A Guide to Fair Contracts for ‘As a Service’

As a Service Guiding Principles in Standardized Models of the IT Industry

Summary Report, March 2019

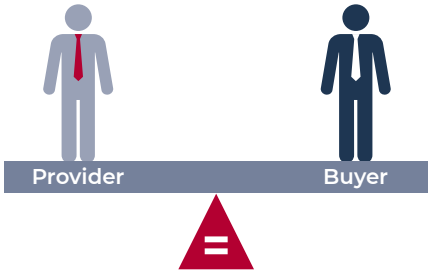
IACCM
International Association for Contract & Commercial Management

Contents

Introduction

The objective of this paper is to provide a reference point for contract terms in the technology and platform-based As a Service (or aaS) marketplace.

The intent is to introduce some balance into the equation to take into account both provider and buyer perspectives. Our overall aim is to narrow down the scope of issues requiring negotiation in one-to-many technology aaS environments. This in turn will have the positive effect of reducing friction between parties and go-to-market timescales.



The intent it to introduce balance into the provider-buyer equation.

The following general notes are important in setting out the context and scope of this paper.

Background and Use Case for As a Service Offerings in the Technology Sector

After years of internal technological build-up and accrued complexity, businesses are increasingly finding that their internal systems are unable, even with significant investment, to adapt to the fast-paced and disruptive change of the new era. In order to survive and thrive, businesses need to be able to access and leverage the powerful forces of analytics, social media, and new technology with agility and with much shorter leadtimes. They also need the flexibility to move on quickly between products, as the market and their needs evolve.

In this context, the value proposition of aaS offerings is clear, in contrast to a traditional in-house system implementation:

- Limited upfront investment for the buyer – and spend is shifted from capex to opex;
- Superior scalability and volume flex;
- Lower cost, driven by a highly scaled and standardized approach;
- Superior investment in product roadmap and evolution, particularly in a competitive market;
- Flexibility and (relative) ease of change of provider.

Drivers of As a Service Terms

While there will always be differences, it is possible to discern a similarity of contracting approach across large aaS providers. It is useful to understand some of the drivers behind this standardization.

One-to-Many

As a Service offerings, by their nature, operate on a one-to-many model. They deploy a common product or technology set, which will usually offer very limited ability for customization or variation to respond to buyer preferences. The drive to continually reduce costs and offer better value for a consistently reliable service is also an influencing factor. Built into the price points and business model for aaS is the concept of the correct and 'fair' allocation of risk i.e. when is it appropriate for aaS providers to accept risk and when should it be borne by buyers?

The drivers for standardized terms at a high level can be summarized as:

- Standardized approach to operational matters including service levels, security and data processing;
- Preservation of operational freedom to maintain, update and change the service (primarily for the overall benefit of clients);
- Rights of access only – no acquisition of intellectual property rights by clients;
- Standardisation of warranties, remedies and liabilities across the client base, reflecting the one-to-many model; and
- Charging model which may be based on one or more per user (or 'seat') charge, a transaction charge which will generally have a base level fee, with volume bands (at decreasing per unit cost) above the base level, or a simple subscription model.

Cloud Backdrop for Software as a Service (SaaS) or Platform as a Service (PaaS)

Most aaS offerings are hosted in the Cloud. The Cloud may be provided by the relevant service provider, or may be hosted on a public Cloud. It is important to be aware that the underlying public Cloud infrastructure can significantly impact the freedom of an aaS provider to negotiate terms as there generally must be a flow down of terms to the ultimate Cloud provider.

The public Cloud is now a commoditized, standardized offering that comes with attached terms and conditions. Further, often Cloud providers place positive obligations to flow up their terms into the SaaS provider's contracts with the buyers. Accordingly, this will likely have significant influence on the negotiability of the contract. Where a private Cloud is being provided, there will be more flexibility to negotiate contract terms and therefore room to agree upon certain variations to the aaS principles defined in the present document.

As a Service offerings deployed on the public Cloud are commoditized one-to-many.

Principles for Standardized As a Service Models in the IT Industry – Guidance and Rationale for Model Terms

IACCM has gathered input from nearly 300 member organizations to establish the topics that arise most frequently in aaS negotiations.

Many of these relate to specific risks, both regulatory and operational, and these are highlighted below and represent the proposed market relevant aaS terms for establishing 'principles' in the one-to-many environment of the information technology sector.

There are further topics not on this list – such as service scope, performance and price. These are areas where elements of variability are inevitable and therefore we are not including them as defined 'principles'.

Service Level Agreements (SLAs) and Remedies

1. Due to the one-to-many nature of the service, aaS providers typically offer the same service level (SLA) commitment to all buyers for a particular offering. SLAs may vary between offerings.

2. Each offering's SLA will usually be publicly available and typically offer an up-time commitment of between 99.0% and 99.5%. While most aaS providers will give an indicative incident response time, the pricing points for aaS will generally not cater for the ability of the provider to commit to resolution times as it would place a high burden on the provider in the event of breach.

3. Typically, the sole remedy for any failure to meet up-time commitment is explicitly limited to service credits. Service credits may take the form of:

a) a credit towards the next invoice;

b) a discount on the applicable price or sometimes;

c) an extension of the aaS agreement term by a certain number of days. In the first two forms, service credits are usually capped at a percentage of the overall transaction price. Although buyers often react negatively to service credits as sole remedy for up-time failure, an advantage to service credits is that they represent an immediate remedy for the buyer in the event of an SLA breach, without having to prove loss or damage.

4. As a Service providers may consider offering additional comfort to buyers where business critical systems are at stake. In such circumstances, aaS providers often use solution architecture where simultaneous instances are hosted across different zones to increase service availability probability. Beyond these operational models, in the event of persistent or severe service failure aaS providers may consider allowing buyers to terminate the service if a committed minimum term has been agreed. Risk to the provider of offering a termination remedy should be low, assuming that the provider has confidence in its offering. Another angle where business critical systems are involved could be to increase the overall service credits cap to a meaningful level i.e. if the provider is consistently missing uptime targets, it will hurt.

5. Buyers will typically want good visibility, tracking and governance around service levels, which should be provided as part of the service.

The service credits cap could be increased where business critical systems are at stake .

Hosting Location and Data Sovereignty

1. Most aaS providers offer full transparency to buyers for the locations of their data centers. They also typically allow buyers to choose a region or geography within which to host their solutions and data. The aaS providers will often agree not to transfer data out of that region/geography, unless they are compelled by law to do so, for example owing to a binding court order. Global aaS providers may, however, require buyers to agree to temporary access from outside the geography for the purposes of providing support. Any such access would typically be subject to prior consent from the buyer.

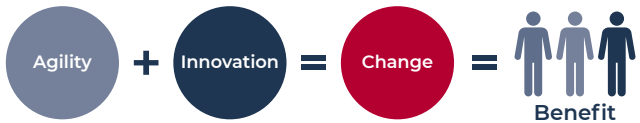
2. The data protection framework in Europe requires transparency to buyers about the location of their data. Most aaS providers offer a specific permission only process if they wish to/need to access data from outside the European Economic Area. As a Service providers may offer other mechanisms to get around specific permission based access such as binding corporate rules, adhering to the Privacy Shield, signing up model clauses etc. Yet aaS providers need to pay close attention to these mechanisms to ensure that they are effective and comply with data privacy legislation. Many countries/regions are reviewing and adopting data protection legislation similar to the European Economic Area. Understanding what is applicable for buyer business is critical.

Data Processing and Security Policies

1. The standardized nature of aaS operations means that aaS providers will generally apply the same data processing policies and the same security mechanisms (e.g. for access controls and data integrity) across their offering for all buyers. The business model will not support deviating from a standard operational set-up. That said, some aaS providers may, for a corresponding fee, offer a fully segregated service for individual buyers.

2. Most larger aaS providers will provide a data processing policy or agreement that is designed to meet the requirements of the European Union GDPR (General Data Protection Regulation), and this will cover how data breach/security incidents are dealt with including buyer notification processes and timescales. As a Service providers often, publish minimum security standards that they adhere to for all offerings. Greater transparency around GDPR compliance should be addressed by smaller aaS providers.

3. As a Service providers typically also publish relevant security certifications and accreditations and will generally agree to keep these current. These standards are good news for buyers and give a greater comfort when buying aaS offerings.



Leaving aaS providers free to change services brings agility and innovative that ultimately benefits buyers.

Changes to Services

1. As a Service providers do not contractually commit to making improvements to their services. The commercial reality, however, is that aaS providers have a clear interest in continuing to improve their services to stay relevant in the highly competitive and fast changing marketplace.

2. Contractually aaS providers generally reserve the right to make changes to their services. Although unilateral change provisions can often be a sticking point for buyers, the commercial reality is that they are necessary for aaS offerings to evolve. Agility and innovation in the marketplace will ultimately benefit buyers.

3. Often, to ensure the absence of operational impact for buyers, aaS providers accept some limitations to this right of change i.e. they commit that the changes will not be materially detrimental to the buyer's use of the relevant service and that the offering functionality or security features will not be degraded.

4. Some aaS providers also require the flexibility to withdraw a service or part of a service, particularly if the overall contractual commitment is long term. In such cases, buyers will need a notice period that gives them sufficient time to either swap the service out for an alternative service offered by the provider or to find an alternative provider. Typical withdrawal of service notice periods are 12 months.

5. Additionally, aaS providers should offer assistance services for moving to an alternative technology. These services will typically be chargeable.

Termination of Service and Termination Assistance

1. Most aaS provider terms include provisions for termination for material breach, where the provider materially defaults on the provision of the service.

2. Buyers should have the option to call on aaS providers in the event of termination to provide support for the return of buyers' data so they can be easily exchanged between the incumbent and the new aaS providers, etc. Generally the return of data 'as is' will not be a chargeable service.

At termination, aaS providers should return buyers' data.

Suspension Rights

1. As a Service providers generally reserve the right to suspend aaS services in situations where the buyer puts the provider, its platform or services at risk of:

a) a technical or security threat;

b) third party claims due to infringing or illegal content or data; or

c) subject the provider to some other liability or risk.

2. Any right of suspension should be balanced especially when aaS services are mission critical to buyers, as they require certainty of service provision. As a Service providers can give some comfort by using suspension as the remedy of last resort i.e.

a) As a Service providers should allow buyers a reasonable time period (unless immediate suspension is critical to avoid harm or they are compelled by law to suspend the service) to fix/eliminate or mitigate the relevant issue before suspension occurs; and

b) As a Service providers should only undertake suspension under circumstances that are not reasonably capable of other mitigations or remedies.

3. Some aaS providers may also agree to only suspend the directly affected service, provided that such partial suspension is technically feasible and otherwise reasonable.

4. As a Service providers should have the obligation to restore the suspended service(s) as soon as possible after the cause of the suspension has been corrected or eliminated.

5. Most aaS providers will continue to charge during any such period of suspension.

Intellectual Property Rights (IPR)

1. Intellectual Property Rights (IPR) are sometimes not part of the terms included in aaS agreements in the information technology sector, as buyers receive a service (and not a license to use of software, for example), which is based on a one-to-many offering.

2. Where addressed, aaS providers will insist that they own all IPR vested in the systems, software etc. over which the relevant aaS services are being provided whether existing, enhanced or new IPR, i.e. this applies to any modifications and add-ons as well. This secures not only the provider's basic business ideas but also a more competitive technology for the aaS services and more competitive price levels for the buyers. Some aaS providers, however, will allow buyers to own the insights gained from using the relevant service. This can often be important for aaS providers in selecting a service as these insights can provide a competitive advantage.

Warranties

1. Public aaS providers tend to provide very tight warranties, which rarely go beyond the following:

a) the service will comply with the relevant service description;

b) the service will be provided in a professional manner consistent with industry standards; and/or

c) the aaS provider does not guarantee that the service will be error-free, virus-free or uninterrupted.

2. Such tight warranties are linked directly to one-to-many pricing models and are largely non negotiable.

Indemnification for Infringement of Intellectual Property Rights (IPR)

1. As a Service providers tend to offer a 'defend and pay' type of indemnity to protect buyers against any third party IPR infringement claims.

2. Recoverable damages tend to be limited to amounts awarded by a final court against the buyer or settlement amounts preapproved by the provider. They generally do not include service replacement costs.

3. When considering the appropriate allocation of risk here, buyers should be mindful of the price points for aaS models. Uncapped damages, to include all possible buyer costs, will not generally achieve the appropriate balance. In practice, rights owners are more likely to pursue the aaS providers themselves for infringement claims.

4. Some aaS providers require inbound indemnities from buyers, often related to third party claims relating to buyer content. Such inbound indemnities are not popular with buyers and are often renegotiated.

Limitation of Liability

1. Typically, the liability of either party in an aaS agreement will be excluded for consequential, punitive and other indirect damages that do not flow proximately from the breach. Damages such as lost profits, loss of business revenues, loss of anticipated savings, and loss of goodwill are also generally excluded.

2. The aaS marketplace standard starting point for liability caps tend to be the preceding 12 months service fees.

3. The landing point for liability caps will depend on a number of factors, including the size and length of the service commitment and the relative strength of negotiating positions. The more commoditized the service, the less likely that a provider will deem it reasonable to agree a non standard liability cap. A consideration for buyers on agreeing a cap will be the nature of the service itself and whether it is business critical.

The aaS market place standard liability caps are based on the amount of service fees paid in the preceding months.

Liability for Loss of Data

1. As a Service providers often accept limited liability for loss, destruction or corruption of data, where it is linked to a breach of the provider's data security obligations. As a Service providers accept that this is a concern for buyers using standard aaS models and in many instances will agree a separate liability cap in relation to such breaches.

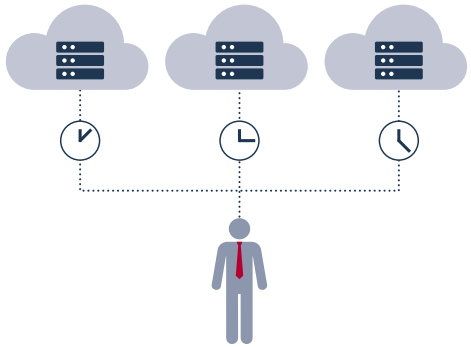
2. Often buyers will seek to keep breach of confidentiality separate and some demand uncapped liability for that. There is clearly a tension between what the buyer is seeking and what the provider may be prepared to agree in a one-to-many environment. Buyers are concerned about their customer's data. A sensible compromise can be a separate cap for data security breaches, applying the principles referred to in **3** below.

3. As a Service providers often seek to link liability associated with data security breaches to a demonstrable assessment of probable direct losses associated with the breach. Reputational risk will be a factor in any such assessment.

4. For pure loss or corruption of data concerns, buyers should ensure that they have provisioned regular data back-ups.

Compliance with Laws

Many aaS providers explicitly state that it is the responsibility of the buyer to ensure that the way they intend to use the service will comply with any laws, particularly with any industry specific laws that their business may be subject to. The aaS provider will generally agree to state that its services comply with any laws that are directly applicable to such aaS provider in the provision of the services.



For data loss or corruption concerns buyers should make regular back-ups.

Audit Rights

1. As a Service solutions are often provided on a multi-tenanted platform, which means that it could compromise security and performance for such platforms or services to be subjected to numerous physical audits by varying third parties, consuming the provider's internal resources and potentially compromising the integrity of the aaS provider's platform.

2. Instead, aaS providers normally have independent third-party auditors that carry out annual security audits, and capture their findings in a report (SOC1, SOC2 etc.), which most aaS providers then will share with the buyers.

3. Some aaS providers have buyers from regulated industries (e.g. from financial services or pharmaceutical sectors). Such buyers often require contractual rights of audit for themselves and their regulators. These requirements have become prolific in the marketplace since the introduction of the *European Banking Authority Recommendations on Outsourcing to Cloud Service Providers* ('Recommendations'). The general interpretation is that the Recommendations apply to aaS offerings. These, together with the statutory backstop right of audit provided in the European Union GDPR, make it more difficult for aaS providers to side step offering rights of audit to buyers. Physical audits, however, should generally be the remedy of last resort if other methods, such as reports, prove inadequate.

Tim Cummins *President IACCM*
tcummins@iaccm.com

Sally Guyer *Global CEO IACCM*
shughes@iaccm.com

www.iaccm.com

IACCM
International Association
for Contract & Commercial
Management