west midlands
ACADEMIC HEALTH SCIENCE NETWORK

Digital Health
West Midlands

Information Governance & Cloud

Table of Contents

What is cloud computing?

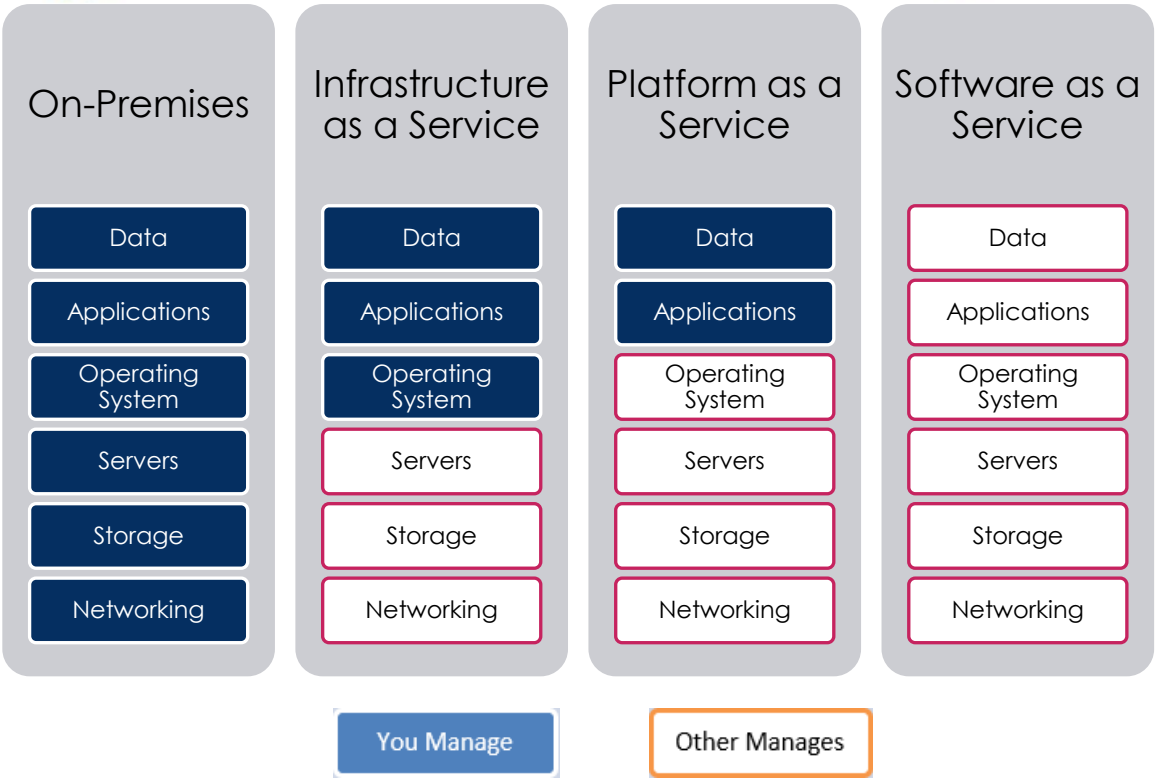
Cloud computing is a general term for the delivery of hosted services over the internet. Cloud computing enables companies to consume a compute resource, such as a virtual machine (VM), storage or an application, as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in house. This contrasts with the model of on-premises IT where the organisation buys, configures and manages the servers, storage and network to run software applications.

There are three main categories of cloud:

- **Public** - Public cloud services provide infrastructure and services to the public, and you, or your organization, secure a piece of that infrastructure and network. Resources are shared by hundreds or thousands of people. Gmail and Drop Box are examples of public cloud services.
- **Private** - Private cloud services are dedicated to one organisation or business, and often have much more specific security controls than a public cloud.
- **Hybrid** - Hybrid cloud services are a blend of public and private clouds. An example of a hybrid cloud solution is an organisation that wants to keep confidential information secured on their private cloud, but make more general, customer-facing content on a public cloud.

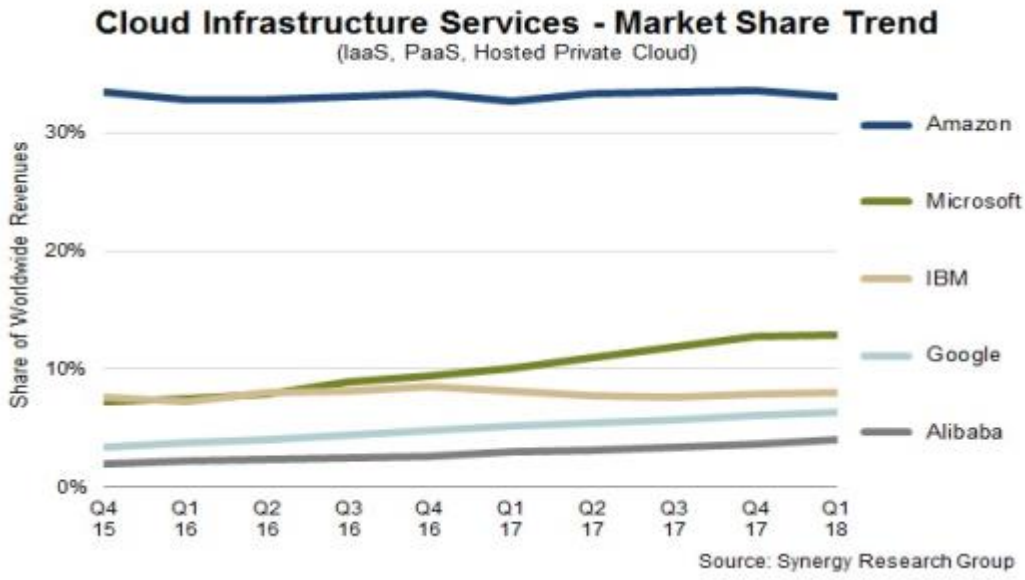
Cloud services can be consumed in three different models, as shown below:

- **Infrastructure as a Service –** The company rents servers from the vendor. They are responsible for running the operating system and applications. Examples include servers in Azure or Amazon S3. These are specified in terms of their size, e.g. CPU, RAM and disk.
- **Platform as a Service –** The company rents the platform which includes the operating system (e.g. Windows Server or Linux).
- **Software as a Service –** The entire application is operated by the vendor. Examples include Google Mail, Office 365 or NHSmail.



Who provides cloud computing?

Cloud services are provided by a wide range of companies however the market is dominated by large companies that have a global network of data centres, including in the UK. As the chart shows below, Amazon has a significant lead with others challenging for second place.

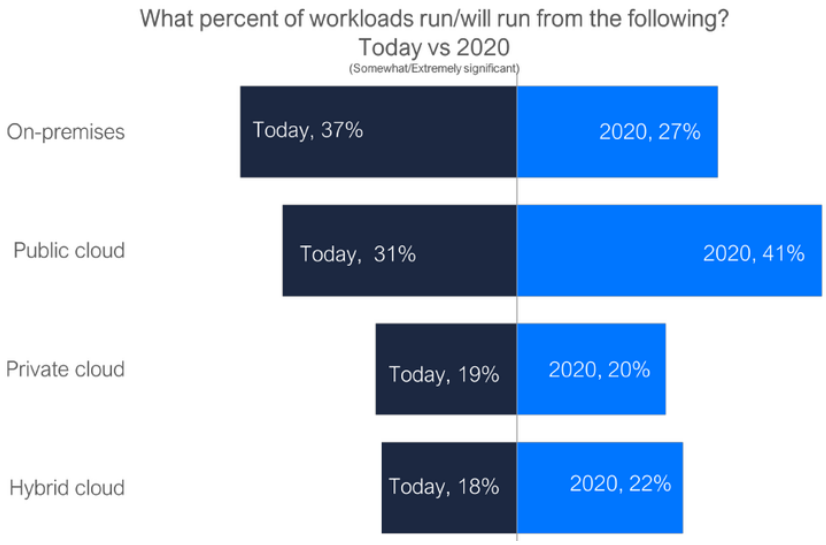


Source: CNBC

Each global player has made had significant investment (billions of dollars) in scale, security, reliability and operating efficiency. For example, a recent Microsoft data centre cost almost £2 billion and the company has more than 100 facilities.

Who uses cloud computing?

Cloud is used extensively across the world and will continue to grow.



Source: Forbes

Within the NHS private cloud services are used for NHSmail, the Electronic Staff Record, electronic patients records (e.g. Lorenzo, Cerner, Badgernet) and GP systems. Public cloud is used by NHS Choices, CRM, case-notes scanning, Trust finance and procurement systems (Oracle, SAP).

What are the rules and regulations?

The Government has had a policy of cloud first since 2013. This was endorsed by the Department of Health in November 2014 and confirmed as health policy by the Secretary of State for Health in November 2018, as described in the vision for technology.

The Data Protection Act 2018 does not include any specific provisions with respect to cloud. Its rules apply to all Data Processors. There are no specific assertions for cloud in the Data Security & Protection toolkit. Trusts need to be able to demonstrate compliance for all its suppliers.

Both NHS Digital and the Information Commissioner's Office has issued guidance on the use of cloud. These describe how organisations can demonstrate they comply with. NHS Digital states that "NHS and Social care providers may use cloud computing services for NHS data. Data must only be hosted within the UK - European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.

Senior Information Risk Owners (SIROs) locally should be satisfied about appropriate security arrangements (using National cyber security essentials as a guide) in conjunction with Data Protection Officers and Caldicott Guardians."

What are the opportunities & risks?

Cloud (especially public cloud) has the following advantages for digital innovation:

- **Cost** – Costs scale with demand as the supplier only pays for what is used.
- **Time** – Setting up cloud services takes minutes rather than days, weeks or months.
- **Focus** – Outsourcing operation of infrastructure allows a focus on the innovation itself.

This is countered by a loss of control. Cloud providers operate using standard terms and conditions that they will not vary for individual customers. Customers have few sanctions beyond walking away from the provider, but this is not always practical and can be costly.

NHS Trusts have been concerned around the cyber security of cloud. Over the past few years the balance of risk has changed. Cloud services have demonstrated their adherence to security good practice through standards such as ISO27001 or the Cloud Security Alliance CCM 3.0 (see here for an explanation). This far exceeds the standards enforced for on-premises IT. Compliance certificates are published on the cloud websites.

All but Google of the top 5 providers have both UK or EU data centres. They allow data to be locked to a region however this must be selected when creating the cloud service. This gives control of data sovereignty.

Cloud services are designed to be highly available but do suffer from downtime. In 2016, this varied between 2h30 and 17h depending upon the supplier. The cloud service is also only as reliable as the Internet connection to the Trust. As with all digital systems, consideration needs to be given to business continuity.

What are the practical steps to adoption?

The first step is to recognise that cloud is a growing part of digital services. It will already be used in the Trust through contracts (e.g. PAS), provided by the centre (e.g. NHSmail) or consumed directly by staff (Google search & maps, Uber). Its use is only going to become more significant over time.

An innovation or new service requires a data protection impact assessment. The use of cloud services should form part of the impact assessment. It is best to take a risk-based approach to this. An example has been provided below.

Training may help to ensure all involved in cloud services are aware of their strengths and weaknesses. This extends to the data protection and information governance team.

west midlands ACADEMIC HEALTH SCIENCE NETWORK

Digital Health West Midlands

Example Risk Assessment

Source of Risk and Nature of Potential Impact	Mitigation	Likelihood of Harm (Remote, possible or probable)	Severity of Harm (Minimal, significant or severe)	Overall risk (Low, medium or high)
Unable to enforce contract as lack of control over supplier. This means that the Trust is unable to enforce patient's GDPR rights.	Contract review Build strong relationship with supplier Document walk-away plan	Remote	Minimal	Low
Supplier does not follow Data Protection Act in violation of law and contract. This means that the Trust is unable to enforce patient's GDPR rights.	Consider reputation of supplier prior to contract Document walk-away plan	Remote	Minimal	Low
Change in Government or NHS policy (e.g. because of Brexit) imposes additional controls or prohibits use of EU data centres.	Select a cloud supplier with a UK data centre. Document walk-away plan	Possible	Minimal	Medium
Cyber security issues result in information breach	Ensure supplier has appropriate security compliance certification Review security settings in application	Possible	Significant	High
Unable to retrieve data at end of contract	Ensure data extract process known before contract signed. Document walk-away plan and test prior to live service	Possible	Significant	High
Data ownership doesn't rest with Trust	Review terms and conditions to ensure where ownership rests	Possible	Minimal	Low