

## **Software as a Service (SaaS)**

### **SaaS - Understanding the model - a legal view**

Andrew Hartshorn, partner and head of the ICT practice at law firm Shakespeare Putsman, looks at the benefits and risks of implementing SaaS and argues that the legal risks associated with implementation of SaaS are more akin to those of a managed services or outsourcing contract rather than software licences.

SaaS is growing apace. There has been a growing recognition over the last 18 months or so that SaaS has moved from revolution to mainstream - indeed McKinsey predicts that SaaS will represent 35% of annual software budgets by 2011. Whether Nasstar's CEO Charles Black will be proved correct in his prediction that by 2013 web-based applications in the workplace will make IT departments redundant is yet to be seen.

However, in the current climate with businesses looking to save on all aspects of their cost base, SaaS is seen as a good opportunity to reduce costs and allow for future growth without capacity constraints.

My view is that customers should see the SaaS model as being more akin to a managed service or an outsourcing contract than the traditional software licence model. In a managed service model, whilst the customer might develop their own business requirements and specifications which are priced and delivered by a managed service provider, with SaaS the provider has pre-developed the specification and the software and the opportunity for customisation is limited. As with any system implementation, businesses still need to understand their own processes to ensure that they can map to the SaaS service and gain full value from the implementation.

### **The SaaS Model**

In the SaaS model, a software application (and particularly complex software such as Customer Relationship Management, HR and accounting packages) is hosted by either the software vendor or a third party and the use of the application is provided remotely to the customer over the internet. The host is responsible for the operational environment including the software and hardware, dealing with upgrades and patches and data storage.

The customer accesses the application using a client side application which may be bespoke or a standard web browser.

## **Benefits**

It is argued by the service providers that SaaS provides a number of benefits particularly regarding cost and flexibility.

## **Cost**

Rather than undertaking expensive and time consuming software development projects, its proponents say that SaaS is ready as an off the shelf solution. The standard pricing model is based around annual fees either on a per-user or an enterprise wide basis which enables budgets to be managed on an annual basis without the need for major investment in the initial implementation.

Pricing models do vary however with some providers charging for additional storage capacity over a particular level. Training may also be a chargeable item as may any specific configuration requirements of the customer.

## **Scalability**

With SaaS, the customer is not tied to particular hardware platforms for its installation of the software – instead the provider manages the hardware. If the customer wants to add a raft of new users, it merely ups the user numbers and pays the additional annual fees. Active monitoring of users' requirements for the software is important to avoid spiralling costs for users who don't need to use the software.

## **Maintenance**

With the provider responsible for looking after the system, the customer does not need to worry about managing patches and upgrades.

## **Access**

With web access, many SaaS applications are available 24/7 from any location where internet access is enabled. Clearly in an era where many businesses are looking to empower mobile working, the provision of remote access to business critical applications such as CRM can be a valuable business tool. Mobile working is implicitly catered for by SaaS applications because they are internet-based and therefore not dependent on a private network.

## **Market specific**

The fact that the provision of a SaaS service does not require the physical presence of the provider at any particular location enables the development of market specific applications. Thus an Australian SaaS provider could develop a CRM application that is particularly suitable for, say, media companies. UK media companies would be equally able to access this application from Australia as they would a UK based application.

## **Downsides/Risks**

The very benefits that SaaS offer can also be interpreted as risks facing businesses who are considering adopting a SaaS application. In this section we look at the risks associated with SaaS and the contractual approaches to managing them.

## **Control**

One major challenge associated with SaaS is the ceding of control to the SaaS provider. By asking the SaaS provider to manage the system, the customer loses control over the system. The customer is reliant on the SaaS provider to respond to faults and to decide when and how to implement upgrades. In weighing up the pros and cons of adopting a SaaS approach, a customer must understand (as with a managed services contract) the fix times (and consequences of not meeting these fix times) offered by the provider. The customer will have no ability to manage the fix itself.

Nor is the customer likely to have any say over the functionality of new versions of the software implemented by the SaaS provider. With the standard software licence model (and even in managed services contracts) the customer would expect some degree of control over the timing of the implementation of new versions and could decide for itself whether the functionality provided by the new version merited an immediate upgrade or whether to continue on the current version. As with any business change, there are costs other than the pure IT costs of implementation of a new version of software.

## **Integration**

A major consideration for any business considering implementing an additional or alternative software application is the cost of integration of the application into the existing ICT infrastructure schema of the business. This is no less true for SaaS solutions.

Without looking at the particular technical challenges of SaaS implementation, the integration of SaaS solutions may well require use of specialist third party SaaS integration tools or the development of a bespoke solution to enable appropriate integration with existing applications. This could require either in-house or specialist third party support to enable the integration which needs to be factored in to the annual costs.

SaaS providers also control the timescale for release of upgrades and new versions of their product. Whilst reputable providers of SaaS solutions are likely to consider backwards compatibility, there is no guarantee that newer versions of SaaS applications will not require further implementation work for customers.

Whilst SaaS is sold as deployed offsite, it is sometimes necessary for the customer to concern themselves with deployment or upgrade of packages such as Java or other “add-ins” to ensure the smooth operation of the SaaS

software. The customer will also need to ensure that they are using a consistent and supported version of their internet browser.

### **Data security/recovery**

As with any offsite managed service, the customer in a SaaS service is reliant on the application provider to manage data security. Whilst a SaaS provider is unlikely to leave a laptop with the customer’s data on the train, both the protection of a business’ reputation and data protection laws require customers to understand exactly how the provider will manage all aspects of data security. Many of the cost benefits of SaaS are predicated on a “one size fits all” approach and there is likely to be little opportunity to require the SaaS provider to move to a data security regime different from its standard offering without pricing implications. Indeed, for smaller customers, the offering is likely to be on a take it or leave it approach.

I do not propose in this article to run through all aspects of data protection that need to be covered off in the SaaS delivery contract (and much will depend on the nature of the data itself) but as a minimum the following aspects should be documented:

- Back-up processes
- Any ability of the SaaS provider to send data overseas
- Disaster recover procedures
- Exit provisions (see the section on exit below)

### **Loss of expertise/Vendor lock-in**

As with an outsourcing, the transfer of responsibility for management of an application away from the customer may enable the customer to reduce the cost base of its IT department. Whether or not this is the case, in any event the customer is at risk of diluting the skill set of its in-house team. However, unlike outsourcing, it is unlikely that any employees of the SaaS provider will TUPE back to the customer on termination of the SaaS contract potentially leaving the customer with a skills deficit. Whilst customers may ask for support on exit (see below) as outsourced customers have sometimes found this does not necessarily equate to in-house expertise. Whilst there is always a challenge and cost of moving applications, the loss of in-house expertise may add to the problems faced by a business looking to migrate away from a SaaS provider.

### **Exit**

With a standard licence model exit should not be an issue – the customer is in control of the implementation and data and can carry out all tests that it considers appropriate to provide comfort that, once it switches over to the new application, it will not suffer any unmanageable teething problems. This

is not the case with an outsourced service as the customer is reliant on potentially two competing third parties to assist in transition.

Any managed services contract should therefore deal with exit. A SaaS contract is no different. Whether the exit is planned or forced, the customer needs to know that the transition away from the incumbent provider to the replacement (whether in-house or third party) will be seamless and with as little interruption in service as is practicable. It is important to ensure that the SaaS provider is not able to switch off access resulting in the loss of business-critical systems before the business has an alternative solution.

The exit provisions need include the ability of the customer to recover its own data. Whilst one would expect this to be a given, certain SaaS provider terms explicitly deny this right to customers in the event of non-payment by the customer.

### **Summary**

Clearly there can be benefits of adopting the SaaS model. The pricing model offered by the SaaS community is clearly articulated and may, on the face of it, provide a clear saving over the equivalent in-house licence model. Some of the obvious benefits of SaaS (such as simple remote access) may also be persuasive. As with any investment decision though, businesses need to understand the total cost of ownership including the medium term costs and potential disadvantages such as loss of in-house skills. Understanding the risk allocation in the contract clearly forms a part of this decision.