

**About the cloud**

The cloud is a term used for a series of remote access services that exist on the internet. When you access services or store information in the cloud, they are not located on your own personal device (e.g. the hard drive on your laptop, your phone or external drives), but on a computer owned by someone else and located somewhere else.  The computers used for cloud services are usually housed in massive data centres and can be anywhere in the world.

**Where is the cloud?**

Most computers used for cloud services are owned by private organisations such as Amazon, Microsoft or Apple, they keep millions of peoples’ data that is made accessible to them via the internet. The biggest data storage servers in the world are located in China, USA and India, some are even situated at the bottom of the ocean.  The location of the computers in ‘the cloud’ that hold your data is very important.  This is the legal location of the data, and if that is ‘personal data’, you may be breaking the law if it is located outside the UK or the European Union.  It is also important to know something about the company that is hosting the cloud service and looking after the computers which hold your data.  Many data centres are kept up to date and secure, but some are not, and may put your data at risk.

**Cloud computing ‘as a service model’**

A widely used cloud service is office software and web-based applications, which is known as **Software as a service or SaaS**.  An example of SaaS is Office 365, where you can sign into your Microsoft account on any machine and access applications such as Microsoft Word, Excel and PowerPoint.  You can also access your files. The web applications and files are all stored on a computer in a data centre (the cloud), and this makes them accessible remotely from any computer as long as there is an internet connection.

In addition to SaaS, consumers can rent one of the computers and operating systems in the data centre themselves, this is known as **Platform as a Service or PaaS**. With PaaS, consumers do not have the responsibility of managing, updating and maintaining that computer and operating system that hosts the application and can therefore focus more on software development or providing other services to customers. Examples of PaaS services are AWS Elastic Beanstalk and Google Cloud.

**Infrastructure-as-a-Service or IaaS** takes this one step further. The cloud service provider owns the infrastructure components that were traditionally present at a larger company’s location, including servers, storage and networking. Microsoft Azure and AWS Cloud provide infrastructure services to their clients. In this case, the client is responsible for managing and updating systems on this remote infrastructure even though it is at a data centre, often in a different country.

**Benefits of cloud services**

When a business signs up for services with a **Cloud Service Provider** **(CSP),** they must initially transfer their business data to the cloud computers located in the data centres.  They will not have to look after the servers themselves (which includes updating them regularly), because the data centre does this for them. Using a CSP not only allows the business to access the very latest technology, but it also gives them the flexibility to try out applications offered by the CPS. The latest applications are already bought and installed in the data centre and this provides options for a  business without them needing to invest in change upfront. With a pay as you go model, cloud applications can simply be cancelled if they don’t perform as hoped.

Another benefit of the ‘as a service’ model is that because a professional company is managing your technology, their level of support and maintenance, means more of your budget and time can be spent on business strategy and less on IT and security. Cloud services provide access to automatic updates which can be included in your service fee.

As long as you ensure that you choose a reputable CSP, their cyber security expertise and investment will most likely be much higher than anything you could afford.  For this reason,  data is usually more secure in cloud data centres than on the computers of small companies. Having your data stored in the cloud can help with business continuity, as system and infrastructure backups prevent data loss from natural disasters, power failures and other crises.

Your business can scale up or scale down your operations and IT systems to suit your situation, allowing for more flexibility as your needs change.  If you start off by buying quite a small amount of cloud services, you can simply increase this as your company grows, without needing to change and invest in your IT infrastructure yourself.

**Security risks of the cloud**

As seductive as it is to relax in the hope that your CSP is managing all the security risks, this may not be the case. It is vital that organisations adopting cloud technologies and choosing cloud services and applications fully inform themselves about the ever-changing threats, risks and vulnerabilities associated with the cloud. It is also vital that they properly research their CSP to ensure that the security policies adequately reflect their business’ requirements.

A cloud environment experiences the same threats as traditional companies. Hackers will always be trying to exploit vulnerabilities which can be found in all software, wherever it is run. In cloud computing, responsibility for mitigating these security risks is shared between the CPS and the cloud customer.

**Minimising the risks**

* Use two factor authentication or multi-factor authentication – If you can access your data remotely, so can cyber-criminals. Multi-factor-authentication (MFA) gives a crucial layer of added security when logging into your cloud accounts. Instead of just a password, MFA asks a user to provide another form of authentication. This might be a password plus a code received as an SMS or a fingerprint scan.
* Limit and monitor the access of your users. Limiting access can limit the impact when account information like user-names and passwords are stolen or a disgruntled employee wants to cause harm. (see guidance [about accounts](https://getreadyforcyberessentials.iasme.co.uk/about-accounts/))
* Encrypt data – Encryption is the process of encoding information so that only people with access to a secret key can understand it. This helps provide data security.
* Provide anti-phishing and security training. It is important that the individuals who use the system are educated about best practice behaviour and the tactics used by people who send phishing emails. Phishing attacks are a common way that hackers access even the most secure cloud databases.
* Cloud customers are advised to develop a thorough understanding of the services they are buying and to use the security tools provide by the CSP. If you are not confident in this area, it is advisable to ask an IT consultant to help you check the security policies of your CSP.
* Most CSPs give significant guarantees against loss of data, however no system is perfect. Major cloud service providers have accidentally lost customer data. Ensure that your chosen CSP has data backup and recovery processes that meet your organisation’s needs.