

# Guidelines

F o r I T M a n a g e m e n t



March 2010 – Number 334

## A Leap into the Unknown?

### Securing Data in the Cloud



Since 1966, the National Computing Centre (NCC) has been helping organisations to manage IT processes and systems development and equip people with the skills to ensure business effectiveness. We do this through a unique membership service that brings together professionals and experts to identify, create and disseminate knowledge and experience across the spectrum of IT issues.



National Computing Centre  
Oxford House, Oxford Road  
Manchester M1 7ED

**NCC Guidelines**

The National Computing Centre  
Oxford House  
Oxford Road  
Manchester  
M1 7ED

Website: [www.ncc.co.uk](http://www.ncc.co.uk)

Tel: 0161 242 2121  
Fax: 0161 242 2499

© The National Computing Centre 2010  
No part of this publication can be reproduced, stored in a retrieval system, transmitted or made available to the public in electronic form or by any other means (electronic, mechanical, photocopying, recording or otherwise) without the written permission of the publisher. Whilst every care has been taken to ensure the accuracy of the

editorial content the publisher makes no representation and gives no warranty as to its accuracy and cannot accept any liability for any direct, indirect or consequential damage or loss howsoever caused arising out of or in connection with the content of this publication.  
First Published March 2010

<b>Contents</b>	page
1. Introduction	3
2. A Virtual Revolution	3
2.1 Moving toward a definition	3
3. Safety First	4
4. What is e-Disclosure?	5
5. Legal Risks of Cloud Computing	7
5.1 Security and data integrity	7
5.2 Back-up and recovery	8
5.3 Data location	8
5.4 Retention policy compliance	9
5.5 Business continuity and transferability	9
6. Choosing a Supplier	10
7. Conclusion	11
8. Definitions and Glossary	12

## About the authors



### John Lang, IT Director at Epiq Systems

Epiq Systems is a leading provider of integrated technology solutions for the legal profession, enabling clients to streamline the administration of bankruptcy, litigation, financial transactions and regulatory compliance matters. It offers innovative technology solutions for electronic discovery, document review, legal notification, claims administration and controlled disbursement. Epiq's clients include leading law firms, corporate legal departments, bankruptcy trustees and other professional advisors who require innovative technology, responsive service and deep subject-matter expertise.



### Peter Wood, Member of the ISACA Conference Committee and founder of First Base Technologies

Peter founded First Base Technologies in 1989 as a vendor-independent consultancy. He has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as penetration testing, social engineering and skills transfer. He is also a world renowned security evangelist, speaking at many conferences and seminars on ethical hacking techniques and Internet security. He is a Fellow of the British Computer Society and a Chartered IT Professional, and was recently rated the BCS number one speaker. He also serves on the ISACA conference committee for Information Security Management and Network Security in both the US and Europe.



### John Enstone, Partner, Faegre & Benson LLP

### Anna Byford, Trainee Solicitor, Faegre & Benson LLP

Through its London office, Faegre & Benson LLP advises clients on finance and investment, trade and commercial matters in the UK, EU and in many emerging markets where English law is the preferred system. While John's practice covers many industries, he specialises in the IT and telecoms sectors, in which he has more than 25 years of experience. Anna is a trainee solicitor working in the firm's litigation and finance and restructuring practices.



### Adam Bosnian, VP of Products, Strategy and Sales at Cyber-Ark

Cyber-Ark® Software is a global information security company that specialises in protecting and managing privileged users, applications and highly-sensitive information to improve compliance, productivity and protect organisations against insider threats. With its award-winning Privileged Identity Management (PIM) and Highly-Sensitive Information Management software, organisations can more effectively manage and govern application access while demonstrating returns on security investments. Cyber-Ark works with more than 600 global customers, including more than 35 percent of the Fortune 50. Headquartered in Newton, Mass., Cyber-Ark has offices and authorised partners in North America, Europe and Asia Pacific. For more information, visit [www.cyber-ark.com](http://www.cyber-ark.com).

## 1. Introduction

Although the principle of Cloud Computing is a sound one and offers many benefits to companies, using Cloud Computing architecture can create some real dangers for businesses if care is not taken and the right questions are not asked at the outset.

The data that companies generate is both an asset and a liability. How data is stored and managed can make the difference between winning and losing 'bet the company' court cases. It can cause companies to fall foul of powerful regulations and lead to reputational damage if mishandled.

In these Guidelines, we look at how companies and other organisations can take advantage of Cloud Computing while avoiding the security pitfalls. We consider the growth and application of Cloud Computing and in this context explain the challenges of 'e-disclosure' (the process of retrieving and collating data to be used as evidence in court or as part of a regulatory investigation).

These Guidelines go on to highlight the key issues that need to be addressed by companies when contemplating moving key functions into a Cloud Computing environment before any contracts are signed and look at how negotiations should be approached.

Cloud Computing looks set to revolutionise the provisioning of technology services, but as with any new technology, mistakes will be made and some early adopters will pay the price. These Guidelines can help your organisation avoid this fate.

## 2. A Virtual Revolution

Market intelligence firm IDC estimates that the global value of SaaS contracts alone is now \$10 billion per year – and this figure is likely to continue growing as companies balk at the cost of buying in proprietary systems during the economic downturn. Nevertheless, the market for the provision of Cloud Computing is very young and fragmented; new providers are still emerging and there is little evidence of consolidation going on amongst more established companies in the market.

Companies are unlikely to move their IT infrastructure wholesale into the cloud, but will adopt cloud services when confronted with peaks in demand or the need for new applications or technology. As time goes on, however, many companies are looking closely at the return on investment on capital expenditure. For many capital intensive technology projects, this is difficult to demonstrate. This leaves firms with the choice of outsourcing their future software, processing and storage needs via the cloud – or sticking with their existing ageing and potentially inefficient IT infrastructure.

### 2.1 Moving toward a definition

Cloud Computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models.

#### **Key Characteristics:**

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service's provider.
- Ubiquitous network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).
- Location independent resource pooling. The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for rent often appear to be infinite and can be purchased in any quantity at any time.
- Pay per use. Capabilities are charged using a metered, fee-for-service, or advertising based billing model to promote optimisation of resource use. Examples are measuring the storage, bandwidth, and computing resources consumed and charging for the number of active user accounts per month.

Clouds within an organisation accrue cost between business units and may or may not use actual currency.

Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

**Delivery Models:**

- Cloud Software-as-a-Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Cloud Platform-as-a-Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g. Java, python, Net). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.
- Cloud Infrastructure-as-a-Service (IaaS). The capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g. firewalls, load balancers).

*'Is my data safe?  
The short answer  
is yes – and no'*

**Deployment Models:**

- Private cloud. The cloud infrastructure is owned or leased by a single organisation and is operated solely for that organisation.
- Community cloud. The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- Public cloud. The cloud infrastructure is owned by an organisation selling cloud services to the general public or to a large industry group.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting).

Each deployment model instance is one of two types: internal or external. Internal clouds reside within an organisations network security perimeter and external clouds reside outside the same perimeter.

### 3. Safety First

Is my data safe? The short answer is yes – and no. Cloud Computing does carry some inherent risks – breaking up and sharing data between servers does create greater vulnerabilities than retaining data on a dedicated server in a known location. These risks, however, are not insurmountable and the key to ensuring data security in a cloud environment is less an issue of what security is in place, but who is providing it.

The extent and sophistication of encryption can vary between providers. There are a number of different kinds of encryption, and varying levels of sophistication. For example, the security gold standard is 256-bit encryption but many providers, for cost reasons, only offer 64-bit or 128-bit encryption. Some even throw the risk back at the client to ensure that their data is securely encrypted.

#### Encryption in the Cloud

Typically, encryption is intended to prevent unauthorised disclosure of data. The risks of unauthorised disclosure are considerable, with the potential for exposure of customer details, credit card data, personal information, business plans and more. The impact could range from loss of competitive advantage to criminal prosecution and loss of shareholder confidence. There are three fundamental areas of risk for unauthorised disclosure to consider in a Cloud Computing model: the cloud provider, data in transit and at the cloud customer.

### 1. The Cloud Provider

There are a number of ways disclosure could occur at the cloud provider, including attacks against their Internet-facing devices, unauthorised access by their staff, malware infection of internal systems and even unintentional or deliberate access by other customers. In this scenario, encryption of data is a sensible countermeasure that can ensure that data at rest within the cloud provider's network can only be accessed by the customer.

There are two ways to encrypt data in the cloud. The first involves encryption at the customer's premises prior to transfer to the provider. This is secure, since the provider has no way to access the data, since the encryption keys are held by the customer. The alternative is to grant the provider a second set of keys that allow access to the data. This then permits the provider to offer additional services such as search, archiving, and format conversion. This less secure alternative will require the customer to assure themselves of the provider's operational security.

### 2. Data In Transit

The risk of data disclosure during transmission is such that encryption is essential. When data is transported across an untrusted or uncontrolled network like the Internet, it must be encrypted. Typically this is achieved by SSL or TLS (via an HTTPS connection), although care should be taken to ensure that only the strongest versions are used. Cloud services that use unencrypted HTTP connections should be used only if the data being sent is already public or if the data is already encrypted at the customer's premises.

### 3. The Cloud Customer

The most common source of data loss or disclosure remains the employees or contractors within the organisation that owns the data. Staff may have legitimate access to the data but use it in an unauthorised way, or poor access controls may permit them to gain access to the data.

In this situation, blanket encryption is not practical. Instead, sensitive or confidential data should be protected on a case-by-case basis, using file-level encryption or encrypted documents using strong passwords.

#### Summary

Organisations intending to store data in the cloud should plan thoroughly, ensuring that they consider each risk area and the relevant countermeasures carefully. A combination of encryption techniques for data at rest in the cloud, during transmission and at the customer's premises is essential to mitigate these risks. Only when the organisation is happy with the plan, and all the necessary controls are embedded in the contract with the provider, should they consider entrusting their data to 'somewhere in the cloud'.

*Peter Wood, Member of the ISACA Conference Committee and founder of First Base Technologies.*

As well as the integrity and safety of company data, there is also some growing concern of the risks of losing precious intellectual property by placing it in the cloud. As record companies, amongst others, know to their cost, once the distribution of material goes out of their control, it can be very difficult to get it back.

Given the variables, transparency is key. Some providers can be very coy about revealing exactly how, and where, the data entrusted to them is handled. This should ring alarm bells. If customers – or their consultants – are to be able to properly evaluate the security of their data with a Cloud Computing service provider, then it is imperative that they are given access to their security architecture as well as being provided with detailed information on their data management policies and processes.

In addition to the type and level of encryption used by a provider, some of the important questions to ask revolve around the hardware they use – do they use storage area network (SAN) solutions, or do they rely on network attached storage (NAS)? What types of V-LAN servers do they have and what switches do they use? There are not necessarily right or wrong answers to these queries, but all can have security implications in certain contexts. Moreover, even with those providers that can demonstrably tick all the right boxes, it is also wise to check what would happen in the event that they are taken over by another provider.

It can be a struggle to elicit this information as some Cloud Computing service providers like to retain as much flexibility as they can and, in a price sensitive market, keep their overheads to a minimum. The good news is that there are plenty of providers – both large and small – in the marketplace that can provide both the security and the transparency that businesses need. The challenge, in what is still an immature market, is to sort the wheat from the chaff. If in doubt, walk away.

### 4. What is e-Disclosure?

E-Disclosure (also known as e-Discovery) is the process of finding, securing and providing electronic data with the intention of using it as evidence. Simply put – it's the process of turning data into evidence.

The disclosure process is a well-established one, but the growth in electronic documents has created new challenges for companies and their lawyers when faced

with a document review exercise. The first of these is volume. Where, in the past, reviewing 50,000 documents would have been considered a big project, it is now not uncommon for the number of items involved in document reviews to run into the millions. Documents also come in many more forms than in the past, most notably in the form of emails. This growth of electronic documents has made the process increasingly unwieldy, potentially inaccurate and, ultimately more expensive.

The need to be able to find key documents quickly and accurately is becoming more acute in the present economic climate. Not only does the amount of litigation usually rise in a recession, but one response to the financial and corporate failings that led to the credit crunch has been to give regulators enhanced investigatory powers and the official will to use them. In practice, this has led to a sharp rise in the number of dawn raids and information requests.

These can present a particular challenge for companies due to the tight timetables that regulators usually impose on their targets. For many companies, document retention and discovery policies have generally been formulated in anticipation of litigation rather than regulatory interventions. However, where the timescale for discovery in litigation can be measured in months, sometimes years, regulators commonly expect to receive the evidence they require within 30 days. Moreover, regulatory investigations are very often much wider in scope and, as a result, involve many more documents, which may come in a variety of forms.

Failing to produce documents for a regulator or in the course of litigation can have serious consequences for companies, as can failing to implement adequate data management and retention policies in the first place.

### Controlling your IP in the cloud

Cloud Computing has a huge potential impact on our businesses. With a whole host of benefits such as cheaper to run 'pay as you go' structures and minimal set up costs, businesses are eager to get involved. In fact, with computing resource giants like Amazon, IBM, Google and Microsoft moving towards offering information and software in the cloud, it appears that Cloud Computing is more than just the latest buzz word.

However, as a new concept, Cloud Computing carries untested risks to your businesses' intellectual property (IP). No company should enter the world of Cloud Computing without conducting a thorough due diligence and risk analysis, and putting into place the necessary protections.

Cloud Computing still allows for the creation and storage of original work in the cloud. As with all other IP, the appropriate contractual clauses need to be established and, where possible, registrations made to protect such works. In particular, if the relationship between the cloud provider and you, the cloud customer, leads to potential confused IP rights as it frequently does, it is advisable to have in place an agreement setting out which party will own, and have a right to use, the IP prior to any activities in the cloud.

As many IP protections available come in a contractual form, the relative bargaining power between you and the cloud provider comes into play. Where the cloud provider is in a strong bargaining position, or you simply do not have the ability to negotiate contractual clauses, it is important that you first assess the value of your IP and then the risks posed by the cloud. Do the IP provisions put in place by the provider allow you to protect your IP sufficiently? If not, will any further contractual protections compromise the quality of the service provided?

When you are in a strong bargaining position, it is desirable to be able to demand substantial compensation for the breach of any IP clauses, including express circumstances whereby you can terminate the agreement.

Rules should be established early on governing the IP rights through confidentiality and non-use clauses which expressly preserve sensitive information, in particular the rights and obligations of both you and the cloud provider in protecting such information. Equally important are provisions allowing for early notification of security breaches so your business can quickly minimise the damage personally, rather than waiting for another party to do so.

Fortunately, many of the potential IP pitfalls related to Cloud Computing are not exceptional. Existing risks and protections for other internet services are a useful starting point when managing the risks facing IP in the cloud. The key is not to be blinded by the hype, to determine exactly what IP you own and to enter into the cloud fully informed and prepared for the risks involved.

*John Enstone (jenstone@faegre.com) is a Partner in Faegre & Benson's London office, where he leads an IT, IP and outsourcing practice. Anna Byford is a Trainee Solicitor who works closely with John.*

## 5. Legal Risks of Cloud Computing

If care is not taken, Cloud Computing and companies' legal obligations can be a toxic mix. Failure to meet regulatory requirements can lead to hefty fines, negative publicity and criminal convictions for leading executives. Moreover, in litigation, failing to meet deadlines to disclose documents can lead judges to draw adverse consequences, potentially costing companies millions of pounds.

There are a number of ways in which Cloud Computing can lead to problems of this nature. Some are obvious, some less so. In all cases, transferring the service to a cloud provider does not transfer the responsibility if things go wrong. A problem shared is not a problem halved!

### 5.1 Security and data integrity

Data security is by some measure the biggest single concern that companies have about using Cloud Computing services, and presents a number of security challenges for companies over and above the usual. The provision of Cloud Computing services is comprehensive, but it is still a new industry and care needs to be taken when selecting the providers of services, possibly with the aid of a consultant. One of the reasons that service providers are able to provide a cost-effective service is due to the economies of scale they achieve by hosting software remotely from their clients and effectively sharing it between large numbers of different clients. In this situation, it is also common for the client's data to be stored on servers with other companies' data. The key to keeping data safe is to encrypt it.

If companies have researched the regulatory requirements first and have specific needs, they can specify to their service provider what form of encryption is applied to their data. (It is also possible to apply different levels of security and encryption to data sets that are kept on the same server. This capacity is not yet widely available, but it will become so.)

Many regulators have yet to fully appreciate the additional issues associated with Cloud Computing and have yet to develop specific rules for data that is stored in a cloud environment. However, financial regulators are often very aware of the latest standards and are very specific about the levels of security they expect to see, even down to which algorithms are used for encryption. Some even have this information on their websites. Other regulators apply a broader brush. Where this is the case, then security that meets the ISO/IEC 27001 standard (see box) will usually be sufficient, although it is wise to check with the relevant regulators first.

However, in April 2009, the ISO/IEC released a new standard naming six encryption methods which can ensure the confidentiality and integrity of data (see box). It remains to be seen whether regulators begin to insist that this is applied, but it is highly likely that many will.

In addition to encryption, it is also important to know who within the organisation has access to the data, and where they are geographically located – if too many people are authorised to access and/or amend a company's data, it can represent a serious security and accountability risk. Moreover, service providers should be able to limit access as narrowly or widely as the client requires and should also be able to provide logs of who has accessed the data and when.

It is also wise for companies to look not only at how a provider will protect the confidentiality of their data, but also its integrity. What is often less appreciated in this respect is the importance – and fragility – of the integrity of data and in particular, the 'metadata' contained in electronic documents. Much of the value of electronic evidence is often contained in its 'metadata', the invisible record of who has read a document, for example, or when or how it was amended.

This can be damaged irrevocably by the careless handling of electronic documents. In some instances, metadata can be destroyed or altered simply by copying files from one medium to another, or just by turning a computer off and then on again, as its internal processes constantly update the metadata. Failing to properly protect or select electronic evidence, including metadata, can lead to negative inferences by regulators or the courts. In the US, the concept of 'litigation hold' is applied to electronic data. Data is extracted and held in a stable environment as soon as litigation proceedings or an investigation is launched, so that the integrity of electronic evidence is maintained. While the case law around spoliation is developing in the US, it remains untested in the UK courts. This can only be a matter of time, however.

*'If care is not taken, Cloud Computing and companies' legal obligations can be a toxic mix'*

**The ISO/IEC 27001 Standard**

The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organisation for Economic Cooperation and Development) principles, governing security of information and network systems. It is supported by a robust audit and certification scheme.

ISO/IEC 27001 requires that management:

- Systematically examines the organisation's information security risks, taking account of the threats, vulnerabilities and impacts;
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable; and
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

**The ISO/IEC 19772 Standard**

The standard, ISO/IEC 19772, Information technology – Security techniques – Authenticated encryption, specifies six encryption methods (based on a block cipher algorithm) that can be used to ensure:

- Data confidentiality (protecting against unauthorised disclosure of data)
- Data integrity (enabling recipients to verify that the data has not been modified)
- Data origin authentication (helping recipients to verify the identity of the data).

The standard takes the specific security needs of different operations into account. For instance, while encryption may be used to prevent eavesdropping when data is being exchanged, Message Authentication Codes (MACs) or digital signatures are ideal for protecting data from being modified.

**5.2 Back-up and recoverability**

In the event of an e-disclosure exercise, speed and accuracy are usually essential, especially in the context of a regulatory enquiry where deadlines can be extremely tight.

Data must be stored in such a way that it can be quickly recovered in the event of litigation, regulatory, or criminal investigation, and it is essential that organisations have a plan in place for the recovery of data before the event.

Regulators in particular can impose extremely tight timescales on companies to provide them with information and draw very negative inferences from a company's failure to produce documents on time. While in litigation the discovery process can take months, regulators often impose a 28-day deadline, even where the number of items involved in document reviews runs into the millions. A poorly-conceived back-up and storage system can make the e-discovery process extremely slow, which, in itself, has led to regulatory penalties being levied on companies when the response to an information request is too tardy. In the event of an adverse judgement a perceived obstruction can also lead to an increase in the main penalty.

Deficient back-up systems can also lead to the loss of key documents, especially emails, and the failure to produce important pieces of evidence will almost always be viewed very seriously by courts or regulators. There is no ISO standard for how back-up procedures are implemented, although regulators and the courts will often apply an 'industry best practice' test.

It is also increasingly important that litigants are able to describe and demonstrate the methodology they used to recover documents as well as the scope of a disclosure exercise. Very often, different parties will be using different technologies and methods to conduct their respective searches. Bringing the e-disclosure service providers into the initial meeting can help the parties to develop and document a common approach to the process and explain it to the court if necessary.

**5.3 Data location**

One of the features of the cloud is its disregard for political borders. Cloud service providers often move data around the world, sometimes splitting it up and sending it to different locations depending on capacity, use and bandwidth. But data protection, security, privilege and data retention rules vary enormously between individual countries and this can have serious – and unanticipated – ramifications in the context of Cloud Computing.

It is very possible for companies to find themselves in breach of another country's rules, simply because its data is located on a server there. It can also mean that, in litigation, companies may also find that information they thought was confidential can be discovered by their opponents or by regulatory or fiscal investigators because it is on a server in a country with different data protection laws. In some cases, it

has even led to the courts or regulators of one country claiming jurisdiction over a case simply because a company's data was stored in that country, or was accessible from that country. Data protection and privacy laws can also make accessing that data more difficult in some countries so court orders may be required to access some types of document.

The dispersion of data around the world can also slow up any retrieval exercise due to language differences. Just because a server is located in a particular country, does not automatically follow that all the documents contained on it will be written in that country's mother tongue. In a cloud environment, documents held in one country can often originate from many different places and are written in a variety of languages. This means that the primary language of individual documents needs to be identified and documents collated into their respective language groups before review.

Tools exist to do this, but it can add delay and expense to a disclosure exercise.

'Safe harbour' agreements – the best known is between the US and the European Union – can protect a company's data from falling foul of these problems, but it is usually safest for companies to get legal advice on where these problems may arise and to insist that the movement of their data is limited to a definitive set of locations. Some suppliers, such as Amazon, can provide their customers with a 'dashboard' showing where their data is located, and more are bound to follow suit as awareness of the challenges of the global dispersal of data grows.

#### **5.4 Retention policy compliance**

Many companies, especially larger ones that operate in regulated sectors, often have to comply with a myriad of data retention rules and regulations. It is therefore essential to ascertain how much experience the service provider has in dealing with multiple data retention policies and whether a potential provider has direct experience of dealing with multi-national companies in the same sector. It is also important to check that their data retention and back-up extends to emails. Some regulators demand that these are kept for years, but are sometimes regarded as less important than other documents by some data storage and cloud service providers.

It also important for companies to ascertain whether the service will also destroy data when its retention period has expired. Keeping documents and emails for longer than is necessary exposes companies to unnecessary legal risk and makes any disclosure exercise more unwieldy.

Reputable providers will often take legal advice on what will be required from a regulatory point of view before taking on a new client and it is wise for companies to do the same.

#### **5.5 Business continuity and transferability**

There is considerable debate raging in parts of the technology world over whether the growth of Cloud Computing is re-introducing a lack of standardisation to the IT market, after the gradual demise of proprietary standards in conventional software. In reality, the standards used by most Cloud Computing providers are pretty open and inter-operability with other providers remains generally good.

Nevertheless, potential users of cloud systems should take care over what provisions are in place for the transfer of their data in the event of dissatisfaction with their service or the failure of the provider. Specific standards for transferring data between Cloud Computing providers have yet to be developed, although work began on this in March 2009, with the launch of the 'Open Cloud Manifesto' (see links).

The architecture is important here. In the event of insolvency, or breach of contract, some providers are very well set up to transfer a company's data in structured form so that the new provider can pick up where they left off. Others, however, may only return the information without the associated architecture, meaning that the data will need to be re-structured – an expensive and time-consuming exercise. It is important to ask for the source code for their applications in ESCROW (see definitions), so that it can be accessed if the company ceases trading.

It is also important that provisions for the transfer or return of data are clearly laid out at the beginning of the relationship if problems are to be avoided further down the line.

Another potential risk for companies using cloud services is the seizure by regulatory authorities of another company's data if it is co-located on the same server as its own. In April 2009, an FBI raid on a Texas data centre led to the seizure of a hardware cabinet containing the data of a number of businesses in addition to the company under investigation. Despite the crippling effect that this had on these businesses, the court turned down their attempt to get their data back, although the FBI did offer to copy it to blank tapes.

More generally, it is also important that appropriate disaster recovery and business continuity plans are in place. Providers should archive their clients' data so that it can be accessed in the event of a catastrophic failure.

## 6. Choosing a Supplier

Getting any form of outsourcing deal right is always a matter of hoping for the best, but preparing for the worst. Cloud Computing is so new that it is difficult to predict where future problems will arise and how the use of the cloud will conflict with meeting regulatory requirements. Many of the potential problems are not immediately obvious and these issues often only get addressed when it's too late.

In particular, it is important to look into the background of the company providing the service, as well as the people that own and run the company. Cloud Computing is a new industry, and if there are incompetents or rogues involved, it may be too early for this to have become evident without a high level of scrutiny.

That is why it is so important to ask questions about a provider's security policies and to review the credentials of the people administering those policies. It is critically important that companies get comprehensive answers before they jump into the cloud. The cost savings are palpable, but the downsides can be significant if insufficient care is taken at the outset.

Although there are some big names that provide Cloud Computing services, it remains an immature and fragmented industry. Brand names have yet to be established, so when evaluating a service provider, it is important, in particular, to ask for references from their other clients in your sector to ascertain whether they have the experience to deal with your company's retention policies and regulatory environment.

Companies should also ask what legal advice the provider has taken in relation to the issues that they face – and ask for proof. It is also wise for companies to get their own legal advice on what regulators and courts will expect to see in the event of a disclosure exercise. It is certainly helpful to work with a provider that is familiar with the issues and is able to take a strategic approach to the storage and retrieval of their information. Being able to provide more than just the infrastructure is now a key point of competitive advantage for Cloud Computing providers and many are spending considerable time and resource to ensure that they understand and can comply with the needs of their clients.

In the earliest days of Cloud Computing, many contracts were concluded in quite a casual way, with relatively little consideration of what would happen at the end of the contract. However, as with any other form of outsourcing, it is imperative that detailed service level agreements are put in place.

These should ensure demonstrable legal and regulatory compliance, searchability, customer care, persistent data integrity and reliability, storage security and integrity for electronically stored information in the cloud. The contract should also spell out the obligations of both parties in the event that the contract is terminated.

*'...it is also important that appropriate disaster recovery and business continuity plans are in place'*

### Advice from Cyber-Ark

Virtually all company IT systems are engineered to support physical drives, so integrating a cloud environment into the IT resource usually involves a lot of work on the software and integration front.

In the real world, you can see your PC or drive has been stolen, but in the virtual world, there are no such comforts.

As a result, meeting compliance and regulation issues is very difficult.

But even secure cloud services have an increased risk of data going walkabout – for any reason – than having your organisation's data neatly tucked up on your own servers. To counter these issues, it is necessary to employ a carefully defined risk analysis of IT systems and procedures before a decision on which cloud technology and service is the best option for your organisation, before later steps such as the creation of service level agreements, remediation procedures and penalty clauses are started.

**The four main stages in this analysis are as follows:**

- 1) ID management and Access Control – who is authorised to do what and when?
- 2) Regulatory requirements – Basel II, SOX, PCI, SAS70
- 3) Data handling processes – where is the company's data located? And how is it managed?
- 4) Staff management – when someone leaves, comes on board or changes roles, what happens?

Whilst Cloud Computing changes the data handling ballgame significantly, provided the IT security technology that is being employed – or planned – by the organisation can handle cloud, as well as conventional, IT data storage systems, the gap between network and cloud-based security analyses is not as great as some experts report it to be.

What is required is an assessment of the expectations that management and the business have for the cloud outsourcing contract – i.e. what precise functions are required to be completed by the outsourcing company? And what are the performance and security criteria that the provider will be held to.

#### Questions to ask your cloud service provider:

##### Who can see my information?

Data loss is now a reality and a sizeable chunk of all data loss incidents are down to third party providers. As a result, you need to know whether the service provider, who is the administrator of the system, can see your data. Most admins have this ability. Therefore, do they have the controls in place to avoid sending, copying, emailing etc your data?

##### What happens if the service provider lost some of your data?

You need to ask your cloud service provider what their data protection policy is and what their audit procedures are. And then you should perform due diligence on those procedures.

##### Are you happy with data co-location?

What does the third party organisation do to separate information and systems? Could your competitor – who is also using the service – get their hands on your data? Remember that, in the cloud, you cannot tell whether your data is copied. So you really need to get this one answered!

##### What happens in the event of data corruption?

How many copies of your data does the third party have? Do they use incremental backups and can they reconstruct an image of your data at a given point in the past from these partial backups. How far back do their backups go in calendar terms?

##### How easy is it to migrate to another cloud service provider?

This a question few companies ask – until it's too late. Porting data between cloud service providers is a relatively new capability and only a small number of service providers have implemented what will become a very necessary service.

##### Are you relying too much on service level agreements?

A service level agreement (SLA) is the contract between you and the cloud service provider. Whilst figures are usually central to most SLAs, you need a remediation process in the event the service provider does not meet their agreement. Things can – and do – go wrong, so it is important to agree the remediation process, as the fate of your company could rest on the integrity of the agreement. Compensation is only part of the equation, as by the time the money is paid, you could be out of business.

Cloud Computing can really work for most organisations, but the principle of caveat emptor – let the buyer beware – applies.

Do your homework and know your options. Nothing can protect you against the unexpected, but for a reasonable cost, you can usually reduce the likelihood of a disaster.

*Adam Bosnian, VP of Products, Strategy and Sales at Cyber-Ark [www.cyber-ark.com](http://www.cyber-ark.com)*

## 7. Conclusion

Cloud Computing offers many benefits for companies and other organisations – the additional legal risks should not stop them from taking advantage.

The potential problems associated with Cloud Computing are not insurmountable, but the youth of the industry and some of the inherent issues that the lack of a defined physical repository for data create, means that much more care needs to be taken when selecting and contracting with Cloud Computing service providers. (See NCC's Legal Guidelines 11: Contracting in the Cloud)

In essence, this means doing detailed due diligence into the background of prospective service providers, asking the right questions about its security policies, back-up and business continuity provisions and ensuring that a comprehensive service level agreement is put in place before any agreement is signed. It also means both customer and provider getting legal advice to ensure that their regulatory and legal requirements are understood and can be met within a cloud environment.

The cost savings from using Cloud Computing are clear, but the downsides can be significant if insufficient care is taken at the outset. Companies will also need to be clear that the whole risk of getting data management wrong continues to reside with the company, even when services are outsourced. This means that the decision over whether to move key functions into the cloud goes well beyond a technical one that can be left to the IT department.

Getting the use of Cloud Computing right can have a significant effect on the whole organisation, for good or ill. Hence it is a whole-business issue that needs the full attention of senior management and not just the IT department. The cost versus risk analysis is a fundamental business decision for companies. It is a decision that needs to be taken by the business as a whole.

*'...the decision over whether to move key functions into the cloud goes well beyond a technical one that can be left to the IT department'*

## 8. Definitions and Glossary

### The ISO (International Organisation for Standardization) and the IEC (International Electrotechnical Commission)

The ISO is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 161 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. The ISO is a non-governmental organisation that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

The IEC is the world's leading organisation that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as 'electrotechnology'. Within this field, the aim of the IEC is to support safety and performance, the environment, electrical energy efficiency and renewable energies. The IEC also manages conformity assessment systems that certify that equipment, systems or components conform to its International Standards.

Both the ISO and IEC have a strategic partnership with the World Trade Organisation (WTO) to assist with underpinning the WTO framework by encouraging international technical standardisation and work jointly to develop international standards in their common areas.

#### Software-as-a-service (SaaS)

The provision of software applications through the internet, typically accessed through a web browser. The software, and consequent data, is stored on the provider's servers rather than the consumer's and the control, maintenance and management of the software is handled by the provider.

#### Infrastructure-as-a-service (IaaS)

The rental of access to processing data storage and network systems through the internet. Unlike SaaS, the user retains ownership of the software and operating systems used, which is usually contained on its own systems, and retains much control over where and how data is located and used.

#### Platform-as-a-service (PaaS)

The use of the provider's infrastructure to host (usually consumer-related) applications developed by the user, which use applications and development tools which are common to both. The user retains control of the application, but not the underlying infrastructure or storage. The most common example is website hosting.

#### Utility computing

The use of computing services – both software and processing power – through the internet on a metered basis in a similar manner to the way that energy is consumed and paid for.

#### Escrow

Source code escrow is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

As the continued operation and maintenance of custom software is critical to many companies, they usually desire to make sure that it continues even if the licensor becomes unable to do so, such as because of bankruptcy. This is most easily achieved by obtaining a copy of the up-to-date source code. The licensor, however, will often be unwilling to agree to this, as the source code will generally represent one of his most closely guarded trade secrets. As a solution to this conflict of interest, source code escrow ensures that the licensee obtains access to the source code only when the maintenance of the software cannot otherwise be assured, as defined in contractually agreed-upon conditions.

#### Links

[http://www.mofo.com/international/EU\\_en/news/15687.html](http://www.mofo.com/international/EU_en/news/15687.html)

<http://www.enterprisestorageforum.com/continuity/news/article.php/3814821>

[http://news.cnet.com/8301-19413\\_3-10258721-240.html?tag=mncol;mlt\\_related](http://news.cnet.com/8301-19413_3-10258721-240.html?tag=mncol;mlt_related)

[www.opencloudmanifesto.org](http://www.opencloudmanifesto.org)

<http://www.standardsinfo.net/info/livellink/fetch/2000/148478/6301438/index.html>





The National Computing Centre  
Oxford Road  
Manchester  
M1 7ED  
[www.ncc.co.uk](http://www.ncc.co.uk)

