Appendix F. Cloud Provisioning Contracts

A *cloud provisioning contract* is the fundamental agreement between the cloud consumer and cloud provider that encompasses the contractual terms and conditions of their business relationship. This appendix drills down into the common parts and sections of a generic cloud provisioning contract and further provides guidelines for choosing a cloud provider (partially based on the contents of cloud provisioning contracts).

F.1. Cloud Provisioning Contract Structure

A cloud provisioning contract is a legally binding document that defines rights, responsibilities, terms, and conditions for a scope of provisioning by a cloud provider to a cloud consumer.

As shown in Figure F.1, this document is typically comprised of the following parts:

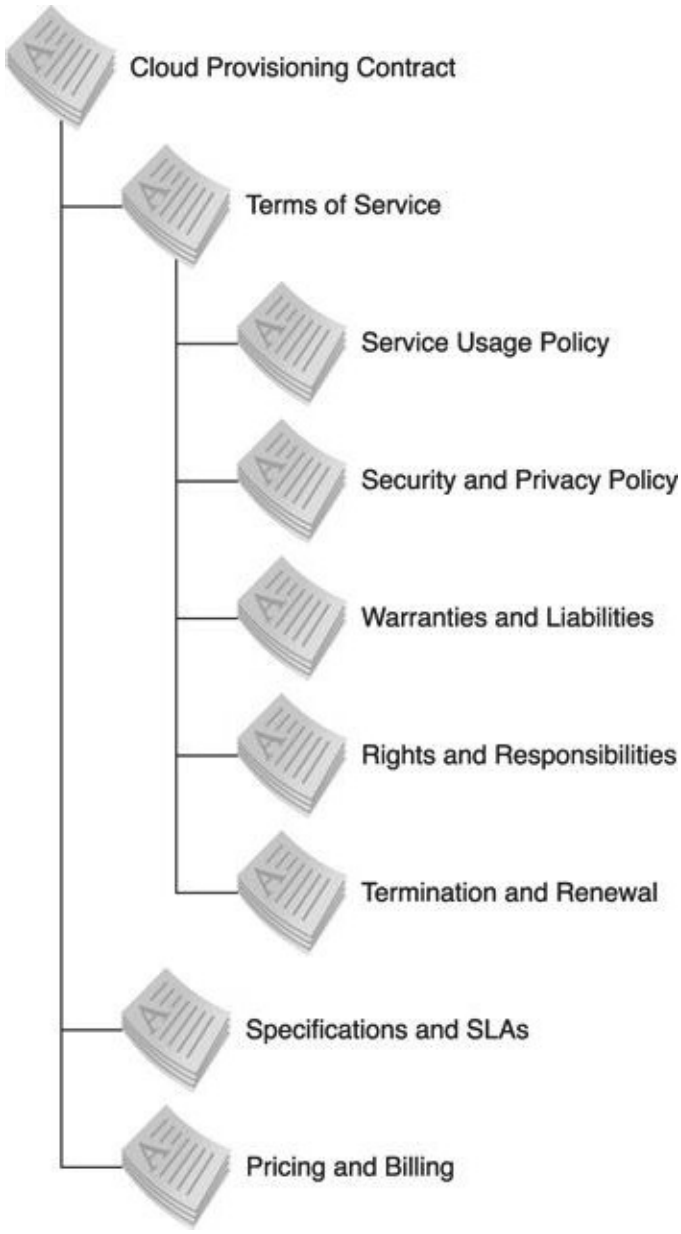

Figure F.1. A sample cloud provisioning contract table of contents.

- *Technical Conditions* – specifies the IT resources being provided and their corresponding SLAs
- *Economic Conditions* – defines the pricing policy and model with cost metrics, established pricing, and billing procedures
- *Terms of Service* – provides the general terms and conditions of the service provision, which are usually composed of the following five elements:
  - *Service Usage Policy* – defines acceptable service usage methods, usage conditions, and usage terms, as well as suitable courses of action in

response to violations

- *Security and Privacy Policy* – defines terms and conditions for security and privacy requirements
- *Warranties and Liabilities* – describes warranties, liabilities, and other risk reduction provisions including compensation for SLA non-compliance
- *Rights and Responsibilities* – outlines the obligations and responsibilities of the cloud consumer and cloud provider
- *Contract Termination and Renewal* – defines the terms and conditions of terminating and renewing the contract

Cloud provisioning contracts are usually based on templates and provided online, where they can be accepted by cloud consumers with the click of a button. These contracts are, by default, generally geared to limiting the cloud provider's risk and liability. For example, common clauses that specify the provisioning and responsibilities in contract templates include:

- Cloud services are provided "as is" without warranty.
- Liability limitations do not offer compensation for most kinds of damage.
- Warranties are not provided for performance metrics.
- Warranties are not provided to guarantee service continuity.
- The cloud provider has minimal to no responsibility for data security breaches and damages incurred from these events.
- The cloud provider can unilaterally modify the terms and conditions without prior notice.

Furthermore, typically slack data privacy warranties and clauses permit the "sharing" of cloud-based data and other potential threats to data privacy.

Terms of Service

This part defines the general terms and conditions that can be broken down into the following sub-sections:

Service Usage Policy

A service usage policy, or acceptable use policy (AUP), comprises definitions of acceptable methods of cloud service usage, including clauses with stipulations such as:

- The cloud consumer shall be solely responsible for the content of the transmissions made through cloud services.

- Cloud services shall not be used for illegal purposes, and any transmitted materials shall not be unlawful, defamatory, libelous, abusive, harmful, or otherwise deemed objectionable by third parties or legal regulations.
- Cloud service usage shall not infringe on any party's intellectual property rights, copyrights, or any other right.
- Transmitted and stored data shall not contain viruses, malware, or any other harmful content.
- Cloud services shall not be used for the unsolicited mass distribution of e-mail.

Some elements of the service usage policy that cloud consumers may need to review and negotiate include:

- *Mutuality of Conditions* – Conditions should be identically applicable to the cloud consumer and cloud provider, since the actions and business operations of one party directly impact the operations of the other.
- *Policy Update Conditions* – Even though many contract templates state that policy updates do not require advance notice, unilateral modifications to cloud service usage terms and conditions can be detrimental for cloud consumers. Cloud consumers should formally acknowledge any changes before they are applied to the policy, especially for larger contracts.
- *Actions in Response to Violation* – Specifications on how violations are detected and notified, how much time is allowed to issue and carry out corrective responses, and cloud service termination conditions in the event of non-compliance.

Security and Privacy Policy

Conditions pertaining to security and privacy can be complex and difficult to define in measurable terms. Therefore, these issues are commonly isolated in a dedicated section of the cloud provisioning contract.

Many contract templates are designed to favor the cloud provider by limiting their liability and warranties in the event of data breaches and other security violations. It is not uncommon to have loose or vaguely defined security and privacy specifications that oblige the cloud consumers to be responsible for security-related cloud service configuration and usage. Some contract templates even contain policies that grant the cloud provider the right to share cloud consumer data with third parties using generalized, subjective, and/or ambiguous terms, under conditions that were deemed necessary to:

- prevent fraud and/or other illegal activities

- prevent imminent bodily harm
- protect other cloud consumers from security and privacy policy violation

An important policy criterion is making sure that the multiple levels of the cloud architecture are differentiated, since policies often need to encompass and address a broad range of data security concerns.

Common issues that require additional consideration when assessing and negotiating security and privacy policies include:

- *Security Measures* – Policies need to clearly describe the cloud provider's measures for protecting cloud service operations and cloud consumer data, and further identify those that are the cloud consumer's responsibility.
- *Access Control* – The different ways of accessing cloud services, the cloud mechanisms that control and monitor usage, and any data the cloud services manipulate all need to be well-defined.
- *Vulnerability Control* – The cloud provider's methods for handling security vulnerabilities and any patching approaches required by the cloud consumer need to be documented.
- *Data Transfer* – Security policies on data entering and leaving the cloud need to address how the cloud provider intends to defend against insider and external threats during data transmission.
- *Data Security* – Policies need to clearly define the management of data ownership and the warranties that protect information security, which pertain to issues concerning:
  - *Data Access* – when and how to access data, and the optimal format for reducing the risk of cloud provider lock-in
  - *Data Blocking Conditions* – conditions for blocking data access
  - *Data Classification* – ownership and confidentiality requirements that differentiate between public and private data
  - *Technical and Organizational Measures* – controls to ensure the confidentiality and integrity of data in cloud storage, transmission, and processing
- *Disclosure of Data* – Conditions for disclosing cloud consumer data to the cloud provider and third parties, including:
  - *Law Enforcement Access*
  - *Confidentiality and Non-Disclosure*
- *Intellectual Property Rights and Preservation* – Original software that is

created on IaaS and PaaS platforms can be exposed to and potentially exploited by cloud providers and third parties.

- *Data Backup and Disaster Recovery Procedures* – This policy needs to outline the terms to adequately provision for disaster recovery and business continuity planning to preserve service continuity. These provisions should be detailed and specified at lower levels. Most often, these are related to the use of data replication and resilient implementations in different geographical locations.
- *Change of Control* – This policy needs to clearly define how the cloud provider will honor contractual obligations in the event of a change of control and/or ownership, as well as terms of contract termination.

Warranties and Liabilities

Many contract templates state that services are to be provided "as is" without any guarantees. The limitation of liability excludes most forms of monetary damage, with little or no cloud provider responsibility for data security breaches. Measurable terms of compensation are also typically absent in contract templates, while conditions of service failure and unavailability periods may be vaguely defined. One of the only recourses for cloud consumers that are receiving unsatisfactory service is to terminate the cloud provisioning contract prematurely, usually resulting in monetary penalties.

Cloud consumers can attempt to negotiate an arragement whereby part of the payment is due only when other terms of service and the SLAs are being complied with, which is an awards-based approach. This "at-risk" payment can be an effective way of ensuring that risk is being shared with or transferred to the cloud provider.

Rights and Responsibilities

This section establishes the legal duties and rights of both parties in the agreement.

The duties of the cloud consumer are generally to:

- comply with the terms of service and associated policies
- pay for the cloud services being used, in accordance with the pricing model and rates

The rights of the cloud consumer are to:

- access and use the IT resources as stated in the cloud provisioning contract
- receive reports on IT resource usage, SLA compliance, and billing

- receive due compensation in the event of cloud provider SLA non-compliance
- terminate or renew IT resource usage terms, as per the agreement

The duties of the cloud provider are to:

- comply with the terms of service and associated polices
- provide IT resources in compliance with predefined conditions
- accurately manage and report SLAs, IT resource usage, and billing costs
- compensate the cloud consumer in the event of SLA non-compliance

The rights of the cloud provider are to:

- receive payment for the IT resource usage provided, in accordance with the pricing model and rates
- terminate IT resources in the event of breach of contract by the cloud consumer, after sufficient review of the agreement stipulations

Termination and Renewal

This sub-section addresses the following:

- *Renewal Conditions* – The conditions for agreement renewal, including the maximum prices applicable to a renewed agreement.
- *Termination of Initial Term* – The expiration date for the contract, after which access to IT resources is discontinued if the contract is not renewed.
- *Termination for Convenience* – The condition for contract termination, usually as requested by the cloud consumer, without requiring the cloud provider to have been at fault or breach.
- *Termination with Cause* – The terms and conditions for contract termination due to a party's breach of the terms of service.
- *Payment on Termination* – The payment conditions for contract termination.
- *Period for Data Recovery After Termination* – The duration for which data needs to remain restorable by the cloud provider after contract termination.

Specifications and SLAs

This part of the contract provides a detailed description on the IT resources and QoS guarantees. A large section of the SLA deals with monitoring and measuring service quality metrics, with its benchmarks and targets identified.

Many SLAs that are based off of SLA templates are incomplete and use vague

definitions for QoS guarantees, such as service availability. Besides clearly identifying metrics and measurement procedures, the specifications for availability also should allow for the definition of:

- *Recovery Point Objective (RPO)* – A description of how an IT resource resumes operation after a failure, and an identification of possible types of resultant loss.
- *Recovery Time Objective (RTO)* – A definition of how long an IT resource remains non-operational upon failure.

Pricing and Billing

In addition to providing the details of the pricing structure, models, and applicable fees, the following are fundamental billing types:

- *Free of Charge*
- *Billing in Arrears/Post-Payment* (charges are issued after IT resource usage has commenced)
- *Billing in Advance/Pre-Payment* (charges are issued prior to IT resource usage)

Other Issues

Legal and Compliance Issues

When laws and regulations are applicable to how a cloud consumer will use provisioned IT resources, the cloud provisioning contract needs to provide sufficient warranties so that both the cloud consumer and cloud provider can fulfill legal and regulatory requirements. Some cloud providers use contract templates that are customizable using pre-defined criteria. For example, they may already have templates for when the physical location or geographic area proposed for the hosting of cloud consumer data raises legal concerns.

Auditability and Accountability

Auditing applications, systems, and data enables research and investigation into failure instances, causes for failure, and the parties involved. Auditability and accountability requirements are commonly present in cloud provisioning contracts and need to be assessed and discussed during contract negotiations.

Changes in the Contract Terms and Conditions

Contracts signed with large-scale cloud providers are often subject to adjustments over time, especially since these cloud providers may include a generalized clause that allows contractual modifications to be made without

prior notice.

F.2. Cloud Provider Selection Guidelines

Choosing a cloud provider can be one of the most important strategic decisions made by a cloud consumer organization. Depending on the extent to which cloud-based IT resources are adopted and relied upon, the success of a cloud consumer's business automation can be heavily dependent on the extent to which its cloud provider follows through on commitments made in the cloud provisioning contract.

This section contains a checklist of questions and considerations that can be used for evaluating cloud providers.

Cloud Provider Viability

- How long has the cloud provider been in business and how have its service offerings evolved over time?
- Is the cloud provider financially stable?
- Does the cloud provider have a proven backup and recovery strategy?
- How transparently are the cloud provider's business strategy and financial status communicated to its clients?
- Is the cloud provider subject to acquisition by another company?
- What are the cloud provider's current practices and vendor partnerships with regards to its infrastructure?
- What are the cloud provider's current and projected services and products?
- Are reviews on the cloud provider's past provisions available online?
- What type of technical certifications does the cloud provider have?
- How does the cloud provider's security and privacy policy support the cloud consumer's requirements?
- What are the capabilities of its security and management tools? (And, how mature are these tools compared to the rest of the market?)
- Is the cloud provider supporting the development or application of any relevant cloud computing industry standards?
- Does the cloud provider support auditability and security laws, certifications, and programs? These can include industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), Cloud Controls Matrix (CCM), and Statement on Auditing Standards No. 70 (SAS 70).

Negotiating multiple cloud provisioning contracts and SLAs with different cloud providers may be necessary to meet all of an organization’s specific business requirements.