and multiple utility suppliers.

- *Control security of cabling.* In particular power cabling and telecommunications cabling, to prevent accidental or malicious damage.

- *Proper equipment maintenance.* Should be preformed to ensure that services are not disrupted through foreseeable equipment failures.

- *Control of removal of assets.* Required to avoid theft of valuable and sensitive assets.

- *Secure disposal or re-use of equipment*. Particularly any devices which might contain data such as storage media.

- *Human resources security*. Appropriate controls need to be in place for the staff working at the facilities of a cloud provider, including any temporary or contract staff.

- *Backup, Redundancy and Continuity Plans.* The provider should have appropriate backup of data, redundancy of equipment and continuity plans for handling equipment failure situations.

Effective physical security requires a centralized management system that allows for correlation of inputs from various sources, including property, employees, customers, the general public, and local and regional weather. For more detail on the controls and considerations that apply to each of these items, refer to the ISO 27002 standard.

Step 9: Manage security terms in the cloud SLA

Since cloud computing typically involves two organizations - the service consumer and the service provider, security responsibilities of each party must be made clear. This is typically done by means of a service level agreement (SLA) which applies to the services provided, and the terms of the contract between the consumer and the provider. The SLA should specify security responsibilities and should include aspects such as the reporting of security breaches. SLAs for cloud computing are discussed in more detail in the CSCC document "Practical Guide to Cloud Service Level Agreements, Version 1.0".

One feature of an SLA relating to security is that any requirements that are placed on the cloud provider by the SLA must also pass on to any peer cloud service providers that the provider may use in order to supply any part of their service(s).

It should be explicitly documented in the cloud SLA that providers must notify consumers about the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur. Due to the high financial and reputational costs resulting from a breach, consumers may want the provider to indemnify them if the breach was their fault.

Metrics and standards for measuring performance and effectiveness of information security management should be established prior to subscribing to cloud services and should be specified in the cloud SLA. At a minimum, organizations should understand and document their current metrics and how they will change when operations make use of cloud computing and where a provider may use different (potentially incompatible) metrics. Refer to the following resources for specific information on security metrics:

- ISO 27004:2009[16]
- NIST Special Publication (SP) 800-55 Rev.1, Performance Measurement Guide for Information Security[17]
- CIS Consensus Security Metrics v1.1.0[18]

Measuring and reporting on a provider's compliance with respect to data protection is a tangible metric of the effectiveness of the overall enterprise security plan. A *data compliance report* should be required from the cloud provider and reflects the strength or weakness of controls, services, and mechanisms supported by the provider in all security domains.

The importance of role clarity is increased when discussing security implications. This is also complicated by the cloud computing technical architecture. Each cloud computing model requires distinct responsibilities for the provider and consumer.

In the IaaS model, the onus for securing and reporting upon the infrastructure falls on the provider, but all responsibility for the software stack from the operating system to the application is the responsibility of the consumer.[19] In the PaaS model, the provider is responsible for securing the infrastructure and platform, and the responsibility of the application lies with the consumer. Finally, in the SaaS model, the provider has total responsibility for security. Even in an instance where the provider bears all responsibility, the consumer should validate that the provider has instituted the appropriate measures to ensure a secure environment.

[16] See http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106.

[17] See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[18] See http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110.

[19] The cloud provider is responsible for logging and timely data retrieval and provision to the consumer in an incident response scenario.

Step 10: Understand the security requirements of the exit process

The exit process or termination of the use of a cloud service by a consumer requires careful consideration from a security perspective. The overall need for a well defined and documented exit process is described in the CSCC document "Practical Guide to Cloud Service Level Agreements, Version 1.0".

From a security perspective, it is important that once the consumer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the consumer's data should remain with the provider. The provider must ensure that any copies of the data are wiped clean from the provider's environment, wherever they may have been stored (i.e. including backup locations as well as online data stores). Note that other data held by the provider may need "cleansing" of information relating to the consumer (e.g. logs and audit trails), although some jurisdictions may require retention of records of this type for specified periods by law.

Clearly, there is the opposite problem during the exit process itself - the consumer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the consumer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.

Cloud Security Assessment

The critical questions that cloud consumers should ask themselves and their cloud providers during each step of the security assessment are highlighted in Table 6.

Table 6. Cloud Security Assessment

Security Step	Assessment Questions
1. Ensure effective governance, risk and compliance processes exist	• Does the consumer have governance and compliance processes in place for the use of cloud services? • Does the provider have appropriate governance and notification processes for their services, as required by the consumer? • Is it clear what legal and regulatory controls apply to the provider's services?
2. Audit and ensure proper reporting of operational and business processes	• Is audit information available for the provider services? Does the audit information conform to one of the accepted standards for security audit such as ISO 27001? • Does the provider have mechanisms in place to provide reporting for both normal or exception behavior relating to their services? • Is it clear that the provider's management interfaces (for use by consumers) have adequate security controls in place? • Is there an Incident Reporting and Incident Handling process that meets the needs of the consumer?
3. Manage people, roles and identities	• Do the provider services offer fine grained access control? • Is single sign-on possible with the provider's services? • Can the provider give reports for monitoring user access? • Is it possible to integrate consumer identity management with the

	identity management facilities of the provider?
4. Ensure proper protection of data and information	• Is there a data asset catalog for all data which will be used or stored in the cloud environment? • Is there a description of responsible parties and roles? • Has the handling of all forms of data been considered, in particular unstructured data such as images? • For structured data held in databases within the cloud provider's environment, is there proper separation of data belonging to different consumers in a multi-tenant environment? • Has appropriate confidentiality, integrity and availability been applied to data used or stored in the cloud environment?
5. Enforce privacy policies	• Is PII going to be stored/processed by the cloud services? • Do the provider's services have appropriate controls in place for handling PII? • Are responsibilities for handling PII stated in the SLA? • If there is a security breach, are responsibilities for reporting and resolving the breach clear, including priorities and timescales?
6. Assess the security provisions for cloud applications	• Is it clear whether responsibility for applications running on cloud infrastructure lies with the consumer or with the provider? • Where the responsibility lies with the consumer, does the consumer have governance and policies in place that ensure the appropriate security provisions are applied to each application? • Where the responsibility lies with the provider, does the SLA make the provider's responsibilities clear and require specific security provisions to be applied to each application and all data?
7. Ensure cloud networks and connections are secure	• Is network traffic screened? • Does the provider's network have intrusion detection & prevention in place? • Does the network provide the consumer with logging and notification? • Is there separation of network traffic in a shared multi-tenant provider environment? • Is consumer network access separated from provider network access?
8. Evaluate security controls on physical infrastructure and facilities	• Can the cloud service provider demonstrate appropriate security controls applied to their physical infrastructure and facilities? • Does the service provider have facilities in place to ensure continuity of service in the face of environmental threats or equipment failures? • Does the cloud service provider have necessary security controls on their human resources?
9. Manage security terms in the cloud SLA	• Does the cloud SLA specify security responsibilities of the provider and of the consumer? • Does the SLA require that all security terms must also pass down to any peer cloud service providers used by the provider? • Does the SLA have metrics for measuring performance and effectiveness of security management? • Does the SLA explicitly document procedures for notification and handing of security incidents?
10. Understand the security requirements of the exit process	• Is there a documented exit process as part of the contract/SLA? • Is it clear that all consumer data is deleted from the provider's

	environment at the end of the exit process? - Is consumer data protected against loss or breach during the exit process?

Additional References

Cloud Standards Customer Council (2011). *Practical Guide to Cloud Computing.* http://www.cloud-council.org/10052011.htm
This guide provides a practical reference to help enterprise information technology (IT) and business decision makers adopt cloud computing to solve business challenges.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute.* Gaithersburg: National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
This white paper defines cloud computing, the five essential characteristics, three service models, and four deployment models.

Article 29 Data Protection Working Party. *Opinion 05/2012 on Cloud Computing*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
In this Opinion the Article 29 Working Party analyses all relevant issues for cloud computing service providers operating in the European Economic Area (EEA) and their clients specifying all applicable principles from the EU Data Protection Directive (95/46/EC) and the e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) where relevant.

IBM (2011). Craft a Cloud Service Security Policy
http://www.ibm.com/developerworks/cloud/library/cl-cloudsecurepolicy/
In this article, the author explains how to craft a cloud security policy for managing users, protecting data, and securing virtual machines.

Catteddu, D. & Hogben, G. (November 2009). Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
This white paper provides security guidance for potential and existing users of cloud computing.

Cloud Security Alliance (August 15, 2010). *CSA GRC Stack including CCM v1.1.*
https://cloudsecurityalliance.org/research/initiatives/grc-stack/
This is an integrated suite of four CSA initiatives: CloudAudit, Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire and the CloudTrust Protocol.

Cloud Security Alliance (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing Version 3.0.* http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
This document provides an actionable, practical road map to managers wanting to adopt the cloud paradigm safely and securely.

Daskala, B. & Marinos, L. *EFR* (March, 2010). *Emerging and Future Risks Framework, Introductory Manual*. European Network and Information Security Agency. http://www.enisa.europa.eu/act/rm/files/deliverables/efr-framework-handbook.
This handbook provides the documentation of the EFR Framework which consists of a scenario-based process model developed in order to assess and manage emerging and future risks.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media. http://www.amazon.com/Cloud-Security-Privacy-Enterprise-Perspective/dp/0596802765.
Insight from knowledgeable experts including a former Chief Security Strategist for RSA on how to keep your virtual infrastructure and web applications secure.

Appendix A: Worldwide Privacy Regulations

Region	Regulation
Asia Pacific region, Japan, Australia, New Zealand, and others	• These regions have adopted data protection laws that require the data controller to adopt reasonable technical, physical, and administrative measures in order to protect personal data from loss, misuse, or alteration, based on the Privacy and Security Guidelines of the Organization for Economic Cooperation and Development (OECD)[20], and the Asia Pacific Economic Cooperation's (APEC) Privacy Framework.[21]
Japan	• In Japan, the Personal Information Protection Act[22] requires the private sectors to protect personal information and data securely. In the healthcare industry, profession-specific laws, such as the Medical Practitioners' Law[23], the Law on Public Health Nurses, Midwives and Nurses[24], and the Dentist Law[25], require

[20] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted on 23 September 1980, see http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.

[21] In 2004, the APEC Privacy Framework was endorsed by APEC Ministers for more details see http://www.worldlii.org/int/other/PrivLRes/2005/4.html.

[22] Act on the Protection of Personal Information (Act No. 57 of 2003) – see http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf for details.

[23] Medical Practitioners' Law (Law No. 201 of July 30, 1948) - http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[24] Law on Public Health Nurses, Midwives and Nurses (Law No. 203 of July 30, 1948) - http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[25] Dentists Law (Law No. 202 of July 30, 1948) - see http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf for details.

	registered health professionals to protect the confidentiality of patient information.
Europe, Africa, Middle East	• The European Economic Area (EEA) 30 Member States have enacted data protection laws that follow the principles set forth in the 1995 European Union (EU) Data Protection Directive and the 2002 ePrivacy Directive (as amended in 2009). These laws include a security component, and the obligation to provide adequate security must be passed down to subcontractors. • Other countries that have close ties with the EEA, such as Morocco and Tunisia in Africa, Israel and Dubai in the Middle East have also adopted similar laws that follow the same principles.
Americas	• North, Central, and South American countries are also adopting data protection laws at a rapid pace. Each of these laws includes a security requirement that places on the data custodian the burden of ensuring the protection and security of personal data wherever the data are located, and especially when transferring to a third party. • In addition to the data protection laws of Canada[26] and Argentina[27] which have been in existence for several years, Colombia, Mexico, Uruguay, and Peru have recently passed data protection laws that are inspired mainly from the European model and may include references to the APEC Privacy Framework as well.
United States	• There is no single privacy law in the Unites States. A range of government agency and industry sector laws impose privacy obligations in specific circumstances. There are numerous gaps and overlaps in coverage. • Current industry sector privacy laws include: o The Federal Trade Commission Act [28] which prohibits unfair or deceptive practices - this requirement has been applied to company privacy policies in several prominent cases. o The Electronic Communications Privacy Act of 1986[29] which protects consumers against interception of their electronic communication (with numerous exceptions).

[26] Personal Information Protection and Electronic Documents Act (PIPEDA) - see http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ for details.

[27] Law for the Protection of Personal Data (LPDP), Law No. 25.326 - see http://www.protecciondedatos.com.ar/law25326.htm for details.

[28] See http://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I for details.

[29] See http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc18.wais&start=3919965&SIZE=21304&TYPE=TEXT for details.

	o The Health Insurance Portability and Accountability Act (HIPAA)[30] which contains privacy rules applying to certain categories of health and medical research data. o The Fair Credit Reporting Act[31] includes privacy rules for credit reporting and consumer reports. o The Gramm-Leach-Bliley Act (GLBA)[32] govern the collection, disclosure, and protection of consumers' nonpublic personal information for financial institutions o These laws hold organizations responsible for the acts of their subcontractors. For example, the security and privacy rules under GLBA or HIPAA require that organizations compel their subcontractors, in written contracts, to use reasonable security measures and comply with data privacy provisions. • Government agencies, such as the Federal Trade Commission (FTC) or the State Attorneys General have consistently held organizations liable for the activities of their subcontractors.
Worldwide	• The Payment Card Industry (PCI) Data Security Standards (DSS)[33], which apply to credit card data anywhere in the world, including data processed by subcontractors has similar requirements.

Appendix B: Acronyms & Abbreviations

Abbreviation	Meaning
AICPA	American Institute of Certified Public Accountants
CSA	Cloud Security Alliance
CoBIT	Control Objectives for Information and Related Technologies A framework created by ISACA to support governance of IT by defining and aligning business goals with IT goals and IT processes

[30] The final HIPPA regulation and modifications can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

[31] See http://www.ftc.gov/os/statutes/fcradoc.pdf for details.

[32] See http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html for details.

[33] PCI DSS provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. See https://www.pcisecuritystandards.org/security_standards/ for details.

CSCC	Cloud Standards Customer Council
ENISA	European Network and Information Security Agency
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
PaaS	Platform as a Service
PCI	Payment Card Industry (Security Standards Council)
PII	Personally identifiable information
SaaS	Software as a Service
SLA	Service Level Agreement
SSAE	Statement on Standards for Attestation Engagements