TECHNOLOGY FOR GOVERNMENT

LEGAL CONSIDERATIONS

THE PRESENTER

Sean King

Sean is a Director of Proximity. He is a highly regarded commercial advisor and lawyer with significant experience acting for Australian Government, private sector and non-profit clients on numerous large information and communication technology transactions.

Sean has significant experience as a commercial, procurement and legal advisor to large ICT projects covering systems integration, IT services, hardware acquisition, software licensing, terrestrial communications, mobile communications and satellite services.

Sean has advised the Australian Government on leading ICT transactions covering big data, cloud computing, subscription licensing, virtualisation, data security, SSL and whole of government arrangements.

Sean has advised on many ICT projects, receiving positive feedback for his combination of legal, commercial and management abilities. Sean is based in Canberra and has a current NV2 (top secret) security clearance with AGSVA.

In addition to his law degree, Sean has a Bachelor of Computer Engineering.

INTRODUCTION

Technology is becoming an increasingly important part of our personal lives and the operations of business and Government.

Increasingly we are moving away from face-to-face engagement with service providers in favour of technology enabled interactions. People are banking online, shopping online, watching television online and even dating online.

The push is on to ensure that government keeps pace with our preference. A large proportion of the population want technology that allows them to apply for their passport online, ant to make and receive payments electronically rather than using cheques, and to receive information through email or social media rather than print.

Government uses technology for two key purposes:

- To provide online and technology enabled services to citizens
- To provide the technology that supports public servants to perform their work

As the pervasion of technology increases, it is inevitable that the legal frameworks and legal input into technology transactions will also increase.

The tech world and public service are both renowned for their love of buzzwords and acronyms, so a seminar on ‘Technology for government’ could be a bit ridiculous.

My plan for this seminar is to pick out 6 current tech buzzwords (buzz phrases) and give you the background to that aspect of technology and the primary legal considerations for each. The Big 6 for this presentation are:

- Cloud
- Virtualisation
- SAM
- Big data
- Agile
- Internet of things

These represent some of the major current technology trends, and areas that are likely being actively explored or implemented by each of your organisations.

CLOUD COMPUTING

What is the cloud?

Cloud Computing or Cloud Services refers to the access over the internet to business software and user data stored on servers at a remote location or locations.

The word cloud is used as a metaphor for the Internet and a standardised cloud-like shape is used to depict the Internet in computer network diagrams. In these diagrams, the cloud represents a collection of technology that is removed from the main network and therefore appear invisible as though they are obscured by a cloud.

Despite the fancy name, cloud computing is actually just a different technology delivery method.

Why cloud?

Some of the characteristics of Cloud Computing are:

- Agility – technology infrastructure is quickly available
- Device and location independence – access from anywhere
- Maintenance – installation of computing applications is easier
- On-demand self-service – users can unilaterally obtain and deploy resources
- Reliability – improved if multiple redundant sites are used
- Scalability and elasticity - no need for users to engineer for peak loads
- Virtualisation – increased utilisation by running several operating systems on a single Central Processing Unit (CPU)

Cloud computing should therefore result in lower costs and increased efficiency and flexibility in ICT Procurement.

Cloud service models

Cloud computing services are typically offered in one of the following three models: Software as a Service, Platform as a Service and Infrastructure as a Service. The difference between each of them is the amount of the service that is outsourced to the cloud provider.

- Software as a Service – The user's access the software over the internet through a web browser, and the cloud services provider is responsible for ensuring everything works. The cloud provider takes care of the whole package – software, platform and

infrastructure (ie physical tin boxes). This model simplifies maintenance and support. Examples include Gmail, Salesforece and O365.

- Platform as a Service – the Cloud provider delivers a computing platform (which could include operating system, programming language execution environment, database and web server) over the Internet and the user manages the end user applications. Examples include AWS Elastic Beanstalk, Windows Azure
- Infrastructure as a Service – the Cloud provider offers access to additional computer infrastructure (servers, storage, networking, and power) but users are responsible for managing applications, data, operating systems and everything else needed to make the infrastructure perform the required task. Examples include Amazon Web Services and Microsoft Azure.

Cloud procurement

Cloud first policy

The Commonwealth has a 'cloud first' policy. Under the policy agencies are required to adopt cloud services for new and refreshed ICT capabilities where the cloud services are:

- fit for purpose
- provide adequate protection of government data
- deliver value for money

Much like the procurement of other ICT services, an agency will need to comply with the usual Commonwealth procurement legislation and policy.

Cloud Services Panel

The *Cloud Services Panel* is a whole of government panel developed by the Department of Finance. Agencies are able to procure cloud services across IaaS, PaaS, SaaS and Cloud Specialist Services. *The Cloud Services Panel* has 114 suppliers offering 474 different services.

The *Cloud Services Panel* replaces the *Data Centre as a Service Multi Use List*. The greatest change other than the inclusion of new services and service providers, is the change from a Multi Use List to a Panel. The Multi Use List was in place for three years from October 2012 to October 2015, and in that period the expenditure was approximately $1.9 million divided as follows:

- IaaS: $620,000
- PaaS: $930,000
- SaaS: $330,000

Cloud contracts

There are likely to be many times when agencies intend to purchase cloud services directly rather than using the Cloud Services Panel. Government does not have a template contract for cloud services, so agencies will need to develop a cloud services contract or use a law firm that has existing cloud services template.

Information access

The benefits of cloud computing are numerous. However, there are risks that you need to understand. Commonwealth procurement officials should ensure that the key risks are

managed through the procurement and contract drafting process. Some of these key risks are set out below.

Privacy

Privacy issues with cloud computing can arise at both the Australian and trans-border levels.

Privacy and data security considerations must be addressed when transferring any confidential information or personal information into a Cloud environment.

The Department of Finance website has a Better Practice Guide – Privacy and Cloud Computing for Australian Government Agencies[1].

If services are to be provided from outside Australia, particular care must be taken to put in place enforceable provisions that protect personal information. Agencies should identify what countries data will be stored in and ensure they comply with the obligations in the Privacy Act 1988 (Cth) relevant to the transfer of data overseas.

Agencies should maintain control over use and sharing of information through effective contractual protections. At the very least Commonwealth Agencies must discharge their responsibilities under the Privacy Act 1988 to take contractual measures to ensure that service providers do not breach the privacy principles. The contract should contain specific provisions such as:

- requiring the service provider to comply with principles regarding collection, use and disclosure of personal information
- ensuring the agency has the right to access, recover and correct personal information at all times
- restricting the flow of data off-shore
- providing for how the information is dealt with at the end of the contract.

Some service providers may have data centres in multiple and undisclosed locations, giving jurisdictional uncertainty. The customer can seek to specify in the contract the region or regions where the data will be stored and accessible, or where the data services centre will reside.

FOI Compliance

Any Cloud services arrangements must permit the relevant agency to comply with its obligations under the *Freedom of Information Act 1982 (Cth)*, in particular accessing information in the event that an FOI request is received.

In relation to compliance with Australian laws and regulatory requirements generally, be aware that information may be stored or processed through the Cloud in places with significantly different jurisdictional risks.

Security

Foreign government rights of access to data will apply in many overseas jurisdictions. It is important that Agencies understand which foreign laws apply to their data and assess the appropriateness of these laws. If an Agency is comfortable with a particular foreign government accessing the data in accordance with foreign laws, the contract should restrict such disclosure of data to circumstances where the disclosure is needed to meet an enforceable governmental request. The contract should require the service provider to notify

[1] http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

the customer if data has been disclosed – and to notify the customer in advance of any disclosure, if permitted by law.

The Privacy Amendment Act, and the Australian Privacy Principles which came into effect in March 2014, imposed more onerous requirements in relation to cross-border data flows in particular regarding notification to and consent from individuals. Agencies should ensure their contracts reflect these new requirements, and that existing contracts are reviewed and updated if needed.

Data security for cloud customers is a business risk as well as a legal risk. Some typical data security issues, and the types of physical, technology or procedural controls that can be applied under customer contracts in order to maintain data security, are as follows:

To protect data from unauthorised access by a third party:

- Data encryption
- Monitoring and management
- Gateway technologies
- Email content filtering
- User authentication
- Service provider's security posture – physical & IT

To protect data from unauthorised access by other customers:

- Customer segregation
- Dedicated servers
- Media sanitisation

To protect data from access by unauthorised employees:

- Data encryption key management
- Vetting
- Agency or service provider auditing
- Restrictions on subcontractors

Handling data security incidents:

- Incident response plan
- Notification
- Access

The above refers to data security generally. Refer to the Australian Signals Directorate's Cloud Computing *Security Considerations* for guidance on issues to consider and development of a risk assessment.

Business continuity and disaster recovery

Cloud computing arrangements can raise some very important business continuity and disaster recovery issues as the Agency may have a reduced understanding of how and where its data is stored and its reliance on an uninterrupted service (whether that be a software application or communication network).

It is important that contracts for cloud services address these risks. Some protections that can be included in these contracts include:

- Ensuring the supplier develops and maintains a detailed and robust business continuity and disaster recovery plan
- Ensuring the supplier has a geographically separate disaster recovery site with quick 'failover' to that site
- Ensuring the supplier has uninterruptable power supply and back-up generators that allow for uninterrupted service
- Not allowing the supplier to rely on force majeure provisions unless all business continuity and disaster recovery obligations have been complied with

Ownership and access to data

It is important for Agency's to review the service provider's contract or terms of service carefully. There should be clear provision for customer ownership of the data, and ability to access or transfer it within reasonable timeframes. If it is not clear and appropriate terms cannot be negotiated, then consider whether the data is appropriate for cloud storage.

Depending on the nature of the data and how it is processed, it may also be necessary to provide for the customer's ownership of the results of any processing of the data, and limiting the service provider's use solely to that which is necessary for it to fulfil its obligations under the contract.

The customer should also plan in advance for the end of the contract if circumstances change (if better solutions become available, or the service provider is acquired or goes out of business). The right to retrieve data might not only be business-critical, but also affects legal compliance requirements such as corporate record keeping and litigation (or other regulatory) discovery actions.

The contract should provide for the customer's rights to access data and should stipulate:

- The period of time after termination in which the customer can migrate the data
- The process for retrieval (if the amount of data is very large, for example)
- The transition-out assistance from the service provider (even if at additional cost)
- The format for provision of the data (in particular, not in a proprietary format)
- The requirements for deletion of the data, and sanitisation of the service provider's media
- Any rights of customer audit.

IT Governance

One risk with easy access to cloud software as a service is that each business unit in the organisation may acquire different cloud solutions to address a similar need. John Sheridan, the Australian Government CTO, referred to the possible 'explosion of IT' with the risk that a 'business discovers it has five or six financial management systems [or]…discovers that it doesn't know where its data is [or]…discovers that important corporate data is distributed' widely across dozens of disparate data stores systems.

This risk can be mitigated through appropriate ICT governance and maintaining an architectural view of ICT across the organisation.

Further information

AGIMO has developed very useful guidance material[2] to assist Agencies with procuring cloud services including guidance relating to:

- implementing cloud services
- privacy and cloud computing
- legal issues in cloud computing agreements
- financial considerations for using cloud services

SOFTWARE ASSET MANAGEMENT

The high volume, low value problem

The proliferation of software means that organisations often have a high volume of low value software purchases to make each year. The majority of low value software will be licensed on the vendor's standard terms. This creates challenges around how the licence agreements for the software items will be reviewed.

Is it practical to have a lawyer review every software licence? If the licence is not reviewed, what risk is the agency taking?

Templates and terms

The value and complexity of software purchased or leased by the Commonwealth can vary significantly. It is therefore important to determine what contractual terms are appropriate for the procurement. Some of the factors that will influence the template or other terms you adopt include:

- Whether the software is commercial-off-the-shelf (COTS) software, COTS software that requires modification, or new software that needs to be developed by the service provider (bespoke software);
- If the software is developed software, whether you want to own the software or receive a broad licence to the software
- Whether you require upgrades, updates, bug fixes and/or technical support for the software
- Whether you require extensive modification and adaptation rights
- Whether the software includes a high number of components owned by other third parties
- Whether the software will be integrated with other software and systems or has complex installation requirements

The Australian Government's SourceIT template suite has the following two software procurement templates:

- SourceIT COTS licence only
- SourceIT COTS licence and support
- SourceIT Plus for developed software

[2] http://agimo.gov.au/policy-guides-procurement/cloud/

The SourceIT website provides guidance on when the templates should and shouldn't be used[3].

Most vendors will not agree to apply a SourceIT template to low value software licences. Their volume and leverage positions means they would often rather forgo the sale than negotiate licence terms,

Licence rights

Standard licence terms

The licence rights to the software that your Agency requires will depend on a range of factors including:

- how the business area or other Agency personnel will use the software;
- who needs access to the software (e.g. contractors that provide services integrated with the software or an Agency's outsourced provider);
- the platforms on which you will install the software (e.g. on a server or on individual desktops etc);

The licence will generally address:

- Usage rights
- Duration
- Termination
- Geographic application
- Exclusivity
- Assignment

Licensing and pricing models

It is critical to determine the basis on which the number of licences is determined. This may have a significant impact on the price and may result in a Customer breach if the Customer does not comply with the contracted licence terms. Software can be licensed on a number of bases including:

- Per user based licensing – total users, names users or concurrent users
- Per desktop (or seat) licensing
- Enterprise licensing (e.g. a whole Agency)
- Per server licensing

If user based licensing is adopted, it is important to determine what a 'user' is. Does a user include contractors? Are users only FTE personnel or all personnel who might access the software? It is critical that Agencies have a strong understanding of the licence terms they require and comply with those terms.

[3] http://agimo.gov.au/policy-guides-procurement/sourceit-model-contracts/

Additional licence terms and protections

Agencies may require additional or alternative licence terms in order to manage particular risks or achieve broader rights to the software. Some of the additional rights Agencies should consider include the right to:

- Customise and configure the software
- Transfer the software between the Agency's systems at no additional cost
- Make copies of the software for user training purposes
- Maintain and support the software if the supplier breaches its support obligations
- Re-install software without affecting the software warranties
- Deploy the software and documentation to servers or desktops through the use of virtualisation technologies

If the supplier is providing software that contains software sub-components that are owned by a different entity to the software supplier, try to secure the same licence terms for all the software or ensure that the supplier offers minimum standard terms for the third party component.

Some software suppliers will bundle and unbundle their standard software options during the term of the licence. For example, the supplier may sell you software A and then later bundle software A with software B to create software C. The supplier may then seek to charge the customer for the new and improved product. It is important to ensure the software licence in the contract applies to any bundled, rebundled, or rebranded software without any additional charges being payable by the customer.

Similarly, if the supplier removes functionality from the existing software as part of a rebundling of the software or the sale of that functionality to another software company, the contract should include an obligation for the supplier to provide that removed functionality at no additional charge and on the same licence terms.

Restrictions

It is common for software suppliers to include some restrictions in their licence terms. Whether certain restrictions are acceptable will of course depend on the Agency's requirements but some common restrictions that are generally acceptable include:

- No Decompiling, disassembling or reverse engineering or otherwise trying to derive the source code from the object code
- No selling, renting, leasing, timesharing, transferring or sublicensing (unless otherwise authorised under the licence)
- a requirement for the Agency to ensure its personnel comply with the software terms (this will require personnel to be well trained)

Software development terms

If an Agency requires a supplier to develop new software or modify the supplier's existing software, the Agency should consider including a number of additional protections, for example:

- a requirement for all intellectual property rights in the developed software to be owned by the Commonwealth or a very broad licence to that developed software
- a requirement that the source code, documentation and all other material needed to support the software are held with an independent escrow agent to ensure the customer

can access this material in certain circumstances (see below for more details about escrow)

- a software engineering and development process with clear and detailed Acceptance Criteria and rigorous Acceptance Testing to establish compliance with the Acceptance Criteria

IP ownership

It is critical that Agencies consider whether developed software will be owned by the Agency or owned by the contractor. The Agency should conduct an 'IP Needs Analysis' to determine the Agency's preferred position with respect to the IP rights in the software. This is determined by working out what the Agency's needs are in relation to the software. Some considerations include:

- Is the software highly sensitive and use of the software by another party could impact national security (this may indicate that the software should be owned by the Commonwealth)
- Could the Agency, Commonwealth or marketplace benefit from the supplier owning the software and commercialising it (e.g. increasing the supplier's client basis may drive efficiencies for the supplier which reduce future licensing and support costs for the supplier's clients)
- Could the commercialisation of the software by the supplier improve innovation in a particular market?
- Does the Agency have a need to commercialise the software (it is unlikely that it will unless commercialisation is part of the Agency's business (e.g. CSIRO)
- If the Agency does seek to own modifications that it has paid a supplier to make to the supplier's software, are the new software elements separately useable by the Agency. If not, there is little benefit in the Agency owning the modifications

If an Agency agrees to the supplier owning software developed for the Agency, the Agency should consider seeking a price discount that reflects the benefits the supplier is obtaining through ownership (i.e. the ability to commercialise a product for which the Agency has paid the supplier to develop). Agencies should not act as 'R&D' financiers.

Escrow

When including an escrow requirement, it is important to be clear about the escrow process including:

- When the supplier has to deposit source code in escrow (e.g. at incremental stages of the software development process or just upon final Acceptance of the developed software)
- How often the supplier is required to update the source materials in escrow
- The events that trigger a requirement for the escrow agent to release the source materials (e.g. expiration or termination of the software development contract or if the supplier fails to comply with its software support obligations)
- Which party pays for the cost of escrow (e.g. the costs are split between the customer and supplier or just the supplier)

Support

If your Agency requires support and maintenance for the software you will need to consider the specific support requirements and some of the risks. These considerations include:

- What manuals and supporting documentation is required
- What consulting services are required
- What help desk and other help channels are required
- When is support and maintenance required (do not commence until after the software has been formally accepted)
- Do you need updates? (eg bug fixes and changes that are made to overcome defects)?
- Do you need New Releases? (a substantially enhanced version of the software with new and improved functionality)
- How long do you need to evaluate New Releases?
- What service levels will apply (eg response times and resolution times, defect reporting timeframes, maximum number of outstanding defects etc)

For developed software, it is important to ensure the supplier does not charge for services it is obligated to provide under its warranty obligations.

Negotiating with large software suppliers

The ability to negotiate with large software suppliers will largely depend on the value of the contract.

In large high-value contracts, it is often possible to negotiate the inclusion of protections in software licenses with some of the world's biggest software giants. In the last 5 years or so, more 'customer favourable' terms have been achieved with suppliers such as SAP, Microsoft and IBM on large deals and WoG arrangements.

In small low-value contracts, it may not be possible to secure some of the protections outlined above when negotiating with large software suppliers. Minor variations to the supplier's standard terms might be acceptable and it may not represent value for money to seek to negotiate broader protections. However, software procurements should involve at least consideration of these protections (and other protections included in more customer favourable government software purchase contracts).

An Apple example.

It is worth liaising with other Agencies who have had recent experience procuring software from large suppliers to see if piggy-back options are available and to discuss additional protections the Agency has achieved, subject to the confidentiality restrictions in their software contracts.

Embedded software

If there is software or firmware (including operating system software) that is installed or provided on the hardware, the contract should include, at a minimum, an obligation for the supplier to grant the Agency a licence to use that software. The licence should allow the Agency to use the hardware for the purposes outlined in the contract. If the contract also separately covers the license of software and that licence provides more extensive rights (as outlined in the software section of this paper), the Agency should seek to include an obligation for the software contained on the hardware to be subject to the terms of that more extensive licence.

VIRTUALISATION

What?

Thin-client computing is a computer architecture in which a significant proportion of the computer processing is performed by servers in a centralised data centre rather than on individual desktop computers at employee workstations.

In traditional thick-client computing, software applications (ie the computer programs used by employees) run on individual desktop computers at employee workstations. In thin-client computing, software applications run on centralised servers and are then distributed to the employees' thin-client terminals over the organisation's computer network.

Why?

The purported benefits of thin-client computing include:

- Increased efficiency through use of centralised computing resources (less hardware and less energy consumption)
- Increased security and control (including increased protection from the use of unauthorised software and viruses)
- Software, hardware and application changes are made once at the data centre
- Reduced purchasing costs for end-user devices (because desktop computers are replaces with less expensive thin-client terminals with no internal or attached hard drives for data storage)
- Reduced maintenance costs (primarily through less IT support staff required to fix problems with individual desktop computers)
- Increased productivity (primarily through greater uptime and shorter repair times)
- Increased mobility.

Software licensing in the thin-client environment

The two most significant software licensing issues to consider when transitioning to a thin-client or virtualised environment are:

- software pricing models that could result in higher licensing costs for software applications in the thin-client environment
- licence restrictions that prohibit use of the software application in a thin-client environment.

Software Pricing Models

Software applications are licensed using many different pricing models. Common software pricing models include pricing models based on processing power running the software, number of devices on which the software application is installed, number of people using the software application, size of the organisation using the software application and outputs produced by the software application.

The software application pricing models that are most likely to cause increased cost in a thin-client environment are deployment based pricing models (eg per device licence) and geographic pricing models (eg per site licence).

- Example 1 – A software application is currently licensed per device. If the thin-client architecture assigns the software application based on user profile (not device), a single user may require multiple licences for the software application if they use the software application on multiple devices.
- Example 2 – A software application is currently licensed per processor. If the thin-client architecture has dynamically load balanced resource pools, every processor in the resource pool may need a licence (even if the virtual processors created out of the resource pool only use a fraction of the pools processing power).
- Example 3 – A software application is currently licensed per instance. If for a single user the thin-client architecture will run the software application on both the server and the virtual machine, a single user may require multiple licences.
- Example 4 – A software application is currently licensed for a particular site or region. If the thin-client architecture assigns software applications based on user profile (not device), a single user may require multiple licences if they use the software application at multiple sites.
- Example 5 – A software application is currently licensed per instance. If the transition plan involves running both the current thick-client environment and the new thin-client environment in parallel for a period of time, a single user may require multiple licences.
- If a thin-client transformation project is not managed appropriately, this can lead to significant increases in software application licensing costs. This increased cost could exceed the benefits of the new architecture. The good news is that if the issues are managed early they can usually be addressed.

Common Restrictions that May Affect the Thin-Client Architecture

The typical 'purchase' of a software application does not give you ownership of the software application, but rather a license to use the software application. The licence agreement sets out how you can use the software.

A software application is only permitted to be used in accordance with the terms of the software licence that applies to that software application. Software licences include various restrictions. Common restrictions in software licences that should be considered to determine if they prohibit use of the software application in a thin-client environment include:

- VIRTUALISATION: You may not use the software application within a virtual (or otherwise emulated) hardware system.
- DEVICE: You must not install the software application on a device other than the device on which the software application was originally installed OR You may only install the software application on an authorised device.
- SERVER: You must not install the software application on a computer file server.
- MODIFY: You must not modify or adapt the software application, including by removing the installer program.
- EXPORT: You must ensure that the software application is only used in the country in which it was purchased.
- NOTICES: You must not remove any notice from the software application. You must not allow the end user licence agreement file to be separated from the software application.
- AUDIT: You must provide audit reports on your usage of the software application on a quarterly basis.

Using software applications in a way that is not permitted by the licence risks:

- infringing the intellectual property rights in the software application and being sued by the IP owner or for government agencies, having to make a payment to the IP owner under a crown copyright licence
- breaching the licence agreement and being sued by the licensor.

What to do

The best approach to dealing with software application licensing issues in a thin-client environment will depend on many factors including your specific organisation, architecture and objectives. Common steps include:

Step 1: Conduct an audit to identify all of the software applications for deploying on the thin-client environment

Step 2: Review the software licences to determine if use of the software application in the thin-client environment:

- will result in higher licensing costs (that are not budgeted)
- is prohibited by a restriction in the licence.

Step 3A: If the software licence is okay, deploy the software application in the thin-client environment.

Step 3B: If the software licence is not okay, there are various options including:

- seek permission from the software application vendor
- obtain additional or expanded licences
- package and deploy the software application differently
- do not migrate the software application to the thin-client environment and retire it or replace it with an alternative .

Some specific project level actions that may assist include:

Action 1: For software applications that have a ‘per device’ pricing model

- in the short term, use IP address control functionality to only allow the software application to run on the end user’s primary device
- over time (and immediately for those applications for which use of the IP address control functionality is not suitable), liaise with the software vendor to convert the licence for that software application to a ‘per user’ pricing model.

Action 2: For software applications with a licence that prohibits use outside Australia, use IP address control functionality to only allow the application to run on devices in Australia.

Action 3: For licences that prohibit removing the installer, do one of the following:

- use a software application packaging method that does not remove the installer
- write to the vendor seeking approval to remove the installer for the purpose of packaging the software application for deployment on the thin-client environment.

Action 4: Ensure that software application groups include only current software application users.

Action 5: For software applications that are licensed per instance, do not deploy the application in parallel on the current environment and thin-client environment without vendor approval.

Action 6: Package the software applications in a way that notices (eg copyright notices and EULA text files) are not removed during the packaging process.

Action 7: For software applications that are licensed as part of a suite of products, ensure that the software applications that are part of the suite are deployed together (and not distributed between multiple users).

Above all, seek expert legal advice from someone who understands both the legal and technical aspects of thin-client environments.

Ongoing compliance

For each software application that is deployed on the thin-client architecture, ensure that there are controls in the new architecture to remain compliant with the software licence into the future.

Example 1 – A software application is licensed on a virtualisation subcapacity basis and is deployed on the thin-client architecture. It is necessary to ensure that the processor capacity available to the software application is limited to the amount licensed. During initial deployment it is not uncommon for more processor capacity than initially intended to be made available. This could result in licence fees that significantly exceed the amount funded.

Example 2 – A software application is licensed on a concurrent user basis and is deployed on the thin-client architecture. It is necessary to ensure that there are controls in place to prevent the number of users accessing the software application at any one time from exceeding the number of concurrent users permitted by the licence.

Example 3 – A software application is licensed as a package of products. It is necessary to ensure that there are controls in place to prevent the packaged products being distributed between multiple users or devices where that is prohibited by the licence.

Example 4 – A software application is licensed per instance. It is necessary to decommission virtual machines that are no longer needed to avoid paying excess license fees.

Example 5 – A software application is licensed per device connected to the server. It is necessary to understand and then control whether this is for every connected device or only those devices that are running or able to run the software application.

KNOW THIS

- Big Data
- Agile
- Internet of Things

QUESTIONS?