Proposal for a Standard Cloud Service Agreement Template

Draft for Review

A Discussion Paper from the OMG Cloud Working Group

November 2022

Document cwg/2022-11-03 (not the final document number)

This discussion paper presents guidance that has been carefully crafted by industry and technology experts from OMG's Cloud Working Group, and approved for publication by OMG's Middleware and Related Services (MARS) Platform Task Force. While the paper has not been endorsed by OMG's Board of Directors and is not a standard, readers are encouraged to follow this guidance, participate in wider discussion on this topic, and help OMG evolve it by participating in future work of the Cloud Working Group.

Table of Contents

Copyright Notice

Acknowledgements

Development of this proposal was a collaborative effort that brought together diverse customer-focused experiences and perspectives into a single guide for cloud customers and providers. The following participants provided their knowledge and time to this effort:

- Troy Anderson – Wells Fargo
- Claude Baudoin – cébé IT & Knowledge Management
- Rick Sturgeon – Dassault Systèmes
- Steven Woodward – Cloud Perspectives

Executive Overview

This OMG Discussion Paper proposes that there should be a standard structure for a Cloud Service Agreement in order to facilitate the comparison and purchase of such services, and it presents such a structure for discussion and potential adoption.

While the paper aims to provide useful guidance in its own right (in particular, it can immediately be used by cloud service customers to assess the completeness of a CSA proposed by a cloud service provider), it also marks the beginning of discussions that may lead to an OMG standardization effort. Specifically, this proposed common structure could be integrated into an existing OMG project on Model-Based Acquisition, or if this not fully appropriate due to differences in scope or intended audiences, then it may become its own specification through one of the well-honed OMG processes to that effect: a Request for Proposal (RFP) or a Request for Comments (RFC).

OMG encourages discussion, feedback, and especially active participation in the Cloud Working Group, in order to determine the best path forward. Comments should be addressed to cloud-chair@omg.org.

Abbreviations

CSA	Cloud Service Agreement
CSC	Cloud Service Customer
CSP	Cloud Service Provider
SLA	Service Level Agreement

Background and Rationale

How Did This Come About?

OMG published, and revised twice, two Discussion Papers related to CSAs:

- The *Practical Guide to Cloud Service Agreements* [1] explained the "anatomy" of a typical CSA, based on a review of existing ones that are made publicly available by various CSPs. It explained what clauses tend to appear where, and how to interpret them to understand what the CSP is committing to deliver, what the CSC's obligations are, and where various guarantees and remedies can be found.
- A companion paper, *Cloud Service agreements: What to Expect and What to Negotiate* [2] examined in detail several dozen CSAs in order to tell CSCs where to focus the discussion with a CSP regrading clauses that might represent a significant burden or a risk or might be ambiguous. The premise of that paper was that the initial CSA presented by a CSP need not be a "take it or leave it" proposition. We attempted to explain what kinds of clauses are unavoidable, because they legitimately protect the CSP against situations that could threaten its viability, and therefore attempting to negotiate them away would be a waste of time; vs. what clauses can be negotiated, either because the CSP is planning a large purchase and therefore has leverage, or because a higher level of service can be obtained by paying more.

In subsequent discussions, the idea of going one step further emerged. Specifically, we had noted that while there was some commonality to the CSAs proposed by CSPs, it was often hard to determine where to find certain clauses. CSPs tend to offer their "standard CSA" to potential customers, but in fact those documents are not standard at all, and there does not exist (yet) such a standard from any of the usual

standard development organizations (ISO, IEEE, ANSI, etc.). In fact, ISO explicitly states that "ISO/IEC 19086-3:2017 does not provide a standard structure that would be used for cloud SLAs." Hence the reason for this proposal for such a standard structure.

Who is the Intended Audience?

Consistent with the Cloud Working Group's charter, the primary audience is made up of organizations that are adopting cloud services or considering changes in the services they use (for example, changing providers or adding a provider in a multicloud environment). For those readers, this paper can be used immediately (i.e., regardless of whether it eventually becomes a standard) in several ways:

- to assess the completeness of a proposal from a CSP, and in particular to avoid overlooking important issues that might "come and bite you" later on,
- to build a rating matrix to compare multiple proposals,
- to attach the proposed template to an RFP and request that responding CSPs follow that structure, thus making it much easier to compare the competing offerings.

The OMG Cloud Working Group also addresses itself indirectly to providers, resellers and integrators of cloud services. For this audience, the document can be used:

- to understand what their customers need to see in a proposal (and will *expect* to see once they exploit this paper),
- to have substantial internal discussions about gaps in their offerings revealed by this template, and whether the service should be upgraded or "tiered" to fill those gaps,
- ultimately, to rework their existing CSAs to conform to the proposed structure, which may result in greater credibility and authority in the market.

What the Proposed Template Is Not

The template does not stipulate what terms, conditions, guarantees, service levels, remedies, etc., should be offered. Those remain (a) at the discretion of the CSP in the first place, and (b) the subject of potential negotiation and adjustment between the parties.

This document only proposes that such terms, conditions, etc., be listed consistently by all providers, and that a minimum set of points be listed in each section using language that reduces the risk of ambiguity and conflicting interpretations.

Intended Roadmap to an OMG Standard

At the time of this paper's publication, two potential directions appear possible:

- An effort is underway, related to OMG's Unified Architecture Framework, to develop a "model-based acquisition framework." This template might form a "module" within that framework when the acquisition effort is about cloud services. However, that framework may be mostly oriented to very large organizations (government, military…) or we may discover that there isn't a good fit after all for some other reasons.
- A stand-alone OMG specification could be developed using one of the two OMG processes for this purpose: an RFP, if multiple proposals are likely to be submitted; or an RFC, if the specific criteria for this option are met (refer tom OMG's Policies and Procedures for details).

The authors expect to determine the appropriate course of action during 2023.

Proposed Cloud Service Agreement Template

The proposed template starts after the horizontal line below and ends before this document's Appendix, as indicated by another such line.

Typographical conventions:

- Text in Roman font, which mostly consists of the CSA headings, should be reproduced in the generated CSA. The CSA author may change the font to conform to their corporate guidelines. If a language other than U.S. English is used, the authors should research and use the closest possible translation. We encourage them to submit such translations of the template back to OMG, and may republish them as ancillary documents for the benefit of the worldwide cloud community.
- Text in *italic font,* within each template section, consists of explanations to guide the writer of a CSA, and should be deleted and replaced by the actual content. For a CSC, this guidance text can be used to decide whether the text inserted in its place by a CSP in their proposed CSA is responsive.

When preparing a CSA using this template, the paragraph numbering should be kept intact. If a section is not applicable, it should be marked as such, not deleted. This is in order to preserve the CSC's ability to readily compare multiple CSAs.'

Wherever appropriate, subsections may be added within the sections specified in the template. For example, in Section 2.1 (Overview of Services Provided), subsections 2.1.1, 2.1.2, etc., may be inserted for clarity.

Cover Letter

This is a free-form cover letter presenting the CSA. It is unnumbered. It does not need to be entitled "Cover Letter" since it is obvious that it is one by virtue of its placement. The cover letter should include at minimum:

- *the name and logotype of the Cloud Service Provider,*
- *the title "Cloud Service Agreement,"*
- *If the agreement is specific to a customer, the words "Prepared for:" and the name of the Cloud Service Customer,*
- *a version number,*
- *the date of preparation (for a single customer) or the last revision date (for a multi-customer document),*

- *the legal designation and address of the Cloud Service Provider, and any additional legal mentions that may be required by local laws and regulations.*

While the rest of the Cover Letter is generally at the discretion of the CSP, it may also include certain points requested by the CSC.

The cover letter should not repeat any of the material contained in the following sections.

Table of Contents

If the CSA is a single multi-part document, it should include an auto-generated Table of Contents that lists section numbers, titles, and page numbers.

1. Introduction

This is a free-form explanatory section. It may serve as a "reading guide" or as an explanation of the benefits the CSP claims as a result of contracting for its services.

2. Customer Agreement

The Customer Agreement describes the overall relationship between the CSC and CSP. Some CSPs use the title "Master Agreement," "Terms of Service," or simply "Agreement." Using the term "Customer Agreement" is recommended instead.

2.1. Overview of Services Provided

Specify the service model and the deployment model, using the terminology set by the NIST Cloud Reference Model (SaaS, PaaS or IaaS for the service model; private, public, hybrid or community for the deployment model).

If appropriate, refer to the services offered using the terminology of OMG's XaaS Glossary.

Specify the deployment technologies adopted; it is advisable to reference the appropriate sections of OMG's Practical Guide to Cloud Deployment Technologies rather than redefining those technologies, such as virtual machines, containers, etc. For an IaaS or PaaS service, specify whether the environment is virtualized or physical, single- vs. multi-tenancy, etc.

If applicable, especially if this is a PaaS service, specify how application packages are made available (e.g., WAR or GAR archives, OVF format for VMs, etc.).

List the components of the services or ancillary services provided or available, such as:

- *a private connectivity offering besides the public Internet*
- *a set of APIs*
- *security audit services*
- *data analytics*
- *self-service facilities to manage the provisioning, upscaling or downscaling of resources, accounts, etc.*
- *a test environment*

Describe any service tiers (especially If the customer can move across tiers under the same CSA).

Indicate clearly whether the services described in this section are the specific services that the customer is renting, or an exhaustive list of the CSP's offerings. And in the latter case, indicate where the subset available to the CSC, either throughout the duration of the agreement, or at a given point in time, is defined.

2.2. Scalability of the Service

This section describes the limits and mechanisms used to scale the service up or down. Is a scale change manual or automatic?

Indicate any limits on upscaling: can the CSC elect to use 2x, 10x, 100x the initial level of usage, and for how long, or is there a fixed limit to what they can use? This section may refer to Section 7.8 (Excess Usage Management).

2.3. Disaster Recovery and Business Continuity (DR/BC)

This section specifies:

- *Where are the services physically hosted*
- *What redundancy is provided across multiple locations, and whether switching to a backup location for business continuity is automatic or manual*
- *What disaster recovery infrastructure is in place at the CSP to ensure service continuity (alternate power supplies, multiple independent network connections, etc.)*

List the types of events that can result in the execution of a DR/BC plan, and what provisions are made by the CSP to address them, including:

- *natural events (fires, earthquakes, flooding)*
- *electric grid failures*
- *connectivity failures*
- *security breaches, malware attacks or denial-of-service attacks*
- *business failure (e.g., bankruptcy and liquidation)*
- *law enforcement actions, including seizure of assets.*

Describe the levels of redundancy implemented to minimize or mitigate outrages, including any hot/warm recovery sites and whether they are location in a different geographical area or in the same one, or other measures taken so that the customer data is replicated or securely backed up in a location not likely to be affected by the same disaster as the primary resource.

If there is one or more backup site, is it enabled and usable all the time as a second site (so-called active/active configuration) or is it only usable when the primary site is down (active/passive)?

The following should also be explicitly addressed:

- *What actions will be taken in the event of a prolonged disruption or a disruption with a serious business impact?*
- *What is the process of performing disaster recovery testing, and how often are the tests conducted? What tests are conducted (full, partial?) Are they automated? How are the reports of the tests provided to clients?*
- *What are the key service CSP and CSC contacts (names, phone numbers, email addresses, alternate means of contact in case of communications disruption)?*
- *What events are excluded from the guarantees in the CSA?*
- *Does the CSP provide cloud insurance to mitigate user losses in case of failure?*

How, and how often, is the DR plan tested?

This section may refer to recovery point objectives (RPO) and recovery time objectives (RTO) that will appear in Section 7.

2.4. Cost of Services

This section specifies:

- *The cost of the services during normal use, including any formulas or rules used to calculate such costs*
- *Costs for excess usage (and how they are calculated)*
- *Any applicable fees and taxes (and which jurisdiction is used to determine applicable taxes)*
- *Invoicing practices and payment terms*
- *How credit or penalties, potentially incurred by the CSP, are applied.*
- *When and how any remaining credit/debit balances are settled upon termination.*

If the CSC has (or may have) multiple accounts with the CSP, describe any provision for pooling of accounts, transfer of credits from one account to another, etc.

Describe the methods used to report, investigate and rectify inaccurate bills, or to handle objections or requests for justification, and any temporary credit that may be applied during an investigation.

2.5. Activation of Service

This section defines at what point the service will be activated, and what action may need to be taken to cause this to take place.

2.6. Excluded Services

This section provides the CSP the ability to explicitly exclude certain services that the CSC might otherwise have expected.

2.7. Renewal of Agreement

Specify in this section:

- *whether renewal of the customer agreement is automatic (tacit) or not*
- *what reminders are sent (and when) before the renewal date*
- *that any planned service changes or price changes at the time or renewal are described in the renewal notice.*

2.8. Third-Party Licenses

Declare:

- *what third-party software is licensed to the CSC as part of the agreement, if any*
- *who has the responsibility to renew such licenses*
- *who has the responsibility to perform updates, upgrades, or patches to such products? Are these updates mandatory or is there a grace period?*
- *Whether there is a test environment where the CSC can try out new versions before updating the operational environment?*

2.9. Transferability of Services

Specify the right of the CSC to transfer an unexpired agreement to a successor organization in the event their business is acquired.

Conversely, specify whether the CSP guarantees that an acquirer or successor will honor this CSA until its normal expiration.

Specify whether the agreement is bound by any regulation, such as the European Union GDPR, stipulating that CSCs must be able to change CSPs easily, or whether the CSP freely offers such a commitment.

2.10. Termination of Services

Specify the conditions under which either party may (or may not) terminate the services before the end of the specified agreement duration (if there is such a fixed term). Consider:

- *non-compliance with a commitment or definition contained in this Agreement*
- *repeated or serious failure to ensure the service levels specified*
- *the right of the CSC to terminate the agreement early if the CSP's business is acquired or divested (the CSC may not wish to do business with the new entity, which may be a competitor or may not offer the same terms)*
- *the right of the CSC to terminate the agreement after being notified of a change in the CSA that they deem unacceptable.*

Specify the notification rules and when the termination is effective.

Describe, or provide a reference to, a well-defined exit process, including the respective responsibilities of the parties. This must include detailed procedures to securely and rapidly transfer customer data and applications to another service. Service levels related to the exit process are specified in Section 7.11. This description must specify:

- *the level of CSP assistance with the exit process, and what actions if any may be billed separately. In most cases, there should be no additional cost associated with the exit process.*
- *assurance that the CSP shall be responsible for removing customer data from their IT environments, or at least helping the customer extract and erase their data by providing clear and concise documentation. Specify what form of verification is possible.*
- *the format of the data transmitted from the provider to the customer to enable portability to a new service. This should be a standard data format whenever possible, and the transmission of the data from the CSP to the CSC or a new CSP should use standard packaging and data transfer techniques.*
- *the time period (typically 1-3 months, which gives the customer sufficient time to find a new provider and to continue receiving service from the current provider in the interim) during which all data and information belonging to the customer is maintained after the termination date.*
- *that all customer data is completely removed and destroyed after that time, but only with the customer's written approval, and that this deletion is confirmed in writing.*
- *what happens to data backups, since in a multi-tenant cloud service, and depending on the backup technique used, it may not be possible to selectively erase customer A's data from a medium that also contains data from customers B and C.*

The CSA should confirm that appropriate business continuity protection continues through the exit process, and more generally that no services shall suffer degradation during the transition process (from the invocation of the termination clause to the actual end of the service).

2.11. Roles and Responsibilities

This section documents the roles and responsibilities of the CSP and the CSC, referring to the terminology of ISO/IEC 17789 or ISO/IEC 22123.

Provide a list and definition of any CSP sub-roles within those roles, and whether any roles or sub-roles are fulfilled by third parties as opposed to the CSP itself.

2.12. Service Reviews

This section describes the parties' agreement to hold regular service reviews, including:

- *their scope*
- *their frequency*
- *how they are convened and help (virtually, in person…)*
- *how the results are reported and to whom*
- *who is tasked to follow up on any action items.*

2.13. Support Services

This section describes services provided by the CSP to enable the CSC to take full advantage of the services provided. These may be services offered to all customers of the CSP, or services negotiated with the particular CSC signing this CSA.

A sub-section may be created to describe each such service, such as training, consulting, customization, data import/export, integration with other systems, special reports, etc. For each such services, specify, if known in advance:

- *the nature and description of the service*
- *its cost, and/or how it will be quoted*
- *the procedure to request the service and track the request.*

Any metrics regarding the performance of these services can be added in Section 7.4.8.

2.14. Standards and Regulations

In this section, the CSP lists standards and regulations that it complies with. Those may be:

- *industry-specific standards or regulations (e.g., PCI DSS or ANSI X9.125 in finance, or HIPAA in healthcare)*
- *region/country/jurisdiction-specific standards or regulations (e.g., GDPR),*
- *technology standards*
- *other standards and regulations requested by the customer and mutually agreed.*

Here is a non-exhaustive list of technology standards:

- *Topology and Orchestration Specification for Cloud Applications (TOSCA) from OASIS*
- *Cloud Infrastructure Management Interface (CIMI) from DMTF*
- *Open Virtualization Format (OVF) from DMTF*
- *Cloud Data Management Interface (CDMI) from SNIA*

- *Service-Oriented Cloud-Computing Infrastructure (SOCCI) from the Open Group*
- *Open Cloud Computing Interface (OCCI) from OGF*
- *OpenStack*
- *ANSI or other standards related to encryption key management, when applicable*
- *Frameworks for planning disaster recovery (such as ISO 22301:2012, NIST SP 800-34, ASIS ORM.1, ISO/IEC 27031:2011, or ISO 24762:2008*
- *The Uptime Institute's Tier III rating for the cloud data center*

Specify the reports and certificates provided by the CSP regarding each of the standards listed, including:

- *who performs the certification,*
- *how often.*

Specify whether the CSP will provide an annual Statement on Standards for Attestation Engagements 18 Service and Organization Controls (SSAE 18 SOC 2) report.

Specify the standards and regulations which the CSC is responsible to implement themselves.

2.15. Liability and Limitations

While this section is typically boilerplate text from the CSP's legal department, the following should be specified:

- *CSP liability in case of a security breach, in particular if that breach is the result of negligence (unpatched system, etc.)*
- *That the CSP is jointly and severally liable with any subcontractors.*

Limitations of liability shall be specified, including:

- *Consequences of emergency power or network outages*
- *Force majeure*
- *Suspension of service due to legal reasons*

2.16. Indemnification

This is typically boilerplate text from a legal department, and must be reviewed by the other party's legal department.

2.17. Jurisdiction

Another boilerplate clause, which indicates where (in the courts of which jurisdiction) legal recourse may be pursued. Do not specify vague jurisdictions, such as the name of a country in which there may be different contract laws according to the state or province.

2.18. Insurance

This section declares and describes what relevant insurance policies are held by the CSP, including cyber insurance.

Specify whether the CSP or a third party offers optional insurance against business losses resulting from a failure or underperformance of the contracted services.

2.19. CSA Change Management

This section specifies how this document may change over time, including:

- *the scope of changes that may be implemented, such as:*
    - *addition or end of life of a service, feature, or functionality*
    - *change of functionality of a service, API, etc.*
    - *change of service level objectives*
    - *change of pricing*
    - *change of any other terms in the CSA*
- *any predetermined periodic revision schedule,*
- *how much advance notice is given of a proposed change before it is enacted,*
- *the right of the CSC to discuss, negotiate, or reject the changes,*
- *whether rejection implies termination of the agreement (in which case Section 2.10 applies)*
- *the ability of the customer to continue to receive the services under the initial agreement until termination.*

3. Acceptable Use Policy

This policy must specify three things:

- *which activities, or uses of the provided resources, are not allowed by the CSP – for example, spamming, distribution of malware, or illegal activities (specify which laws are being considered for this last case),*
- *the actions the CSP may take in case of a violation of this policy,*
- *the procedures available to the CSC to appeal such measures so as to avoid disruption to its business if the CSP was incorrect in its assessment of the activities in question.*

4. Data Handling Agreement

This section specifies the measures and guarantees related to the handling of the customer's data by the provider. A preamble to this section may indicate that data security measures are specified in Section 5.4.

4.1. Data Integrity and Preservation

Describe the methods and procedures used to minimize the risk of data loss or corruption, including integrity checks and backups or redundant storage.

For backups, specify the types of backups (partial or full), their frequency, the media used, the storage location, the retention period, how has access to the backups, and the procedures to be invoked to restore data, as well as to test the availability and integrity of backups/

Specify what tasks (if any) are required of the customer to ensure that the effectiveness of these measures.

Describe any testing capabilities offered to the customer to test the data preservation measures.

Specify that in the event of a dispute between the CSP and CSC, the customer's data will remain available to the customer at all times.

4.2. Data Availability and Portability

Specify in which formats and media types the CSC's data is stored, if this is under the CSP's control (this may not apply to an IaaS service), and other relevant information to ensure that data can be reused on a different platform.

Include how encryption keys and other security information) is stored, including standard formats to ensure data portability.

For a SaaS offering (where the data structure and format is part of the application design under the cSP's control) indicate the type of database management system or file system used.

4.3. Privacy and Confidentiality

Specify which data about the customer is collected by the provider, for what purpose, for how long, and how that data is protected so that it is only available to those with a need to know it.

For data about third parties stored by the customer using the provider's services (e.g., personal data about the customer's employees, partners, or its own customers) specify how the provider ensures that this data cannot be accessed or exploited by its personnel, including system administrators.

Declare which laws and industry regulations on data protection the CSP complies with (e.g., HIPAA, GDPR, CCPA, etc.).

4.4. Data Residency

This section shall list the locations where the customer's data may be stored (including backup locations), or through which it may transit. This includes locations from which a system administrator or support agent may be able to view the data as part of their work.

Indicate the potential consequences of storing data in, or transmitting data through, countries or jurisdictions other than those where the customer operates. In particular, indicate:

- *whether there are restrictions placed by the country/jurisdiction of origin of the data against "exporting" certain types of data to the country/ jurisdiction where the data may reside,*
- *whether the country/jurisdiction where the data may be located (at rest or in transit) imposes certain restrictions, such as prohibitions against encryption, right of inspection by authorities, etc.*

If needed, this section may refer to an appendix listing the applicable data residency laws and regulations. Any measures taken by the CSP to avoid negative consequences should be indicated.

Specify whether the customer may elect <u>not</u> to store or send their data in/through certain countries or jurisdictions. Describe how to request such exclusions and any associated costs or impact on the services provided and their service levels.

The CSP should commit not to change the list of data storage/transit locations without informing the customer well in advance and giving the customer an option to reject the change or terminate the agreement.

If data can be stored in multiple locations, specify whether a facility is offered to the customer to query the location of a given piece of data, or whether reports are provided periodically indicating where the customer's data is stored.

4.5. Data Seizure

Specify the notifications provided by the CSP if it receives a request or order from law enforcement authorities or other government agencies to surrender data that belongs to the CSC.

In particular, declare whether the CSP is subject to U.S. Cloud Act of March 2018 (under this Act, all cloud providers are obligated to surrender data requested by U.S. law enforcement agencies, regardless of data location), or similar laws.

Specify what measures the CSP will take to assist the customer by objecting to such measures or delaying the execution of the data seizure through appropriate legal means.

4.6. Third Party Use of Data

Declare whether the CSP is sharing any of the data pertaining to the customer with marketing partners or other third parties, and how the customer can deny such information sharing.

5. Security

5.1. Security Governance

Describe in this section:

- *the overall security principles applied by the CSP*
- *the security controls implemented to ensure security of the services and of the data*
- *the methods used for risk management*

It is highly recommended to include, here or in an Appendix, the CSP's responses to the Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ).

Describe how the CSP and CSC shall cooperate so that the CSP is fully aware of the CSC's security requirements, including its data security classification matrix (if any).

5.2. Physical Security

Describe the methods used to physically secure the CSP's computing resources, including how facilities are locked and alarmed, and how authorization to access them is granted, managed, logged, and revoked.

5.3. Access and Authorization Credentials

Specify the authentication mechanism for users of the service: is there a mechanism to synchronize authorization and access rights granted internally by the CSC, through some form of identity federation? Or does the CSP manage authorization and access credentials, based on requests from the CSC?

Specify whether access is identity-based or role-based.

Specify any special access rights given to:

- *CSP system administration staff or managers,*
- *CSC system administration staff or managers,*
- *any third parties, such as contractors.*

For each type of access granted to a user or administrator, indicate the authentication mechanism: username/password, hardware token, multi-factor authentication, etc.

Describe how any such access is requested, validated, granted, recorded, and revoked. Response times for provisioning and de-provisioning of access rights must be specified in Section 7.4.3 (security service level metrics).

5.4. Data Security

This section shall describe all measures taken to endure the security of the customers data.

In particular, describe data encryption capabilities, whether they are applied by default or at the customer's request. Alternately, in an IaaS/PaaS service, this section may specify that encryption is entirely under the control of the customer.

Specify whether data is encrypted at rest, in transit (between the CSC and the CSP, or between multiple CSP facilities), or both, and on backup media.

Declare whether the CSP or the CSC are limited in the strength of encryption they can use due to any applicable laws and regulations, and whether there is an obligation to place decryption keys under escrow with a government authority.

If the CSP is responsible for data encryption, or offers to be responsible for it by agreement with the customer, then specify who generates, holds and manages the keys. Is there a root key, key-encrypted keys, etc.? Does the CSP hold a Federal Information Processing Standard (FIPS) certification or a similar certification valid in other jurisdictions where it or the CSC operate?

5.5. Software Security

Specific the security measures used to ensure that any software code provided or used by the CSP is free of malware and vulnerabilities. This applies to application code in the case of a SaaS service, as well as to management tools developed by the CSP.

Does the CSP use the NIST Common Vulnerability Enumeration (CVE) and test its software against it, or the Common Vulnerability Scoring system (CVSS)?

Describe any security controls in place (e.g., from NIST SP 800-53, NIST SP 800-171, ISO 27001, CIS Security Controls, or the CSA Cloud Controls Matrix).

5.6. Security Auditing

Describe what periodic or continuous assessments/audits are performed, including vulnerability detection and penetration tests, who performs them (the CSP or an independent third party), and how the results are made available to the CSC?

Specific whether the CSC has a right and the ability to inspect/audit the CSP themselves.

Alternatively, declare any self-assessment certifications, such as recorded in the CSA STAR repository.

5.7. Security Incident Notification and Recovery

Specify how and when the CSP shall notify the CSC of the occurrence of any breach of its system, regardless of the parties or data directly impacted.

The CSP should commit in this section to:

- *include specific pertinent information in the incident notification,*
- *stop the data breach as quickly as possible (and inform the customer of its progress in doing so),*
- *restore secure access to the service as soon as possible,*
- *apply best-practice forensics in investigating the circumstances and causes of the breach,*
- *make long-term infrastructure or procedural changes to correct the root causes of the breach to ensure that it does not recur.*

6. Integration Capabilities

Specify the service and data integration mechanisms (APIs, web services, etc.) offered to facilitate integration between the CSP's services and the CSCs, or between the CSP's systems and those of other CSPs (e.g., in a multicloud architecture).

Indicate what standards are followed (e.g., from W3C or OASIS). Indicate whether there are specific security provisions that go along with such integrations (e.g., to authenticate the requester).

7. Service Level Agreement (SLA)

Note: if the CSA describes multiple tiers of services (e.g., "bronze, silver, gold") that the CSC may choose from, then various sections below may contain tables showing the committed service levels for each tier.

7.1. Service Guarantees

Specify whether different service levels apply to different services, and/or which services are not covered by the rest of this section. These distinctions may apply to:

- *testing or pre-production environments vs. the production environment,*
- *ancillary services such as performance testing, analytics, security scanning, backup, virtual desktops, etc.*

7.2. Subcontractor Service Level Agreements

Specify whether some services are provided by subcontractors, and whether such parties are bound by the service levels specified in this section, or are covered by distinct SLAs.

7.3. Conformance to Standards

Specify how, if any service is defined in terms of conformance or compliance with a standard, how the CSP maintains this conformance or compliance if that standard changes.

The CSP should commit to:

- *inform the CSC as soon as it knows that a change causes the CSP to no longer be compliant,*
- *let the CSC know of its plan to bring its practice into compliance (including target dates), or whether they reserve the right to not upgrade.*

7.4. Service Metrics

Notes: Whenever possible, each metric shall be described with the following elements:

- *name*

- *limitations (e.g., excluded elements or time periods)*
- *measurement/collection method (included any standards used)*
- *frequency of collection*
- *clarification or comments*
- *how non-performance results in incident reporting and remedies (or how above-expected performance results in bonuses, if there are such provisions)*

For all applicable metrics, the metric definition shall be specific, unambiguous, and measurable. In particular:

- *Measurement time windows must be specified – for example, a "day" may be a moving 24-hour window, or a midnight-to-midnight interval, and these alternate definitions can result in different numbers; similar ambiguities must be avoided for all time units, such as weeks, months, years).*
- *If certain periods are excluded from the measurement (nights, week-ends, holidays, etc.), this should also be specified beyond any ambiguity.*
- *When referring to concepts such as "working hours," "weekdays," "holidays," etc., the reference time zone or the reference calendar (e.g., "U.S. federal holidays") must be specified since their definitions vary across regions.*

Certain service metrics may be irrelevant for the services provided under the CSA. In that case, the subsection in question should not be deleted, but should be marked "Not applicable.

7.4.1. Availability Metrics

Specify the guarantees of percentage of uptime, and over which measurement windows.

Specify the maximum time needed to reboot a computation or storage server.

Include a table in case there is a distinction between critical services vs. other services to which a lower uptime guarantee applies. In particular, indicate whether some features be disabled at times under certain circumstances (e.g., partial failure of the infrastructure, network slowdown, etc.)

Specify whether there are "scheduled downtime" periods excluded from the computation, and whether this applies only to fixed time periods, or to any period notified in advance (how long in advance?) by the CSP.

In case of a service failure, indicate the RPO (recovery point objective) and RTO (recovery time objective).

7.4.2. Performance Metrics

Specify response time commitments that are appropriate for the type of service (SaaS, PaaS, IaaS) provided. This may include:

- *Computing performance – e.g., processing speed, including under peak loads.*
- *Network performance: bandwidth, latency, packet loss, mean/maximum jitter) both internally (e.g., data transfer speeds between a compute server and a storage network) and externally (to/from the Internet, or end-to-end between the CSP and CSC)*
- *Storage performance: input/output speeds, backup and restore performance (time taken to backup or restore a terabyte), database performance (number of queries or updates per second), etc.*
- *Application response time (when the application is under the control of the CSP, i.e., in a SaaS offering). Indicate how response time is measured (from where to where) and whether a specific application benchmark used. Address any response time that matters to the quality of the*

service experienced by the customer; for example, in a unified communication service (UCaaS), the customer cares about delays in voice, video, or instant message transmission.

- *Response times of any other relevant components of the service, such as the response time of an API call, etc.*

7.4.3. Security Metrics

Specify metrics related to the performance and effectiveness of information security management, as outlined for example in ISO 27004:2009, NIST Special Publication 800-55, or the CIS Consensus Security Metrics.

7.4.4. Data Backup and Restoration Metrics

Specify the maximum "lag" between the time when data is modified and the time when it is captured in a backup (i.e., how "out of synch" can the backup be, or how much work may have to be redone in case of a failure followed by a data restore).

Specify the maximum time taken to restore data (as a function of the amount of data to be restored), from the time the restore procedure is invoked to the time the restored data is available for use.

In the case where resiliency is implemented through a replicated storage scheme, specify the maximum time required to bring online a new complete and operational replica if the primary storage failed and the system switched over to using the original replica, (i.e., the time during which there only one copy in place).

7.4.5. Agility Metrics

This section specifies the guarantees of response time to various change requests:

- *provisioning of a new service*
- *upscaling or downscaling of a service (e.g., adding/deleting a server, a storage medium, etc.)*
- *addition and enablement of a new user account*
- *customization of an application (or at minimum the time taken to respond to the request and provide an implementation plan)*
- *… or any capability within the scope of the contracted services*

7.4.6. Service Monitoring – Metrics Collection and Reporting

Indicate the monitoring practices and tools implemented by the CSP to measure the performance of the services and ensure that the committed service levels are respected. Indicate the frequency and granularity of the monitoring (e.g., aggregate data vs. detailed data per server or per component, instantaneous data vs. averaged data, etc.).

Indicate how the monitoring results are made available to the customer (periodic reports, API, web services, access to an online dashboard, etc.).

Specify whether the CSC has the ability to perform their own monitoring, and how (through APIs, web services, or by deploying monitoring tools that monitor the services' performance or detect incidents. If such tools are allowed but the CSP wishes to limit the impact of those tools, specify such limits (e.g., frequency of "pings," amount of data sent/retrieved during monitoring/measurement actions, etc.)

7.4.7. Accuracy

Specify the margins of error, if any, for the measured data.

7.4.8. Additional metrics (for additional services in 2.12 in particular)

Specify here any metrics related to additional services (such as those listed in Section 2.13) that do not fit within Sections 7.4.1 through 7.4.5.

7.4.9. Metrics Discrepancy Resolution

Specify:

- *how the CSC may report measurements that differ from those reported by the CSP*
- *in that case, how the CSP can obtain the CSC's measurements in order to investigate the discrepancy*
- *the process to resolve the difference and reach agreement on the correct value of the metric.*

7.5. Change Management

Specify any changes that can be predicted (e.g., certificate renewal, service password changes, scheduled quarterly or annual application upgrades, etc.).

Specify which changes are expected to require downtime or a temporary degradation of the availability or performance of one or more components of the service.

Specify who is responsible for the testing of changes to the cloud configuration and architecture, and in particular what changes are tested by the CSP or jointly, and how (use of a "sandbox" environment, unit testing, regression testing, integration testing, …) to verify that they will not cause a failure or degradation of the services.

Specify:

- *how and when (how much in advance) the CSP notifies the CSC of an impending change,*
- *whether the CSC has the ability to request a delay in implementing the change, due to a perceived risk of disruption during a critical time for its operations, and in that case, how long that delay may be, how much flexibility the CSC need to offer, etc.,*
- *how the CSP informs the CSC of the execution of the change, and of its success or rollback.*
- *whether there are any special communication procedures for the CSC to report unexpected behavior during the execution of the change.*

Conversely, specify what changes the CSC should inform the CSP about and the equivalent of the above bullet points, reversing the roles of the parties.

Describe the change management process used by the CSP, or to be used jointly by the CSP and CSC, including:

- *responsibility for generating change requests*
- *decision process to authorize the change*
- *exceptions for emergency changes (define what constitutes an emergency)*
- *notification of impending changes, and regular reminders*
- *planning process before the change*
- *problem reporting and resolution during the change*
- *rollback decision process and procedures, when required*
- *post-mortem activities (e.g., retrospectives)*

7.6. Service Incident Management

7.6.1. Definition of an Incident

Specify what events constitute "incidents" (see below the provision for alternate terminology) for the purpose of the rest of this section, regardless of whether the CSP controls the components that might malfunction, including:

- *unavailability of all or part of the services described in Section 2.1*
- *failure of network infrastructure components*
- *failure to start an application*
- *failure to execute a service request (e.g., a web service or API call)*
- *data corruption, unavailability, or inaccuracy*
- *failure to restore data*
- *failure to restore a service after a change (planned or not)*
- *security breach, including data exfiltration, unauthorized access to resources, denial of service, key compromise, etc.*

If the CSP uses different terms to describe events of varying severity (such as "incident," "outage," "failure," etc.), provide the list of those terms together with clear definitions and unambiguous criteria to decide what category an event qualifies for. Then, assign one of those terms to each event listed above.

State whether security incidents are categorized in terms of priorities based on the NIST Common Vulnerability Enumeration (CVE) severity rating or any other similar source.

Specify which events are excluded *from the definition of a failure; for example, an outage during planned maintenance does not constitute an incident if services resume as planned, but it becomes a failure if services are not restored at the time they should be.*

It should be specified that the identification of recurring problems or negative trends during regular service reviews also constitutes an incident.

7.6.2. Incident Detection and Notification Responsibilities

Specify who must report an incident and how. This may be presented as a table, with each row corresponding to a type of incident listed in 7.6.1.

In this table (or equivalent text):

- *if the responsibility to detect and report a certain type incident lies with the provider, indicate whether it uses automated monitoring tools or manual processes to do so;*
- *if the customer is responsible for notifying the provider of an incident, whether the customer is allowed to deploy monitoring tools to automate and speed up that detection (tools that may be running at the customer's site, or on the cloud platform itself) or to engage a third party to perform the monitoring and incident detection*
- *specify what constitutes the start and end times of the incident*
- *specify the customer's role and rights in agreeing or disagreeing to declared the incident closed.*

Describe the incident notification procedure: is there an automated interface between the CSC and the CSP that transmits a notification of a service failure in either direction? Alternately, is there a trouble ticket system to which the CSP provides access, allowing the CSC to report a problem?

Specify one or more alternate notification methods in case the incident affects the primary reporting mechanism itself.

Describe how those tools and processes are tested regularly, in collaboration between the provider and the customer, such as through periodic simulations.

7.6.3. Incident Management

Describe the processes used by the CSP to manage incidents from the initial notification until resolution.

This may include an incident management matrix that indicates various response times to incidents based on their priority, as shown below, where:

- *The description indicates objective criteria to determine what priority is assigned to an incident (performance degradation vs. complete unavailability, number of users affected, time of day, etc.)*
- *The target response time is a commitment to acknowledge the incident and initiate the incident management procedures*
- *The target update time is a commitment to provide the customer with information about the expected resolution of the problem within a certain amount of time after the incident start time*
- *The target fix time is the expected total time between the incident start time and the full restoration of the affected services at their normal performance level.*

Priority	*Description*	*Target response time*	*Target update time*	*Target fix time*
P1				
P2				
…				
Pn				

When applicable, in the above table or separately. describe the commitment to incident resolution in terms of recovery point objective (RPO) and recovery time objective (RTO)

Times specified in this matrix must be defined unambiguously: if they are not the total elapsed "clock time" between two timestamps, for example if they are defined in terms of "business hours," "next business day," etc., those terms must be clearly defined since the CSP and CSC may have different definitions of those concepts.

Specify what access the customer has to the system used by the CSP to log and track trouble reports, and what information the CSC is allowed to view and/or modify in the record of an incident that affects them.

Describe the problem management methodology used to identify and remedy the root cause of a problem and avoid its recurrence.

7.6.4. Incident Escalation

Describe the "escalation" or crisis management procedures that will be triggered for severe incidents, or those that exceed a pre-determined impact level or duration threshold. In particular, specify:

- *what criteria determine the need to escalate the incident*
- *how that decision is made in cooperation between the parties*
- *what additional resources are mobilized when an incident is escalated*
- *how incident management processes differ for an incident that has been escalated.*

For incidents that can be addressed through a failover mechanism (e.g., moving to a different address, changing network address, using a standby system or provider, restoring the system to a previous checkpoint, etc.), describe the criteria and process to trigger the failover.

7.6.5. Incident KPIs

Indicate the availability, content, frequency, and handling of reports containing key performance indicators (KPIs) about incidents. Specify whether these are made available to the customer in the form of interactive dashboards, static web pages, periodic reports, etc.).

Indicate the availability of the following KPIs:

- *total number of incidents reported in the current reporting period, split by priority level*
- *statistics about the time to resolution of high-priority incidents*
- *number of open problems at the end of the period (by priority),*
- *statistics on the length of time those problems have been open*
- *number of incidents closed during the period (by priority) with the time it took to resolve them*
- *number of incidents not resolved within the target fix time*
- *trend in the number of problems being reported (current period vs. previous ones).*

7.7. Service Prioritization

Specify whether there is a provision for degrading certain services deemed less critical in order to preserve the performance of the critical ones in the presence of some disruption. Provide all necessary definitions and the processes used to implement this degradation and to restore normal performance when the need has passed.

7.8. Excess Usage Management

Specify what happens if the customer's use of the services reaches a predetermined maximum, specified in Sections 2.1 or 2.2:

- *Is the customer blocked from using additional resources, or is the customer allowed to use additional resources, and charged for the excess usage on top of the base cost of the service?*
- *Is the customer notified in advance that they are approaching their limit?*
- *If excess usage is allowed, does the customer receive periodic updates on the additional costs being incurred?*
- *What mechanisms are offered to the customer to authorize a new temporary limit?*

7.9. Remedies

Specify the remedies offered by the CSP to the CSC if the committed service levels were not met.

Indicate:

- *what issues trigger the availability of remedies,*
- *what those remedies are (e.g., service credits, service extension, cash rebates, free additional services, etc.),*
- *the precise calculation method for the amount of the remedies,*
- *whether the remedies are applied automatically, or need to be requested explicitly by the CSC, and how,*
- *whether the CSP offers remedies, including through cyber insurance, to "make the customer whole" in case a service failure caused harm to its business,*

- *how disputes about the availability and amount or remedies can be initiated and are managed.*

7.10. Performance Bonuses

Some CSAs include provisions for payment of a bonus in the case of outstanding performance, such as zero incidents during a month, or service levels significantly exceeding the commitments in the SLA. If this is the case, specify in this section the criteria and the calculation formulas for such bonuses, and how they are paid.

7.11. Exit-Related Service Levels

Specify the services, and service levels, related to transferring customer data and applications back to the CSC or to a successor CSP during the exit process (i.e., after termination is invoked).

These services and service levels may include:

- *the delivery of data exports*
- *the release of encryption keys or their secure transfer to a new provider*
- *consulting services to help the migration process*
- *delivery of applicable documentation*
- *secure deletion of customer date, once authorized in writing by the customer*
- *deliver or erasure of backup media, per the customer's preference, and after a period of time (which will extend beyond the termination date)*

Specify how the customer retains leverage to compel the performance of these services, for example by retaining a portion or the entirety of the last payment for the services until those exit services have been satisfactorily performed.

8. Signatures

The Customer Agreement should generally end with the signature blocks that signify the execution of the agreement. A signature block includes the name of the individual signing the agreement, their handwritten signature, their title, and the date of signing.

Appendices

Include here any appendices referred to in the above sections. For clarity, it is recommended to call them "Appendix A: <Title>," "Appendix B: <Title>," etc.

References

[1] Object Management Group: *Practical Guide to Cloud Service Agreements, V3.0.* February 2019. https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm

[2] Object Management Group: *Cloud Service Agreements – What to Expect and What to Negotiate, V3.0.* September 2019. https://www.omg.org/cloud/deliverables/cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

[3] Object Management Group: *Practical Guide to Cloud Deployment Technologies, V1.0.* March 2019. https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-deployment-technologies.htm

[4] Object Management Group: *XaaS (Anything as a Service) Glossary, V1.0*. June 2022. https://www.omg.org/cloud/Anything-as-a-Service-Glossary-22-06-08.pdf

