Cloud Insights

By Dr Sara Cullen

IAAS CONTRACTS

Cloud computing agreements vary widely across the many providers and the many forms of cloud services. The contract can range from a vendor's standardized click-wrap agreement for a vanilla SaaS to a multi-layered, heavily negotiated contract comprised of SaaS, PaaS, and IaaS in public and private clouds.

In this Insight we'll look at IaaS (Infrastructure as a Service) contracts and the contentious clauses you might expect to see from an IaaS vendor. We'll focus on a public (unrestricted) IaaS, because a private one (restricted to just your organization) is nearly identical to a typical outsourcing agreement in which you have physical servers hosted at a vendor's site. In reality, you'll probably be using both as the majority IaaS-using organizations have a multi-cloud strategy (multiple clouds and multiple vendors).

When negotiating a public cloud IaaS contract, each subscribing organization has varying degrees of bargaining power.

When negotiating a public cloud IaaS contract, each subscribing organization has varying degrees of bargaining power depending on how much money is at stake and the attractiveness of the subscriber's brand as part of the vendor's logo stable. At one end of the spectrum, some subscribers will be able to dictate many of the terms. On the other end subscribers have to live with the contract of their provider, because the provider is happy to live without that subscriber.

Assuming you're closer to the latter rather than the former, this Insight explains why cloud vendors have certain provisions in their contracts that, at first glance, appear shockingly one-sided and why you needn't be as alarmed as you might think.

First, an IaaS primer

IaaS is the provision of virtual processing and/or storage machines (VMs) delivered via a network, with each VM being allocated a fixed IP address. VMs allow both the isolation of applications from the underlying hardware and other VMs, and the customization of the platform to suit the needs of the end-user. The cloud provider owns the equipment and is responsible for housing, running and maintaining it. The customer deploys and runs the operating systems and applications.

However, the demarcation between VMs as the provider's responsibility and software as the client's responsibility isn't quite that

WHITE PLUME PUBLISHING

simple in reality. IaaS has become IaaS+; the cloud provider supplies additional services that your IT people want (e.g. database, cache, and queue management), in addition to the VM service. A typical IaaS contract will have many software services you can opt in and out of.

The most popular use of public IaaS clouds is to run non-essential to moderately important production applications, in addition to application development and testing, which require elastic scale.[1] Mission-critical production is generally reserved for private clouds, if cloud-based at all. Most would consider a multi-tenant, public infrastructure too high risk in terms of reliability and security to run important applications on a public IaaS.

So the typical scenario is: You want VMs on the vendor's physical machines which are shared with other subscribers. These VMs are loaded with some systems software, to run not-so-important things, with unpredictable usage requirements. This means the stakes aren't high, although you don't want to be unnecessarily exposed.

We'll discuss a few of the issues that have concerned most IaaS subscribers when reading a vendor's contract:

- The provider's business decisions - change of control and subcontracting,
- Data - ownership and backup,
- Infrastructure operations - updates, security, and disaster recovery,
- Liability and indemnities - the lawyer's favorites, and finally
- Termination.

The Provider's Business Decisions

Change of Control

If you're with a little IaaS provider, the founders' dreams were of a sale of business, not to run it long-term.

Cloud providers are being bought and sold non-stop. The big ones are doing most of the buying. It's very likely that if you're with a little IaaS provider, the founders' dreams were of a sale of business, not to run it long-term.

You probably don't share this dream and don't want to be passed around from vendor to vendor. The change of control clause sets out what happens in the event of a sale. The vendor will either be silent on this subject or have an automatic assignment provision. This increases the business' sale value as a purchaser then buys subscribers' contracts in addition to infrastructure and brand goodwill.

[1]Neovise (2013) "Public, Private and Hybrids Clouds", research of 161 US organizations.

You can't stop a sale, but you can decide not to move to the new owner. To do this, you'll need to be notified and to be able to withhold consent (thus terminating the contract). Getting this in a cloud contract isn't too difficult. Most will acquiesce to your needs on this one if they want your money.

Cloud providers do a lot of subcontracting and they don't believe you really need to know much about.

Subcontracting

Cloud providers do a lot of subcontracting and they don't believe you really need to know much about it. Their contracts will be silent on the subject or state something like this one, "We may subcontract or outsource any function as we see fit."

It's perfectly natural to want to know how many fingers are in the infrastructure pie and whose hands they belong to. You'll want to know what's subcontracted out, to whom, and possibly do your own due diligence on the subcontractor before you sign up. You may want the right to terminate if a new subcontractor isn't a desirable supplier.

But recognize that your IaaS provider doesn't want you to know in case you try to contract with the subcontractors directly or let others know who they are. In effect, they look at their supply chain as a trade secret. Accordingly, unlike the change of control clause, this will take some time to attempt to create transparency around the cloud supply chain and to get the options and rights you want. So if subcontracting is a concern to you, you'll save a lot of time if you select a provider that doesn't do much of it and isn't precious about it.

Data

Data ownership

Data ownership will be silent in an IaaS contract because your business data is of no interest to IaaS providers; however, your usage data is. Unless the contract says otherwise, usage data is owned by the provider (they created it). You'll want this data as well, to check billings and when you leave this provider (to negotiate a good deal).

Joint ownership is the most reasonable solution along with a requirement to provide usage data in a form useful to you. The usage report that they provide is just reports against the pricing tariffs, rather than give you useful operations data. If you don't know what that is, you'll need to do a few test runs to make sure its usable and what you need. Do this in the first few months, do not attempt to invoke this after the contract has been terminated and goodwill has faded.

Data backup

Some IaaS contracts will be silent on this; others will have half a page devote to your obligations to backup. Either way, this is your job unless you subscribe to a backup service.

Even then, always have your own independent backup (e.g. stored on a different IaaS provider's infrastructure not located in the area of your primary IaaS provider's data centers). You'll need this if the provider's disaster recovery plan doesn't quite work out (the more tenants and the fewer data centre locations, the higher the risk), if the provider goes bust (administrators are there to get cash for creditors, not support clients), or the contract is terminated (most cloud contracts allow immediate data deletion upon termination).

If you decide to subscribe to a backup service, you will need to warrant that your backup holds only lawful data and doesn't contravene anything.

If you do decide to subscribe to a backup service, you will need to warrant that your backup holds only lawful data and doesn't contravene anything. They do not want to be brought in to any stoush with a regulator, a court, a third party merely because they acted as an offsite filing cabinet for you.

Infrastructure operations

Updates

In traditional outsourcing agreements, clients often have the right to opt in or out of upgrades that might affect their operations. In a public IaaS, do not have this as an expectation.

However, a notification provision helps you prepare for it. Providers are constantly playing with the infrastructure to manage demand and capacity, and generally upgrade frequently, so you need to be specific about what software affects your VM operations, agree what is a notifiable update, and agree a reasonable notice period. Then be ready for constant change; you will not be able to opt out.

Security

While you might think that the main concern here is how secure the provider's network and data centre are, providers are much more concerned with how secure you keep your VMs. Your obligations will probably be spelt out in surprising detail, while the provider's obligations will be cursory at best.

Most providers will reserve the right to boot you out if they believe your practices are a risk to their infrastructure. They don't often spell out what practices you need to have, so it's at their discretion. However, you can negotiate for a temporary suspension and a rectification period - typically 15 days from their defect notice.

While you can try to specify all the security that your provider is to have, and those with significant bargaining power do, there is another option which is far easier and doesn't have much to do with the contract.

Go with a provider which:

- is ISO 27001 certified - this is the Information Security Management standard. Make sure there is a notification clause in the event they no longer are certified, and if so, ensure you have the right to terminate;
- is CSA STAR certified (Security Trust and Assurance Registry) - this is a new certification specifically for cloud providers performed by licensed certifiers as is the ISO standard;
- is FedRAMP certified (Federal Risk and Authorization Management Program) for government subscribers - a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services; and
- gives an annual SOC Type 2 report to all subscribers - prepared by an independent auditor who assesses and tests the provider's internal controls.

Disaster Recovery

Most IaaS customers expect strong disaster planning and recovery from their cloud providers. This is reasonable. If any cloud provider doesn't have it, then run. But you won't see much mentioned in the contract on this. What you will see is that data restoration is your decision and your job - unless you subscribe to their data restoration service (if offered; many don't).

The more tenants and the fewer the physical data centre locations, the higher the risk.

The more tenants and the fewer the physical data centre locations, the higher the risk your VMs will be out of action for longer than is comfortable for you. With severe weather events occurring more frequent and with longer durations, this is just common sense - no one's data centre is infallible. Hence consider another cloud provider for a hotsite DRaaS (disaster recovery as a service) if you can't afford to be offline for too long. It will happen at the worst time - like Google Fiber going offline in Kansas City for up to three hours during the opening game of the World Series.

Indemnity and Liability

Indemnity

You'll need to indemnify the provider against anything you do that could give rise to a third party claim (e.g. a person claims that content on your VMs infringes their copyright, moral rights, or patents). Many have a clause stating that your prepaid account (and top up facility) can be used if they need to defend themselves from someone making a claim based on the content or use of your VMs). Basically, your VM is your business. But if they get dragged into it, you will need to underwrite their involvement.

Nonetheless, this clause should never be one-sided in any outsourcing contract, cloud or otherwise. It should be a mutual

indemnification if one party gets caught up in the other party's third-party infringement claim, as well as any negligent, unlawful, illegal, fraudulent or dishonest act, error or omission of the other party and its personnel.

Liability

In common with traditional outsourcing agreements, cloud providers minimize their liability by having exclusion clauses and liability caps (e.g. the total amount paid to date to the vendor).

They will agree to no cap on the following, as this is customary in all contracts:

- intellectual property infringement (third party or otherwise)
- breach of privacy and confidentiality obligations both in contract and in law
- unlawful or illegal acts or omissions by the vendor, its personnel, or subcontractors
- although not really relevant to the cloud, personal injury or death and damage to physical property are also excluded from caps in any standard contract

These won't be your main concern however. It will be data loss - even more so if this loss causes you to lose revenue (consequential damage) or incur heavy restoration/recreation costs (direct damage). Because consequential damage is extraordinarily difficult to prove in court and VM backup/restoration is your responsibility, your chances of getting a public IaaS provider to take on liability due to data loss is unrealistic. If your backup and testing is inadequate and/or you want to have data loss protection, you are better off getting your own insurance policy or acquire your own infrastructure.

Your chances of getting a public IaaS provider to take on liability due to data loss is unrealistic.

Termination

Public IaaS providers are socialists. They will put the good of their subscriber population above the needs of an individual subscriber. This means subscribers causing trouble with the infrastructure can get terminated. Just like living in an apartment complex, no one likes bad tenants.

In a typical nine-page public IaaS contract, only half a page will be devoted to the provider's obligations. The rest will be about yours, for which breach will be a terminable offense.

The provider may terminate the service if:

- you don't have enough money/hosting credits in your account[2]
- the provider believes your VM security isn't sufficient
- you breach the usage policy, including excessive or unusual use that they believe may jeopardize their operations
- your IP addresses are used for disreputable services, or are blacklisted (e.g. on spamhouse.org)
- you don't act promptly to any information request by the provider, or IP infringement notice by a third-party, or a complaint by the user.
- your organization doesn't clearly identify itself as the VM's owner (the provider doesn't want to be involved in your affairs). Many will devote about 10-20% of the contract's content to your identification requirements and those of the people you grant access.

However, unlike if you were a renter in an apartment block, the vendors' contracts are silent with regard to an eviction notice period - which means it can be immediate and without notice. But notice will be critical and must be included. In all likelihood, you'll need to negotiate different notice period for different offences and some inevitably will be immediate (e.g. your IP address is blacklisted or is under DDoS attack[3]). This is why you need your own backup.

Conclusion

A public utility furnishes everyday necessities to the public at large. Computing as the 5th utility was predicted some time ago in 1969 by Leonard Kleinrock, one of the chief scientists of the Advanced Research Projects Agency Network (ARPANET) project which seeded the Internet.

But we're not quite there yet.

Essential services like water, electricity, gas, and sewage are all heavily regulated with government oversight bodies, unlike the very light touch we see in the cloud industry. In the other utilities, it is also relatively easy to switch providers. The proprietary interfaces that cloud providers use to access their services restrict the ability of subscribers to swap one provider for another. But we are seeing the wholesale/retail splits markets emerge which are present in other utilities, and peak/off peak pricing mechanisms. So, while not a true utility, the cloud has many utility characteristics.

[2] Public IaaS providers generally make you prepay which gives you credits that are automatically topped up from a corporate credit card or direct debit facility.

[3] A DDoS attack occurs when bandwidth gets overloaded by a compromised system (for example a botnet) flooding the targeted VM with traffic.

Cloud vendors write contracts like a utility contract. You don't have many rights, you do have obligations, and they can cut supply if you breach the contract. While everyone likes a simple contract, these are perhaps over simplified. You will always need help interpreting them ... not for what has been said, but for what hasn't.

But to try to turn these into the traditional ITO client-written master/servant contracts of 60-600 pages (like I've seen many try to do) is misunderstanding the basic premise. When you hire a taxi, you haven't bought the car and driver to command at will. You get to go for a ride if you don't pose a risk - the driver can refuse and can ask you to get out. You don't get to take over the car, or transfer title, if you don't like the driver or the ride - you just get out.

Keep the contract simple and rational, behave well, and always have another taxi number on speed dial.

About the Author

Dr Sara Cullen

Managing Director, The Cullen Group
Fellow, University of Melbourne
Research Assoc., London School of Economics

Sara Cullen is the Managing Director of the Cullen Group, a specialist firm offering consulting, training, and publications, a Fellow at the University of Melbourne, and a Research Associate at the London School of Economics. Prior to starting her own firm, she was a National Partner at Deloitte in Australia, where she ran the outsourcing consulting division and was the Global Thought Leader for outsourcing.

Dr. Cullen specializes in the design and management of outsourcing agreements, for buyers and sellers alike. She has consulted to 150 government and commercial sector organizations, spanning 51 countries, in over 190 contracts comprising $18 billion in contract value.

Sara is a widely published author having written 143 publications since 1994. Her books include *Outsourcing: All You Need to Know*, *The Outsourcing Enterprise*, *The Contract Scorecard*, *Toward Reframing Outsourcing*, *Intelligent IT Outsourcing*, and *Outsourcing: Exploding the Myths*. She has conducted research with various universities since 1994. Her expertise is globally recognized and she performs peer reviews regarding outsourcing research for the Harvard Business Review, California Management Review, the Journal of Information Systems (UK), and the European Conference on Information Systems. Dr. Cullen has lectured at many universities in Australia, Asia, and the Americas.

Dr. Cullen has a BSc in accounting from St. Cloud State University (US), a Masters of Management (Technology) from Melbourne Business School, and a PhD in the area of outsourcing from the University of Melbourne. She is also a Chartered Accountant (US) and a Certified Mediator.

She can be reached at scullen@cullengroup.com.au.