Cloud Computing Toolkit

Guidance for outsourcing information storage to the cloud

Nicole Convery
26/08/2010

Toolkit to guide information professionals in assessing cloud computing services for information use and storage and in developing a cloud computing strategy and specific cloud service requirements for their organisations.
Contents

1. Introduction ............................................................................................................................ 4

1.1. Purpose........................................................................................................................................... 4
1.2. Scope .............................................................................................................................................. 4
1.3. Audience ......................................................................................................................................... 5
1.4. Content and structure .................................................................................................................... 6

2. Overview ......................................................................................................................................... 7

2.1. Definition of cloud computing ........................................................................................................ 7
2.2. Benefits of cloud computing ........................................................................................................ 10
2.3. Challenges of cloud computing .................................................................................................... 13
2.4. Top 10 Questions when outsourcing to the cloud ....................................................................... 17

3. Preparing for the cloud .......................................................................................................... 18

3.1. Selection of cloud services and deployment models ................................................................. 20
3.2. Information classification ............................................................................................................. 25
3.3. Risk analysis and assessment ....................................................................................................... 27

4. Managing the cloud ............................................................................................................... 30

4.1. Information management ............................................................................................................ 31
4.2. Legal and regulatory compliance ................................................................................................. 34
4.3. Contract ........................................................................................................................................ 37
4.4. Cost ............................................................................................................................................... 39
4.5. Monitoring, auditing and reporting.............................................................................................. 41
4.6. Exit strategy .................................................................................................................................. 43

5. Operating in the Cloud ........................................................................................................... 45

5.1. Security ......................................................................................................................................... 46
This page was intentionally left blank
1. Introduction

1.1. Purpose
The purpose of this toolkit is to guide information professionals in assessing cloud computing services for information use and storage and in developing a cloud computing strategy and specific cloud service requirements for their organisations.

The toolkit should be used as a starting point for

- a thorough risk assessment exercise to determine the risks and benefits associated with outsourcing services and thus information storage to the cloud, and
- the development of a cloud strategy, specification or requirements for storing information in the cloud.

Users can refer to any sections as required as the toolkit is divided into four specific areas that need to be addressed by different stakeholders or professionals.

The toolkit refers to the use and storage of ‘information’ in the cloud throughout. The use of the broad term ‘information’ is intentional and includes data and records in all electronic formats.

1.2. Scope
The toolkit covers four main areas that should be considered when an organisation intends to outsource business processes and information storage into a cloud environment and should help develop a consistent cloud computing strategy as well as requirements for the required cloud service.

Each of the four main sections proposes questions that should be taken into consideration by the organisation or that should be addressed to the prospective cloud service provider:

- **Overview of cloud computing** – Cloud computing definition, benefits and challenges
- **Preparing for the cloud** – Cloud service selection and risk assessment
- **Managing the cloud** – Information management, compliance, contract and cost
- **Operating in the cloud** – Information security, access and availability

The toolkit is to be used as an aide to the development of organisational strategies and requirements. It is not to be used as a standard or the sole basis for developing a formal contract. The toolkit needs to be used in conjunction with existing organisational policies and strategies that cover information management and security, risk management, outsourcing and procurement, compliance and IT. Each organisation must take into account its own operating environment and ensure that all applicable legal and regulatory requirements form part of any cloud strategy and the resulting contracts with cloud service providers. Legal and regulatory requirements will be referenced in the toolkit but it is outside the scope of this document to provide a detailed analysis.
It is assumed that users of this toolkit will have established a cloud computing strategy and have identified potential processes or information types that lend themselves to be outsourced to the cloud. The toolkit will assist in matching these to the cloud service and deployment models that will best suit the organisation’s business requirements, risk and compliance frameworks. It does not go into detail about how to establish a cloud computing strategy or how the organisation should select processes, applications or information to be moved to the cloud.

The toolkit does not address issues of digital preservation in the cloud because this wide filed is assumed to be a separate organisational concern relating to the management of information that was out of scope of this small project. It is acknowledged that preservation considerations should be part of any information management exercise and they are to some extent covered in section 4.1 of this toolkit.

The premise of this project was to produce guidance on the storage of information in the cloud and not to consider organisational use of social media (or web 2.0) as such. Social media is only one part of a particular cloud service model (Software-as-a-Service or SaaS) when the service is offered via the internet by an external provider and only of interest to this toolkit where information is stored outside the organisational IT infrastructure in the cloud.

1.3. Audience
The principle audience for this toolkit are information professionals (including archivists, records and information managers, compliance managers, information systems and security managers) in public or private sector organisations.

The development of a cloud computing strategy and more specific cloud service requirements is a multi-disciplinary approach that should involve (but is not limited to) a wide range of stakeholders including:

- Records and Information managers,
- IT professionals,
- Legal and compliance professionals,
- Project and risk managers,
- Procurement teams,
- Business process or information asset owners,
- and the cloud service user community

Combined efforts and expertise from these stakeholders will ensure that the envisaged cloud strategy and services will provide return on investment while at the same time fulfilling the organisation’s compliance and business requirements.
1.4. Content and structure

The toolkit consists of four main sections:

Overview – provides an introduction to cloud computing and summarises benefits and challenges facing organisations’ looking to outsource business processes and information to the cloud.

Preparing for the cloud – covers considerations for establishing the right fit between cloud service models and business requirements, for the identification and classification of information to be stored in the cloud, and for the nature of risk assessment needed for such an outsourcing exercise.

Managing the cloud – contains considerations for the management of the information lifecycle to meet governance and assurance requirements for information stored in the cloud as well as contractual, cost and audit issues.

Operating in the cloud – covers technical considerations regarding information (and infrastructure) security and access as well as the availability of services and information in the cloud.

Each section contains a range of considerations covering particular aspects of the overall section topic. Not all considerations might apply to all organisations but each organisation should be clear that is has identified where and why that is the case. Considerations assist in the risk assessment exercise that every organisation needs to perform before outsourcing business processes and information storage to the cloud. Each consideration contains the following elements:

Consideration: The text for each consideration provides a brief description of an issue that should be considered before outsourcing the storage of information into the cloud.

Rationale: The rationale provides the context and reasoning for each consideration. Where appropriate it will identify benefits of implementing the consideration or the risk of not doing so.

Questions: Questions are included to prompt the user to address issues in order to meet the requirements of each consideration. When responding to each question, consideration must be given to the impact of each response for the specification of the cloud service as well as for governance and assurance requirements.

The questions address issues that are particular to the outsourcing of processes and information to the cloud and should be read as in addition to standard outsourcing, contract or procurement procedures of the organisation. The questions are indicative of the issues to be addressed and by no means exhaustive.

References: Add the end of each section resources or standards are provided that can be consulted to gain a more detailed overview of the issues to be addressed.
2. Overview

2.1. Definition of cloud computing

Cloud computing can be described as the ability to access a pool of computing resources which is owned and maintained by a third party via the internet. It is not a new technology but a new way of delivering computing resources based on long existing technologies such as server virtualisation. The 'cloud' as such is composed of hardware, storage, networks, interfaces and services that provide the means through which infrastructure, computing power, applications and services are accessed by the user on-demand and independent of location. Cloud computing usually involves the transfer, storage and processing of information on the provider’s infrastructure which is outside the control of the customer.

Cloud computing paves the way for a business model in which access to ICT resources is outsourced to a 3rd party provider, accessed on-demand via the internet and paid for on a metered basis. Cloud computing services can often be set up quickly, are highly flexible and scalable, and relatively commitment-free which makes them attractive to organisations looking to cut the cost of their ICT provisions and to improve efficiency of business processes. Common cloud-based activities include storing photos and videos online, using online applications such as Google’s Office suite or Microsoft Office Live, using webmail like Gmail or Hotmail, storing computer files online or backing up files online using services such as Jungle Disk or AWS.

There is as yet no standard definition for cloud computing in circulation but the definition from the National Institute of Standards and Technology (NIST) appears to be the most comprehensive to date. It identifies 5 characteristics of cloud computing, 3 main service models and 4 deployment models as follows:

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

**Essential Characteristics:**

- On-demand self-service - users can set themselves up without the help of anyone else
- Broad network access - available through standard Internet-enabled devices
- Resource pooling – computing resources are shared between customers
- Rapid elasticity - consumers can increase or decrease capacity on demand
- Measured Service - consumers are charged based on their usage of computing power, bandwidth use and storage

**Service Models:**

Software as a Service (SaaS) is software offered by a third party provider, available on demand, usually via the internet configurable remotely. The customer does not control the underlying cloud infrastructure (network, servers, operating systems, storage, or individual applications), with the possible exception of limited user-specific configuration settings. Examples: Microsoft Office Live, Google Docs, CRM, project management or payroll services

Cloud Platform as a Service (PaaS) allows the customer to develop new applications using APIs deployed and configurable remotely. The customer does not manage or control the underlying cloud infrastructure but has control over the deployed applications and operating systems. Examples: Microsoft Azure, Google Apps and Force.com

Cloud Infrastructure as a Service (IaaS) provides virtual machines and other abstracted hardware and operating systems. The customer does not control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications. Examples: Amazon EC2 and S3, Windows Live Skydrive

**Deployment Models:**

*Private cloud* - The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.

*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). It may be managed by the organisations or a third party and may exist on premise or off premise.

*Public cloud* - The cloud infrastructure is made available to the general public and is owned by an organisation selling cloud services. Cloud computing resources are shared between all customers in multi-tenancy and exist off premise.
Hybrid cloud - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability.


A more in-depth explanation of the NIST definition can be found at http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/CloudComputingExplained/206526
2.2. Benefits of cloud computing

The list of potential benefits of cloud computing is long and depends on the organisational context in which types of cloud computing services are deployed. One of the main and most cited benefits is that of a reduction in capital expenditure when outsourcing information storage and business processes to the cloud. Instead of investing heavily in new hardware and software which is often not used to its full capacity to store and process corporate information and to provide ICT services, organisations can tap into a large amount of readily available computing resources provided by cloud computing services. These cloud service providers often own large data centres that make use of virtualisation technologies - which is the abstraction of computing resources from the underlying hardware.

Applications, storage, servers and network are then allocated flexible across virtualised servers in a multi-tenancy environment to maximise computing and storage capacities. From a provider perspective, high utilisation of shared resources results in higher efficiency and the ability to offer cloud computing services at low costs. From the customer perspective, this results in the acquisition of flexible computing resources at lower cost than providing that kind of infrastructure in-house but also in the fact that all customers share resources and physical storage in a multi-tenancy environment that relies on logical isolation mechanisms to separate their information from that of other customers.

In terms of records and information management, using cloud-based services and applications can improve business processes, facilitate a collaborative, location-independent working environment, and allow access to computing resources and information outside normal office hours.

Below is an overview of some of the main benefits identified by organisations wanting to make use of cloud computing:

- **Reduced ICT spending**: Organisations often look to increase IT functionality while at the same time trying to minimise capital expenditure. Instead of investing in their own data centres to meet increasing demands for computing power and storage capacities, organisations can avoid capital expenditure by purchasing only the amount of computing resources on demand that the organisation needs to keep systems running or perform business transactions. Cloud services are metered and billed based on actual usage and can therefore be treated as an operational expense.

  In some cases, outsourcing services and applications to the cloud, e.g. moving from Lotus Notes to Gmail, can shift the burden of managing applications and services from the in-house IT department to the third party provider. As a result in-house IT staff can be reduced or re-assigned to focus on more business-critical tasks. (For an example refer to case study 2 in the appendix)

  **BUT**: While organisations can achieve high cost savings in terms of infrastructure, there are costs involved in preparing the organisation for the cloud as well as implementing and configuring cloud services to integrate with existing business processes. On-going management and monitoring of cloud services will add to the overall cost of outsourcing to the cloud.

- **Higher flexibility and scalability**: Instead of estimating and provisioning for peak computing resource demands in in-house data centres, organisations can access nearly unlimited
amounts of computing power and storage capacities in the cloud on demand. Cloud services are highly elastic and allow customers to scale up computing power for periods of high demand and down for periods of less demand.

Scalable cloud service models are particularly interesting to organisations with seasonal or periodic high demands on their computing resources such as tax related businesses because they can scale up resources flexibly without having to invest in infrastructure that is only used infrequently.

But: The promise of unlimited resources on demand needs to be tested carefully to understand how quickly and to what extent a cloud provider can indeed provide up or down scaling capabilities. As usage of cloud resources is metered companies need to monitor (and if necessary restrict) usage to ensure that cloud service running costs do not outweigh perceived benefits.

- **Ease of use:** Implementation of cloud services and applications can be faster (depending on the chosen service model and the interoperability needs with other business applications) than the traditional software deployment where hardware and software have to be bought and systems have to be installed, tested, and configured because cloud services often only require a simple sign up and are instantly available.

  There is often no long-term commitment needed to sign up for a service, so that particular products and services in the cloud can be tested for little up-front investment and discontinued should they prove unsuitable for the business. In addition, cloud applications and services can be accessed from anywhere with an internet connection and are easy to use because standard interfaces are often familiar to users.

  But: Due to the lack of standardisation within the cloud computing industry, interoperability can become an issue when attempting to combine different cloud services and might result in longer implementation time and higher cost.

- **Improved reliability and security of scale:** Due to the often large computing resources held by the cloud provider, server or virtualised instances failure does not usually impact service availability as providers can automatically default to a different server. On a larger scale, customer information is usually redundantly stored in multiple locations to prevent loss of information or service should a data centre be affected by outages. Most cloud providers are confident to offer SLAs of 99.999 % uptime.

  Established cloud providers dedicate far greater resources to improve their network and application security processes and acquire greater expertise in information security practices than individual organisations will be able to achieve as information security and service availability are only one aspect of IT departments’ many responsibilities. Security measures are cheaper and easier to implement on a larger scale. Defensive measures such as patch management, hardening of virtual instances, virus scanning can be implemented quickly across the cloud provider’s infrastructure through the use of virtualisation and automation which allow the rapid replication of security configurations. Similarly, early incident detection mechanisms can reduce response times to security breaches and incidents considerably.
**But:** Cloud providers do have outages and resumption of services will then be out of the control of the cloud customer. In the case of a cloud provider not meeting agreed availability SLAs, customers usually only receive free service time as compensation.

- **Modernisation of business processes:** Instead of having to go through a lengthy procurement process to acquire licences for business software which bind organisations to a provider’s proprietary products, many innovative and regularly updated business applications and services are available as SaaS products which allow organisations to flexibly mix and match cloud services to meet the needs of the business either in the long-term or for a short term project. The ability to combine different cloud services, e.g. CRM services with cloud based performance monitoring and security as a service products, to create a highly customised service can have a positive impact on organisational efficiency and productivity.

Cloud computing can also have a positive impact on innovation as it can lower the cost of and barriers to developing new applications by avoiding upfront investment in infrastructure and by allowing to provision/deprovision computing resources quickly and flexibly when needed for testing of ideas.

Applications and services available over the internet from everywhere facilitate collaborative working internally and externally through sharing of information and the ability to collaboratively edit documents in real time.

**BUT:** Many of the innovative applications and service are built to suit a broad customer base and therefore lack the ability to customise to suit the organisations’ needs, e.g. user set up and management is often very restricted and does not allow for fine-grained privilege and access provisioning.

- **Business continuity/disaster recovery:** Storing corporate information in the cloud can facilitate business continuity and disaster recovery strategies while at the same time allow significant cost savings. Instead of investing money in the traditional model of acquiring a large amount of hardware to replicate information onto and store in an off-site location which is then only used in an emergency, organisations can make use of relatively cheap storage capacities of cloud infrastructure providers. This saves up-front cost, eliminates on-going maintenance efforts and due to the provider’s capabilities for further redundant replication of information improves the availability of information in the event of a disaster. (For more information refer to case study 2 in the appendix)

**BUT:** Even though the actual infrastructure costs are significantly reduced, value-added services such as performance monitoring and extra security that might need to be implemented due to compliance considerations can add significantly to the overall cost.
2.3. Challenges of cloud computing

Outsourcing services and information storage to the cloud generates challenges mainly surrounding information security and the security and availability of the cloud provider’s systems. Many other challenges such as infrastructure and network security and unauthorised access are not new to IT departments and information security managers but pose different problems in a cloud environment. Some challenges such as availability and interoperability, however, are specific to the cloud environment and need to be assessed thoroughly before moving into the cloud. The following overview of challenges is not definitive and focuses on areas that have a direct impact on records and information management practices. It should, therefore, only be taken as a starting point for a thorough risk assessment exercise.

- **Compliance and e-discovery**

  The use and storage of personal information in the cloud can have an impact on compliance with the Data Protection Act 1998 in terms of
  
  - where the information is physically stored on the provider’s servers
  - how it can be checked and proven that the cloud provider has appropriate security measures in place to protect personal data in the cloud.

  (For a more detailed discussion of the Data Protection issues, please refer to section 4.2)

  If information stored in the cloud is held in different jurisdictions, information stored in data centres in high-risk countries with unpredictable legal practices could be subject to disclosure or seizures.

  Confiscated hardware in multi-tenant environments due to a legal case involving one of the cloud provider’s customers can result in the unintentional disclosure of other customers’ information stored on the same physical drive.

  In the case of legal proceedings against an organisation, cloud customers need to be able to locate and retrieve information needed as evidence in court easily and without harming the authenticity and integrity of the information.

  Existing compliance to standards such as ISO9000, ISO27001, or ITIL might be affected by the move to the cloud when some aspects of information security processes are transferred to the cloud provider who might not be in compliance with these standards. Most existing information security and compliance standards are not designed to apply to cloud services as they often require the information owner to be able to point to its physical location which is not achievable on a multi-tenant platform. This can result in the loss of certification.

- **Integrity and confidentiality of information**: When information is stored or processed in the cloud, many of the responsibilities for keeping that information secure are transferred to the cloud provider.
The integrity, authenticity, reliability and confidentiality of information rests on the ability to demonstrate that it has not been tampered with or been accessed by unauthorised persons. In the cloud environment, information is additionally at risk of being compromised by

- unauthorised access by malicious insider at the cloud provider
- interception while in transit over an unsecured network
- being commingled with information of other customers in a multi-tenant environment
- being accessed while processed in unencrypted state
- remanence when it has only nominally been removed from hard drives

A robust access and authentication management regime as well as good encryption should be able to alleviate many of these risks but it is the responsibility of the customer to ensure that the provider has the necessary information security procedures in place. The responsibility to encrypt data and manage keys often falls to the cloud customer too.

- **Availability and reliability of services**: Cloud providers are -due to the nature of their business- a much higher target for hackers or malicious insiders. Even though they might invest much more in security and incident response procedures, they have to be able to prevent or react to DDoS or malware attacks, hacking, port scanning and other potential security threats.

Availability and reliability of services are often expressed in SLAs at around 99.5 – 99.999% depending on the service. This is probably a higher availability than many in-house servers will achieve. However, if a cloud service goes down, there is little organisations can do than wait for the service to resume. Loss of service, income and reputation can be higher than the small amount of compensation offered by the cloud service provider.

The way in which resources are available and allocated among a cloud provider’s customers can have an impact on the reliability of their services. If a smaller provider underestimates demands on their computing power, services can become slow or unresponsive and allocation priorities for customers need to be established and defined.

Availability of services is compromised in a more general way when cloud providers go out of business or are being acquired by a competitor. Services can either become suddenly unavailable or might be subject to changes to products or interfaces which can have detrimental impact on organisations that depend on the services of a cloud provider for important business functions or even aspects of their customer service processes.

If providers go out of business, there are currently no regulated processes for the administrator to return customer information to them, so contingency planning has to be applied in these situations.

- **Portability and interoperability of cloud services**: The cloud computing market is still emerging and services often use different, sometimes proprietary interfaces and programming languages. There are a few initiatives (www.cloud-standards.org) to standardise APIs or procedures but to a certain extent cloud providers have an interest in keeping customers locked into their products. The lack of standardised interfaces and procedures can make it difficult or expensive to transfer services or information from one cloud provider to another.
The lack of standardisation can also impact when organisations want to outsource and combine services to a range of cloud providers to achieve maximum efficiencies and flexibility or when trying to get their in-house systems to interact with the cloud provider’s systems. Reconfiguration of systems to achieve interoperability can be time consuming and requires considerable technical expertise.

- **Information retrieval and destruction (exit strategy):** If the cloud provider does not offer a standardised export procedure for information, the organisation needs to develop their own programme to extract their information. Some cloud providers offer help with information retrieval but that might come at a cost to organisations.

If information extraction requires a change of format of information, this can have serious consequences for the authenticity and reliability of corporate records and impact on their legal admissibility.

Most information that is stored or processed in the cloud is automatically replicated in a redundant location for security reasons by the provider. It is important for organisations to understand how many copies of their information exist in the cloud and how to access and retrieve them for legal compliance such as data access and FOI requests as well as for destruction and retrieval procedures.

An essential records management process is the routine execution of corporate retention decision in order to demonstrate compliance. The destruction of information stored in the cloud according to approved destruction mechanisms might be difficult to achieve. Most cloud providers will delete nodes pointing to information in virtual instances, so that locating that information on the vast amount of physical hardware will be impossible but information is not actually wiped from the hard drive. It will be overwritten over time and Google estimates that information is usually overwritten completely within 4-10 days. Alternatively, encrypted information can easily be deleted by destroying the encryption key remotely (whether the keys are held by the organisation itself or by the provider needs to be established). It depends on the organisation’s compliance regime whether that constitutes acceptable destruction procedure.

- **Loss of governance:** When storing information in the cloud, organisations transfer responsibilities for information security to the cloud provider. The extent of the loss of control over information security procedures depends on the chosen cloud services model and it can generally be said that the customer has less control the higher up the stack they go, e.g. customers have typically no control over SaaS provider infrastructure and systems whereas they control much of the applications and systems deployed on IaaS environments.

Many cloud providers do not share audit logs for access to and use of an application or service nor do they share incident logs and responses with their customers. It is often difficult to for customers to monitor cloud services using their own monitoring and logging systems. Accountability and compliance can be impacted by a lack of audit trails and systems access logs.

This loss of governance can lead to the inability of complying with the organisation’s legislative and regulatory environment and can impact on the ability to demonstrate the authenticity, integrity and reliability of corporate information that has been stored in the cloud.
• **Integration and management:** Even though the service is outsourced and much of the maintenance and security of the underlying cloud service infrastructure is transferred to the cloud service provider, management and maintenance can increase depending on the chosen cloud service model, especially in IaaS environments, customers will need to manage and secure the operating system, any deployed applications, and virtual instances.

In addition, organisations will need to monitor cloud services to see how well they perform against SLAs and governance frameworks.

Cloud services will have to be integrated into the organisation’s IT operations and that requires in-house expertise and can be time and cost intensive.
2.4. Top 10 Questions when outsourcing to the cloud

Which process, application and information can be moved to the cloud to gain efficiency and cost benefits while satisfying the organisation’s security and compliance requirements?

How can the organisation be harmed if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?

How are information and systems protected against unauthorised access (e.g. hacking, interception, user misuse) by the cloud service provider?

How can the organisation ensure the integrity, authenticity and reliability of information stored in the cloud?

What are the organisation’s responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

How can the organisation apply its records and information management programmes (e.g. classification, retention) in the cloud environment?

What is the impact of outsourcing services and information to the cloud on the legislative and regulatory requirements of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing etc.)?

How should the organisation audit and monitor cloud services and establish relevant service level agreements?

Will the organisation be able to negotiate contracts and agreements that fit their risk assessment and compliance environment?

What are the total costs of setting up and managing the cloud services?

References:


3. Preparing for the cloud

Outsourcing business processes or information storage to the cloud can cut costs and increase efficiencies and performance. However, the organisation needs to carefully assess which processes and types of information can safely be moved to the cloud while at the same time providing the expected benefits to the business and the users. It is assumed that users of this toolkit will have identified potential processes or information types that lend themselves to the outsourcing process and now need to match these to the cloud service and deployment models that will best suit the organisation’s business requirements, risk and compliance frameworks. Reasons for outsourcing process or information storage to the cloud can include:

- An organisation-wide drive to outsource non-core business processes or information
- A vision to standardise business processes and centralise information storage
- A move to re-engineer a particular business process

Some of the applications or processes that lend themselves to be moved to the cloud because they can be provided cheaper, are more efficient, and/or provide better functionality and that have a direct impact on how information (including records) is managed when used and stored in cloud-based systems are:

- Email
- Document management
- Disaster recovery
- Collaboration tools such as project management and shared document editing
- Productivity tools such as customer relationship management and payroll systems
- Simple, long-term storage of inactive information for business or regulatory reasons

The reasons behind an organisation’s decision to investigate outsourcing to the cloud will affect the process, timeframes and the nature of the cloud services to be acquired. These reasons should form part of a comprehensive cloud computing/service strategy which is informed by the organisation’s business and IT strategies as well as by its information assurance and governance frameworks.

Selecting the cloud service and delivery models that offer the best fit for the technical, business and governance requirements can be difficult because the cloud computing market as it is at the moment often does not offer many alternatives, e.g. providers may offer only a public or a private cloud but not both. Many cloud services do not allow the degree of customisation that the organisation might have been used to from traditional software or hardware contracts. With this in mind, it is important that the organisation understands exactly what is on offer in the market and in how far available services and products fulfil the established technical and governance requirements.

It is part of the risk assessment exercise to determine which requirements can be approached flexibly and which requirements are essential for the organisation. As a whole, outsourcing information storage to the cloud is predominantly a risk assessment exercise and based on a good knowledge of
the cloud provider’s services and the division of responsibilities for the management and security of services, applications and information in the cloud between the provider and the organisation.

In order to assess the risk information is exposed to when stored in the cloud, it is necessary to have identified and classified all that is stored or used in the cloud information in terms of its criticality for the business. Information classification is also essential for the application of essential records and information management processes such as retention and access management etc.

To guide organisations through the assessment of cloud models based on an extensive risk assessment, the following section is therefore looking at considerations for

- the selection of the right cloud services model (SaaS, IaaS or PaaS),
- the selection of the right cloud deployment model (public, private, community or hybrid),
- the identification and classification of information to be stored or used in the cloud,
- a comprehensive approach to the analysis and assessment of the risks involved in the outsourcing process

Stakeholders in the process are:

- The owners of the business process or information asset that is to be moved to the cloud
- The prospective cloud service users
- Project and risk managers who assess the overall risk of the outsourcing exercise as well as the cost benefit ratio
- Records and information managers who will be responsible for managing information stored in the cloud
- IT professionals who will be responsible for setting up and maintaining the cloud service
3.1. Selection of cloud services and deployment models

Consideration: Identify information, processes, and applications that can be outsourced to a cloud provider to achieve operational and cost benefits. For these processes, then determine which cloud service model and cloud deployment model best fit the business, information governance requirements of the organisation.

Rationale: Cloud computing is a new way of delivering computing resources to the business over the internet and as such can improve efficiency and reduce cost for some business processes. However, not all processes and information can easily be outsourced to the cloud because it may involve

- a lengthy and complicated integration process, if processes are linked to other processes and legacy applications
- an increased risk to the security and availability of critical business processes and sensitive information

Before outsourcing to the cloud, the organisation needs to ensure that the selected information or process are fit for the cloud and that outsourcing will generate the expected cost and efficiency benefits. Business-critical processes as well as highly sensitive, confidential information should not be transferred to the cloud.

When not already pre-determined by the type of process to be outsourced, the organisation must ensure that it chooses service and deployment models that fit into the organisation’s overall corporate and IT strategies and that do not compromise governance and compliance frameworks. Choices are often limited to what the cloud provider offers (e.g. Google does not offer a private cloud, whereas Amazon does).

The organisation needs to be aware of how responsibilities for the management and security of cloud services and application are distributed between the provider and the organisation depending on cloud service and deployment models. In general, the lower down the infrastructure stack the organisation moves, the more responsibility it has to secure and manage it.

Questions:

Which process, application and information can be moved to the cloud to gain efficiency and cost benefits?

Can the cloud provider deliver a better service for a particular process or application than the organisation can internally while remaining cost-effective and satisfying the organisation’s security and compliance requirements?

Which cloud providers are there in the market that address the organisation’s business requirements and how established are they?

How do cloud services fit into the organisation’s overall corporate and IT strategy?

How will the organisation ensure that users and customers are well supported by services that are moving to a cloud?

How does outsourcing of processes and applications impact on the security of information utilised within these and consequently stored in the cloud?
Can the organisation lose control over processes and applications deployed in the cloud without compromising compliance and risk frameworks?

For more on risk and compliance refer to sections 3.3 and 4.2 respectively

Does the organisation have the necessary capabilities (staff, expertise, technology) to move processes and applications to the cloud and integrate with in-house applications?

Are processes relatively independent, that is, not coupled to other processes or applications, so that they can operate independently in the cloud?

Are the processes relatively new, so that legacy systems do not have to be moved to the cloud?

Are the points of integration well defined, so that applications in the cloud can be integrated easily with in-house applications?

Is the organisation satisfied with storing information in a multi-tenant environment where it cannot be classified, have retention or metadata applied to it once it has been transferred to the cloud?

For more on information classification refer to section 3.2

Is the pay-per-use model for the cloud service cost-effective and does it meet business requirements?

For more on costs of cloud computing refer to section 4.4

Is it an acceptable risk to transfer data and information to the cloud provider via an open network like the internet?

For more on risk assessment refer to section 3.3

**Software as a Service**

Does the organisation want to have quick access to a purpose-built business application like email, word processing or project management, in the cloud without having to
• buy, configure and install software, hardware and operating systems

• maintain the network, hardware, operating system or the application itself?

Is the organisation looking for a product that is easy to acquire and access but only provides limited ability to customise it or modify user settings?

Can control over the entire system stack, including responsibilities for information and infrastructure security, be confidently transferred to the cloud provider?

**Platform as a service**

Is the organisation looking to write or deploy their own cloud-ready business applications, software or websites on the cloud provider’s infrastructure without having to

• buy the underlying hardware, servers and network

• maintain servers, hardware and network?

Does the organisation have the technical capabilities to create and deploy their own applications and maintain them, including assuring information and application security?

Is it an acceptable risk to develop and deploy applications and websites on the provider’s proprietary APIs which could effectively lock the organisation into a particular development environment with limited interoperability?
Infrastructure as a Service

Is the organisation looking to acquire computing resources (servers, networking technology, storage, OS, and virtualisation technology) as a utility from an off-site storage provider in order to

- store or compute large amounts of information
- flexibly provision their own applications or websites?

Does the organisation have the technical capabilities maintain software and platform environments, including assuring information and application security?
Cloud deployment models

Which cloud deployment models are available for the services or applications the organisation wants to outsource to the cloud (e.g. Amazon offers a public and also virtual private cloud)?

What are the risks and benefits associated with the different deployment models for the organisation?

Are there security or compliance requirements that prevent the organisation from selecting one of the deployment models?

Public cloud

Is the organisation looking for a highly scalable and flexible platform to access and deliver services in the cloud?

Is it acceptable that the infrastructure on which services and applications are run and information is stored are hosted, operated and managed by the cloud service provider outside the control of the organisation?

Does the fact that public cloud services are offered to multiple customers in a multi-tenant environment in which computing resources are shared have an impact on the organisation’s information security and governance frameworks?

Private cloud

Does the organisation want to emulate cloud computing capabilities on their own infrastructure because

- it has already invested in significant data centre operations
- it does not want to hand over control to a cloud provider
- information security and compliance frameworks prohibit the move to an open cloud environment?

Does the organisation have the right internal capabilities to buy, build and manage a data centre and deploy virtualisation technologies?

Is near unlimited scalability and flexibility not a priority for the organisation?

Community cloud

Does the organisation want to share computing resources with trusted partners in a private cloud environment?

Hybrid cloud

Is the organisation looking to improve efficiencies by running non-core applications in a public cloud and core applications and sensitive and confidential information in the more controlled private cloud?

Is there sufficient internal expertise for the integration of services run in a public cloud with those run internally?
3.2. Information classification

Consideration: Identify all data and information that will be transferred, processed and stored in the cloud and classify it according to applied classification standards in your organisation. Consider criticality and confidentiality of each information type.

Rationale: Information stored or processed in the cloud needs to be managed just like internally held information in accordance to the organisation’s information and records management programme. It is essential for the organisation to identify and classify information to be stored in the cloud in order to

- facilitate the risk assessment of a chosen cloud service based on the criticality, sensitivity and confidentiality of the information to be stored in the cloud
- enable the management (retention and preservation) of that information in a coherent manner

Information can be classified by function, case number, project name, format, or retention period or in broader terms of mission-critical information, management and support information, and personal data.

For each identified information type, an assessment of the impact of breaches to confidentiality, integrity and availability should be made to inform decisions about what type of information can be stored in the cloud within acceptable risk parameters for the organisation. Some information might be too sensitive or important to be exposed to the cloud computing environment, other information might be deemed to be only of operational value and be safe to store in the cloud. Below is an example for the categorisation of information types in terms of confidentiality, integrity and availability:

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>LOW</th>
<th>POTENTIAL IMPACT</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
<td></td>
</tr>
</tbody>
</table>

Questions

Has all the information to be transferred, processed or stored in the cloud been identified?

Has information to be transferred, processed or stored in the cloud been classified according to an established system used in the organisation?

Does information to be transferred, processed or stored in the cloud contain enough metadata to identify and retrieve it for information access requests and retention decisions?

Has the impact of breaches to confidentiality, integrity and availability to information been assessed for each information type identified?

Are there any regulatory, security, and confidentiality issues to be considered for any of the information types to be transferred, processed or stored in the cloud?

How would the organisation be impacted, if information stored in the cloud is accessed by unauthorised people, intercepted or leaked to the public?

What impact would it have on the organisation, if information would be unexpectedly changed or unavailable for any length of time?

Is there any information to which the organisation needs immediate and continual access?
3.3. Risk analysis and assessment

Consideration: Identify, analyse and develop a response to the security and governance risks associated with moving processes, applications and information to the cloud.

Rationale: When outsourcing to the cloud, the organisation transfers much of the control over computing resources, services and information to the cloud service provider. However, the organisation remains responsible for the security and management of these resources and needs to assess what risks are associated with outsourcing to the cloud. The risk assessment exercise should follow accepted corporate methodology (such as PRINCE2) for risk management and should include

- risk identification,
- risk assessment,
- risk analysis,
- risk response planning, and
- risk monitoring.

The main factors when assessing the risk associated with a particular cloud service and deployment model are

- the criticality of the business process to be outsourced to or information to be stored in the cloud
- the sensitivity of information to be transferred, stored and processed in the cloud
- the compliance environment in which the organisation operates
- the total cost of setting up and using the cloud service
- the ability to audit and monitor the provider’s service and security processes
- the organisation’s risk strategy and appetite

Following the identification of risks involved in the selected cloud service and deployment models and of the type of information to be transferred to the cloud, the organisation needs to

- perform ‘due diligence’ when selecting a particular cloud service provider
- manage risks by establishing contractual arrangements with the provider
- monitor the service for compliance with the agreed arrangements.

Some of the risks will be familiar to the organisation from other outsourced processes that involve information storage off-site, others are more specific to the chosen cloud service and deployment model. In any outsourcing arrangement it is, for example, impossible to guarantee the absolute security of systems and information. Information and services, therefore, need to be protected in direct proportion to the risk they are under.
In the context of this toolkit two main categories of risks are identified that need to be considered by the organisation and which are addressed in more detail in the next 2 sections of the toolkit:

Management risk refer to section 5
Includes information management, compliance, contract and cost risks

Operational risk refer to section 4
Includes security, access, and business continuity risks

Below is an overview of the main questions that need to be addressed for each risk category.

Questions:

**Operational risk**

How can the organisation be harmed if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?

How is infrastructure and information protected against unauthorised access (e.g. hacking, interception, user misuse) by the cloud service provider?

How can the organisation ensure the integrity, authenticity and reliability of information stored in the cloud?

What are the organisation’s responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

**Management risk**

How can the organisation apply its records and information management programmes (e.g. classification, retention) to the cloud environment?

What is the impact of outsourcing services and information to the cloud on the legislative and regulatory requirements of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing etc.)?

How should the organisation audit and monitor cloud services and establish relevant service level agreements?

Will the organisation be able to negotiate contracts and agreements that fit their risk assessment and compliance environment?

Does the cloud provider have ‘cyber’ insurance to mitigate the risk of information breaches or unexpected downtime that can cover the customer’s resulting losses?

What are the total costs of setting up and managing the cloud services?
References:


4. Managing the cloud

When moving information and services to the cloud some of the responsibilities for managing and maintaining services and information are also transferred to the cloud provider. Even though the organisation might hand over aspects of control over information to the provider, it is still ultimately responsible for ensuring that information is kept and managed in such a way that its authenticity, integrity, reliability and accessibility can be demonstrated over time when necessary. Many organisations already have information governance frameworks in place to ensure that

- policies and procedures for information security are implemented
- information is managed according to these agreed-upon policies and procedures
- information provides value to the organisation by supporting business aims
- the organisation understands and complies with legislative and regulatory requirements

However, these frameworks were often not established with cloud computing services in mind, and policies and procedures need to be adapted to reflect changes in the information management environment when information is stored or used outside the organisation’s immediate control. Good governance in the cloud is built on being able to trust that all stakeholders involved recognise their responsibilities and will do what they are expected to do in accordance with the agreed policies and procedures for information management and security. Managing cloud services requires a clear picture of

- the information management processes that need to be performed in the cloud
- the compliance environment in which the organisation and the cloud provider operate
- the specific contractual terms that related to outsourcing to the cloud
- the total cost involved in moving information and processes into the cloud
- the strategies needed to ensure a seamless exit from cloud services

Stakeholders for this section are:

- Information assets or business process owners
- Records and information managers
- Archivists and digital preservation specialists
- Legal and compliance experts
- Procurement teams
- Information technology and security professionals
4.1. Information management

Consideration: Ensure that information stored in the cloud will be managed according to the organisation’s information management and compliance programmes in order to maintain authenticity, reliability, and integrity of information over time and to ensure that information is accessible and retrievable for legal and regulatory compliance.

Rationale: The organisation needs to ensure that policies and procedures surrounding the management of the whole life-cycle of information are administered and validated for information stored in the cloud in the same way they are administered onsite. The main aspects of managing records are the classification, appraisal and disposal of information (and records) in order to improve efficiency and facilitate compliance.

Timely destruction of information is not only of importance for compliance reasons but also saves cost in a pay-per-use environment where the organisation is charged for the amount of information stored.

The information life-cycle stages and relevant concerns for each stage can be summarised as follows:

1. Creation
   - Determine the right format in which information should be created and stored in the cloud
   - Establish relevant metadata schemes to ensure enough contextual information is captured for the use, management and retrieval of information stored in the cloud

2. Active
   - Determine who can access information stored in the cloud and how that access is established and managed

3. Semi-active
   - Develop and implement retention or disposal schedules for each information category based on business value and compliance requirements

4. Final outcome
   - Make arrangements for the secure destruction of information no longer needed
   - Make arrangements for the long-term preservation of information that is to be kept permanently

Questions:

What impact will the management of information stored in the cloud have on existing information management policies and procedures?

Can the cloud providers assure that their information security systems can support the authenticity and reliability of the organisation’s information (including metadata and log files)?
Will it be possible to show that information is fully encrypted and protected against unauthorised disclosure?

--- for technical aspects of information security refer to section 5

**Creation**

In which format is information created, transferred and stored in the cloud?

Will the format in which information was created be changed when it is transferred or stored in the cloud?

What implication does the format of information in the cloud have for access, retrieval and preservation?

What metadata can be applied to information stored in the cloud and can it be managed and searched?

How is metadata applied (e.g. automatically through software or manually)?

Does the organisation need to apply additional metadata to information stored in the cloud than it would apply to information stored in-house? What kind of metadata would that be?

**Active**

Will it be possible to show that information is fully encrypted and protected against unauthorised disclosure?

Has all information stored or processed in the cloud been classified and supplied with relevant metadata to ensure efficient identification and retrieval?

--- for technical aspects of availability management and SLAs refer to section 5

Has the organisation procedures in place to provision access and usage rights (by job role, seniority, group membership etc.) to categories of information stored or processed in the cloud?

How can these access rights be implemented in the cloud?

--- for technical aspects of identity and access management refer to section 5

**Semi-active**

Does the organisation have retention and disposal schedules in place for each information category to inform when records are no longer needed for business or compliance reasons?

How can these schedules be applied to information stored in the cloud (e.g. manually, through the provider’s user interface, via metadata) and at what level?

Who is responsible for the allocation and execution of retention and disposal schedules?

**Final outcome**

How will information be destroyed by the cloud provider (e.g. shredding of drives, deletion of nodes, crypto-shredding)?
Is the destruction method in line with the compliance requirements of the organisation?

Is it acceptable that images of destroyed information might be accessible on the provider’s hardware until they have been sufficiently overwritten and how long are the timeframes for a complete overwrite?

Can the cloud provider produce evidence or audit trails to certify the destruction of information?

Does the cloud provider understand and support the organisation’s information preservation needs?

Does information for permanent retention need to be transferred to a digital archive or to a place of legal deposit for preservation purposes or can it remain in the cloud?
4.2. Legal and regulatory compliance

Consideration: Determine which legislation and regulations the organisation is subject to and how storage and processing of information in the cloud can impact compliance with applicable legal and regulatory requirements.

Rationale: Cloud computing brings new complexity to legal and regulatory compliance because most laws, regulations and standards were not established with cloud-based IT services in mind. The organisation needs to find ways to meet compliance requirements in this changed environment and adopt existing policies and procedures to meet cloud computing security challenges.

Access legislation and regulations such as the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 requires public sector organisations (only the Data Protection Act applies to the private sector) to make certain types of information available to the public on request within a defined time frame. Non-compliance with the acts or regulations can result in legal enforcement and financial penalties through the Information Commissioner’s office. In order to be able to comply with these acts and regulations, the organisation needs to know exactly

- what information is held by the organisation
- where it is held
- and how it can be accessed and made available to the public.

Storing or using information in the cloud can make it more difficult for the organisation to determine exactly what information is held and where when cloud migration processes are unstructured and information in the cloud is not classified and managed in accordance with the organisation’s records and information management processes. The organisation needs to assess how storing information in the cloud can impact on legal and regulatory compliance and how processes need to be established or modified to ensure continued compliance.

The use and storage of personal information in the cloud does have an impact on compliance with the Data Protection Act 1998 for all organisations because they need to ensure that personal information is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with your rights
- secure
- not transferred to other countries without adequate protection
The organisation needs to ensure compliance with all of these principles but the following three principles pose particular challenges to the organisation:

Principle 8 of the act does not allow the transfer of personal information to a country outside the European Economic Area that does not provide the same level of protection with respect to personal information of EU residents (the US is such a country). The organisation therefore needs to ensure that it knows where personal information is physically stored on the cloud provider’s hardware. Some cloud service providers allow the customer to specify in which country or on which continent data is stored (Amazon); others will not disclose data centre locations to customers for security reasons (Google now offers a separate service for government agencies to alleviate that problem).

Principle 7 specifies that appropriate technical and organisational measures shall be taken against unauthorised processing and accidental loss of personal data. The organisation needs to assure itself that the cloud service provider has in place a reasonable level of security to protect such information by performing due diligence and being able to audit the providers information security processes.

Principle 5 specifies that information is not kept for longer than necessary for the specified purpose. The organisation needs to ensure that retention actions are applied to information stored in the cloud and executed immediately and to the specified security standard.

Organisations are obliged to make electronic information available in case of litigation procedures. E-discovery preparedness is based on the application of consistent information management procedures which need to be extended to information stored in the cloud. The organisation needs to be in a position to identify, retrieve or put a destruction hold on any relevant information required during litigation processes that has been stored in the cloud. Interestingly, there are also cloud-based solutions in place (e.g. Iron Mountain http://www.stratify.com/products_services/current_product.html) that can facilitate searching and indexing vast amounts of information stored in disparate locations.

Existing compliance or certification to industry standards such as ISO9000, ISO27001 or SAS 70 Type II (FISMA in the US) can be adversely affected by moving information to the cloud because these standards were not designed to apply to cloud services as they often require the information owner to be able to point to its physical location which can be difficult to achieve. The organisation therefore needs to assess how existing certifications can be upheld and how the cloud provider’s certifications can assist in that process.

Questions:

Legislation

What legal and regulatory frameworks does the organisation need to comply with?

How will compliance be affected by the fact that information is stored in the cloud?

Are responsibilities for legal compliance clearly established between the organisation and the cloud provider?
Is it clear that the organisation retains sole ownership of information stored in the cloud?

Where is personal information physically stored? Where is provider’s infrastructure located?

Can the organisation specify where information is physically stored?

If the cloud provider is located in the US, do they have a Safe Harbour certification and when was it issued?

Will the cloud provider use 3rd party providers whose infrastructure is located outside of that of the cloud provider?

Is the organisation satisfied that the cloud provider has appropriate technical and organisational processes in place to protect information against unauthorised processing and accidental loss?

For an assessment of technical security measures refer to section 5

Can the organisation ensure that personal information is not kept for longer than necessary?

Can the organisation ensure that information is authentic and reliable?

For an assessment of information management processes refer to section 4.1

Can information be easily identified and retrieved for information access requests (DP, FOI, EIR)?

**E-Discovery**

Are responsibilities relating to e-discovery, including litigation hold procedures, discovery searches, and expert testimonies, clearly established between the organisation and the cloud provider?

Do the organisation and the provider have a standard process for responding to subpoenas and other legal requests?

How will the cloud provider notify the organisation, if a third party makes a discovery request?

Is the information stored in the cloud easily identifiable and retrievable in the case of a legal request?

Can litigation hold procedures be easily applied to information stored in the cloud to prevent scheduled destruction of information needed during litigation?

How much will e-discovery in the cloud cost?

**Standards and certification**

What industry standards does the organisation comply with or is certified to?

How will certification or compliance be affected when information is moved and stored in the cloud?

What standards does the cloud provider comply with or is certified to that would provide the organisation with reassurances regarding information security?
4.3. Contract

Consideration: Ensure that the contract or service agreement with the cloud provider meets the organisation’s compliance and security requirements and represents value for money.

Rationale: The organisation will have specific purchasing frameworks to ensure that services are purchased according to correct procedures. However, these frameworks might cover traditional outsourcing contracts and agreements well but not cloud computing contracts. The organisation therefore needs to ensure that any additional contractual requirements are identified and specified within the cloud contract or agreement. Additionally many of the bigger cloud service providers such as Google provide customers with a standard contract or agreement that cannot be negotiated. In these situations, it is essential to consider the contract terms carefully and assess the operational and management risks that the standard contract might generate.

Questions:

Can the contract be negotiated with the cloud service provider or do they issue a standard contract?

Which aspects of the contract can be negotiated (e.g. price, SLAs, technical specifications)?

Can monitoring and reporting processes (e.g. for information and access security, availability, incident response) be built into the contract?

Can the organisation perform full contract due diligence (including financial condition, reputation, controls, personnel, disaster recovery, insurance, subcontractors, and communications) to determine responsibilities and accountability?

Does the cloud provider have ‘cyber’ insurance to mitigate the risk of information loss or unexpected downtime that can cover the customer’s resulting losses?

What jurisdiction does the cloud provider operate in and what impact does that have on enforceability of contract terms?

Will any of the provider’s services be outsourced or subcontracted and how does that impact compliance?

Does the contract

- include a right to audit clause to fulfil compliance requirements?
  
  ➔ For more on audit and reporting requirements refer to section 3.5

- stipulate that information remains in the ownership of the organisation

- stipulate how information will be returned to the organisation when the contract is terminated?
  
  ➔ For more on exit strategies refer to section 3.6

- prohibit the provider to suspend or terminate the service abruptly?

- contain a litigation cooperation clause?
• refer to any outside documents (ToS or SLAs)?
• stipulate how changes to the contract, ToS or SLAs will be communicated and applied?
4.4. Cost

Consideration: Calculate the total costs that moving information or services to the cloud will incur and assess the cost benefit ratio for the organisation.

Rationale: Cloud computing can save cost through the reduction of capital expenditure for hardware and software as well as through a reduction in staff time for systems set up and maintenance. However, the true costs of cloud computing are sometimes difficult to establish. The organisation needs to take into consideration both running and conversion costs over time to establish how much return on investment a move to storing information in the cloud can generate and whether it might actually be cheaper for the organisation than building up their own data centre.

Cost calculations need to include:

- Data transfer charges
- Monthly storage charge
- Monthly usage charge
- Bandwidth
- Staff time (includes set up and integration, maintenance and monitoring, compliance management)
- Cloud service provider support
- Information retrieval

If the organisation wants to make use of regular up- and down-scaling of resources to optimise usage, monthly costs can vary widely every month or even day and it might become more difficult to monitor operational expenditure. As with most managed services, the organisation can use cloud-based devices (such as CloudSplit http://cloudsplit.com/) to monitor cloud computing usage and cost. Some cost/usage monitoring services are also offered by bigger cloud service providers themselves such as Amazon and Salesforce as add-ons to their usual services.

It is essential to assess the cloud provider’s pricing structure for a particular service model and ensure that all costs have been identified and calculated before contracts are signed to avoid hidden charges at a later stage.

Questions:

How much will it cost the organisation migrate information and processes to the cloud and integrate them with in-house systems?

How much will it cost to monitor and maintain cloud services for availability, security and compliance?

Is the cloud provider’s pricing structure easy to understand and transparent?

Are prices given in standard pricing units (e.g. cost per gigabytes of storage, cost of each user licence each month or year) that can be compared with that of other cloud providers?

Are user licences bought annually or monthly and how easy is it to cancel or buy additional licences?
How is customer support provided and how much does it cost?

How much is the cost for

- storage of information (per Gigabyte)
- computation of information (per instance or CPU unit)
- transfer of information to and from the cloud (per Gigabyte)
- requests to information (including for use, virus scanning, indexing or back up)
- applications that can be built on the platform
- database objects
- additional features such as WORM or information lifecycle management?
4.5. Monitoring, auditing and reporting

*Consideration:* Establish which aspects of the cloud provider’s services need to be monitored for compliance, information security and performance measurements to ensure that services are run according to agreed SLAs and compliance requirements.

*Rationale:* In order to ensure that the cloud provider delivers the service in accordance with the agreed contractual terms, established SLAs and compliance requirements, the organisation must be able to audit, monitor and analysis aspects of the cloud provider’s service and systems. The extent to which a cloud provider will allow the organisation to audit their systems and security processes varies from provider to provider and should be established before any contract is signed. In order to gain a full picture of the service provided in the cloud, the organisation needs to establish

- what aspects of the service need to be audited for compliance
- what needs to be monitored for performance and security
- what the SLAs and KPIs are against which aspects of the service are monitored
- how aspects of the service can be monitored
- how SLAs and compliance requirements can be enforced.

*Questions:*

Can the organisation audit the cloud provider’s systems for compliance and information security aspects?

Does the cloud provider provide any standard audit documentation and reports that can inform the organisation’s audit and due diligence processes?

How often is the provider audited by external bodies and when did the last audit take place?

What are the provider’s internal audit procedures?

How can the following aspects of the cloud provider’s service be measured and monitored to ensure successful governance:

- Performance and availability of the service
- Incident monitoring and response
- Cost and usage of the service
- Access to information, applications and infrastructure?

Does the cloud provider have tools that allow the organisation to monitor whether service levels are being met?

How will the provider communicate performance information to the organisation (e.g. email, dashboard, RSS)?

What information is kept in audit logs and how long are these logs kept?
Does the organisation have adequate resources and expertise for monitoring the necessary aspects of the cloud provider’s services?

Can the organisation implement its own monitoring tools or that of third party providers?

How are SLAs and KPIs established, monitored and enforced by the organisation?
4.6. Exit strategy

Consideration: Ensure procedures are in place to facilitate the retrieval of information from the cloud provider’s systems once the contract is terminated. Customers need to ensure that the providers systems allow easy migration to another cloud service provider.

Additionally, the customer must ensure that the provider has the right processes in place to completely destroy information stored in the cloud, if requested.

Rationale: Part of the outsourcing strategy should be a strategy for how information will be retrieved from the cloud provider infrastructure once the contract is finished. This should include agreement on

- Any cost associated with the information extraction process
- The format in which information will be exported
- The timeframes in which export is taking place
- Any assistance with information export provided by the cloud service provider

The exit strategy must ensure that no information is lost or its integrity compromised and responsibilities need to be clearly assigned between provider and customer.

As with any outsourcing to third party providers, the exit strategy should also include measures to be undertaken in the event of the cloud provider ceasing operations.

When deleting information from applications and systems, remanence can occur, that is, residual representation of information that has been nominally deleted can exist and be inadvertently disclosed to third parties.

Questions:

- What are the costs involved in migrating or exporting information from the cloud provider?
- Exactly what assistance will the provider provide for migrating and exporting customer data?
- Are there documented procedures and standardised APIs for exporting information from the cloud?
- Does the cloud provider provide interoperable export formats for all information stored within the cloud?
- Are there any provisions for exporting user-created applications in a standard format?
- Are there processes for testing that information can be exported to another cloud provider?
- Can the organisation perform its own information extraction to verify that the format is universal and is capable of being migrated?

References:


Amazon Simple Storage Service (S3): [http://aws.amazon.com/s3/#pricing](http://aws.amazon.com/s3/#pricing)


5. Operating in the Cloud

Cloud computing can provide organisations with a cost-effective, flexible and scalable alternative to traditional ICT provision. However, concerns about security breaches and information loss hold organisations back. For cloud computing to be a viable option, organisations need to be certain that their applications and information are safe in the cloud by assessing the cloud provider's information security policies and processes. Ideally, organisations should be able to audit these processes or assess the security regime through the provider's certification to accepted industry standards such as ISO27002 or SAS 70 Type II etc. Both options are often not available as cloud providers often refuse to be audited to keep their security processes secret from potential misuse and because the sheer number of individual audits from customers would effectively impact on their ability to operate the service. Similarly, most existing information security standards were not developed with cloud infrastructures in mind, so that certification might not actually reflect necessary security practices needed in a cloud environment.

Running applications or storing information in a multi-tenant environment in the cloud creates risks not usually found in internal data centres. Traditional security measures such as firewalls, encryption and security processes that create a secure perimeter around the in-house operations need to be extended to the cloud to establish end-to-end protection regimes. When conducting security due-diligence, organisations must consider new issues specific to cloud computing in addition to existing security concerns such as information isolation and access, protection of infrastructure and networks from internet-based attacks etc.

The following sections take account of the cloud-specific security issues that should be addressed by organisations when assessing a potential cloud service provider regarding their information and infrastructure security processes. It is by far not an extensive list but should alert stakeholders in this process to the main areas of infrastructure security that need investigating further.

Stakeholders in this should include

- the records or information professionals responsible for the management of information to be stored or processed in the cloud
- IT professionals who are expert in information and infrastructure security and have been involved in any internal certification processes
- project and risk managers who assess the risk a cloud services’ infrastructure and information security processes might pose to the security of the organisation’s information
5.1. Security

Consideration: Assess policies and processes for physical, personnel, infrastructure, information and access security to ensure that the cloud provider has in place an adequate and well maintained system of security procedures to protect data centres and hardware contained in them.

Rationale: When outsourcing information storage or processes to the cloud, part of the network, system and applications in which information is stored and processed will come under the control of a third party provider. Responsibility for information security needs to be shared between the cloud service provider and the customer depending on the cloud service model chosen, the service level agreement and provider-specific capabilities. It is a good starting point to clarify

- what security the customer needs to provide above those provided by the cloud service provider and
- how the customer can assess the cloud provider’s information security practices and procedures

In general it can be argued that customer responsibility for information security processes diminishes the further up the cloud stack one moves, e.g.:

The following table provides an overview of the division of information security responsibilities depending on the chosen cloud service model:

<table>
<thead>
<tr>
<th>Cloud service model</th>
<th>Provider responsibility</th>
<th>Customer responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-as-a-service (SaaS)</td>
<td>Availability management, Access control (partial), Vulnerability management, Patch management, Configuration management, Monitoring systems use and access (partial), Incident response (partial)</td>
<td>Access control (partial), Monitoring systems use and access (partial), Incident response (partial)</td>
</tr>
<tr>
<td>Platform-as-a-service (PaaS)</td>
<td>For underlying infrastructure: Availability management, Access control, Vulnerability management, Patch management</td>
<td>For customer deployed applications: Availability management, Access control, Vulnerability management, Patch management</td>
</tr>
</tbody>
</table>
Physical security

*Rationale:* Every organisation will have varying needs regarding the physical security of the provider’s premises and equipment. General precautions that for the security of premises, such as access controls to and physical defence of buildings against natural disasters and sabotage, apply but should be supplemented to include:

- Asset management procedures for tracking and protecting equipment
- Protection of electronic access points and communication lines
- Protection of power supply and physical environment for electronic equipment

If the data centres and equipment such as computer hardware are not adequately protected, the organisation can be subject to an information security breach.

*Questions:*
Are regular risk assessments of the premises carried out, including neighbouring buildings?

Are date centres secured with intrusion alarms and CCTV as well as access technology such as cards and security logs to prevent unauthorised access?

Does the provider control and monitor who has access to the data centre?

Is electrical equipment kept in rooms that are fitted with environmental controls systems (heating and cooling systems) and adequate fire detection and prevention systems?

Is power supply protected physically and are UPS and back-up generators in place?

Does the provider maintain an accurate inventory of physical equipment such as computer hardware that is updated regularly when equipment is moved or discarded?

Are all network access points and cables secured and protected?

What processes and procedures are in place to destroy old media or systems when required to do so?

**Personnel security**

*Rationale:* Most issues relating to personnel security will be familiar to organisation’s based on their own (IT) personnel screening and security procedures. Ensuring that all employees of the cloud service provider with access to data centres, hardware or software have been screened prior to employment and are aware of their responsibilities regarding information security is essential to prevent unauthorised access to information.

Access rights to restricted areas or equipment should be allocated by employee role and be monitored and regularly reviewed.

*Questions:*

What policies and procedures does the provider have in place when hiring IT or staff with systems access (pre-employment checks etc.)?

Does the provider have policies and procedures in place to assign information security responsibilities to staff, make them aware of these responsibilities and provide the required training to enable them to carry out those responsibilities?

How are access rights allocated, reviewed and removed?

**Infrastructure security**

*Rationale:* When outsourcing information storage to the cloud, part of an organisation’s network, system, applications and ultimately information will be under the cloud provider’s control. This will result in a transfer of some security responsibilities to the cloud provider depending on which cloud service model is applied:

It is essential that both parties understand how responsibilities for infrastructure security are shared, monitored and reviewed. Infrastructure security comprises network, server (host) and application security as well as availability management and resource provisioning.

*Questions:*
Are the provider’s information systems audited and compliant with relevant standards such as ISO 27001/2 or SAS 70 Type II and NIST 800-53 in the US?

Does the provider maintain documented operating procedures for information systems and configurations?

Does the provider have change control procedures to manage configuration changes to the information system using an organisationally approved process?

Are audit logs kept for incident investigation?

How long are logs kept, what information do they contain and how are they protected from unauthorised access?

Are there structured processes in place for identifying, acquiring, testing and deploying patches that cover the whole infrastructure (network, server, virtualisation software, applications etc.)?

**Network security**

*Rationale:* The cloud provider’s network needs to be secured from service attacks to ensure the confidentiality and integrity of information in transit to and from the cloud provider.

*Questions:*

What protection mechanisms are in place against denial of service attacks (DDoS)?

Are there defences against internal as well as external attacks?

What level of isolation is used?

Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa?

Is the virtual network infrastructure used by cloud providers secured to vendor or best practice standards?

**Server (host) security**

*Rationale:* Cloud service providers do often not publicly share their processes for securing servers and operating systems to avoid potential misuse of this information. Depending on the cloud services model selected, responsibilities are shared between provider and customer as follows:

- PaaS and SaaS host security responsibilities are transferred to the provider
- IaaS customers are primarily responsible for securing the hosts provisioned in the cloud for virtualisation software security and the guest OS or virtual server security.

*Questions:*

Does the provider ensure virtual images are hardened by default?

Are virtual images monitored and tracked in an inventory?

Is the hardened virtual image protected from unauthorised access?
Can the provider confirm the virtualised image does not contain the authentication credentials?

Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?

Can a host-based intrusion prevention service be run in the virtual instance?

Is physical and logical access to hypervisors restricted to authorised personnel?

**Application security**

*Rationale*: Many information security breaches can be traced back to the exploitation of web application vulnerabilities (cross-site scripting, SQL injection, malicious file execution etc.) It is common practice to protect internal applications through physical, network and host security mechanisms but in the web-based environment in which many cloud applications are deployed, security needs to be written into the code. Responsibilities for insuring application security are shared between provider and customer depending on the chosen cloud service model:

- **SaaS** application security rests entirely with the cloud provider as they manage the suit of applications delivered to the customer. Customers are responsible for user and access management within the constraints of the application’s administration controls available to them.

- **PaaS** application security encompasses two software layers: the PaaS platform and the applications deployment on the platform. The cloud provider is responsible for the security of the PaaS platform itself, while the customer is responsible for the application they deploy onto the platform

- **IaaS** application security rests entirely with the customer as applications are deployed to the virtual server and managed by the customer.

Cloud service providers do often not disclose detailed information on their application and platform security mechanisms but customers should seek information that will allow them to assess security risks associated with a particular application in order to prevent information security breaches.

*Questions:*

What controls are used by the provider to protect the integrity of the operating system and applications software used?

What software development design and coding standards are applied during the development process?

How are new releases of software evaluated as being fit for purpose?

What practices are followed to keep the application safe?

Is a software release penetration tested to ensure it does not contain vulnerabilities?

How are multi-tenant applications isolated from each other?
What assurances can the provider give that access to customer data is restricted to customer users and to the applications they own?

Does the provider ensure that the sandbox is monitored for new bugs and vulnerabilities?

Does the provider offer security features such as: user authentication, single sign on, authorisation and SSL/TLS?

**Information security**

**Rationale:** To ensure the security, integrity and authenticity of information stored in the cloud is the overriding concern when outsourcing to the cloud and most of the controls discussed here address that issue. However, data and information itself needs to be protected when at rest or in transit using encryption mechanisms and access protection. Data and information in transit can be encrypted but any use of information in the cloud, other than simple storage, requires that information to be decrypted to enable processing, indexing and searching. This means that data in a SaaS and PaaS environment is usually not encrypted and in IaaS only when used for simple storage without searching or indexing capabilities.

**Questions:**

Is information automatically encrypted by the provider when at rest or in transit to and from the customer’s network?

Can the customer encrypt information intended for simple storage?

Are encryption keys created in a secure and industry-approved manner?

Who holds encryption keys and how are they kept?

Are security controls in place for reading, writing and using encryption keys?

Can keys be revoked simultaneously across multiple sites?
5.2. Availability management and resource provisioning

Consideration: Define availability terms and establish adequate service levels for availability and resource provisioning of the provider’s systems.

Rationale: Availability describes how often, in what periods a service can be used. Cloud service providers often guarantee availability of their services for up to 99.999% of the time (that equates to the service being inaccessible for just 5 minutes and 15 seconds a year) and offer refunds should they not be able to meet the SLA. However, cloud service downtime can have a huge impact on business activity and can lead to a loss of income or reputation. It is therefore important to understand the cloud provider’s availability management procedures and define performance monitoring procedures. In addition, it is important to define what exactly availability comprises, e.g. are all features and functions of a service included (Gmail including calendar and docs?) and are planned downtimes included for maintenance?

One of the main benefits of using cloud infrastructures is the ability to flexibly and rapidly commission and de-commission resources such as processing, memory, storage and network. It is important for the customer to understand how resources are provisioned and authorised as well as how much and how fast they can scale up and down in order to ensure continuity of business activity.

Questions

Does the provider have policies and procedures in place to ensure service change control, availability, reliability and performance?

And how is that availability defined exactly (e.g. includes all features and planned downtimes, are there interdependencies with other systems with lesser availability)?

Is the availability level covered in the SLA or contract?

How is performance measured and communicated to the customer (email, dashboard, website information or RSS etc.)?

What controls are in place to prevent unauthorised and unintended information transfer via shared system resources (data remanence) in a multi-tenancy environment?

In the event of resource overload what information is given about the relative priority of a customer’s request (e.g. are some packets tagged for higher priority)?

How much and how fast can customers scale up? Does the provider offer guarantees on maximum availability of supplementary resources within a minimum period?

What processes are in place for handling large-scale trends in resource usage (e.g. seasonal effects)?

What guarantees does the provider offer that customer resources are fully isolated?

Assuming physical machines are not shared between customers, to what degree are storage, memory and other data traces fully erased before machines are reallocated?
5.3. Incident response

Consideration: Define acceptable incident response and patch management procedures.

Rationale: A main threat to the availability and security of cloud services is the ability for hackers and malware to exploit systems and infrastructure vulnerabilities in order to gain access to services and information in the cloud. While it would be ideal to prevent attacks to systems and networks in the first place, not all security incidents can be prevented. The cloud provider should have procedures in place to

- detect incidents rapidly
- minimize the impact of the incident
- restore systems and networks rapidly
- analyse how the incident happen and
- identify weaknesses of systems and networks

Questions:

Preparation

Does the provider have policies and procedures in place to assess the risk of vulnerabilities?

Does the provider have formal policies and processes in place for detecting, identifying, analysing and responding to incidents?

Is this process rehearsed to check that incident handling processes are effective?

How are incidents reported to the customers (e.g. periodical reports, dashboards, emails)?

Are procedures in place to prioritise incidents based on the criticality of the affected system?

Detection and Analysis

Does the provider have automated detection capabilities in place such as intrusion detection systems, anti-virus software and log analysers?

Is there real time security monitoring in place?

How can the customer report anomalies to the provider?

How are incidents documented and is evidence collected, especially when logging and data is co-located for multiple customers?

How much access does the customer have to these logs?

What controls are in place to prevent malicious activities by insiders?

Containment, eradication and recovery

What mechanisms are in place to contain the incidents (e.g. shutting down the system, disconnect from network, disabling systems functions, isolation parts of the infrastructure)?
How are components of the incident eradicated (deleting malicious code, disabling breached accounts)?

How are systems recovered and hardened to prevent similar incidents (restoration from clean backup, rebuilding system from scratch, changing passwords)?

How does eradication and recovery impact on the customers’ services and stored information?
5.4. Identity and Access management

Consideration: Ensuring the provider has identity and access management policies and procedures in place to effectively support authentication, authorisation and auditing of internal and external users’ access to cloud infrastructure. In addition, the customer needs to ensure how cloud provider supports the customer’s own access and security policies for accessing services and information in the cloud.

Rationale: Most organisations will be familiar with identity and access management mechanisms within the organisations’ private network where access to networks, systems and applications is secured by virtual private networks (VPN), intrusions detection systems, strong authentication mechanism (passwords) and encryption. In the cloud environment, responsibilities for network and application security are to an extent transferred to the provider. Cloud customers need to ensure that the provider has identity and access management in place for the systems under their control to protect unauthorised access to systems and information internally. They also need to ensure that adequate identity and access mechanism are offered by the provider to enable the customer to provision their users with fine-grained access to the system or information in the cloud that mirrors their internal access policies (usually established through Active Directory). Controls to consider include:

- Authentication – the process of verifying the identity of a user
- Authorisation – the process of determining access privileges the user should be entitled to after identification

Questions:

Authentication

Are critical systems and information protected with strong authentication mechanisms such as two-factor authentication (e.g. password and token) or three-factor authentication (e.g. something the user has, something the user knows and something the user is)?

Are systems set to automatically lock out a user after a period of inactivity?

Does the provider support strong authentication mechanisms (specifying password length and difficulty etc.)?

Are authentication procedures regularly audited to ensure compliance and detect security breaches?

Do customers have access to audit logs?

Authorisation

Do any accounts have system-wide privileges?

How are accounts with the highest level of privilege authenticated and managed?

Does the cloud provider use role-based access controls and follow the principle of least privilege to ensure users only have access to the systems and information they need to?

Is there an administrator role for the customer that allows fine-grained user provisioning and privilege assignment?
Are authorisation procedures and assigned privileges regularly audited to ensure compliance and detect security breaches?

Is system access monitored and logged? Do customers have access to audit logs?

What processes are in place to provision and de-provision privileges simultaneously throughout the cloud system and across multiple locations?

Does the cloud provider support identity federation?

Is the cloud provider interoperable with third party identity providers?

Does the provider support single sign-on?
5.5. Business continuity

Consideration: Assess what measures are in place to counteract interruptions to business activities due to provider information systems failure.

Rationale: Business continuity and data recovery plans are part of any outsourcing process and should be familiar to organisations. However, in the cloud environment it is important to consider additional factors such as:

- Frequency of back-up taken of information stored or processed by the provider (instantly, daily?)
- Communication methods and recovery priorities

Any agreement or contract should address responsibilities in the event of disruption and needs to include service level agreements for recovery actions. It is important to define the frequency of backups according to the business need and the category of information in question. Lines of communication and recovery measures and timeframes need to be defined, so that the user is aware of how long a disruption might affect business activities and what priority the user is assigned among the cloud providers customers.

Questions:

Does the provider have adequate disaster recovery and business continuity plans in place that protect customer information?

How often are these plans reviewed?

Does the provider maintain logs of activity that detail the impact of a disruption?

What are the lines of communication to end customers in the event of a disruption?

Has the provider categorised the priorities for recovery and what would be customers’ priority to be restored?

Is all customer data replicated across multiple data centres to ensure redundancy?

Is the data being backed up at a frequency appropriate to its business value and instantly when it is changed?

Are back up and information recovery processes and procedures regularly checked and reviewed?

References:


6. References


Hammond, M. et al. (2010). *Cloud computing for research: final report*. Bristol, JISC. Online: 
http://www.jisc.ac.uk/whatwedo/programmes/researchinfrastructure/usingcloudcomp.aspx#downloads

Jericho Forum. (2009). *Cloud Cube Model: selecting cloud formations for secure collaboration*. Online: 
http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf


Government Accountability Office. (2010). *Federal guidance needed to address control issues with implementing cloud computing*. Washington: GAO. Online: 

www.whitehouse.gov/assets/.../Cyberspace_Policy_Review_final.pdf


7. Case studies

Guardian Media Group – Google Apps Case Study

Organisation

Guardian News & Media (GNM) is the core division of Guardian Media Group with ca. 1,850 employees. It publishes the Group’s flagship national newspapers – the Guardian and the Observer – as well as the guardian.co.uk website. The newspapers are some of the UK’s leading daily and weekly titles, and the Guardian.co.uk website - voted the best newspaper site in the world - now delivers the Guardian’s liberal journalism to a global audience.

The organisation is committed to provide a working environment that is fit for a dynamic media organisation and the 21st century by supporting flexible and collaborative working across teams and with external customers.

Challenge

GNM faced a similar challenge to many media organisations with a highly mobile workforce: catering for the diverse IT needs of a large number of people with finite resources. Being a dynamic organisation operating in a fast-paced digital media environment, GNM’s work processes are strongly focussed on the ability to collaborate across teams and locations and around the flexible access to and use of information resources. Previously GNM’s 1,850 strong workforce communicated mainly via email using Lotus Notes and collaboration centred on sending large email attachments around project teams. Project spaces were laboriously set up and maintained by the IT department via shared drive structures. Apart from setting up VPN connections to home PCs, there was no process in place that enabled access to documents online. That approach appeared inflexible and slow and as a result, some employees looked for easier collaboration tools online.

To foster an environment of easy and flexible collaborative working online and to ensure that company data is not being lost in the cloud by individuals, GNM’s IT department was tasked in 2008 with finding a collaboration tool that would allow staff to collaborate on documents and access them from dispersed locations. IT started to look for a flexible productivity tool that would allow for:

- Easy online collaboration on documents across teams and locations
- Version controls
- Simultaneous editing
- A direct link between documents and email to reduce the amount of attachments circulated

At this initial stage in their brief, the IT department was not looking into outsourcing their email client but added that services at a later stage.

“Google provided a good level of support for our deployment project and were responsive to service and functionality improvements. The user response has been a collective sigh of relief - primarily as a result of the vast increase in mail storage capacity and the improved remote access. For Google Mail training requirements were limited although migration of existing mail from Lotus Notes smoothed the way significantly. Uptake on Google Docs has been user led and greatly improved ad-hoc collaboration across the business.” GNM IT Implementation Team
Solution

While GNM looked at a variety of productivity and collaboration products (including IBM and Microsoft), they quickly felt that Google Apps provided better functionality for less cost than most other products. As a result, the Guardian acquired yearly-renewable user licences for a fixed price for all staff because it provided the functionality needed and was cost-effective by saving on internal infrastructure and the provision of 24/7 support from Google. GNM rolled out the following Google Apps (Google Docs and Sites) in addition to existing productivity tools such as Microsoft Office and provided staff with

- documents, spreadsheets, drawings and presentations online and shareable
- secure, coding-free web pages for intranets and team managed sites
- instant messaging service including group chat, voice, and video

Implementation

As Google Apps was a supplementary service and use was voluntarily, IT rolled out the service with a big bang by issuing staff with a login and a randomly generated password that could be changed by the user. Training took place through non-traditional routes such as lunch time drop-in sessions and a focus on online support through FAQs, and webinars. It was felt that there was little need for formal training due to the similarity of Google Docs to traditional office products and Google easy user interface.

Email

After a few months of using Google Docs successfully thereby testing the product and Google’s customer service, GNM felt confident enough in the product and the service to make the decision to switch email clients and to migrate to Google Mail. This was part of the drive to increase productivity by integrating documents and email but also due to the perceived need for a better email service. Google Mail offers staff a GNM branded account, generous amount of email storage (25GB), excellent email search and classification options as well as 24 hours support. Flexibility and functionality of the product were again the main drivers for the implementation but also savings in internal IT infrastructure and extended professional support.

Google Mail was initially tested in 6 departments for functionality, bugs and also training needs and then slowly rolled out department by department. Existing email archives and contacts in Lotus Notes were copied into the new Google Mail account for each member of staff, so that no loss of information and minimal disruption occurred. Similar group and drop-in sessions, as well as extensive online help were provided by the IT department.

Results

A survey following the pilot amongst staff following the roll out of the new email service came back overwhelmingly positive and the amount of support calls to the IT department decreased significantly. In the 2 years of using Google Apps, GNM experienced only one outage of the service but at the same time enjoyed a variety of service updates and improvements. IT service calls are now widely reduced to issues with support for mobile working and GNM expect to see a significant drop in help desk calls in the long-term.
Melrose Resources plc – Disaster Recovery case study

Organisation

Melrose Resources plc is an oil and gas exploration, development and production company. Founded in the 1990s, it is now listed on the London Stock Exchange and was admitted to the FTSE 250 share index. The group’s activities range from frontier exploration in upper Egypt to mature enhanced recovery projects onshore in the USA. The company’s strategy is to maintain a balanced portfolio of production, development and exploration assets in politically stable and low cost environments.

Challenge

Melrose Resources plc has been growing steadily as a business over the years and the company felt that it had reached a point at which it was necessary to develop a strategy for business continuity and the protection of corporate information from possible disaster as part of their governance regime. The Systems Manager tasked with finding a solution initially looked at a traditional set up of replicating corporate information redundantly on company-owned infrastructure in a remote location. Information to be backed up was held in a variety of applications and systems such as

- Email
- SharePoint
- the internal file system
- SQL databases (ERP solution, HR, intranet)
- Active Directory

The capital expenditure involved in acquiring hardware and infrastructure as well as the on-going operating and maintenance cost appeared prohibitive. The systems manager was soon looking for a solution that would provide flexible, scalable and secure access to replicated information when needed in an emergency without having to acquire large amounts of hardware that would remain unused for large periods of time. The requirements were:

- Secure, instant replication of data to an off-site location
- Highly flexible and scalable access to replicated information in case of emergency
- Reduction of operating costs when disaster recovery systems are on stand-by
- Outsourcing of as many IT and infrastructure management processes as possible to streamline IT expenditure and focus on mission-critical areas

Solution

The company found that cloud computing and in particular Amazon’s Web Services (AWS) could provide what it was looking for: a business continuity solution that would allow the company to consume 100% of services and capacity to access replicated corporate data stored redundantly on virtualised servers when needed for disaster recovery but that would incur only minimal cost and maintenance when primary systems would run as normal. The possibility to outsource the storage of large amounts of data to a cloud service provider like Amazon for a fraction of the cost that would be
required to set up an in-house data centre appeared to be a cost- and time-effective solution that was flexible enough to be expanded to other business areas

“A traditional disaster recovery strategy would have both taken longer to implement, and been more expensive, believes the systems manager: “Long lead times and heavy capex is not a good combination. I'd say we saved something in the region of £50,000 in capital expenditure. Ongoing costs are lower too.” (Systems Manager at Melrose Resources Plc)

**Approach**

Melrose’s IT strategy is Internet-centric and focused on outsourcing most of the traditional IT support and maintenance processes to reduce cost and improve efficiency. Following that strategy, Melrose’s Systems Manager decided to contract a 3rd party provider, CloudReach, to set up, manage and monitor the services on top of the Amazon storage facility used to replicate the organisation’s corporate information in the cloud such as

- managing the invocation process
- moving the company’s Active Directory and DNS applications into the cloud
- developing and managing a secure open VPN gateway for data transfer to and from the cloud
- managing and patching virtual instances in the cloud
- and capacity & performance management

The company felt that even though outsourcing services to a 3rd party has security and supply-chain management implications, the benefits of developing a partnership with providers that have more expertise in the area of cloud computing than is available in-house is more cost-effective and leads to long-term business benefits as Melrose have now expanded their cloud computing approach from disaster recovery to the monitoring of their production environment in co-operation with CloudReach.

Storing information in the cloud necessitates a different approach to managing IT services and represented a steep learning curve for the systems manager but with the help of the 3rd party provider, Melrose have now developed a blueprint that can be applied to their other offices or even to further business processes to be moved to the cloud.

One area in which they had to invest more to enable cloud-based disaster recovery was that of capacity management to enable the reliable transfer of large amounts of information over an Internet connection. To ensure adequate bandwidth in peak times and when information is transferred into the cloud, they had to over-provision their Internet communications to provide a buffer.

The security of information stored in the cloud and compliance with relevant legislation was initially a concern for the company but they are satisfied with Amazon’s information security processes certified through SAS 70 Type II accreditation. Melrose did not negotiate any special SLAs in the contract, however, they would have been able to see the content of Amazon’s SAS 70 Type II audit after signing an NDA but chose not to. The company took the view that Amazon showed openness to share information on security and compliance and has a vested interest in keeping customer information secure and can also deploy much more resources towards the security of their systems than Melrose would have been able to.
Before moving information into the cloud, Melrose underwent a risk assessment exercise with all stakeholders (legal and business process owners) that involved the categorisation of information from a business point of view. It divided information into two broad categories – corporate information and technical information - and analysed what the impact for the business would be, if the data would be accessed by an unauthorised party or be disclosed to the public. Corporate information was singled out for replication in the cloud as this was information needed to continue business as usual. The technical information was deemed to be too sensitive and also too large an amount to be transferred into the cloud in terms of bandwidth. This information remains on the company’s own servers. Data protection was not a major issue as the company only has a few clients and does not hold large amounts of personal data. This certainly facilitated the decision to move data into the cloud.

Results

Using cloud services and storage facilities was a perfect match for the disaster recovery initiative at Melrose Resources plc. It enabled a quick, flexible and cost-effective way to set up a business continuity that supports good information governance. The cloud has delivered

- quick deployment and on demand capacity
- an easy, secure and automatic process for replicating corporate information
- value for money through less up-front investment and less on-going costs
- no long-term contractual tie-ins and little or no Capex
- a way to scale for future needs
Cabinet Office – The G-Cloud

The G-Cloud is part of the government’s ICT strategy which aims to improve efficiencies and cut cost through standardisation and consolidation of infrastructure and capabilities and the adoption and promotion of common standards. The government is looking to create a private cloud which will consist of the following 3 strands

- Government Cloud (G-Cloud): The government aims to establish a private cloud on its existing IT infrastructure which will enable public sector organisation’s to host IT applications and services in a secure and cost-effective shared environment. This private cloud will be set up to be compliant with a set of selected, existing industry standards which will be adopted by government. The adoption of existing standards will facilitate interoperability, information security and the general adoption of cloud computing in a trusted environment.

- Data centre consolidation: The public sector has an estimated 300,000 servers but utilises less than 10% of its computing capabilities. The aim is to reduce IT infrastructure down to an optimum number of modern, resilient, efficient and secure data centres that also act as infrastructure for the G-Cloud.

- Government Applications Store (G-AS): The government is in the process to develop an apps store similar to that established by the US government, offering central and local government online access to shared business applications, services and software. Applications available in the apps store will predominantly be developed externally by 3rd party developers on commission.

In cloud computing terms, these three strands will cover all three cloud service models as follows:

- Software as a Service (SaaS) which includes managed services, common, utility and custom services, all of which can be configured for use by many Public Sector bodies.

- Platform as a Service (PaaS); a framework overseen by the CTO Council that will be used to create and manage provisioning of new business applications based on shared re-usable components; and

- Infrastructure as a Service (IaaS) for hosting existing applications. This includes services providing capability for managing, securing and storing data hosting applications

(Source: Bellamy, M. and Gallagher, G.)

All G-Cloud services are expected to have common characteristics such as pre-certified standards compliance for service delivery, technical (data, inter-operability etc) and information assurance. They will be provisioned from an efficient and sustainable data centre, and will be available through G-AS at a ‘value for money’ best public sector price. The G-Cloud will be a private cloud but in future will include trusted public cloud services. Current constraints of public clouds are

- Information Assurance requirements e.g. data centres are outside the UK

- End to end performance of services from public clouds may not be guaranteed

- Proprietary standards used by some public clouds create the risk of lock in
Once these constraints are addressed and the public sector ICT needs are met by public cloud providers, this cloud delivery model will be used more in the future.

It is not the intention to make adoption of cloud computing technologies mandatory. The aim is to make the apps store the first place for organisations to look for business solutions and services and foster a sense of consuming applications as utilities. Most applications are expected to be developed externally on commission. Should there be a need for a specialised product that is not available from the apps store, organisations will be encouraged to adapt procurement strategies, so that they are able to undertake negotiations in such a way that allows the new product to be incorporated in G-AS.

Applications The store will most likely have a pool of certified, pre-procured applications as well as a place for innovation and will also provide price and performance ratings that allow comparison of applications.

The Cabinet Office has completed the high level design for the server consolidation and the application store and is currently awaiting political direction and funding to take the project to implementation stage. Plans are to make the G-AS live as a prototype in 2011. There are no plans to develop a central document repository or to centralise electronic records management. It appears that records and information managers have at this stage not been identified as stakeholders in the G-Cloud initiative but the project team is talking to the National Archives regarding information management standards. There are plans for an overall authority for the G-Cloud responsible for

- agreeing standards,
- overseeing procurement and certification
- encourage public sector organisations to use G-Cloud and Apps store
- support the creation of new cloud-based services

The Cabinet Office is also working with a wide range of stakeholders with experience in cloud computing like the NHS, in information assurance like the CESG, and in procurement like the OGC. Information security has been identified as a major challenge and the project team is currently looking to select established industry standards with which the G-Cloud infrastructure needs to comply but it is aware that it will need to rely on the willingness of the public sector and potential suppliers to engage in the process and to establish relevant mechanisms to ensure a robust and secure framework for the government’s private cloud.
8. Questions by section

Preparing for the cloud

Cloud service models

Which process, application and information can be moved to the cloud to gain efficiency and cost benefits?

Can the cloud provider deliver a better service for a particular process or application than the organisation can internally while remaining cost-effective and satisfying the organisation’s security and compliance requirements?

Which cloud providers are there in the market that address the organisation’s business requirements and how established are they?

How do cloud services fit into the organisation’s overall corporate and IT strategy?

How will the organisation ensure that users and customers are well supported by services that are moving to a cloud?

How does outsourcing of processes and applications impact on the security of information utilised within these and consequently stored in the cloud?

Can the organisation lose control over processes and applications deployed in the cloud without compromising compliance and risk frameworks?

Does the organisation have the necessary capabilities (staff, expertise, technology) to move processes and applications to the cloud and integrate with in-house applications?

Are processes relatively independent, that is, not coupled to other processes or applications, so that they can operate independently in the cloud?

Are the processes relatively new, so that legacy systems do not have to be moved to the cloud?

Are the points of integration well defined, so that applications in the cloud can be integrated easily with in-house applications?

Is the organisation satisfied with storing information in a multi-tenant environment where it cannot be classified, have retention or metadata applied to it once it has been transferred to the cloud?

Is the pay-per-use model for the cloud service cost-effective and does it meet business requirements?

Is it an acceptable risk to transfer data and information to the cloud provider via an open network like the internet?

Software as a Service

Does the organisation want to have quick access to a purpose-built business application like email, word processing or project management, in the cloud without having to

- buy, configure and install software, hardware and operating systems
- maintain the network, hardware, operating system or the application itself?
Is the organisation looking for a product that is easy to acquire and access but only provides limited ability to customise it or modify user settings?

Can control over the entire system stack, including responsibilities for information and infrastructure security, be confidently transferred to the cloud provider?

**Platform as a service**

Is the organisation looking to write or deploy their own cloud-ready business applications, software or websites on the cloud provider’s infrastructure without having to

- buy the underlying hardware, servers and network
- maintain servers, hardware and network?

Does the organisation have the technical capabilities to create and deploy their own applications and maintain them, including assuring information and application security?

Is it an acceptable risk to develop and deploy applications and websites on the provider’s proprietary APIs which could effectively lock the organisation into a particular development environment with limited interoperability?

**Infrastructure as a Service**

Is the organisation looking to acquire computing resources (servers, networking technology, storage, OS, and virtualisation technology) as a utility from an off-site storage provider in order to

- store or compute large amounts of information
- flexibly provision their own applications or websites?

Does the organisation have the technical capabilities maintain software and platform environments, including assuring information and application security?

**Cloud deployment models**

Which cloud deployment models are available for the services or applications the organisation wants to outsource to the cloud (e.g. Amazon offers a public and also virtual private cloud)?

What are the risks and benefits associated with the different deployment models for the organisation?

Are there security or compliance requirements that prevent the organisation from selecting one of the deployment models?

*Public cloud*

Is the organisation looking for a highly scalable and flexible platform to access and deliver services in the cloud?
Is it acceptable that the infrastructure on which services and applications are run and information is stored are hosted, operated and managed by the cloud service provider outside the control of the organisation?

Does the fact that public cloud services are offered to multiple customers in a multi-tenant environment in which computing resources are shared have an impact on the organisations information security and governance frameworks?

**Private cloud**

Does the organisation want to emulate cloud computing capabilities on their own infrastructure because

- it has already invested in significant data centre operations
- it does not want to hand over control to a cloud provider
- information security and compliance frameworks prohibit the move to an open cloud environment?

Does the organisation have the right internal capabilities to buy, build and manage a data centre and deploy virtualisation technologies?

Is near unlimited scalability and flexibility not a priority for the organisation?

**Community cloud**

Does the organisation want to share computing resources with trusted partners in a private cloud environment?

**Hybrid cloud**

Is the organisation looking to improve efficiencies by running non-core applications in a public cloud and core applications and sensitive and confidential information in the more controlled private cloud?

Is there sufficient internal expertise for the integration of services run in a public cloud with those run internally?

**Information classification**

Has all the information to be transferred, processed or stored in the cloud been identified?

Has information to be transferred, processed or stored in the cloud been classified according to an established system used in the organisation?

Does information to be transferred, processed or stored in the cloud contain enough metadata to identify and retrieve it for information access requests and retention decisions?

Has the impact of breaches to confidentiality, integrity and availability to information been assessed for each information type identified?
Are there any regulatory, security, and confidentiality issues to be considered for any of the information types to be transferred, processed or stored in the cloud?

How would the organisation be impacted, if information stored in the cloud is accessed by unauthorised people, intercepted or leaked to the public?

What impact would it have on the organisation, if information would be unexpectedly changed or unavailable for any length of time?

Is there any information to which the organisation needs immediate and continual access?

**Risk analysis and assessment**

How can the organisation be harmed if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?

How is infrastructure and information protected against unauthorised access (e.g. hacking, interception, user misuse) by the cloud service provider?

How can the organisation ensure the integrity, authenticity and reliability of information stored in the cloud?

What are the organisation’s responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

How can the organisation apply its records and information management programmes (e.g. classification, retention) to the cloud environment?

What is the impact of outsourcing services and information to the cloud on the legislative and regulatory requirements of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing etc.)?

How should the organisation audit and monitor cloud services and establish relevant service level agreements?

Will the organisation be able to negotiate contracts and agreements that fit their risk assessment and compliance environment?

Does the cloud provider have ‘cyber’ insurance to mitigate the risk of information breaches or unexpected downtime that can cover the customer’s resulting losses?

What are the total costs of setting up and managing the cloud services?

**Managing the cloud**

**Information management**

What impact will the management of information stored in the cloud have on existing information management policies and procedures?
Can the cloud providers assure that their information security systems can support the authenticity and reliability of the organisation’s information (including metadata and log files)?

Will it be possible to show that information is fully encrypted and protected against unauthorised disclosure?

In which format is information created, transferred and stored in the cloud?

Will the format in which information was created be changed when it is transferred or stored in the cloud?

What implication does the format of information in the cloud have for access, retrieval and preservation?

What metadata can be applied to information stored in the cloud and can it be managed and searched?

How is metadata applied (e.g. automatically through software or manually)?

Does the organisation need to apply additional metadata to information stored in the cloud than it would apply to information stored in-house? What kind of metadata would that be?

Will it be possible to show that information is fully encrypted and protected against unauthorised disclosure?

Has all information stored or processed in the cloud been classified and supplied with relevant metadata to ensure efficient identification and retrieval?

Has the organisation procedures in place to provision access and usage rights (by job role, seniority, group membership etc.) to categories of information stored or processed in the cloud?

How can these access rights be implemented in the cloud?

Does the organisation have retention and disposal schedules in place for each information category to inform when records are no longer needed for business or compliance reasons?

How can these schedules be applied to information stored in the cloud (e.g. manually, through the provider’s user interface, via metadata)and at what level?

Who is responsible for the allocation and execution of retention and disposal schedules?

How will information be destroyed by the cloud provider (e.g. shredding of drives, deletion of nodes)?

Is the destruction method in line with the compliance requirements of the organisation?

Is it acceptable that images of destroyed information might be accessible on the provider’s hardware until they have been sufficiently overwritten and how long are the timeframes for a complete overwrite?

Can the cloud provider produce evidence or audit trails to certify the destruction of information?

Does the cloud provider understand and support the organisation’s information preservation needs?
Does information for permanent retention need to be transferred to a digital archive or to a place of legal deposit for preservation purposes or can it remain in the cloud?

Legal and regulatory compliance

What legal and regulatory frameworks does the organisation need to comply with?

How will compliance be affected by the fact that information is stored in the cloud?

Are responsibilities for legal compliance clearly established between the organisation and the cloud provider?

Is it clear that the organisation retains sole ownership of information stored in the cloud?

Where is personal information physically stored? Where is provider’s infrastructure located?

Can the organisation specify where information is physically stored?

If the cloud provider is located in the US, do they have a Safe Harbour certification and when was it issued?

Will the cloud provider use 3rd party providers whose infrastructure is located outside of that of the cloud provider?

Is the organisation satisfied that the cloud provider has appropriate technical and organisational processes in place to protect information against unauthorised processing and accidental loss?

Can the organisation ensure that personal information is not kept for longer than necessary?

Can the organisation ensure that information is authentic and reliable?

Can information be easily identified and retrieved for information access requests (DP, FOI, EIR)?

Are responsibilities relating to e-discovery, including litigation hold procedures, discovery searches, and expert testimonies, clearly established between the organisation and the cloud provider?

Do the organisation and the provider have a standard process for responding to subpoenas and other legal requests?

How will the cloud provider notify the organisation, if a third party makes a discovery request?

Is the information stored in the cloud easily identifiable and retrievable in the case of a legal request?

Can litigation hold procedures be easily applied to information stored in the cloud to prevent scheduled destruction of information needed during litigation?

How much will e-discovery in the cloud cost?

What industry standards does the organisation comply with or is certified to?

How will certification or compliance be affected when information is moved and stored in the cloud?
What standards does the cloud provider comply with or is certified to that would provide the organisation with reassurances regarding information security?

**Contract**

Can the contract be negotiated with the cloud service provider or do they issue a standard contract?

Which aspects of the contract can be negotiated (e.g. price, SLAs, technical specifications)?

Can monitoring and reporting processes (e.g. for information and access security, availability, incident response) be built into the contract?

Can the organisation perform full contract due diligence (including financial condition, reputation, controls, personnel, disaster recovery, insurance, subcontractors, and communications) to determine responsibilities and accountability?

Does the cloud provider have ‘cyber’ insurance to mitigate the risk of information loss or unexpected downtime that can cover the customer’s resulting losses?

What jurisdiction does the cloud provider operate in and what impact does that have on enforceability of contract terms?

Will any of the provider’s services be outsourced or subcontracted and how does that impact compliance?

Does the contract

- include a right to audit clause to fulfil compliance requirements?
- stipulate that information remains in the ownership of the organisation
- stipulate how information will be returned to the organisation when the contract is terminated?
- prohibit the provider to suspend or terminate the service abruptly?
- contain a litigation cooperation clause?
- refer to any outside documents (ToS or SLAs)?
- stipulate how changes to the contract, ToS or SLAs will be communicated and applied?

**Cost**

How much will it cost the organisation migrate information and processes to the cloud and integrate them with in-house systems?

How much will it cost to monitor and maintain cloud services for availability, security and compliance?

Is the cloud provider’s pricing structure easy to understand and transparent?
Are prices given in standard pricing units (e.g. cost per gigabytes of storage, cost of each user licence each month or year) that can be compared with that of other cloud providers?

Are user licences bought annually or monthly and how easy is it to cancel or buy additional licences?

How is customer support provided and how much does it cost?

How much is the cost for

- storage of information (per Gigabyte)
- computation of information (per instance or CPU unit)
- transfer of information to and from the cloud (per Gigabyte)
- requests to information (including for use, virus scanning, indexing or back up)
- applications that can be built on the platform
- database objects
- additional features such as WORM or information lifecycle management?

**Monitoring, auditing, and reporting**

Can the organisation audit the cloud provider’s systems for compliance and information security aspects?

Does the cloud provider provide any standard audit documentation and reports that can inform the organisation’s audit and due diligence processes?

How often is the provider audited by external bodies and when did the last audit take place?

How can the following aspects of the cloud provider’s service be measured and monitored to ensure successful governance:

- Performance and availability of the service
- Incident monitoring and response
- Cost and usage of the service
- Access to information, applications and infrastructure?

Does the cloud provider have tools that allow the organisation to monitor whether service levels are being met?

How will the provider communicate performance information to the organisation (e.g. email, dashboard, RSS)

What information is kept in audit logs and how long are these logs kept?
Does the organisation have adequate resources and expertise for monitoring the necessary aspects of the cloud provider’s services?

Can the organisation implement its own monitoring tools or that of third party providers?

How are SLAs and KPIs established, monitored and enforced by the organisation?

Exit strategy

What are the costs involved in migrating or exporting information from the cloud provider?

Exactly what assistance will the provider provide for migrating and exporting customer data?

Are there documented procedures and standardised APIs for exporting information from the cloud?

Does the cloud provider provide interoperable export formats for all information stored within the cloud?

Are there any provisions for exporting user-created applications in a standard format?

Are there processes for testing that information can be exported to another cloud provider?

Can the organisation perform its own information extraction to verify that the format is universal and is capable of being migrated?

Operating in the cloud

Security

Are regular risk assessments of the premises carried out, including neighbouring buildings?

Are data centres secured with intrusion alarms and CCTV as well as access technology such as cards and security logs to prevent unauthorised access?

Does the provider control and monitor who has access to the data centre?

Is electrical equipment kept in rooms that are fitted with environmental controls systems (heating and cooling systems) and adequate fire detection and prevention systems?

Is power supply protected physically and are UPS and back-up generators in place?

Does the provider maintain an accurate inventory of physical equipment such as computer hardware that is updated regularly when equipment is moved or discarded?

Are all network access points and cables secured and protected?

What processes and procedures are in place to destroy old media or systems when required to do so?

What policies and procedures does the provider have in place when hiring IT or staff with systems access (pre-employment checks etc.)?
Does the provider have policies and procedures in place to assign information security responsibilities to staff, make them aware of these responsibilities and provide the required training to enable them to carry out those responsibilities?

How are access rights allocated, reviewed and removed?

Are the provider’s information systems audited and compliant with relevant standards such as ISO 27001/2 or SAS 70 Type II and NIST 800-53 in the US?

Does the provider maintain documented operating procedures for information systems and configurations?

Does the provider have change control procedures to manage configuration changes to the information system using an organisationally approved process?

Are audit logs kept for incident investigation?

How long are logs kept, what information do they contain and how are they protected from unauthorised access?

Are there structured processes in place for identifying, acquiring, testing and deploying patches that cover the whole infrastructure (network, server, virtualisation software, applications etc.)?

What protection mechanisms are in place against denial of service attacks (DDoS)?

Are there defences against internal as well as external attacks?

What level of isolation is used?

Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa?

Is the virtual network infrastructure used by cloud providers secured to vendor or best practice standards?

Does the provider ensure virtual images are hardened by default?

Are virtual images monitored and tracked in an inventory?

Is the hardened virtual image protected from unauthorised access?

Can the provider confirm the virtualised image does not contain the authentication credentials?

Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?

Can a host-based intrusion prevention service be run in the virtual instance?

Is physical and logical access to hypervisors restricted to authorised personnel?

Does the provider ensure virtual images are hardened by default?

Are virtual images monitored and tracked in an inventory?
Is the hardened virtual image protected from unauthorised access?

Can the provider confirm the virtualised image does not contain the authentication credentials?

Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?

Can a host-based intrusion prevention service be run in the virtual instance?

Is physical and logical access to hypervisors restricted to authorised personnel?

Is information automatically encrypted by the provider when at rest or in transit to and from the customer’s network?

Can the customer encrypt information intended for simple storage?

Are encryption keys created in a secure and industry-approved manner?

Who holds encryption keys and how are they kept?

Are security controls in place for reading, writing and using encryption keys?

Can keys be revoked simultaneously across multiple sites?

**Availability management and resource provisioning**

Does the provider have policies and procedures in place to ensure service change control, availability, reliability and performance?

And how is that availability defined exactly (e.g. includes all features and planned downtimes, are there interdependencies with other systems with lesser availability)?

Is the availability level covered in the SLA or contract?

How is performance measured and communicated to the customer (email, dashboard, website information or RSS etc.)?

What controls are in place to prevent unauthorised and unintended information transfer via shared system resources (data remanence) in a multi-tenancy environment?

In the event of resource overload what information is given about the relative priority of a customer’s request (e.g. are some packets tagged for higher priority)?

How much and how fast can customers scale up? Does the provider offer guarantees on maximum availability of supplementary resources within a minimum period?

What processes are in place for handling large-scale trends in resource usage (e.g seasonal effects)?

What guarantees does the provider offer that customer resources are fully isolated?

Assuming physical machines are not shared between customers, to what degree are storage, memory and other data traces fully erased before machines are reallocated?
Incident response

Does the provider have policies and procedures in place to assess the risk of vulnerabilities?

Does the provider have formal policies and processes in place for detecting, identifying, analysing and responding to incidents?

Is this process rehearsed to check that incident handling processes are effective?

How are incidents reported to the customers (e.g. periodical reports, dashboards, emails)?

Are procedures in place to prioritise incidents based on the criticality of the affected system?

Does the provider have automated detection capabilities in place such as intrusion detection systems, anti-virus software and log analysers?

Is there real time security monitoring in place?

How can the customer report anomalies to the provider?

How are incidents documented and is evidence collected, especially when logging and data is co-located for multiple customers?

How much access does the customer have to these logs??

What controls are in place to prevent malicious activities by insiders?

What mechanisms are in place to contain the incidents (e.g. shutting down the system, disconnect from network, disabling systems functions, isolation parts of the infrastructure)?

How are components of the incident eradicated (deleting malicious code, disabling breached accounts)?

How are systems recovered and hardened to prevent similar incidents (restoration from clean backup, rebuilding system from scratch, changing passwords)?

How does eradication and recovery impact on the customers’ services and stored information?

Identity and access management

Are critical systems and information protected with strong authentication mechanisms such as two-factor authentication (e.g. password and token) or three-factor authentication (e.g. something the user has, something the user knows and something the user is)?

Are systems set to automatically lock out a user after a period of inactivity?

Does the provider support strong authentication mechanisms (specifying password length and difficulty etc.)?

Are authentication procedures regularly audited to ensure compliance and detect security breaches? Do customers have access to audit logs?
Do any accounts have system-wide privileges?

How are accounts with the highest level of privilege authenticated and managed?

Does the cloud provider use role-based access controls and follow the principle of least privilege to ensure users only have access to the systems and information they need to?

Is there an administrator role for the customer that allows fine-grained user provisioning and privilege assignment?

Are authorisation procedures and assigned privileges regularly audited to ensure compliance and detect security breaches?

Is system access monitored and logged? Do customers have access to audit logs?

What processes are in place to provision and de-provision privileges simultaneously throughout the cloud system and across multiple locations?

Does the cloud provider support identity federation?

Is the cloud provider interoperable with third party identity providers?

Does the provider support single sign-on?

**Business continuity**

Does the provider have adequate disaster recovery and business continuity plans in place that protect customer information?

How often are these plans reviewed?

Does the provider maintain logs of activity that detail the impact of a disruption?

What are the lines of communication to end customers in the event of a disruption?

Has the provider categorised the priorities for recovery and what would be customers’ priority to be restored?

Is all customer data replicated across multiple data centres to ensure redundancy?

Is the data being backed up at a frequency appropriate to its business value and instantly when it is changed?

Are back up and information recovery processes and procedures regularly checked and reviewed?