Public Cloud Service Agreements: What to Expect and What to Negotiate

March 30, 2013
# Contents

Executive Summary ............................................................................................................................ 4

Current Anatomy of a Cloud Service Agreement ................................................................................. 5

Customer Agreement ................................................................................................................................ 5
Acceptable Use Policies (AUPs) ................................................................................................................. 6
Cloud Service Level Agreements ............................................................................................................... 6

What You Can Expect and What You Should Negotiate ............................................................................. 6

Step 1: Understand Roles and Responsibilities ......................................................................................... 7
Step 2: Evaluate Business Level Policies .................................................................................................... 8
Step 3: Understand Service and Deployment Model Differences .......................................................... 11
Step 4: Identify Critical Performance Objectives .................................................................................... 12
Step 5: Evaluate Security & Privacy Requirements .................................................................................. 14
Step 6: Identify Service Management Requirements .............................................................................. 16
Step 7: Prepare for Service Failure Management .................................................................................... 19
Step 8: Understand the Disaster Recovery Plan ..................................................................................... 20
Step 9: Define an Effective Management Process .................................................................................. 21
Step 10: Understand the Exit Process ..................................................................................................... 21

References ....................................................................................................................................... 23

Appendix A: Analysis of AUP Content ............................................................................................... 25
Appendix B: Analysis of Cloud SLAs .................................................................................................. 26
Appendix C – Security ...................................................................................................................... 28
Appendix D – Privacy ............................................................................................................................. 29
Acknowledgements

The major contributors to this whitepaper are: Claude Baudoin (cébé IT & Knowledge Management), Jordan Flynn (eFortresses), John McDonald (CloudOne), John Meegan (IBM), Michael Salsburg (Unisys), and Steven Woodward (Cloud Perspectives).
Executive Summary

As CIOs and CFOs consider efficient, agile and cost-effective ways to deliver business services to the enterprise, they cannot help but consider public cloud technology. Cloud technology provides services at all levels of IT infrastructure, from basic virtualization services to operating system services to application level services. These services can be orchestrated to deliver what is consumed by the enterprise – business services. If any portion of this orchestration does not meet service level objectives, the business can be impacted in many ways, from slow response time to debilitating outages and events that can impact the enterprise’s reputation. Therefore, service agreements from cloud providers need to be understood and balanced against the needs of the business.

For datacenters that have already leveraged outsourced infrastructure, the value of service level objectives and their formal contracts is understood. For datacenters that are using clouds as their first entrée into outsourced infrastructure, service agreements may be totally new. IT managers are not comfortable relying on infrastructure and infrastructure management that are outside their immediate control. Therefore, they are quickly realizing that they cannot guarantee a required level of service without understanding their objectives and formalizing such service level with organizations that are on the critical path of their business services delivery.

This paper provides cloud consumers with a pragmatic approach to understand and evaluate public cloud service agreements. The recommendations in this paper are based on a thorough assessment of publicly available agreements from several leading public cloud providers. In addition to this paper, a great deal of research and analysis regarding the landscape of cloud service agreements is available in the CSCC companion paper, the “Practical Guide to Cloud Service Level Agreements” [2].

In general, we have found that the current terms proposed by public cloud providers fall short of the commitment that many businesses will require. Of course, these providers have reputations to establish or maintain, therefore they will likely employ all reasonable efforts to correct problems, restore performance, protect security, and so on. But neither the specifics of the measures they will take, nor the remedies they offer if they fall short, are currently expressed well enough in their formal agreements in most cases. Furthermore, the language about service levels is often distributed among several documents that do not follow a common industry-wide terminology. We hope that one impact of this paper will be to improve this state of affairs.

When specific examples are used in this document, they reflect the state as of January 1, 2013 and are not meant to be comprehensive lists. The intention is NOT to compare or recommend cloud providers, but rather to highlight key considerations that must be taken into account when evaluating a public cloud service agreement. The specific examples are not intended to discredit or promote one provider over another, but rather to provide illustrations and observations from a vendor-neutral perspective. Similar text will be found across multiple cloud providers and readers needs to perform their own analysis regarding the existing agreements and other contractual expectations/obligations.
Current Anatomy of a Cloud Service Agreement

No standard nomenclature is used across the various cloud providers to define their public cloud service agreements (see references [4] through [23]). This section, and the artifacts mentioned in it, offers a structure that cloud consumers can use to compare agreements from different public cloud providers.

Consumers are advised to pay great attention to the language used in the agreements. Not all agreements were written or edited with the care they require. Wording errors can radically alter the meaning of a clause, making it much more broadly applicable than intended. The right time to catch and correct these errors is before signing a contract, not when a dispute arises.

In general, the cloud agreement can be decomposed into three major artifacts: “Customer Agreement,” “Acceptable Use Policy, and “Service Level Agreement.” Bear in mind that these three artifacts may change at different times, independently from each other.

Customer Agreement

Since business service management includes the processes and procedures of the cloud provider, explicit definitions of the roles, responsibilities and execution of processes need to be formally agreed upon. The “Customer Agreement” fulfills this need, using various synonyms such as “Master Agreement,” “Terms of Service,” or simply “Agreement.” In general, all the public cloud Customer Agreements we reviewed contained the following critical sections, each using slightly different terminology.

• **Use of Service Offerings.** This defines how the customer is expected to use the public cloud offering. Alternate terminology includes “Provision of the Service” and “Services Description.”

• **Fee and Payment.** This describes the method of paying for cloud services. Other terminology includes “Service Charges Schedule,” “Purchasing Services,” and “Payment Terms.”

• **Temporary Suspension.** This describes a process whereby the provider suspends for a time the use of the cloud by a specific customer, based on an issue such as abnormal use of the cloud, security risks, or delinquency in payment. Other terminology can include “Suspension and Removals” and “Term, Termination and Suspension.”

• **Terms and Termination.** This addresses the terms of the agreement and the process for termination. Other terminology includes “Agreement Termination and Closing the Account.” As noted above, the provider may also specify in this section a temporary suspension clause.

• **Indemnification.** This addresses holding the provider harmless against various claims, damages and loss.

• **Disclaimer.** This section describes what is not included in the agreement. It is described under headings such as “Warranties and Disclaimer.”

• **Limitation of Liability.** In the event of a problem, this section specifies a limit on the amount of compensation a customer can claim.
• **Security/Privacy.** The security and privacy of information is a key factor when choosing a public cloud provider. Security and privacy are addressed in various sections of the agreements, including “Content Responsibilities,” “Security, Privacy and Data Protection,” “Privacy Policies,” and “Customer Obligations.”

**Acceptable Use Policies (AUPs)**

All of the public cloud providers we reviewed included acceptable use terms for both the cloud provider and the cloud consumer. For example, the cloud consumer agrees not to install malware on the cloud. The cloud provider agrees not to violate the intellectual property rights of the consumer. In most cases, an Acceptable Use Policy is provided as a separate artifact on its own web page. The AUP sometimes overlaps with, or replaces, the Security/Privacy terms of the Customer Agreement.

**Cloud Service Level Agreements**

Service Level Agreements (SLAs) are formal documents, agreed on by both parties, that define a set of service level objectives. These objectives may concern availability, performance, security and compliance/privacy. However, the analyzed cloud SLAs focused solely on availability and on the remedies offered if the availability target is not met.

**What You Can Expect and What You Should Negotiate**

The CSCC “Practical Guide to Cloud Service Level Agreements” white paper [2] prescribes a series of ten steps that cloud consumers should take to evaluate cloud SLAs in order to compare public cloud service providers or negotiate terms with a provider. The following steps are discussed in detail:

1. Understand roles and responsibilities
2. Evaluate business level policies
3. Understand service and deployment model differences
4. Identify critical performance objectives
5. Evaluate security and privacy requirements
6. Identify service management requirements
7. Prepare for service failure management
8. Understand the disaster recovery plan
9. Define an effective management process
10. Understand the exit process

This section uses the same list of ten steps as a straightforward way to complement and extend the original Guide. For each step, the corresponding subsection describes the range of guarantees found in the cloud service agreements that were reviewed, highlights best-of-breed guarantees, and provides recommendations for what consumers should negotiate with their public cloud providers. Example language from actual agreements is quoted to highlight key points. Assistance on where to find specific information is also provided for each step (i.e., which service agreement artifact should be examined – Customer Agreement, AUP, or Cloud SLA).
Step 1: Understand Roles and Responsibilities

The AUP is the primary artifact that should be thoroughly reviewed by cloud consumers to understand their responsibilities and those of the provider. AUPs are generally not related to technology or financial performance of the cloud relationship, but rather govern the valid and invalid customers behaviors related to using the service.

Although the AUPs that were reviewed contained some common points, each was original to a surprising degree. Some providers focus more on the illegal usage of their services, such as inappropriate material or copyright violations, while others are more concerned with abuse of network bandwidth or overloading the service itself. To put it more simply, some providers are worried about what consumers do with their service, while others are more concerned with performance impact.

Appendix A contains key observations and actual language examples for the most common aspects of public cloud AUPs.

Recommendations

When evaluating the Acceptable Use Policy of a public cloud service provider, consumers should expect the following, and if needed should request clarification.

- **Clarity.** Since the terms of an AUP apply to the overall use of the services, and it is difficult to foresee every possible situation, it is important for the consumer to clearly understand all aspects of the AUP. You should ask the vendor to clarify, in writing, any items for which there is confusion or open interpretation.

- **Brevity.** Most of the AUPs analyzed were succinct and clear. However, a few were filled with legal jargon and seemingly duplicate provisions from one part to another. Such lengthy, wordy provisions were probably never tested in a court of law, and you don’t want to be the first customer to defend yourself against them.

- **Completeness.** While many AUPs covered all the provisions we mentioned in the “Anatomy” section (content, security, service integrity, and rights of others), some AUPs were missing certain provisions. For example, one large cloud service provider said absolutely nothing about the content prohibited on the service, instead relying on vague language that allowed them, in theory, to deem unacceptable anything they chose. This open language is not in the consumer’s best interest, because it places the burden of proof on the consumer, and there is no clear language for a judge or jury to consider in deciding a case.

- **Focus.** Disturbingly, some of the AUPs outlined a very broad scope for what the service provider may decide is acceptable. As an example, one AUP contained a “breach of obligation to any person” prohibition, which, without scope limitations, might place the user in breach of contract if any aspect of their life involved a missed obligation, whether or not it had to do with the service itself! Consumers should shy away from services with such broad statements, or ask for clarification in writing.
In summary, AUPs have little consistency in wording at this stage of cloud service development, although there is a clear pattern to the types of provisions they include. To safely navigate these waters, customers should exercise caution and thoroughly review every provision before agreeing to an AUP.

**Step 2: Evaluate Business Level Policies**

Consumers must consider key policy issues when reviewing a public cloud service agreement since there are interdependencies between the policies expressed in the agreement and the business strategy and policies developed in other aspects of the business. Four specific policies are analyzed in this section, contained primarily in the provider’s Customer Agreement:

- Data policies
- Changes to services, APIs, or agreements
- Suspension of services
- Limitations of Liability

**Data Policies**

The data policies of the public cloud provider, as expressed in the Customer Agreement, are perhaps the most critical business-level policies that need to be carefully evaluated. The “duty of care” that a cloud provider has to its clients and their data is partly governed by the data protection legislation applicable in the user’s local jurisdiction as well as in those jurisdictions in which its data may reside or may be made available. Consumers should carefully consider these legal requirements and how the agreement a provider offers deals with issues such as movement of data to offer multisite redundancy across several jurisdictions.

In general, all public cloud Customer Agreements reviewed contain the following clauses:

- The consumer is solely responsible for the development, content, operation, maintenance, licensing and use of their content.
- The consumer retains all right, title, and interest in their content.
- The consumer is responsible for its end users’ use of their content and of the cloud service, and for their compliance with the terms of the cloud services agreement.
- The consumer is responsible for maintaining appropriate security, protection and backup of their content.
- The consumer is responsible for any individual's personal information or any confidential information that is stored in the cloud. The consumer agrees to comply with all applicable privacy and data protection laws, to obtain all necessary consents, and make all necessary disclosures before including personal information in their content.

In most cases, the Customer Agreement does not allow the consumer to specify where its content will be stored. Among the agreements that were reviewed, there was only one that allowed the consumer to select whether its data should be permanently stored in the United States or the European Union.
This may be unacceptable to customers in certain vertical industries (financial services, health care, oil and gas, etc.) on which authorities often impose stringent data residency obligations.

The Customer Agreement should explicitly state that the provider will not access the consumer’s content. In the event of a valid legal or governmental request, consumers should require immediate notification from their provider, enabling them to file without delay for a protective order.

When evaluating the **data policies contained in the Customer Agreement**, consumers should consider the following best practices:

- Ensure that the agreement allows the consumer to specify the physical location of their security-sensitive content, or content subject to data residency requirements (specifically acceptable locations vary across industries and national legislations).
- Ensure that the cloud provider will not access the consumer’s data, except when required by law and duly requested by law enforcement authorities.
- Under such circumstances, ensure that the agreement specifies that the cloud provider will give immediate notice, allowing the consumer an opportunity to file for a stay of the request.

**Suspension of Services**

Consumers must fully understand the impact that potential suspension of services will have on their data and business services, and on their own clients, and should develop a plan to ensure business continuity in such an event. A suspension of services clause should be part of every Customer Agreement and should describe in detail the circumstances under which cloud providers can suspend services to a consumer. Reasons for suspension will typically include:

- Breach of contract, including payment delinquency
- Behavior posing a security risk to the service or any third party
- Actions that may subject the cloud provider to liability
- Usage that represents a direct or indirect threat to the provider’s network function or integrity, or to anyone else’s use of the service

In most cases, suspension of service is applied to the minimum necessary portion of the service and will only be in effect for as long as reasonably necessary to address the issues giving rise to the suspension. Advance notice is typically given before service is suspended, except in emergency situations. Consumers are typically given 30 to 60 days to address the reasons for suspension before termination of service is initiated.
When evaluating the service suspension policies contained in the Customer Agreement, consumers should consider the following best practices:

- Ensure that the agreement specifies that advance notice will be given for all suspensions initiated by the cloud provider (minimum of 30 days), with the possible exception of well-defined emergency situations.
- Ensure that the agreement provides sufficient time to address the reasons for suspension (minimum of 60 days).
- Ensure that the agreement specifies that the consumer’s content will not be deleted during service suspension.
- Ensure that advance notice will be given before termination commences (refer to the “Understanding the Exit Process” section).
- Ensure that payment will not be due for the suspension period if it is determined that the provider incorrectly decided that the consumer was at fault.

Changes to Services, APIs or Agreements

Provisions for changes to services, APIs and agreements are typically included in the Customer Agreement, describing in detail the circumstances under which cloud providers can make such changes. Consumers must fully understand the impact that such changes may have on their data and business services, and should develop a plan to minimize business disruption.

In most cases, the onus is on the cloud provider to give advance notice (typically 30 days) to their consumers for any such material change. For services, providers usually give themselves the right to change, discontinue, or deprecate any service offering, or change or remove features or functionality of the service offering – at any time. For APIs, providers may change, discontinue or deprecate any APIs for the services from time to time, but will typically commit to apply commercially reasonable efforts to continue supporting the previous version of any API for a period of time (typically 12 months) after the change, discontinuation, or deprecation.

When evaluating the policies concerning changes to services contained in the Customer Agreement, consumers should consider the following best practices:

- Ensure that the agreement specifies that advance notice (minimum of 30 days) will be given for all changes initiated by the cloud provider.
- Ensure that the agreement commits the provider to use commercially reasonable efforts to maintain backward compatibility, or continue to operate the applicable service/API, for an extended period of time (minimum of 12 months) after the effective date of the change.

Limitation of Liabilities

Typically, the limitations of liability expressed in a public cloud service agreement protect the cloud provider and greatly limit the compensation provided to the consumer in cases of breach of contract. Details of liability limitations are contained in the following sections of the Customer Agreement:
• **Limitations of Liability.** This section contains language stating that the provider will not be liable for any deletion, damage or destruction of the consumer’s content, etc. In addition, the aggregate liability is specified (i.e. the maximum amount the provider is liable for). This amount varies for different providers but is typically capped at the amount the consumer has paid the provider for services during the 12 months preceding the claim.

• **Disclaimers.** This section contains language stating that the service offerings are provided “AS IS” and that the provider makes no warranties that the consumer’s content will be secure or not otherwise lost or damaged. Again, the language differs across the public cloud providers that were reviewed, but the general intent and provisions are consistent.

• **Indemnification.** This section states that the consumer and provider will indemnify, defend, and hold each other harmless from all liabilities, damages, and costs arising from a third party claim that technology used to provide the service infringes or misappropriates any patent, copyright, trade secret or trademark of such third party. Although the language differs across the public cloud providers that were reviewed, the general intent and provisions are consistent, although indemnification is not always reciprocal.

When evaluating the **liability limitations** contained in the Customer Agreement, consumers should:

• Carefully review the provider’s **aggregate liability**, since this amount differs across providers.

• Ensure that the disclaimers exclude cases where the provider is negligent.

• Compare the indemnification and disclaimer clauses to ensure there are not significant differences between the public cloud providers being considered.

• Verify that the indemnification clause is reciprocal – it’s not just the consumer protecting the provider, but the other way around too.

### Step 3: Understand Service and Deployment Model Differences

Cloud **service models** and deployment models are defined in the NIST Reference Model [3].

Most services offered by cloud providers follow one of three major **service models**: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model presents significant differences in the levels of cloud resource abstraction, service level objectives, and key performance indicators that are specified in the SLA. The unique characteristics of each service model are described under Step 4 below.

The deployment model covered by the cloud service agreement can be **Private, Community, Public, or Hybrid**. This white paper focuses exclusively on service agreements for public deployments. The other deployment models are out of scope, but it is critically important that the consumer understand the differences between the various deployment models since potential value and risk varies significantly, and other deployment models may provide appropriate alternatives if public clouds fall short of some consumer requirements.¹

---

Step 4: Identify Critical Performance Objectives

The cloud SLA is the document that specifies service commitments by the cloud service provider. All of the public cloud SLAs that were reviewed consisted of four key components: service commitment, credits, credit process, and exclusions.

Service commitments differ across cloud service models; therefore different types of cloud SLAs were analyzed: IaaS SLAs (with a distinction between Compute and Storage services), PaaS SLAs, and SaaS SLAs. In general, service commitments varied across service models, but credits, credit process, and exclusions were consistent.

- **Service Commitment.** All service commitments across service models (IaaS, PaaS, and SaaS) focused almost exclusively on uptime/availability. Few other metrics were specified. Uptime/availability is expressed as a percentage that ranges from 99.0% to 99.9%, 99.95% and even 100%, depending on the service model, and is typically measured on a monthly basis (one SLA measured it on a yearly basis).

For IaaS services, downtime is measured differently across the various SLAs that were reviewed:

- Total minutes when the service is unavailable during a billing cycle (e.g., per month)
- Total number of errors divided by total number of requests during a specific time interval (which ranged from 5 minutes to 1 hour)
- Elapsed time from when a case is filed until when the service is reinstated
- For one SLA, “Failed Storage Transactions” included transactions not processed within a specified time period (although it is not clear how this is measured or monitored)

For PaaS services, the definition of downtime varies significantly across providers. For example:

- An application error rate exceeding 10% for at least 5 consecutive minutes
- All attempts to connect fail or take longer than 30 seconds to succeed during a 5-minute period

- **Credits.** Credits are the sole form of compensation for missed service commitments across all the SLAs that were reviewed, regardless of the service models. The calculation of service credits differs significantly from provider to provider. For example:

- Tiered credit of 10%, 25%, and 50%
- Prorated credit based on unavailability
- 5% of fees for each 30 minutes of downtime

In all cases, maximum credit cannot exceed 100% of the monthly service charge. In some cases, the maximum credit is less than 100% (50% maximum in one instance). This may of course be considerably less than the damage suffered by the consumer (on the other hand, when a consumer suffers a failure of its own on-premise resources, it does not recover anything).

In most cases, if there is more than one SLA impacted by an incident, only one SLA service credit can be claimed.

- **Credit Process.** All of the SLAs that were reviewed required the cloud consumer to take specific action to receive credit. The consumer is required to identify and report failures. The timeframe
for reporting them varied significantly: 48 hours, 5 days, 7 days, 30 days, 10 business days after service is restored, etc. The onus is on the consumer to provide proof of the problem, including dates and times, server request logs, network trace routes, full description of the service interruptions the duration of the incidents, and, in the case of PaaS SLAs, the names of the affected databases, failed operations, and so on. In all cases, the cloud provider reviews claims and makes a final, unilateral judgment on service credits.

- **Exclusions.** For the most part, exclusions are similar across all of the SLAs that were reviewed. The following events are typically excluded:
  - Factors outside of the provider’s reasonable control
  - Force majeure conditions
  - Failures resulting from any actions or inactions of the consumer or any third party, or from equipment, software or other technology operated by the consumer or a third party
  - The consumer’s refusal to allow the provider to perform maintenance deemed necessary to maintain the service – whether it is scheduled or emergency maintenance
  - Periods of emergency maintenance activities, or a consumer-requested maintenance downtime
  - Problems with the consumer connectivity to the Internet

Appendix B highlights the key observations for each of the four aspects (service commitments, credits, credit process, exclusions), focusing on the commonalities and differences that were found, and provides example language to illustrate the observations.

**Recommendations**

<table>
<thead>
<tr>
<th>When evaluating the <strong>service commitments</strong> of a public cloud service provider, or comparing providers, consumers should take the following steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Analyze service availability guarantees and associated credits.</td>
</tr>
<tr>
<td>• Find the observation period over which commitments are measured, and understand the business impact of a single outage corresponding to the maximum downtime occurring once during that time window.</td>
</tr>
<tr>
<td>• Analyze service credit calculations and maximum credit limits.</td>
</tr>
<tr>
<td>• Compare service credit processes, particularly the timeframe within which incidents must be reported and the type of information required to prove that a failure occurred.</td>
</tr>
<tr>
<td>• Examine commitment exclusions.</td>
</tr>
<tr>
<td>• Automate the process for detecting and logging service outages, for example using tools that exercise the cloud service through periodic dummy transactions, recording the response time as well as detecting failures.</td>
</tr>
</tbody>
</table>
Step 5: Evaluate Security & Privacy Requirements

Public cloud providers place considerations about security and privacy in a variety of different documents, with inconsistent titles and language. There is a need to harmonize the names of documents across the industry in order to make it easier for consumers to locate and review the relevant language.

Security language was found in documents called “Customer Agreement,” “Support Agreement,” “Service Level Agreement,” “Enterprise Agreement,” “Contract,” “Technical Overview,” “Acceptable User Practices,” “Security Practices,” “Terms of Service,” and “Privacy Statement.” That last case indicates not only inconsistent naming across providers, but inconsistent classification of content by the same provider, which includes some security terms inside a privacy statement.

It is fairly common for one of these documents to refer the reader to another document. Sometimes there is more than one level of indirection. This does not make it easy to compare security obligations across providers.

One-Sided Security Obligations

Most agreements impose stringent security obligations on the consumer to protect the provider, and serious consequences if these obligations are not met. While it is legitimate for the provider to tell the consumer that certain practices, which would endanger the security of the provider and of its other consumers, are not acceptable, there are two problems with such clauses:

- The provider is solely responsible for determining that a security violation occurred.
- The actions taken by the provider are typically drastic, namely suspension or termination of the account, without easy recourse and without any compensation for the loss of business if the suspension is found to be unwarranted.

On the other hand, the security language rarely imposes any obligation on the provider to protect the security of the consumer. The language in the analyzed agreements falls in the following categories:

- Generic language that says that the provider will protect the consumer’s data with the same level of care as if it was its own. While not very specific, this is standard language in Non-Disclosure Agreements and we therefore take it that this can be considered sufficient to hold a negligent provider accountable in a court of law.
- Language to the effect that the provider will provide some sort of “help,” usually poorly specified, to allow the consumer to maintain its security.
- Vague language about the provider maintaining certain security measures, usually accompanied with an obligation on the consumer to determine if such measures are adequate or not. There were a couple of exceptions where the provider included a detailed description of their process.
- No mention of the provider’s security measures at all.
- “Worse than nothing”: in at least one case, not only does the provider fail to make any security commitment, but it explicitly declines responsibility to restore any lost data “under any
circumstances” even though such circumstances could include its failure to maintain proper security.

A Narrow View of Privacy

Most providers address privacy only to the extent that they tell the consumer what data they will collect from the customer in order to provide the service, and what rights they give themselves to use that data. This data includes customer contact information, IP addresses, billing information, etc., that is, data collected in order to manage the customer relationship.

This is not what most consumers are concerned about when they think of “privacy in the cloud.” They’re not so much concerned about their own names and addresses, but rather about the private data they hold in the cloud about others:

• The medical history of patients in a health care system
• Account numbers and balances of the clients of a financial institution
• Personal information about customers in a CRM system
• Accounts payable and receivable information in an ERP system
• Personal information about employees in an HR system

We have found no assurance of the privacy of any such data in any of the agreements we reviewed, even though it is clear that in many cases, system administrators working for the provider would have access to such information, which is held in clear text in many systems.

In addition to this limited view of what privacy means in the cloud, many agreements contain absolutely no mention of privacy at all. Sometimes, but not always, they refer the reader to another document.

Recommendations

Consumers should request, and providers should consider, the following reasonable practices regarding security and privacy:

• Security and Privacy commitments should be explicit, separate, and in clearly identified documents.
• The provider should commit to specific physical and logical security practices aimed at avoiding disruption to the consumer’s business (not just the other way around).
• When a provider seeks to protect itself by granting itself the right to suspend access to services by a consumer, it needs to provide an emergency mechanism to resolve the issue if the consumer acted in good faith or was actually not responsible for the breach.
• If the provider took such a measure, and it is found later that this was not justified, the consumer should be entitled to a credit that is above the cost of the suspended service (something like the judicial notion of “triple damages” should become an industry standard in case of a business disruption that results from the provider’s lack of competence or attention).

(Continued on next page…)
• If a security attack on the provider causes the loss of consumer data, the provider must be obligated, under severe penalties, to restore the data from a recent, pre-attack backup.
• The provider should offer or subcontract (at a commercially reasonable cost) a security professional service to help the consumer assess and select the appropriate security mechanisms. That service should also be available in an emergency to help diagnose and repair security issues.
• The privacy of the “consumer’s customer’s data” must be addressed in two ways:
  ▪ The provider should disclose the measures it takes to prevent its own personnel’s access to confidential information contained in the cloud systems and services rented by the consumer; and
  ▪ The provider should provide advice to the consumer about the vulnerabilities that exist and the possible remediation, such as the potential need to encrypt data in transit and/or at rest so that confidential information, even if intercepted, cannot be exploited.

Step 6: Identify Service Management Requirements

The findings related to service management and maintenance in public cloud service agreements indicate that consumers should perform due diligence to ensure that the level of service is managed appropriately by the provider. Consumers should not expect much to be specified within the standard service agreements.

Consumers should also be aware that they may need to improve their internal service management capabilities, including monitoring, in order to comply with terms in the cloud service agreement as well as to validate the level of service from their provider.

Service management provisions and language are primarily included in two artifacts, the Customer Agreement and the Cloud SLA, across service models (IaaS, PaaS, and SaaS). The service management considerations covered include: provisioning, audit, on-boarding account setup, services enablement, reporting and monitoring, metering, and support and maintenance.

Service Management Practices

Service management practices are virtually non-existent in the publicly available documents. In some cases, the delivery of mature service management practices by providers is inferred; however, in most situations, the consumer is responsible for clarifying what service management practices are employed.

Consumers may expect certain services to be a standard offering: software maintenance and upgrades, backup, recovery, encryption, etc. In fact, there are three possible situations:
  • Some providers include these features automatically, and they form a foundation for their service offering.
  • Others require signing up for higher, more expensive levels of service.
  • Some do not offer them at all.
These services may be critical considerations for a cloud computing initiative; therefore, they must be carefully evaluated and clarified.

Some system management agreements are complex and/or involve external partners of the provider. Agreements can be different across products and geographical areas, adding to the complexity of fully understanding the agreement’s obligations and constraints.

**Maintenance and Updates**

Within a cloud service agreement, maintenance is usually mentioned in the context of availability to explicitly state that “planned maintenance time is excluded when calculating availability.” Another major provision typically states that the provider may change or remove functionality (including enhancements) at any time, with appropriate notice. Such a change could result in preventing the customer, or its own clients, from operating a business function. In turn, this makes the consumer incur additional costs that impact the total cost of ownership (TCO) of a cloud solution, hence the cost/benefit calculation. Moreover, an immature public cloud solution with frequent releases that modify or remove existing functions may force consumers to consider changing providers or deployment models.

Maintenance means different things across service and hosting models. The key is to clarify early what the maintenance services include, such as delivery cycles and assurances of quality. Service and product defects are seldom inferred in any of the service agreement documents.

**One-Sided Change Management Constraints**

Most agreements impose stringent process constraints on the consumers, but seldom outline the services or processes that the provider utilizes to manage the services that are provided. The various agreements are written by the providers to protect the provider’s assets rather than protect the consumer. In many instances, these agreements state that the agreement itself may be subject to change and termination at the discretion of the provider.

Change management and configuration management are very important cloud considerations as asset licensing and volatility of functionality have significant impact on cloud computing justifications. Most of the responsibility will ultimately fall onto the consumers to ensure that they comply with agreement terms and prepare for changes.

In some cases, a consumer who contracts for one service is no longer permitted to use certain competing products, which may therefore need to be removed. Good configuration management (CM), based on solid enterprise architecture approaches, is extremely valuable to optimize cloud management and to comply with the agreement’s requirements. For example, a CM product may help answer the question: “If we need to terminate product X, what is the impact?”

**Service Metrics Definitions**

Clarification of SLA metrics remains critical: while different cloud providers often use the same names for metrics, the detailed definitions and usage are often different.

To take an example, *availability* is the primary metric identified in the SLAs, but as the “Service Commitments” section highlights, availability is calculated and used in many different ways. Thus, a
99.5% commitment may result in a higher guarantee of service than 100%, due to the way a provider calculates and credits outages.

Another issue presents itself when one provider relies upon others to deliver the complete end-to-end service experience. For example, a consumer may procure a SaaS solution that in turn relies on IaaS services from a different provider. In such a case, these are cascading SLAs that depend on each other, but agreements do not specify how service levels are calculated when such cascading SLAs are present.

It is crucial for the consumer to understand the agreed-upon service metrics, how they are derived, and how they are used. In certain situations, consumers may want to request other measures and metrics be collected for analytics that are critical to meeting their business objectives. Some providers may agree to supply this information, possibly for an additional charge. More information about metrics approaches appears in the CSCC “Practical Guide to Cloud SLAs” [3].

Accreditations and Certification

The most unequivocal assurances often provided in a cloud service agreement concern a provider’s accreditations or certifications by one or more standard-developing organizations (SDOs) or their certified auditors. The agreements reviewed mentioned the following:

- ISAE 3000 international attestation and/or US AT 101 attestation such as a Service Organization Control (SOC) report – especially SOC 2 and SOC 3 reports, which address security and trust
- FISMA (Federal Information Security Management Act) compliance
- Payment Card Industry Data Security Standard (PCI DSS) certification
- ISO 27001 and 27002 compliance certification by an Accredited Registrar
- FIPS (Federal Information Processing Standard) 140-2 validation, related to data encryption

Some accreditations will often require assessment of critical service management processes. Specific service management requirements are not usually cited directly in the agreement, but many accreditations imply that certain mature service management processes will be utilized.

Audit

Audits (by consumers or independent auditors) are not usually specified in cloud service agreements. The accreditations included in many agreements are intended to infer credibility without consumers needing to visit facilities and perform audits.

If the right to audit is an important factor, the consumer should attempt to negotiate it as part of the contract, but this will be at the provider’s discretion. Multi-tenant cloud solutions are particularly challenging with respect to auditing and penetration testing, since the audit process by client A might impact the delivery of services to client B, or may allow client A’s representatives to observe information about client B’s use of the services.
**Recommendations**

When evaluating the **service management policies** contained in the Customer Agreement and Cloud SLA of a public cloud provider, consumers should consider the following:

- They have the ultimate responsibility to fully understand the agreements, terms, responsibilities, activities and accountability related to service management.
- They must precisely define their objectives and ensure that the provider offers the level of support necessary to meet these objectives.
- Customizations or supplementary agreements may be needed to address specific service management objectives and concerns, but obtaining them is unlikely or at best difficult. For services requiring such specific provisions, alternative deployment models should be considered, such as a private or hybrid cloud.
- Consumers need to consider the provider’s commitments to stability of functionality over time, including APIs and Web services, and how changes can impact TCO and their customers’ experience.
- Consumers must examine in detail the definitions and potential impact of each service metric, and the extent to which the metric represents a serious commitment, based on how credits for outages are calculated.
- Consumers should ask questions related to service management maturity in the various topic areas (service management, metrics, etc.) to distinguish actual capabilities from marketing claims.
- Consumers should not totally outsource service management; they need to retain in-house the service management expertise required to monitor and improve cloud performance.

**Step 7: Prepare for Service Failure Management**

Other than the service commitments, credits, and credits process specified in the cloud SLA, there were no other specific references to service failure management capabilities or expectations in any of the public cloud service agreements that were reviewed. Unfortunately, the financial burden for service failure falls predominately on the consumer, with compensation from the provider capped at one month of service credit in most cases. In addition, the onus is on the consumer to identify any failures and to provide proof of the failure to the provider. There are also numerous exceptions for which a provider does not provide compensation. Refer to “Step 4: Identify critical performance objectives” for details.

When considering public cloud offerings, consumers must take into account the potential impact of service failure on their business operations. Given the limited guarantees provided by standard agreements, current public cloud solutions may not be appropriate for some mission-critical services. Private or hybrid cloud approaches may be more appropriate for these services.
Step 8: Understand the Disaster Recovery Plan

Disaster recovery is a subset of business continuity and focuses on processes and technology for resumption of applications, data, hardware, data communications, and other IT infrastructure in case of a man-made or natural disaster. Outsourcing infrastructure, platforms, or applications to a cloud provider does not absolve consumers of the need for serious disaster planning. Every company is unique in the importance it assigns to specific infrastructure and applications; therefore, a cloud disaster recovery plan must be tailored to each organization, and business objectives play an important role in determining the specifics of disaster recovery planning.

In general, current public cloud service agreements provide inadequate guarantees in case of a service outage due to a disaster. Most cloud SLAs provide cursory treatment of disaster recovery issues, procedures and processes. Instead, the cloud service agreements that were reviewed focused on limiting the liability of the cloud provider in disaster events, and were consistently stated in the following areas:

- **SLA Exclusions.** This section of the cloud SLA contains language that excludes service credits for outages caused by factors outside of the provider’s reasonable control, including any force majeure event, Internet access problems, or similar issues.
- **Disclaimers.** This section of the Customer Agreement contains language stating that the service offerings are provided “AS IS” and that the provider makes no warranties that the consumer’s content will be secure or not otherwise lost or damaged.
- **Limitations of Liability.** This section of the Customer Agreement contains language stating that the provider will not be liable for any deletion, damage or destruction of the consumer’s content.

Given the clauses above, the onus is clearly on cloud consumers to define, implement and execute their own disaster recovery plans, leveraging the services of the providers in the best possible manner (i.e., backup services, geographically dispersed redundancy services, etc.).

Recommendations

Despite the limitations in current public cloud service agreements, cloud consumers should address key disaster recovery procedures early in the process of cloud adoption:

- Consumers should devise a disaster recovery plan by identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that is acceptable before there is a significant business impact.
- Consumers should ensure that business critical content is stored redundantly in different geographical locations to help reduce the impact of a disaster.
- Consumers should ensure an appropriate frequency of backups based on the criticality of content.
Step 9: Define an Effective Management Process

Consumers legitimately expect an effective management process for any problems that may arise with their public cloud usage. However, today’s public cloud service agreements contain no provision for consumer-provider management processes. The only formal channels of communication between the consumer and provider specified in the service agreement are breach of contract clauses (credit process, suspensions, termination, etc.). None of the agreements that were reviewed specify status meetings between the parties. There is no defined escalation process which the consumer can invoke to raise the priority of a service level issue.

As a result, consumers must carefully consider the types of services they deploy to the public cloud. Mission-critical business services and data that require careful monitoring and fast resolution of issues may require supplemental agreements specifying an effective management process. At minimum, a single point of contact for service issue escalation should be designated. Ultimately, private or hybrid cloud approaches may be more appropriate for such services.

Step 10: Understand the Exit Process

An exit clause should be part of every cloud service agreement. It describes the details of the exit process, including the responsibilities of the cloud provider and consumer in case the relationship terminates – prematurely or not. It is important that consumers fully understand the impact that termination will have on their data and business services, and develop a plan to ensure minimal business disruption during the resulting migration to another provider.

In most cases, details of the exit process are contained in the Termination clause that is part of the Customer Agreement. All Termination clauses define two basic types of termination:

- **Termination for Convenience.** Consumers can typically stop using cloud provider services at any time. Likewise, cloud providers may terminate the agreement for convenience at any time without liability to the consumer. Advance notice is typically given before termination occurs (usually 30 days). In some cases, consumers may be required to pay a penalty if they terminate an agreement for convenience.

- **Termination for Cause.** Either party may terminate the agreement if there is a material default or breach of agreement by the other party, and that party fails to cure the breach within a certain time period after receipt of notice (typically, 30 days). In some cases, for example when security violations are alleged, the provider gives itself the right to suspend services immediately in order to protect itself and other consumers, pending resolution of the incident or termination of the agreement.

The effect of termination is that all rights under the agreement terminate at the end of the notice period. The consumer is responsible for all fees and charges incurred through the date of termination. Any cloud provider content the consumer has in its possession must be immediately returned or destroyed.

The level of assistance given by the provider during the termination phase varies significantly. In all cases, the onus is on the consumer to extract their content.
Recommendations

When evaluating the termination policies, consumers should consider the following best practices:

- Consumers should ensure their agreement specifies that advance notice will be given for all terminations initiated by the cloud provider (minimum of 30 days).

- Consumers must put in place contingency plans and procedures to find a new service (or bring the service back in-house), extract and reload their data, and switch to the new service within this time window.

- As part of the termination process, providers should offer assistance to consumers to facilitate data extraction (e.g., clear and concise migration documentation, or assistance from a professional services department).

- The agreement should specify that all data and information belonging to the consumer will be maintained for a specific time period after transition (in case it takes some time to discover a problem with the initial extraction process), and then be completely removed immediately after.
  - The typical data retention period is 1 to 3 months, which gives the consumer sufficient time to verify that all data has been correctly migrated to a new service.
  - Only with the consumer’s written notice should data be removed and destroyed before that time.

- At the completion of the exit process, consumers should receive written confirmation from the provider that all of the consumer’s data, including analytical and statistical information derived from it, has been completely removed from the provider’s systems.
References

Foundation Materials


Cloud Service Agreements


**Papers and Articles**


## Appendix A: Analysis of AUP Content

This table contains key observations and actual language examples contained in public cloud AUPs.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Key Observations</th>
<th>Example Language</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content-Based Prohibitions</strong></td>
<td>Every AUP analyzed had some form of prohibition of unacceptable content. Some AUPs described in detail specifically prohibited content types, while others were general policies that put the determination of acceptable content under the subjective control of the cloud provider.</td>
<td>“You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like ‘spam’), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission.”</td>
</tr>
<tr>
<td><strong>Security-Related Prohibitions</strong></td>
<td>Most AUPs contained wording that specifically prohibits activities that would compromise the security of the service itself or the security of another organization, or both.</td>
<td>“You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a “System”). Prohibited activities include: Unauthorized Access; Monitoring of data or traffic; Falsification of Origin.”</td>
</tr>
<tr>
<td><strong>Service Integrity Prohibitions</strong></td>
<td>Most AUPs included specific prohibitions against doing harm to the service itself. These were mostly related to performance (such as network abuse or attack), but sometimes they included attempts to bypass service limitations which could jeopardize the quality of the service for others.</td>
<td>“You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include: Monitoring or Crawling; Denial of Service (DoS); Intentional Interference; Avoiding System Restrictions.”</td>
</tr>
<tr>
<td><strong>“Rights of Others” Prohibitions</strong></td>
<td>Many, but not most, of the services contain some level of prohibition against violating the rights of other people. This is separate and distinct from violating the service levels of others, and reaches into their own legal rights as fellow humans.</td>
<td>“Customer agrees not to, and not to allow third parties (including End Users) to use the Services to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act).”</td>
</tr>
<tr>
<td><strong>Other Prohibitions</strong></td>
<td>There was a wide range of additional prohibited activity unique to some of the AUPs. In many cases those items fell into general category, prohibiting things such as “Abuse” in general, or “Other activities.”</td>
<td>“Prohibited uses and activities include, without limitation, any use of the Services in a manner that, in our reasonable judgment, involves, facilitates, or attempts advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful.”</td>
</tr>
</tbody>
</table>
## Appendix B: Analysis of Cloud SLAs

This table contains key observations and actual language examples specific to Cloud SLAs.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Key Observations</th>
<th>Example Language</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Commitment</strong></td>
<td>All of the cloud service commitments reviewed focused exclusively on uptime/availability.</td>
<td>“If in any month the availability percentage is less than 99.9%, Consumer is eligible to receive a Service Credit...”</td>
</tr>
<tr>
<td></td>
<td>• Uptime/availability is expressed as a percentage</td>
<td>“Customer will receive a service credit for the period of time starting when a Case is filed requesting assistance in accessing Customer data until the service is reinstated.”</td>
</tr>
<tr>
<td></td>
<td>• Typical percentages included 95.0%, 99.9%, 99.95%, and 100%.</td>
<td>’’Monthly Uptime Percentage’ means total number of minutes in a month, minus the number of minutes of Downtime suffered from all Downtime Periods in a month, divided by the total number of minutes in a month.”</td>
</tr>
<tr>
<td></td>
<td>• The uptime/availability percentage is typically measured on a monthly basis (one SLA measured it on a yearly basis)</td>
<td>’’Downtime’ means more than a ten percent Error Rate for any Eligible Application.”</td>
</tr>
<tr>
<td></td>
<td>Uptime/availability is measured differently across the SLAs that were reviewed:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Based on the total minutes the service is unavailable over a billing cycle (e.g., per month)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Based on the total number of errors divided by the total number of requests during a specific time interval</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Based on the elapsed time from when a case is filed until the service is reinstated.</td>
<td></td>
</tr>
<tr>
<td><strong>Credits</strong></td>
<td>Service credits are the sole form of compensation for missed service commitments across all the SLAs that were reviewed.</td>
<td>“If the availability percentage is less than 99.9%, Consumer is eligible to receive a Service Credit in an amount equal to the prorated sum of the per hour charges for the base compute resource for all Instances for the number of the Qualified Outage Minutes.”</td>
</tr>
<tr>
<td></td>
<td>• Calculation of service credits differs significantly, including tiered credit of 10%, 25%, and 50%; prorated credit based on unavailability; 5% of fees for each 30 minutes of downtime.</td>
<td>“The aggregate maximum number of Financial Credits to be issued to Customer for any and all Downtime Periods that occur in a single billing month shall not exceed 50% of the amount due by Customer for the Application for the applicable month.”</td>
</tr>
<tr>
<td></td>
<td>• In all cases, the maximum credit cannot exceed 100% of the monthly service charge. In some cases, the maximum credit is lower (50% maximum in one instance).</td>
<td>“The minimum period of Failure eligible for a credit is 15 minutes, and shorter periods will not be aggregated. The maximum credit for any single Failure is one month’s Service fees.”</td>
</tr>
<tr>
<td></td>
<td>• In most cases, if more than one SLA is impacted by an incident, only one SLA service credit can be claimed.</td>
<td></td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td><strong>Key Observations</strong></td>
<td><strong>Example Language</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Credit Process** | All of the SLAs that were reviewed required the consumer to take specific action:  
  - Consumer is required to identify and report failures.  
  - The timeframe for reporting failures varied significantly: 48 hours, 5 days, 7 days, 30 days, 10 business days after the end of the billing cycle in which the errors occurred, fifth day of the month following the month in which the failure was observed, etc.  
  - Consumer must provide “proof” of breach including dates/times, server request logs, network trace routes, full description of service interruption, the duration of the Incidents, and, in the case of PaaS SLAs, the names of affected databases, failed operations, etc.  
  - Cloud provider reviews claims and makes final, good faith judgment on service credits. | “To be eligible to claim an SLA credit due, the Customer’s master administrative user must open an SLA ticket located inside the Customer portal within seven (7) days of the claimed outage. Customer must include service type, IP Address, contact information, and full description of the service interruption including logs, if applicable.”  
 “To submit a Claim, Customer must contact Customer Support and provide notice of its intention to submit a Claim. Customer must provide to Customer Support all reasonable details regarding the Claim, including but not limited to, detailed descriptions of the Incident(s), the duration of the Incident, network traceroutes, the URL(s) affected and any attempts made by Customer to resolve the Incident.” |
| **Exclusions**    | For the most part, exclusions are similar across all of the SLAs that were reviewed. The following events are typically excluded:  
  - Factors outside of the provider’s reasonable control.  
  - Force majeure conditions.  
  - Any actions or inactions of the consumer or any third party resulting in the outage.  
  - Consumer and/or third-party equipment, software or other technology contributing to the failure.  
  - Customer’s refusal to allow provider to perform maintenance deemed necessary to maintain the Service, whether scheduled or emergency. | “Other activities, customer directs, denial of service attacks, natural disasters, changes resulting from governmental, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties, and other force majeure events.”  
 “The SLA does not apply to any errors: (i) caused by factors outside of provider’s reasonable control; (ii) that resulted from Customer’s software or hardware or third party software or hardware, or both; (iii) that are result of abuses or other behaviors that violate the Agreement.” |
## Appendix C – Security

This table contains key observations and actual language examples about key security issues.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Key Observations</th>
<th>Example Language</th>
</tr>
</thead>
</table>
| Responsibility for security of the other party | Most agreements are asymmetrical: the customer is responsible for protecting the provider, and must notify the provider in case of breach, but not the other way around. A few providers commit to informing the customer promptly in case of a security breach, and to provide all information available to them about what happened. Some providers, as part of a higher-tier support agreement, assign a contact person with responsibility to administer security (e.g., manage user accounts). | “…we and our affiliates are not responsible for unauthorized access to your account. You will contact us immediately if you believe an unauthorized third party may be using your account or if your account information is lost or stolen.”  
“This SLA does not cover (without limitation): ... failures due to denial of service attacks.”  
“You are responsible for determining whether our security meets your requirements.”  
“We do not promise that the Services will be uninterrupted, error-free, or completely secure” |
| Business risk and liability     | Providers assume no responsibility for “making the customer whole” if there is a breach for which they are responsible. Some providers include unspecific assurances that they will assist the customer. Most providers shield themselves from liability, in more or less explicit terms. The language at right is one of the bluntest expressions of this liability limitation. | “We minimize business risk through appropriate procedures, giving you peace-of-mind and allowing your team to focus on what they do best.”  
“...Under no circumstances... shall [provider] or its suppliers be liable to customer or any other person for any indirect, special incidental, exemplary, punitive or consequential damages of any kind...” |
| Restoration of lost data        | Most providers ignore the issue of restoring data that may have been deleted as a result of a security breach. Some explicitly deny having to do anything.                                                                 | “… Under no circumstances will [provider] be responsible for the restoration of any data to cloud storage or for the loss of any data.” |
| Physical security measures      | Most providers are silent about their physical security measures, or about the personnel screening measures they perform to avoid insider attacks. The language at right is a positive exception. | “[Provider] will ensure the presence of a professional security guard in the computer server hosting facilities at all times, charged with enforcing [provider’s] security policies.” |
# Appendix D – Privacy

This table contains key observations and actual language examples about key privacy issues.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Key Observations</th>
<th>Example Language</th>
</tr>
</thead>
</table>
| **Information collected from the customer about himself** | Most agreements specify in some detail the kind of information collected by the provider about the customer itself, and necessary to conduct business, including contact information and billing information. These agreements go on to justify this practice, and to define what the provider may or may not do with this information. | "We may use your Confidential Personal Information to provide you with and manage the services you request, communicate with you ..., personalize the content we deliver, conduct industry or consumer surveys, manage, improve and troubleshoot our network and services, enforce our Terms of Service, or for any purpose otherwise permitted or required by law.”  
"The Receiving Party shall not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement.”  
"Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential.”                                                                 |
| **Information concerning third parties that may be stored by the cloud provider** | Many SaaS applications (collaboration, CRM, ERP, Web conferencing, etc.), as well as IaaS storage services, will result in private information about the customer’s own customers, employees, suppliers, etc., being held by the provider. Yet most agreements make no mention of any protection given to that data. In some cases, the agreement spells out that the Customer needs to protect its own customers, even though it doesn’t say that the Provider is doing so itself (the third example at right is the most egregious in this respect). | "Customer will protect the privacy and legal rights of its End Users under all applicable laws and regulations.”  
"The Customer acknowledges and agrees that the Customer is solely responsible for any personal information that may be contained in the Content...”  
"[Provider] cannot commit to particular confidentiality obligations regarding any Content or Customer confidential information.”                                                                                                                                                                                                 |
| **Location information**                          | Some agreements explicitly acknowledge that the provider may know where the user is located when they interact with the service. There is no assurance that this information will not be exploited.                                                                                   | “When you download or use apps created by [provider] or our subsidiaries, we may receive information about your location and your mobile device.”                                                                                                                                                                                                 |