Cloud
Standards
Customer
Council

Security for Cloud Computing
Ten Steps to Ensure Success
Version 2.0

March, 2015

Contents

Acknowledgements

The *Security for Cloud Computing: 10 Steps to Ensure Success, Version 2.0* 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 major contributors to this effort are: Claude Baudoin (cébé IT & Knowledge Management), Eric Cohen (PricewaterhouseCoopers), Chris Dotson (IBM), Mike Edwards (IBM), Jonathan Gershater (Trend Micro), David Harris (Boeing), Sreekanth Iyer (IBM), Ryan Kean (The Kroger Co.), Yves Le Roux (CA Technologies), Shamun Mahmud (GRC Research Associates), John Meegan (IBM), Barry Pardee (Tailwind Associates), Steven Pogue (IBM), Matt Rutkowski (IBM).

Revisions

Much has changed in the realm of cloud computing security since the original *Security for Cloud Computing* whitepaper was published in August, 2012. Version 2.0 of the document includes the following updates:

- Additional risks have been added to the *Cloud Security Landscape* section.
- All ten steps in the *Cloud Security Guidance* section have been updated to reflect current best practices.
- New appendix on the differences between security and privacy has been added.
- Appendix on worldwide privacy regulations has been updated.
- References to cloud security standards have been updated.
- References have been added to several CSCC whitepapers that have been published.

Introduction

Failure to ensure appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing.

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze 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 from different cloud providers in key areas.

When considering a move to cloud computing, customers 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 service categories: 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 migrating 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 customers with an efficient method of assessing the security capabilities of cloud providers and assessing their individual risk. A questionnaire for customers to conduct their own assessment across each of the critical security domains is provided.

A related document, the *Practical Guide to Cloud Service Agreements* [1], provides additional guidance on evaluating security criteria from prospective cloud providers. The guide titled *Cloud Security Standards: What to Expect & Negotiate* [2] highlights the security standards and certifications that are currently available in the market as well as the cloud specific security standards that are currently being developed.

Cloud Security Landscape

While security and privacy concerns[1] are similar across cloud services and traditional non-cloud services, those concerns are amplified by the existence of 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 components that were previously under the customer's direct control.

Despite this inherent loss of control, the cloud service customer still needs to take responsibility for its 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 customer achieves this by ensuring that the contract with the provider and its associated cloud service agreement has appropriate provisions for security and privacy. In particular, the agreement must help maintain legal protections for the privacy of data stored and processed on the provider's systems. The customer must also ensure appropriate integration of cloud computing services with their own systems for managing security and privacy.

There are a number of security risks associated with cloud computing that must be adequately addressed[2]:

- **Loss of governance.** In a public cloud deployment, customers cede control to the cloud provider over a number of issues that may affect security. Yet cloud service agreements may not offer a commitment to resolve such issues on the part of the cloud provider, thus leaving gaps in security defenses.
- **Responsibility ambiguity**. Responsibility over aspects of security may be split between the provider and the customer, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly. This split is likely to vary depending on the cloud computing model used (e.g., IaaS vs. SaaS).
- **Authentication and Authorization.** The fact that sensitive cloud resources are accessed from anywhere on the Internet heightens the need to establish with certainty the identity of a user -- especially if users now include employees, contractors, partners and customers. Strong authentication and authorization becomes a critical concern.
- **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 tenants (e.g. so-called guest-hopping attacks).
- **Compliance and legal risks.** The cloud customer's investment in achieving certification (e.g., to demonstrate compliance with industry standards or regulatory requirements) may be lost if the cloud provider cannot provide evidence of their own compliance with the relevant requirements, or does not permit audits by the cloud customer. The customer must check that the cloud provider has appropriate certifications in place.

[1] Refer to Appendix A for an explanation of the distinctions between security and privacy.

[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 may be delegated to the cloud provider, but these incidents impact the customer. Notification rules need to be negotiated in the cloud service agreement so that customers are not caught unaware or informed with an unacceptable delay.
- **Management interface vulnerability.** Interfaces to manage public cloud resources (such as self-provisioning) are usually accessible through the Internet. Since they allow access to larger sets of resources than traditional hosting providers, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
- **Application Protection.** Traditionally, applications have been protected with defense-in-depth security solutions based on a clear demarcation of physical and virtual resources, and on trusted zones. With the delegation of infrastructure security responsibility to the cloud provider, organizations need to rethink perimeter security at the network level, applying more controls at the user, application and data level. The same level of user access control and protection must be applied to workloads deployed in cloud services as to those running in traditional data centers. This requires creating and managing workload-centric policies as well as implementing centralized management across distributed workload instances.
- **Data protection.** Here, the major concerns are exposure or release of sensitive data as well as the loss or unavailability of data. It may be difficult for the cloud service customer (in the role of data controller) to effectively check the data handling practices of the cloud provider. This problem is exacerbated in cases of multiple transfers of data, (e.g., between federated cloud services or where a cloud provider uses subcontractors).
- **Malicious behavior of insiders**. Damage caused by the malicious actions of people working within an organization can be substantial, given the access and authorizations they enjoy. This is compounded in the cloud computing environment since such activity might occur within either or both the customer organization and the provider organization.
- **Business failure of the provider**. Such failures could render data and applications essential to the customer's business unavailable over an extended period.
- **Service unavailability**. This could be caused by hardware, software or communication network failures.
- **Vendor lock-in**. Dependency on proprietary services of a particular cloud service provider could lead to the customer being tied to that provider. The lack of portability of applications and data across providers poses a risk of data and service unavailability in case of a change in providers; therefore it is an important if sometimes overlooked aspect of security. Lack of interoperability of interfaces associated with cloud services similarly ties the customer to a particular provider and can make it difficult to switch to another provider.
- **Insecure or incomplete data deletion.** The termination of a contract with a provider may not result in deletion of the customer’s data. Backup copies of data usually exist, and may be mixed on the same media with other customers’ data, making it impossible to selectively erase. The very advantage of multi-tenancy (the sharing of hardware resources) thus represents a higher risk to the customer than dedicated hardware.
- **Visibility and Audit.** Some enterprise users are creating a “shadow IT” by procuring cloud services to build IT solutions without explicit organizational approval. Key challenges for the security team are to know about all uses of cloud services within the organization (what resources are being used, for what purpose, to what extent, and by whom), understand what

laws, regulations and policies may apply to such uses, and regularly assess the security aspects of such uses.

Cloud computing does not only create new security risks: it also provides opportunities to provision improved security services that are better than those many organizations implement on their own. Cloud service providers could offer advanced security and privacy facilities that leverage their scale and their skills at automating infrastructure management tasks. This is potentially a boon to customers who have little skilled security personnel.

Cloud Security Guidance

As customers transition their applications and data to the cloud, it is critical for them to maintain, or preferably surpass, the level of security they had in their traditional IT environment.

This section provides a prescriptive series of steps for cloud customers to evaluate and manage the security of their use of cloud services, with the goal of mitigating risk and delivering an appropriate level of support. The following steps will be discussed in detail below:

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 service agreement
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 portability 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 analysis of 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 constitute the enterprise security governance, risk management, and compliance model.

Security controls for cloud services are similar to those in traditional IT environments. However, the risks may be different because of:

- the division of responsibilities between the cloud service customer and the cloud service provider,
- the fact that technical design and operational control of the cloud service is in the hands of the cloud service provider,
- the interface(s) that exist between the cloud service customer and the cloud service

As part of the transition to cloud computing, it is critical that cloud service customers understand the risks associated with using cloud services and their own level of risk tolerance, and then focus on mitigating the risks that the organization cannot afford to discount.

The primary means cloud service customers have to ensure their applications and data hosted in cloud services are secured in accordance with their security and compliance policies is to verify that the master service agreement between the customer and the provider, along with associated documents such as the service level agreement (SLA), contain all their requirements. It is vital for the customer to understand all the terms related to security and to ensure that those terms meet their needs. If a suitable master service agreement and SLA are not available, then it is inadvisable for an organization to proceed with the use of those cloud services. Refer to the *Practical Guide to Cloud Service Agreements* [1] for details.

The category of cloud service offered by the provider (IaaS, PaaS or SaaS) has a significant impact on the split of responsibilities between the customer 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 customer is typically responsible for the operating system and the entire software stack necessary to run applications, and is also responsible for the customer data placed into the cloud computing environment. As a result, most of the responsibility for securing the applications and the customer data falls onto the customer. In contrast, for software-as-a-service, the infrastructure, software and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the SLA.

From a general governance perspective, cloud service providers should notify cloud service customers 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 changes to correct the root causes of the breach to ensure that it does not recur. Due to the high financial and reputation costs resulting from a breach, customers may want the provider to indemnify them if the breach was the provider's fault.

A fundamental design premise in cloud computing is that, as a customer, your data may be stored in, processed on and transmitted to any of the servers or devices the cloud service provider operates. In some instances, servers hosting customer data may be located in multiple data centers 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 the customer data actually resides, which regulators have jurisdiction and what regulations apply. This matters since some regulations restrict the allowable locations for data.[3]

The jurisdictional issue directly influences the protection of personally identifiable information (PII) and legal and jurisdictional authority access to this data.[4] There is divergence across countries in the laws on investigation and enforcement, including access to encrypted data and investigation of extraterritorial offences. A court can only hear a matter if it has jurisdiction over the parties and the subject matter of the action, while governmental agencies can only exercise their powers within their authorized jurisdictions.

Before migrating applications or data to a cloud computing environment, it is important to understand precisely the specific laws or regulations that apply and the relevant duties or obligations imposed on both the customer and the provider (e.g. data retention, data protection, interoperability, medical file management, disclosure to authorities). This allows customers to identify the legal issues and the related legal risks, and consequently understand the impact these will have on the applications or data 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 prospective customers more confidence in that provider, and the ability to show "due diligence" in provider selection. Which certification is most appropriate depends to some extent on the category of the cloud service (IaaS, PaaS, SaaS) and on the customer's regional and industry requirements.

The most widely recognized international standard for information security compliance is ISO/IEC 27001 [3] which includes national variants and well developed certification regimes. ISO has new standards, ISO/IEC 27017 [4] "Code of practice for information security controls based on ISO/IEC 27002 for cloud services" (targeted for completion in late 2015) and ISO/IEC 27018 [5] "Code of practice for protection

[3] There is an increasing prevalence of cloud services that do provide customers with the ability to specify the location(s) for data storage and data processing or to limit which locations can be used by the provider.

[4] 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://cloudscorecard.bsa.org/2013/ for details.

of personally identifiable information (PII) in public clouds acting as PII processors" (completed in 2014 and available now), which specifically address cloud service security and privacy considerations and which 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 respectively provide the SSAE 16 [6] and CoBIT 5 [7] frameworks. Other organizations provide frameworks for specific services or industries such as the Payment Card Industry (PCI) Data Security Standard (DSS) [8].

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), a certification of cloud security knowledge for personnel, Certificate of Cloud Security Knowledge (CCSK), and a registry to publish the self-evaluation results (STARS) [9].

Step 2: Audit operational & business processes

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

As a baseline, customers should expect to see a report of the cloud provider's operations by independent auditors. The level of 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 audit events, log and report information relevant to a customer's specific data or applications.

Security 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 service customers 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 and how such facilities are secured.

Understanding the internal control environment of a cloud service provider

Using cloud services creates the need for appropriate auditing of the activities of persons employed by the provider, the customer, or the customer’s partners to ensure that the security controls meet the requirements of the customer. Customers should expect to see audit information relating to any cloud service provider they plan to use. There are several standards that can be used as the basis for auditing a provider, such as the ISO 27000 series. These standards provide the basis for assuring customers that proper controls are in place within the provider organization.

Key controls for cloud services include:

- Ensuring isolation of customer applications and customer data in shared, multi-tenant environments,
- Providing protection of customer assets from unauthorized access by the provider's staff.

Auditors may be employed by the customer or by the provider - but the key element is that they should be *independent*. Auditors require access to the policies and procedures of a cloud service provider which relate to security controls. Auditors also require access to logs and records that show whether the policies and procedures are being followed correctly -- and in some cases the auditors may require specific testing 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 customers to have appropriate access to cloud provider events, logs and audit trails that prove enforcement of provider security controls. Auditors need to assure cloud customers that all the necessary information is being logged and stored appropriately by the cloud service provider, 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 customer.

For complete insight into security controls, as they relate to the customer's applications and data, mechanisms for the routine flow of audit information from the provider to the customer are recommended. This flow may include secure logs and reports sent on 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.[5]

Ideally, there should be automated, standards-based, access (through APIs or Web services) to all of these audit facilities, to ensure timely availability of required data and to remove the costs associated with human processing of requests for information.

[5] The DMTF Cloud Audit Data Federation (CADF) Workgroup [10] has developed an audit event data model and a compatible interaction model that describes interactions between IT resources suitable for cloud deployment models.

Assurance of the facilities for management and control of cloud services

In addition to the cloud services themselves, providers generally provide customers with self-service facilities to manage and monitor the usage of their cloud services and associated assets. 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 management 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.

Auditing is essential

The security audit of cloud service providers is an essential aspect of the security considerations for cloud service customers, typically as part of a certification process. Audits should be carried out by appropriately skilled staff typically belonging to an independent auditing organization. Security audits should be carried out on the basis of one of the established standards for security controls. Customers 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 service provider's reporting and logging facilities with the customer's systems, so that appropriate operational and business data flows on a timely basis to enable customers to manage their use of cloud services.

Step 3: Manage people, roles and identities

The use of a cloud solution means that there will be employees of the provider with the ability to access the customer’s data and applications, as well as employees of the customer who need to perform operations on the provider’s systems.

Customers must ensure that the cloud provider has processes and functionality that govern who has access to the customer's data and applications. Conversely, cloud providers must allow the customer 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 customer, in accordance with its security policies, may have an employee whose role allows generation of purchase requests, 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 and Access Management (IdAM) functionality must support simple resource access and robust customer application and service workflows. Any user access to the provider's management platform, regardless of role or entitlement, should be monitored and logged to provide auditing of all access to customer data and applications.

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

Table 1: Cloud Service Provider Support for People, Roles and Identities

Provider Capabilities	Customer Considerations and Questions
Federated Identity Management (FIM), External Identity Providers (EIP)	Enterprises that are cloud service customers may already have an existing IdAM system. If so, it is highly recommended that they leverage it for cloud services and do not replicate user identities in a separate system for each cloud service. This is not only more efficient, it is also more secure because some functions (such as removing users from the cloud service when users leave the organization) happen automatically. Question to cloud provider: Can I integrate my current IdAM system with your cloud services?
Identity Provisioning and Delegation	Customer organizations need to administer their own users; the cloud provider should support delegated administration. Question to cloud provider: If I cannot use my current IdAM system, what 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	Customer 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 may require single-sign-on, sign-off, and authorization across these applications (using standards such as SAML 2.0 [11], WS-Federation [12] and OAuth [13]). 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	Customers 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, customers may require that their provider support strong, multi-factor, mutual and/or even biometric authentication. Question to cloud provider: What forms of strong authentication does your platform support?
Role, Entitlement and Policy	Cloud customers need to be able to describe and enforce their security

Management	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 service providers should have formalized processes for managing their own employee access to any hardware or software used to store, transmit or execute customer data and applications. Providers should be able to disclose and demonstrate these processes to the customer.

Step 4: Ensure proper protection of data and information

Data is 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 brings 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 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. In the cloud, “data assets" may also include application programs or machine images, which can present the same risks 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 services, with some additional cloud-specific considerations as described in the ISO 27017 standard (currently under development, targeted for publication at the end of 2015). Security controls described in ISO 27002 highlight the general features that need to be addressed, to which specific techniques can then be applied.

The category of the cloud service is very likely to affect who is responsible for handling particular security controls.

- For IaaS, more responsibility is likely to be with the customer (e.g., for encrypting data stored on a cloud storage device)
- For SaaS, more responsibility is likely to be with the provider, since neither the stored data nor the application code is directly visible or controllable by the customer.
- PaaS cloud services present unique challenges in that responsibility is likely shared between the customer and provider. It is important to understand how each service being utilized within the PaaS environment handles data security, including encryption as well as log file handling and administrative access. In addition, the customer needs to know what obligations it retains and

what are the available features and configuration of the PaaS service that can facilitate data security.

Table 2 highlights the key steps customers 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	● Identify all data assets, classifying them 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 customer organization and the cloud service provider organization.
Consider all forms of data	● Organizations are increasing the amount of unstructured data held in IT systems, which can include items such as images of scanned documents, pictures and multimedia files. ● Unstructured data can be sensitive and require specific treatment - for example redaction or masking of personal information such as signatures, addresses, or 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 customers' 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 customer. 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, particularly when the data is stored within a cloud provider's infrastructure. The ISO/IEC 27018 standard 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 for load

	balancing or cost reduction.
Apply confidentiality, integrity and availability procedures	● 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 customer system. o An extra consideration when using cloud services 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 customer 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") with appropriate authorization being required before any user is permitted to access sensitive data. In addition, an audit trail of accesses should be available for review. ● 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 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 customer. 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 customer is concerned.

Step 5: Enforce privacy policies

Privacy and data protection is gaining in importance across the globe, often involving laws and regulations relating to the acquisition, storage and use of personally identifiable information (PII). The concern for privacy is heightened by newsworthy cases in which major companies and financial institutions suffered thefts of critical PII such as credit card numbers. Appendix B provides an overview of the worldwide data protection regulations that currently exist around the world.

It is important to note that while security and privacy are related, they are also distinct. A key distinction is that security is primarily concerned with defending against attacks, not all of which are aimed at stealing data, while privacy is specifically related to personal data held by an organization, which may be endangered by negligence or software bugs, not necessarily by malevolent persons.

Typically, data protection requires imposing limitations on the use and accessibility of PII, based on policies that are written by non-IT personnel, especially the Legal and Risk Management departments, which are consistent with applicable regulations and laws, and are approved at the highest levels of the organization. Enforcement of such limitations implies associated requirements to tag the data appropriately, store it securely and to permit access only by authorized users. This requires appropriate controls, which can be more challenging when the data is stored within a cloud service provider's infrastructure. The ISO/IEC 27018 standard addresses the controls required for the protection of PII.

When data is placed in or transferred to a cloud computing environment, the responsibility for protecting and securing the data typically remains with the customer (the *data controller* in EU terminology[6]), even if in some circumstances this responsibility may be shared with others. When an organization relies on a 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 and expectations of the parties, allocates between them the many responsibilities that are attached to the data at stake, and specifies under which circumstances the cloud customer indemnifies the provider for any losses or damages sustained.

It is critical that privacy requirements be adequately addressed in the cloud service agreement. If not, the cloud service customer 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 customer wishes to place health information subject to HIPAA [14] into a cloud service, the customer must find a cloud service provider that will sign a HIPAA business associate agreement.

Certain technologies may be used to reduce the risk of disclosing PII to unauthorized parties, while allowing the customer to gain the benefits of a cloud solution. For example, data may be anonymized before being stored in the cloud service, while the small amount of critical information required to match the anonymous records with the real people they represent is held in a separate database kept on premises.

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. Thus customers have an ongoing obligation to monitor their provider's compliance with customer policies. This includes an audit program covering all aspects of the privacy policies including methods of ensuring that corrective actions will take place.

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

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 essential to ensure the applications are enabling the business rather than introducing additional risk.

Application security poses specific challenges to both the cloud service provider and customer. Organizations must apply the same diligence to application security as they do to physical and infrastructure security. If an application is compromised, it can create financial liability and reputation damage to both the provider and the customer, especially if the ultimate end users of the application are customers of the customer rather than its 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 the others outlined in this white paper (facilities, network, data, etc.).

Table 3: Deployment Model Impact on Application Security

Deployment Type	Application Security Policy Considerations
Infrastructure as a Service	● The customer 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, including the application of all appropriate security patches. ● The application security policy should closely mimic the policy of applications hosted internally by the customer. ● The customer should focus on network, physical environment, auditing, authorization, and authentication considerations as outlined in this document. ● Appropriate data encryption standards should be applied in the handling of data and to user interaction (e.g., secure browsing) by the application. ● System assurance principles, and development and testing methods that minimize the risk of introducing vulnerabilities in the code, should be applied even more rigorously than for an on premises application, since the application will reside outside of the customer's security perimeter. ● If hardware-based trusted computing security measures such as Intel TXT are available, consider using them to block root-kits and other hard-to-detect malware.
Platform as a Service	● The customer 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 customer should focus on audit, authorization, and authentication considerations as outlined in this document. ● Appropriate data encryption and key management standards should be applied. ● The customer needs to define how sensitive data, as part of their data classification, is being handled in general and by configuration options provided by utilized PaaS services. ● In a PaaS model, the customer 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 customer must ensure that these terms meet their confidentiality, integrity and availability requirements. ● It is Important to understand the provider's patching schedule, controls against malware, and release cycle. ● Scaling policies help deal with fluctuating loads placed on the application. Scaling policies are based on resources, users and data requests. ● Typically, the customer 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 customer should ensure that their configuration changes augment; not inhibit the provider's security model. ● The customer should have knowledge of how their data is protected against administrative access by the provider. In a SaaS model, the customer will likely not be aware of the location and format of the data storage. ● The customer must understand the data encryption standards which are applied to data at rest and in motion. ● The customer needs to be aware of how sensitive data, as defined in their data classification, is being handled in general and by configuration options.

It should be noted that there is a cost to the customer 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 with the potential liability and loss of reputation from an application security breach.

When developing and deploying applications in a cloud environment it is critical that customers 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 customers developing software use a structured methodology to engineer security into their cloud applications from the ground up.[7]

Step 7: Ensure cloud networks and connections are secure

A cloud service provider must allow legitimate network traffic and block 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 customers plan to send and receive. Nevertheless, customers 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 potentially dangerous person.

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

[7] See the Open Web Application Security Project (OWASP) at https://www.owasp.org/ for more information.

Table 4: External Network Requirements

Provider Responsibility	Description / Guidance
Traffic screening	● Certain traffic is almost never legitimate – for example, traffic to known malware ports. If the cloud provider does not automatically screen traffic, the cloud customer should do so. ● Screening is generally performed by firewall devices or software. Some considerations: o Does the provider publish a standard perimeter block list that aligns with the terms of service for the offering? If so, customers should request a copy of the block list; a reasonable block list can provide a customer with both assurance of a 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 control 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.
Denial-of-service protection	● Is the provider able to withstand and adapt to high-traffic attacks, such as Distributed Denial-of-Service attacks? DDOS attacks are commonly used for extortion purposes, 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. ● If the solution deployed in the cloud is accessed by the customer's customers, a DDOS attack against the cloud provider may result in loss of business for the customer.
Intrusion detection and prevention	● Some traffic may initially look legitimate, but deeper inspection indicates that it is carrying malicious payload such as spam, viruses, or known attacks. The customer must understand whether the provider will block or notify the customer about this traffic. ● Intrusion detection and/or prevention systems (IDS/IPS) may be virtual or real devices. While a firewall usually only makes decisions based on source/destination, ports, and existing connections, an IDS/IPS looks at 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) will often perform similar functions for certain types of network traffic. ● 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. If the cloud provider provides IDS/IPS services, is there 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 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	● For assurance purposes and troubleshooting, it's important that customers have some

notification	visibility into network health. ● Incident reporting and incident handling procedures must be clear and the customer should look for visibility into the handling process. Note that if any Personally Identifiable Information is stored in the cloud computing environment, there may be legal requirements associated with logging data (limiting what can be stored in logs, for example). ● 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 customers 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 customer may want to perform forensic analysis, and the network logs can be very helpful. o What are the notification policies? As a cloud customer, you should be notified in timely manner if your machines are attacked or if they are compromised and are attacking someone else. o Are historical statistics available on the number of attacks detected and blocked? These statistics can help a customer understand how effective the provider's detection and blocking capabilities actually are.

A cloud environment 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 assume 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. To extend the hotel analogy, the room locks and walls must also be sufficient to protect the customers.

The primary categories of internal network attacks that customers 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)

Customers must evaluate the cloud service provider's internal network controls with respect to their requirements. Each customer’s requirements will be different, but it is recommended that customers 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
Provide tools to	Cloud providers are responsible for providing ways for customers to separate themselves from

protect clients from one another	other customers and from the Internet. Most cloud service providers will provide one or more of the following technologies for this purpose: Virtual LANs, or VLANs, are a technology that virtually places systems on separate Ethernet switches. 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.” Most VLAN technologies allow all systems on the same VLAN to talk with no restrictions, and only prevent communication between systems on different VLANs. Advanced VLAN and firewall technologies may be able to prevent communications on a more granular level, from system to system. Many cloud providers offer private VLANs for customers that no other customers should be able to access. These VLANs may be implemented on physical switches, hypervisors, or a combination of both. It is recommended that customers verify that the provider's VLAN controls address the known VLAN hopping attacks. 1. Virtual Private Networks (VPNs, and also sometimes referred to simply as “tunnels”) can be used to connect a customer's dedicated cloud VLAN back to the customer'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 customer'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). VPNs offer another layer of security, and may sometimes be the only layer of security for protocols without built in security (such as FTP). It is recommended that customers decide whether VPNs are required to protect the data being transmitted, and if so ensure that the cloud provider supports the required operating mode (client-to-site or site-to-site) and implementation. 2. Firewalls block traffic on the network. One typical implementation is an “infrastructure” firewall, which is a separate system that sits between VLANs and blocks traffic flowing through the firewall. Other common implementation is a “host-based firewall”, which only controls traffic coming in and out of the instance. Both implementations can be used simultaneously. Host-based firewalls can allow for greater control of traffic between individual systems, but can be more difficult to manage on larger scales. If using a cloud provider's images, customers should ensure that the images contain proper software firewall capabilities and that the rules are simple to deploy and modify. Per-instance firewalls are particularly important when sharing a network segment with other customers. 3. Hypervisor based filters, such as *ebtables* on Linux, are functionally similar to VLANs and firewalls 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 customer ask what protections are in place to prevent another customer's instance from masquerading as one of your instances.
Protect the provider's network	● 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 customers from the control network. ● Customers 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 customers should ask what types of internal network security incidents have been reported and if there are any published statistics or metrics. ● Customers should also ask for the provider's processes for alerting customers about both successful and unsuccessful internal network attacks.

Step 8: Evaluate security controls on physical infrastructure and facilities

The security of an IT system also depends on the security of the physical infrastructure and facilities. In the case of cloud computing, this extends to the infrastructure and facilities of the cloud service provider. The customer must 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. The security controls include:

- *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 that contain physical infrastructure relevant to the provision of cloud services.

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

- *Control of personnel working in secure areas.* Controls should be applied to prevent malicious actions by any personnel who have access to secure areas.

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

- *Supporting utilities such as electricity supply, gas supply, telecommunications, and water supply should have controls in place.* Controls are required to prevent disruption to cloud services either by failure of a utility supply or by malfunction (e.g. water leakage). This may require the use of multiple routes and multiple utility suppliers.

- *Control security of cabling.* In particular, controls are needed to protect power cabling and telecommunications cabling, to prevent accidental or malicious damage.
- *Proper equipment maintenance.* Controls should be in place to perform necessary preventive maintenance of all equipment to ensure that services are not disrupted through foreseeable equipment failures.
- *Control of removal of assets.* Controls are required on the removal of assets to avoid theft of valuable and sensitive assets.
- *Secure disposal or re-use of equipment*. Controls are required for the disposal of any equipment and 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 service agreement

Since cloud computing typically involves two organizations - the cloud service customer and the cloud service provider, security responsibilities of each party must be made clear. This is typically done by means of a service agreement which applies to the services provided, and the terms of the contract between the customer and the provider. The service agreement should specify security responsibilities and should include aspects such as the reporting of security breaches. Service agreements for cloud computing are discussed in more detail in the CSCC document *Practical Guide to Cloud Service Agreements*. [1]

One feature of a service agreement relating to security is that any requirements that are placed on the cloud provider 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 service agreement that providers must notify customers in a timely manner of 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 and ensure that it does not recur.

Due to the high financial and reputation costs resulting from a breach, customers may want the provider to compensate them if the breach was their fault. An indemnification clause in the contract should not protect the provider from liability in the case of negligence.

Metrics and standards for measuring performance and effectiveness of information security management should be established in advance in the cloud service agreement. At a minimum, customer 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 [15]
- ISO 19086
- NIST Special Publication 800-55 Rev.1, Performance Measurement Guide for Information Security [16]
- CIS Consensus Security Metrics v1.1.0 [17]

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. Certification to a suitable standard like ISO/IEC 27018 is preferable. Otherwise, a *data compliance report* should be required from the cloud provider, reflecting the strength or weakness of controls, services, and mechanisms supported by the provider in all security domains. Alternatively, the provider should obtain an independent certification of the cloud service against one of the data protection standards.

The importance of role clarity is increased when discussing security implications. This is also complicated by the cloud computing technical architecture. Each cloud service category has distinct responsibilities for the provider and customer.

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 customer.[8] In the PaaS model, the provider is responsible for securing the infrastructure and platform, and the responsibility of the application lies with the customer. Finally, in the SaaS model, the provider has responsibility for most aspects of security. Even in an instance where the provider bears all

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

responsibility, the customer should validate that the provider has instituted the appropriate measures to ensure a secure environment.

Step 10: Understand the security requirements of the exit process

The overall need for a well-defined and documented exit process is described in the CSCC document *Practical Guide to Cloud Service Agreements*. [1]

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

Clearly, there is the opposite problem during the exit process itself - the customer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the customer 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 customers 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	● What information security and privacy standards or regulations apply to the cloud customer's domain? ● Does the customer 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, consistent with the customer's requirements? ● Is it clear what legal and regulatory controls apply to the provider's services? ● What do the Master Services Agreement and Service Level Agreement say about the split of security responsibilities between provider and customer? ● Is there a risk related to data location?
2. Audit and ensure proper reporting of operational and business processes	● Is a report by an independent audit agency available, for covering the provider's cloud services? Does the audit information conform to one of the accepted standards for security audit such as ISO 27001/27002? ● Does the provider have mechanisms to report to the customers both routine and exceptional behavior related to its services? Are all appropriate events and actions that have security implications logged? ● Do the security controls encompass not only the cloud services themselves, but also the management interfaces offered to customers?

	● Is there an Incident Reporting and Incident Handling process that meets the needs of the customer?
3. Manage people, roles and identities	● Do the provider services offer fine grained access control? ● Is multi-factor authentication supported for provider services? ● Can the provider give reports for monitoring user access? ● Is it possible to integrate or federate customer identity management systems with the identity management facilities of the provider?
4. Ensure proper protection of data and information	● Is there a catalog of all data assets that 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 in a multi-tenant cloud environment, is there proper separation of data belonging to different customers? ● Have appropriate confidentiality, integrity and availability measures been applied to data used or stored in the cloud?
5. Enforce privacy policies	● Is PII going to be stored/processed by the cloud services? ● What data protection laws and regulations apply, given the industry and the locations in which the customer operates or the locations where the provider stores the data? ● Do the provider's services have appropriate controls in place for handling PII? ● Are responsibilities for handling PII stated in the cloud service agreement? ● Are there appropriate data residency restrictions in the Cloud Service Agreement? ● If there is a data breach, are responsibilities for reporting and resolving the breach clear, including priorities and timescales?
6. Assess the security provisions for cloud applications	● Based on the cloud model used, is it clear who has responsibility for the security of the applications (customer or provider)? ● If it is the customer, does he have policies and methodologies in place to ensure the appropriate security controls for each application? ● If it is the provider, does the cloud service agreement make its responsibilities clear and require specific security controls to be applied to the application? ● In either case, does the application make use of appropriate encryption techniques to protect the data and the user's transactions?
7. Ensure cloud networks and connections are secure	● Is network traffic screening possible? ● What ability does the provider have to deal with denial of service attacks? ● Does the provider's network have intrusion detection & prevention in place? ● Does the network provide the customer with logging and notification? ● Is separation of network traffic possible in a shared multi-tenant provider environment? ● Is customer network access separated from provider network access?
8. Evaluate security controls on the 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 service agreement	● Does the cloud service agreement specify security responsibilities of the provider and of the customer? ● Does the service agreement require that all security terms must also pass down to any peer cloud service providers used by the provider? ● Does the service agreement have metrics for measuring performance and effectiveness of security management?

	● Does the service agreement explicitly document procedures for notification and handling of security incidents?
10. Understand the security requirements of the exit process	● Is there a documented exit process as part of the cloud service agreement? ● Is it clear that all cloud service customer data is deleted from the provider's environment at the end of the exit process? ● Is cloud service customer data protected against loss or breach during the exit process?

Works Cited

[1] Cloud Standards Customer Council. *Practical Guide to Cloud Service Agreements*.
http://cloud-council.org/resource-hub.htm#cscc-practical-guide-SLAs

[2] Cloud Standards Customer Council. *Cloud Security Standards: What to Expect & Negotiate*.
http://cloud-council.org/resource-hub.htm#cloud-security-standards-what-to-expect-what-to-negotiate

[3] ISO/IEC 27001
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[4] ISO/IEC 27017
http://www.iso27001security.com/html/27017.html

[5] ISO/IEC 27018
http://www.iso27001security.com/html/27018.html

[6] SSAE 16
http://ssae16.com/SSAE16_overview.html

[7] COBIT
http://www.isaca.org/COBIT/Pages/default.aspx

[8] Payment Card Industry (PCI) Data Security Standard (DSS)
https://www.pcisecuritystandards.org/security_standards/index.php

[9] Cloud Security Alliance
https://cloudsecurityalliance.org

[10] DMTF Cloud Audit Data Federation (CADF)
http://www.dmtf.org/standards/cadf

[11] SAML 2.0
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[12] WS-Federation
https://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed

[13] OAuth
http://oauth.net

[14] HIPPA
http://www.hhs.gov/ocr/privacy/

[15] ISO 27004:2009
http://www.iso27001security.com/html/27004.html

[16] NIST Special Publication 800-55 Rev.1, Performance Measurement Guide for Information Security
http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

[17] CIS Consensus Security Metrics v1.1.0
https://benchmarks.cisecurity.org/downloads/metrics/

[18] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html

[19] Protection of Personal Information (Act No. 57 of 2003)
http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

[20] Medical Practitioners' Law
http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[21] Law on Public Health Nurses, Midwives and Nurses
http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[22] Dentists Law
http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

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

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

[25]Federal Trade Commission Act
http://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I

[26] Electronic Communications Privacy Act of 1986
http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc18.wais&start=3919965&SIZE=21304&TYPE=TEXT

[27] HIPPA Regulations & Modifications
http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

[28] Fair Credit Reporting Act
http://www.ftc.gov/os/statutes/fcradoc.pdf

[29] Gramm-Leach-Bliley Act (GLBA)
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html

Additional References

Cloud Standards Customer Council. *Practical Guide to Cloud Computing.*
http://cloud-council.org/resource-hub.htm#practical-guide-cloud-computing-v2
This guide provides a practical reference to help enterprise information technology (IT) and business decision makers adopt cloud computing to solve business challenges.

Cloud Standards Customer Council. *Public Cloud Service Agreements: What to Expect and What to Negotiate.*
http://cloud-council.org/resource-hub.htm#public-cloud-service-agreements-what-to-expect-what-to-negotiate

Cloud Security Alliance. *Security Guidance for Critical Areas of Cloud Computing*
https://cloudsecurityalliance.org/research/security-guidance/
The CSA Guidance seeks to establish a stable, secure baseline for cloud operations.

Cloud Security Alliance. *Cloud Control Matrix*
https://cloudsecurityalliance.org/research/ccm/
CCM provides fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Appendix A: Distinctions Between Security and Privacy

There are distinctions between security and privacy that are worth highlighting. We can categorize them as follows:

	Security	Privacy
Main concerns	Of a technical nature: ● Integrity of systems ● Preventing unauthorized access to systems ● Availability of service	Of a legal nature: ● Unauthorized access to personally identifiable information ● Tampering or deletion of personal information
Potential impacts	● Extended outages meaning inability to conduct the business of the organization ● Destruction of data or systems ● Direct loss of business due to outages, manipulation or destruction ● Business impact due to confidential information becoming public	● Violation of a person's rights ● Denial of services or benefits to a person (e.g., refusal to hire or to provide insurance based on private medical or judicial information) ● Loss of reputation with direct impact on business (this is also a risk with security breaches, but those tend to remain secret, while privacy breaches are usually public) ● Violation of regulations or laws ● Lawsuits from affected individuals
Perpetrators	● Malicious agents intent on causing harm, ranging from "script kiddies" to "hacktivists," industrial spies, terrorists, and foreign governments	● Sometimes no one: private information may be revealed accidentally ● Sometimes a "hacktivist" intent on proving that an organization does not protect data correctly ● Sometimes a *domestic* intelligence agency trying to capture information deemed important for national security ● Common criminals looking to steal identities and credentials
Motivations	● Range from demonstrating the lack of security to actually causing harm	● Range from demonstrating the lack of privacy to stealing private information for profit to malicious intent to damage the reputation of the organization

Possible measures and tools	● Intrusion detection ● Perimeter hardening (multiple firewalls, antivirus software) ● Offering a less visible profile by moving to the cloud ● Information security policy	● Encrypting the data ● Vetting of personnel with access to PII ● Strong Identity and access management ● “Split-and-spread”: making the data accessible at any one site incomplete until reassembled in a highly trusted system ● Privacy policy
Job Titles	● Chief Information Officer ● Chief Security Officer ● Security Administrator ● Compliance Officer	● Chief Privacy Officer ● Chief Data Officer ● Legal Counsel (privacy issues cannot be adjudicated by IT security personnel)

Appendix B: Worldwide Privacy Regulations

The state of privacy regulations around the world varies quite rapidly. Any snapshot of this situation, such as provided below, should be revised periodically by the user.

Generally, privacy regulations may cover the following aspects:[9]

- The scope of what is protected
- The entities to which the regulations apply
- The rules about allowing the transfer of protected data to other countries
- Whether the country’s rules provide “safe harbor” status with respect to the stringent European Union laws on data residency
- Whether there is a data protection agency of the government that has special jurisdiction over data privacy (as is the case for example with the CNIL commission in France)
- What special rights the Government gives itself to perform surveillance based on accessing data or obtaining encryption keys
- Whether there is an overriding protection contained in the country’s constitution or other statutes.

[9] This list is derived from the Forrester Global Data Protection Heat Map. See http://www.forrestertools.com/heatmap/

Region	Regulation
Asia Pacific region, Japan, Australia, New Zealand, and others	● Some countries 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) [18], and the Asia Pacific Economic Cooperation's (APEC) Privacy Framework. ● China, Taiwan and Thailand have effectively no data protection regime. ● Malaysia and India have some limited protections. ● South Korea and Singapore have the most stringent privacy regulations of the region. In Singapore, the Personal Data Protection Act 2012 is enforced by the Personal Data Commission established in 2013.
Japan	● In Japan, the Personal Information Protection Act [19] requires the private sectors to protect personal information and data securely. In the healthcare industry, profession-specific laws, such as the Medical Practitioners' Law [20], the Law on Public Health Nurses, Midwives and Nurses, [21] and the Dentist Law [22], require 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 95/46/EC 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. Turkey, by contrast, has minimal restrictions, a situation that is likely to change if and when the country is admitted into the EU. ● Even within the European Union, there are differences in local laws and regulations. The Benelux countries, the Czech Republic, Denmark, Estonia, Finland, Greece, Iceland, Portugal, Slovakia, and Slovenia have the strictest rules. France has had a data privacy law since 1978, enforced by a special government commission, with which any new database containing PII must be registered.
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 [23] and Argentina [24] 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. ● Argentina is the strictest of the hemisphere's countries and the combination of its constitutional protection and laws have earned it recognition by the European Union that it provides equivalent protection. ● In Mexico, the "transparency laws" enacted in order to fight corruption can work at cross-purposes with privacy. For example, any civil servant's name and professional e-mail address is exposed to the public because the law requires the employee directories of all government agencies to be public. On the other hand, data held by the private sector is protected under a series of laws enacted in 2010-2014, and the situation is still

	changing. Data residency restrictions are often invoked as an obstacle against moving to cloud solutions, even though it is hard to pinpoint any text that explicitly imposes data residency within Mexico. ● Paraguay is the exception in the continent, with essentially no restrictions.
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 [25] 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 [26] which protects customers against interception of their electronic communication (with numerous exceptions). o The Health Insurance Portability and Accountability Act (HIPAA) [27]which contains privacy rules applying to certain categories of health and medical research data. o The Fair Credit Reporting Act [28] includes privacy rules for credit reporting and customer reports. o The Gramm-Leach-Bliley Act (GLBA) [29] govern the collection, disclosure, and protection of customers' 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. ● California has progressively reinforced its laws concerning data breaches, as recently as September 2014. It also enacted at the same time the Student Online Personal Information Protection Act (SOPIPA).
Worldwide	● The Payment Card Industry (PCI) Data Security Standards (DSS) [8] which apply to credit card data anywhere in the world, including data processed by subcontractors has similar requirements.

Appendix C: 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
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