Not every cloud has a silver lining

10 Step Guide to Cloud Computing

Arlene Adams
(Founder & CEO of Peppermint Technology)

Arlene Adams pulls on her experience to offer some simple steps for legal providers considering cloud computing. Adams spent many years in the managed service & infrastructure business including her time as UK Board Director at industry technology giant Sun Microsystems/Oracle.

"Not every Cloud has a silver lining"

In the world of technology "Cloud" is the buzz phrase of the moment. Everyone is talking about "Cloud" and it seems like every technology provider is reinventing itself as a "Cloud Provider". Despite the hype, which can become a self-fulfilling prophecy, it is still early days for "pure cloud" technology. The technology has not yet matured to a level of predictability and certainty and for this reason I would not recommend the "pure cloud" approach to legal providers at this point in time.

I would however encourage legal providers to embrace the principles of Cloud Computing but in an environment where the risk of sharing resources is understood and managed. It is in this context Peppermint has established a Private Legal Community Cloud. The Community Cloud is intended to embrace the benefits of shared infrastructure but the service is designed to reflect the needs and sensitivities unique to legal firms.

1. Make sure you are clear about the terms being used

The term "Cloud Computing" is somewhat ambiguous. It is definitely in vogue, and is the focus of most IT companies' marketing effort. However it is also marketed to describe other offerings such as SaaS and Hosting. This makes it tricky to compare like for like offerings and, more importantly, makes it difficult to be clear of the risks involved.

So what is "Pure Cloud Computing"?

In its pure form Cloud Computing can be defined as location-independent computing, whereby shared infrastructure provides resources on-demand. As with the electricity grid, you don't own the infrastructure, you simply consume the output and share the infrastructure with a pool of many others.

The main strengths of Cloud Computing are cost and agility gained through economies of scale. While this is attractive to many legal providers, there are weaknesses. The services tend to be transient and global, making it difficult to audit activity or determine where your data is or where it is being processed. The separation provided between cloud tenants is typically relatively low (in security terms) because the concept of Cloud is one of sharing resources. It is for this reason there is limited uptake of Cloud Computing for certain sectors, such as government agencies.

2. Understand in detail the company you are contracting with

The model of Cloud Computing is typically rental. There are many providers in the market offering everything from rented physical datacentre space, to rented infrastructure (hardware, software, networks) and rented application software. While this is good for choice and competition, the rental model has allowed anyone to act as a broker and resell these services.

The rental model doesn’t require high capital investment therefore many small companies have created a marketing front to these services. Firms need to be very careful they are clear about who they are buying from otherwise they could end up in the position where they are contracting with a reseller who has no control or value to add in the chain.

It may sound obvious, but I would advise you get in writing the number of people in the company supporting this part of the business; preferably an organisation chart and a clear understanding of the skills the company employ directly. Be sure to carryout full research into the trading history and financial position of the vehicle you are dealing with. There are many small companies operating in this space who simply act as middlemen and that’s not who you want to be dealing with, as when you have a problem they will have no control.

3. Understand the ownership structure and tier of the datacentre

The datacentre market is well established. There are clear guidelines and measures to help you be certain as to the level of service you can expect. I would strongly recommend legal providers only consider Tier 3 or above for datacentre provision and nothing below this due to the sensitive nature of the data legal providers have to deal with. Tier 4 is an option but unviable due to cost. It is typically only used by highly secure and sensitive companies and the price tag makes it inaccessible for most legal providers.

The optimal solution, in my view, is a dual Tier 3 datacentre with dual instances of your infrastructure on each site. This gives you a Tier 3 “plus” service. I think this offers the right balance of risk management and price point for legal providers.

Always ask your provider which Telecommunications Industry Association datacentre level they are approved to. Level 3 gives you 99.982% availability by design.

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure guaranteeing 99.671% availability
2	• Fulfils all Tier 1 requirements • Redundant site infrastructure capacity components guaranteeing 99.741% availability
3	• Fulfils all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure guaranteeing 99.982% availability
4	• Fulfils all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability

Be sure to check the financial standing of the datacentre owner and determine whether they own or lease the building. You don't want to find out one year into a contract that you have to expose yourself to the risk of moving just because the lease wasn't renewed or the company goes bust.

4. Understand your risk exposure to data security

Regarding data security, a simple analogy is that there are many kinds of locks: some are basic; some very complex. All are designed to provide security, but you probably wouldn't fit a two lever lock to a bank vault door.

In computing terms a well configured and managed firewall (used between organisation hosted computer systems and the internet) are analogous to 5 lever locks. The security separation between tenants within a cloud environment might be closer to an analogous 2 lever lock. Technology has improved this situation, but only for modern applications that have been architected for the cloud. For users of traditional applications that have been simply been re-badged for the cloud this represents risk. You need to be clear on this before making any decision.

There are also systems that are being described as "Private Clouds". These are mainly created to negate the security issue with Cloud Computing, and are very similar to a traditional outsourced datacentre arrangement. Strengths of this approach include increased security; there are few, if any, areas that are shared. The weakness of this approach is it can only be achieved with added cost and reduced agility compared to “pure cloud”.

5. Qualify who owns the infrastructure and what they can do with it

Be clear on who owns the infrastructure and, more importantly, the access rights to the infrastructure of the company you are contracting with. It is highly likely that any outage may be caused by a failure of infrastructure. Do you really want to be in a long chain of companies if this happens?

Many companies offering cloud solutions don’t actually own the infrastructure and therefore can’t touch it. They rely or sub-contract to another company to solve the problem for them. There are also instances where a supplier may have access to fix problems but only at pre-agreed times and with certain named individuals. This approach is of no use if it’s the wrong time of day and the named person is on holiday.

I would suggest legal providers confirm that their supplier has the ability to manage and control the physical infrastructure. If your service provider has no control over this you may find yourself in a long queue of unhappy customers just having to wait your turn. This is a common problem.

6. Review in detail the technical infrastructure

Be sure you know what you are getting for your money. No two offering in this market are the same and unfortunately the devil is the detail and that means time spent doing your homework. Key things to check include if the service has failover to a second site and if so, it should be at least 20 miles away from where the live service is run. It is also worth checking if the failover environment is like for like with your live service so you know in advance if there will be any service degradation should this event happen.

If you have a failover service it is only helpful if it works. For this reason you should be asking your supplier how often the data is replicated and what tests they put in place to make sure this is working. I would recommend real time replication so you never lose any data. If you compromise on this, because of cost, then be sure to think through the implications of losing data for a period of time.

You should also validate the existing infrastructure on each site. Best practice would suggest that you should have dual instances on each datacentre site. This means you have two of everything to avoid the system failing. It also allows for proactive maintenance to take place in the event hardware or software needs to be changed. This approach allows far greater control and planning. While this approach comes at an additional cost, you have to measure this up against the cost to your business if things go wrong.

7. Review in detail the process of what happens if things go wrong

More often things go wrong because of human error. In my experience the greatest risk of any hosting, outsourced or cloud offering is the lack of process. Process is there to protect against risk. It should be designed based on experience and lessons learned. For this reason it should be constantly reviewed and updated as technology advances and events happen.

An established provider should, in theory, offer an advantage in this area based on their experience, so consider this when selecting your provider. Most importantly ask to see their documented procedures. If a supplier can't show you them, or takes time to provide them, this should be a warning that the processes don't exist or are not embedded deeply into the business. It is good process that influences the ability to respond well to any problem so this needs to be strong. There will be problems – there always are – and understanding your supplier's effectiveness on process is like reading the small print on your insurance contract.

8. Don't focus purely on contractual SLA's

Lawyers know better than anyone else that effective contracts and SLAs (Service Level Agreements) are important. It goes without saying, just because someone offers a good SLA it doesn't mean that they can deliver it. Don't assume because it is written down that it can be met. All the other things I have talked about in this guide are far more important. If you have to trigger the contract or SLA, the damage has already been done.

9. Beware of consultants

Like any profession the consultants in this market are mixed. This is a new and emerging market so be sure to qualify the experience of any consultant you engage.

Consultants can offer valuable insight and experience and definitely have a role to play but make sure this isn't something they have just started to focus on. Stronger candidates are likely to be of a technical background and will certainly have managed and operated infrastructure for a period of years. Only then will they really understand the operational risks. If you go down this route you are likely to benefit from dealing with technical security consultants. The legal market knowledge is less important in this area as you can explain the nature of your work. Understanding the technicalities is far more important.

Be sure to reference check your consultant and speak direct to references. Check the consultant has experience of recommending different solutions and they aren't just making the same recommendation because they know the provider or, worse still, get a referral fee. This decision represents high risk to your business so think hard before engaging any consultant. Always keep close to the detail of this decision, even if using a consultant, as you need to protect your business and the devil is in the detail.

10. Enjoy the benefits

This guide is designed to help manage risk, but I want to close by putting my advice back into context. In all the companies I have worked with over the years there is a clear connection between improved service availability, performance and the provision of managed services. In my experience where companies or firms outsource the technology to a professional IT firm they generally have a better service at a better price point. This approach gives legal providers the ability to access the latest technology, in bullet proof environments, run by specialist qualified people all at a predictable monthly price point. This allows legal firms to focus on doing what they do best – provide legal services – while their IT partner does the same.

While I wouldn't recommend any firm move to "pure cloud" computing just yet, I would encourage firms to embrace the concept and take small steps towards it. Consider the path to Cloud Computing a journey, not a leap of faith.

It is for many of the reasons I have discussed that Peppermint have taken the route we have, to form the Private Peppermint Legal Community Cloud.

This paper is in no way intended to provide all the answers but I hope in sharing my experience we can start a long needed debate around the merits, scope and the timescales of Cloud Computing in the legal sector.

Arlene Adams

CEO and Co-founder Peppermint Technology
E: Arlene.adams@peppermінttechnology.co.uk
@Arlene_Adams