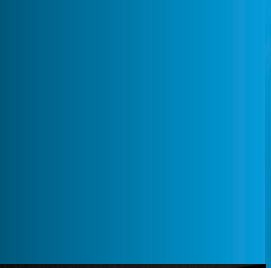
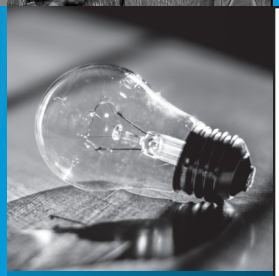










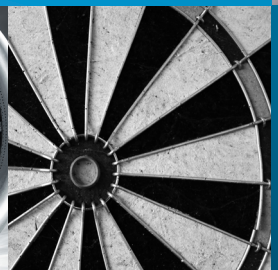


KT SECURE




OPTIMISING CLOUD INFRASTRACTURES SECURELY

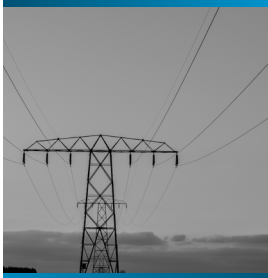


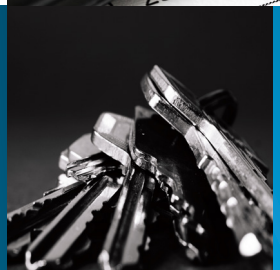
The vast majority of global businesses are moving at least part of their IT service provision to the cloud.

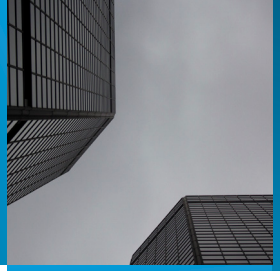
In fact, McAfee's 2017 "State of the Cloud" report[1] found that 93% of companies now use cloud services, with 80% of IT budgets likely to be committed to them in the near future.

This guide discusses the reasons behind this shift in how companies provision their IT solutions. It looks at the nuances around the various different types of cloud solutions, and then moves on to the very important issue of how businesses can ensure their cloud-based infrastructures remain reliable, secure and legally compliant.

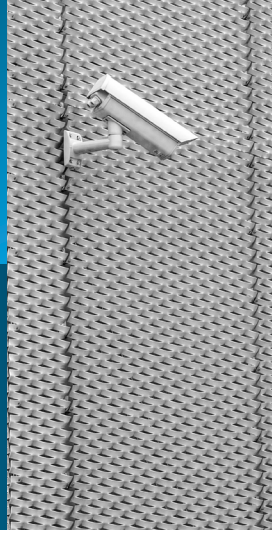


To view this whitepaper online, visit our website: www.ktsecure.co.uk





WHAT IS THE CLOUD?



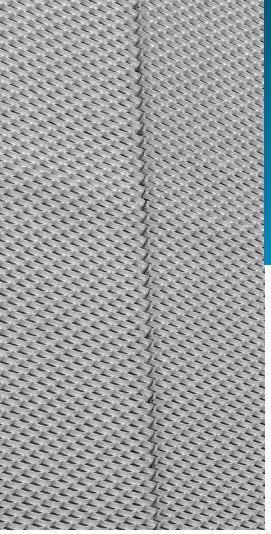
The cloud is a term that's widely used in technical contexts, but not everyone knows what it really means. While the word "cloud" may evoke an image of an enormous and mysterious infrastructure in the sky, it's really nothing as mystical as that!

When IT services and silos of data are "in the cloud," this merely means that they are held on the Internet, rather than on individual office computers or servers. There are still servers involved, but they're typically located in large data centres across the globe.

The vast majority of computer users have been using consumer cloud services for years, perhaps without knowing it. Gmail is a cloud-based email service; Dropbox is a cloud-based service for data storage and file sharing; Netflix and Amazon Instant Video are cloud-based streaming media services.

Business cloud services are no different. Companies nowadays are switching to cloud-based email services instead of running their own email servers in-house, moving data files from local storage to cloud providers who can offer speed, accessibility and resilience, and reclocating line-of-business applications to the cloud instead of maintaining them on their own servers.

As we discuss next, there are myriad benefits for companies who move to the cloud, both technical and financial, but there are security and compliance risks too.



Rise of "Cloud First"

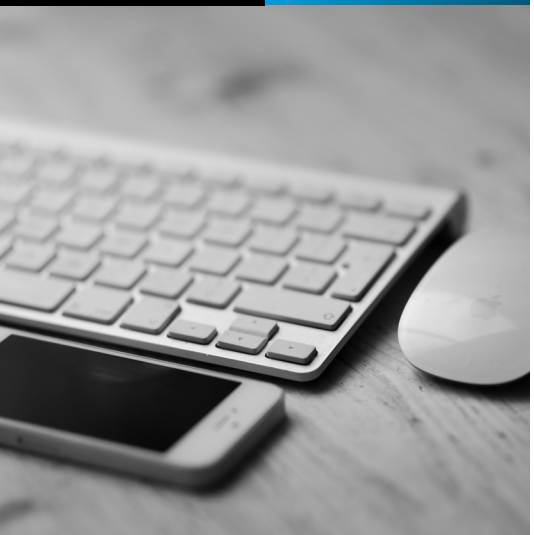
Organisations of all kinds are now adopting a "cloud first" approach to their IT service provision. As an example, the UK government adopted a "cloud first" strategy[2] back in 2013. This essentially means that whenever a new IT system is needed, they look to implement it using cloud services before considering more "traditional" in-house solutions.

The runaway momentum of this trend hasn't grown without creating some issues; one of the most significant is a considerable skills shortage. There simply aren't enough IT professionals out there who are suitably experienced in cloud infrastructures, especially when it comes to keeping them secure. In fact, nearly 50% of companies are having to delay moving systems[3] to the cloud due to this "cybersecurity skills shortage."

While this shortfall in skills is partially caused by the rapid adoption of cloud services, the constant evolution of the cloud environment is a significant factor too. Cyber crime is on the rise globally, with incidents up 63% in the UK[4] in 2017. An ever-changing landscape of security threats means that cloud security has to be a significant and constant priority.
The burden of compliance is also something companies have to deal with, especially when new legislation such as the EU's General Data Protection Regulation (GDPR) comes into effect. One only needs to look at the negative press companies receive in the event of a data breach to know how crucial it is to store data in a safe and compliant manner.

Despite these realities, the trend for moving enterprise IT systems to the cloud continues apace, and this is unsurprising given the benefits such a move brings. Aside from helping companies to use advanced technology economically and flexibly, cloud solutions done right can actually ease many security and compliance pressures - all of which still change and evolve for firms who stick to doing everything "on premise" anyway.

CLOUD PROS AND CONS



Advantages

Financial Flexibility: Companies using cloud services can usually make use of a "pay as you go" model, eliminating the huge capital spends that once went with implementing new IT services. This provides more financial flexibility, and puts sophisticated "enterprise level" systems within easy reach.

Ease of Access: Cloud services support the rise of flexible working patterns[5], in some cases eliminating the need for work to centre around one or more offices! Often, an Internet connection and web browser is all that's required to access cloud services, making it easy for staff to work from anywhere.

Simpler Business Continuity: If a team can work flexibly, traditional "fire and flood" disasters needn't have so much of an impact. Furthermore, companies can build additional failover and resilience features with ease.

More Scalability: If a company requires more storage, more capacity, or the roll-out of a system to a larger base of users, this is generally far more straightforward with a cloud-based system.

Security Automation: With some cloud services, companies are essentially "buying in" to systems that are constantly maintained, patched and monitored, relieving the burden on an in-house team.

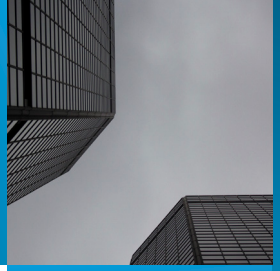
Simpler Compliance: Similarly, companies have the option of buying services from cloud service providers that are already certified and compliant with regulations such ISO 27001, HIPAA or GDPR[6].

Disadvantages

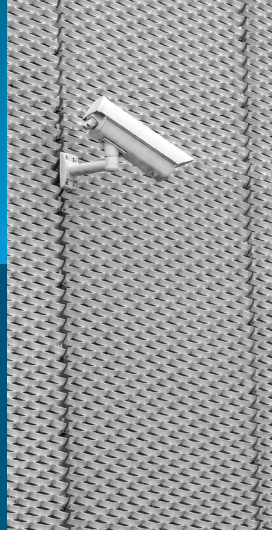
Compliance Risks: Compliance is a double-edged sword when it comes to the cloud. While using well-renowned top cloud providers can ease this burden, smaller suppliers can introduce potential compliance issues, especially if it's unclear where and how they store and protect their data.

Clarity of Responsibility: While it's all very well "shifting risk" to a cloud service provider, moving services to the cloud can muddy the waters of who exactly is responsible for what. This can also apply when data is moving between systems under different jurisdictions.

Risk of Unavailable Systems: While cloud-based systems are arguably more reliable and resilient than their on-premise counterparts, the risk remains that provider downtime or a loss of connectivity could result in a system becoming unavailable.



TYPES OF CLOUDS



Public Cloud

Public cloud services, such as those provided by Amazon Web Services and Microsoft Azure, are essentially shared services where the providers manage the core infrastructure and sell the solution on to clients.

Public cloud environments can be "multitenant," where multiple customers share the same systems and rely on the provider to safely partition their data away from that of other clients.

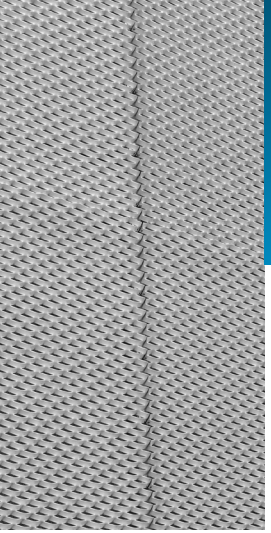
Alternatively, clients can buy a single tenant solution, giving them their own isolated environment. Single tenant public cloud solutions are sometimes referred to as "hosted" systems.

Private Cloud

Private cloud systems involve companies purchasing or leasing their own equipment in data centres, establishing a virtual server environment, and managing their cloud system themselves.

Some confusion exists around whether it's possible to run a private cloud using the infrastructure of a provider like Amazon Web Services (AWS).

It is possible to run what Amazon describe as a "Virtual Private Cloud" by using an infrastructure that's "logically isolated from other networks."[7] However, it's fair to argue that this isn't a private cloud in the truest sense.



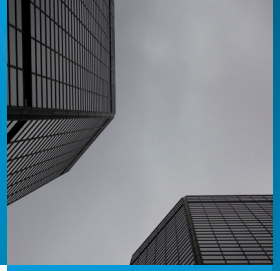
An important thing to understand is that while “the cloud” is a generic term, there’s neither just one cloud, nor only one type of cloud. Many companies now utilise “multicloud” environments, which merge services from different cloud providers, each supporting different applications and / or data stores.

Hybrid Cloud

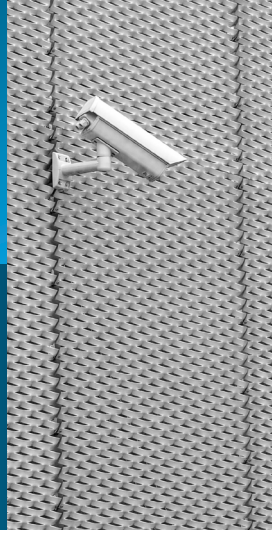
Hybrid clouds are very common and bring together elements of public and private cloud systems to arrive at the totality of the infrastructure a company needs.

There are all manner of ways to build a private cloud system. Companies may, for example, use a front-end system hosted in a public cloud but store their sensitive data in a private cloud.

Alternatively, they may use a private cloud for their corporate database, but a public cloud-based hosted system (such as Office 365) for company email.



TYPES OF CLOUD SERVICES



SaaS (Software as a Service)

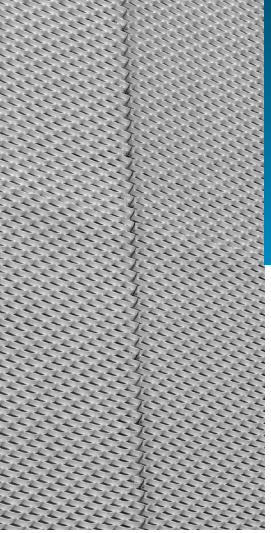
Software as a Service (SaaS) is probably the type of cloud service people are most familiar with. SaaS involves putting specific applications into an environment where they are accessible from anywhere via the Internet.

Examples of top cloud providers in the SaaS world include Salesforce, Dropbox, and Google Apps applications, including Docs and Sheets, which provide an alternative to locally installed office apps.

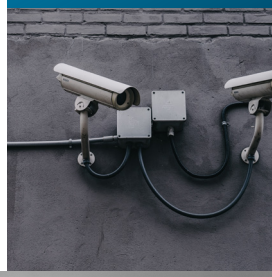
PaaS (Platform as a Service)

Platform as a Service (PaaS) is most commonly used for middleware[8] and custom line of business applications. It allows developers to produce custom software for companies on a virtualised infrastructure that's scalable, and distinct from the rest of the firm's IT systems.

Examples of PaaS include Google App Engine, Microsoft Azure, and AWS Elastic Beanstalk.



As well as the different flavours of clouds, there are different types of cloud services available to companies. Enterprises often use one or more of these options:



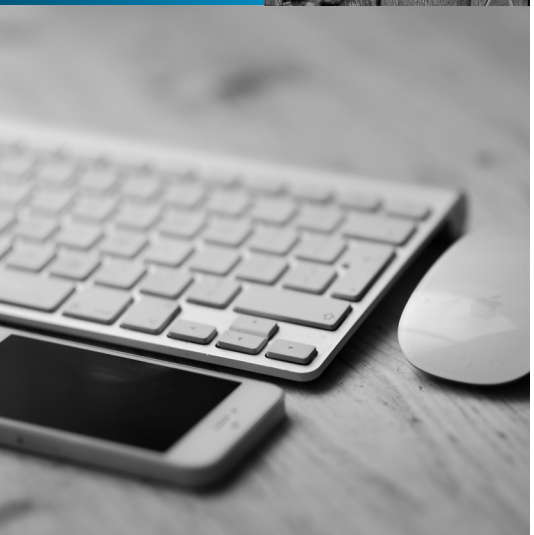
IaaS (Infrastructure as a Service)

Infrastructure as a Service (IaaS) places the core system infrastructure into the cloud, including the servers (usually virtualised), storage and networking components - essentially all of the component parts that would once have been managed " in house."

IaaS gives companies considerable flexibility, and the ability to scale up and down as their needs change. With IaaS, it's conceivable for a company to run with limited in-house hardware beyond low-specced computers and printers, with everything else happening in the cloud.

Examples of IaaS include Rackspace, Microsoft Azure and Amazon Web Services. There are also plenty of smaller players offering bespoke IaaS solutions.

CLOUD SERVICE INTEGRATION



Interconnectivity

Companies using cloud solutions also have to give some thought to how everything connects together. This can include how users connect to cloud resources, and how different cloud services connect to each other.

Options include secure VPN (Virtual Private Network) connections running via the public Internet, dedicated connections to providers (often known as leased lines), “carrier to cloud” connections offered by major telecoms firms, and specialist “cloud exchange” connectivity companies.

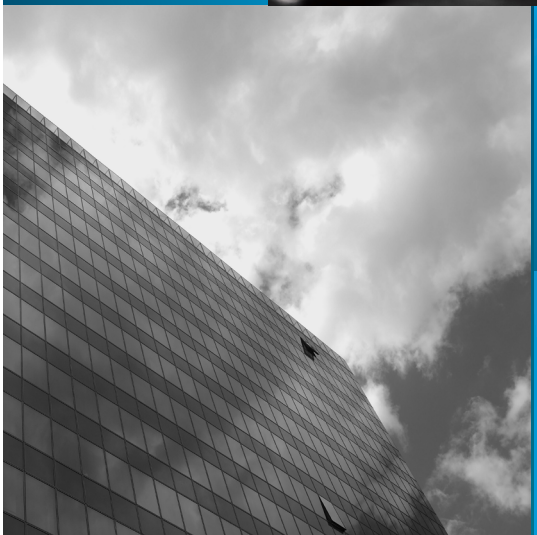
Cloud Service Selection

Choosing the right cloud services can prove a significant task, and there's an abundance of choice. Doing full "due diligence" on any interesting solutions is crucially important for companies who wish to end up with a secure, reliable and compliant system.

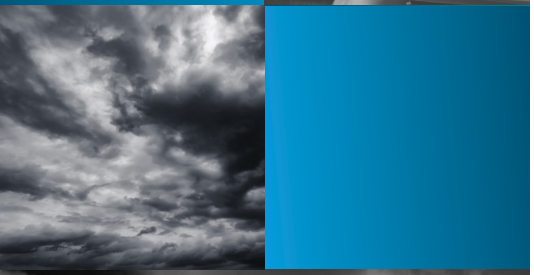
At one end of the scale are cloud-based SaaS applications that fulfil a specific purpose. Often offered by niche providers, these could be anything from databases developed for particular business types to online meeting platforms.

Then you have off-the-shelf solutions from bigger players. Microsoft's Office 365 is a good example of this. While Office 365 offers an array of options for integration with on-premise systems and other cloud offerings, it's often purchased by companies looking for a simple way to move things like email, internal messaging and basic file storage to the cloud. Similarly, Salesforce is a cloud-based solution for Customer Relationship Management (CRM).

At the other end of the scale are solutions like Amazon's AWS and Google Cloud. These highly customisable solutions offer anything from the ability to store basic silos of data, to the option of creating a complete and bespoke IaaS solution.



WHAT IS CLOUD SECURITY?



The Core of Cloud Security

Equally important to choosing the right services and managing the migration from in-house systems, is ensuring the cloud environment is as safe as possible from security threats.

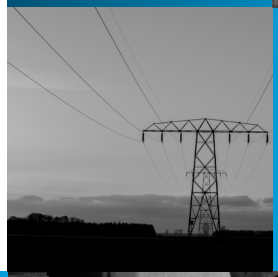
Cloud security is not straightforward; it encompasses many things and requires a multifaceted approach. It's crucially important to understand that cloud security is never an "off the shelf" solution.

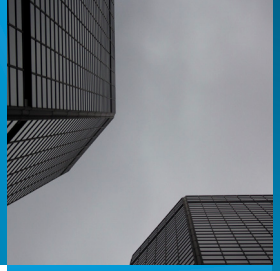
Effective cloud security must include:

- Establishing roles and and responsibilities for security controls, some of which will fall on the company and some on the cloud service provider(s).
- Establishing policies and procedures for the use of cloud-based systems that ensure maximum system security and legal compliance.
- Implementing technical solutions, such as firewalls, intrusion detection systems and secure communications links, to make the infrastructure as secure as possible.
- Ensuring all of the above covers every element of a hybrid infrastructure and doesn't leave any omissions or weak spots.

Good quality cloud security never does any of the following:

- Assumes that leasing systems and services places total security responsibility on the service provider(s).
- Forgets about the importance of effective security at the system endpoints (company premises, laptops, mobile devices AND system users!)
- Stands still and assumes all vulnerabilities are protected against, in a world where threats are constantly evolving.





CLOUD SECURITY THREATS

The list of possible threats facing all cloud environments is a long one, and demonstrates just how many things IT professionals need to mitigate against.

Here are some of the threats that must be considered and protected against:

Data Breaches

High profile data breaches hit the mainstream media all the time, so it's no wonder companies live in fear of being responsible for the next one. Anything from an honest human mistake to a software bug can mark the start of a breach.

Vulnerabilities in Tools and APIs

Cloud infrastructures are usually built up of dozens of different components, application programming interfaces (APIs), plugins and management consoles. Missed patches or weak password security on any one of these components can introduce security flaws.

Poor User Security

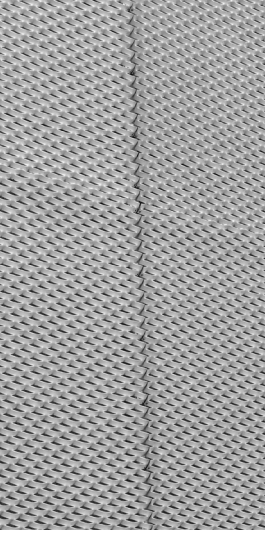
Providing system users with too much system access can compromise both security and compliance, making effective identity management absolutely crucial.

Malicious Behaviour

It's not unique to cloud-based systems, but staff, consultants, or individuals with malicious intent can compromise IT solutions of all kinds. Arguably, cloud-based systems are more vulnerable because people are not tied to one location when they wish to access them.

Risk of Data Loss

Again, this isn't a threat unique to cloud infrastructures, but all the traditional disasters like fire, flood and malicious damage, could affect a cloud service provider and result in the loss of data. As such, it's vital to be fully informed as to every provider's provision for backup and disaster recovery.



Denial of Service Attacks

Denial of Service (DoS) attacks[9] occur when hackers attempt to overwhelm servers with traffic so that they cannot perform their usual functions effectively. DoS attacks can be aimed at company-specific services, or the underlying infrastructures they run on. The use of intrusion detection systems and failover servers are among the steps than can mitigate against these attacks.

Viruses and Malware

Servers in the cloud are at just as much risk from targeted virus and malware attacks as the servers and individual computers in company offices. In early 2018, the "Spectre" and "Meltdown" exploits hit the headlines[10] when vulnerabilities at hardware and driver level were uncovered, creating the need for emergency patching on systems of all kinds. This was a race against time to patch known bugs before malware could be developed to exploit them, unfortunately, patches and vulnerabilities are still ongoing, due to the scale of the problem.

Other Threats

Other issues that can threaten the reliability and security of cloud services include:

- Social engineering attacks (including phishing)
- Account hijacking
- System overloads

There are also potential threats that move beyond IT security that can still cause problems for companies deploying cloud services, such as:

- Unexpected costs
- "Lock in" to specific vendors, and the associated expenses this can cause
- Insufficient due diligence resulting in compliance issues
- Provider problems having a knock-on effect on the companies using their services

LEGAL AND PERSONNEL ISSUES

Legal and Administrative Issues

Compliance was touched on above. While using cloud services that are properly certified and audited can, in some cases, make things easier than designing an entire internal environment to comply with a raft of different legislation[11], there are still issues to be aware of.

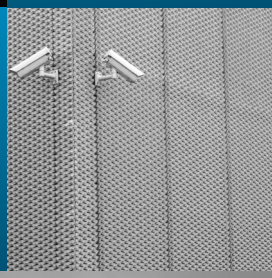
These can include ensuring that every component part of a system uses servers in the correct legal jurisdiction.

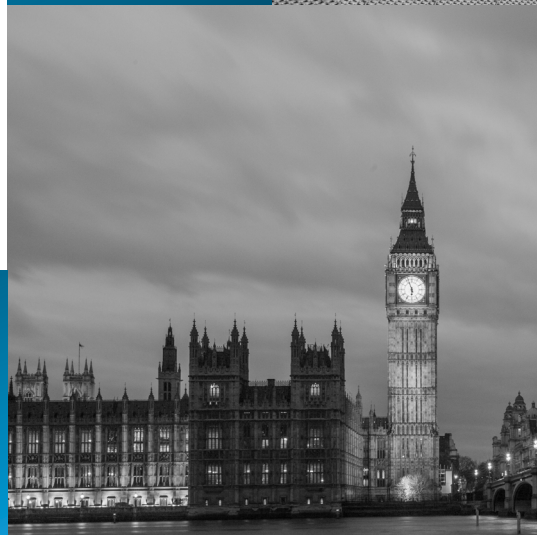
If, for example, a firm is using a company with EU-based servers to help with GDPR compliance, they need to ensure the service isn't mirroring data to a data centre elsewhere in the world.

Cloud Security Policies

Sometimes IT security is as much about policies and procedures as it is about technical tweaks. All system users must understand their obligations when using cloud-based company IT systems and know what rules they must comply with.

These policies must also ensure that the everyone in the company adheres to each cloud service provider's terms of service.



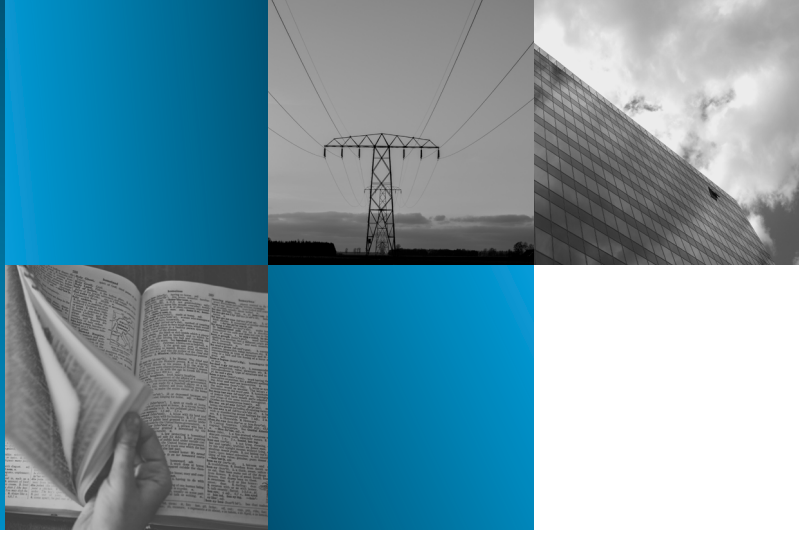


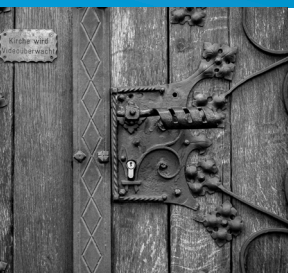
Identity and Access Management

The flexible system access that cloud services provide can prove both a good and a bad thing, especially because it usually allows staff to access company systems from anywhere. As such, it's crucial to ensure that levels of access are kept to the minimum required for each individual to do their job.

Similarly, access management is about ensuring people aren't left with system access when they no longer need it, which means having procedures in place to remove access when staff and consultants leave the business.

VULNERABILITY AND CONTINUITY





Vulnerability Assessment and Penetration Testing

Cloud systems (like all IT systems) should be managed with a rolling program to ensure they are safe from the all recently uncovered bugs and vulnerabilities.

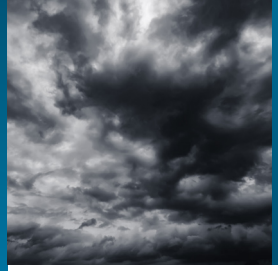
They should also be periodically subjected to “pen testing,” where specialists attempt to (ethically) hack into the systems to expose any unknown areas where the infrastructure could be vulnerable to cyber criminals.

Business Continuity and Disaster Recovery

Business continuity is extremely important for businesses of all sizes. Disaster recovery plans need to encompass every element of a cloud-based system (and how it interfaces with any on-premise equipment) so that there’s a documented way to quickly bring essential services back online in the event of any kind of disaster.

Disaster recovery plans need to cover everything from small incidents (such as the loss of a single IT system), to more comprehensive disasters such as the loss of office space or a total system failure.

CREATING YOUR OWN COMPANY CLOUD SYSTEM



Implementing a cloud service and infrastructure within your company can be a difficult challenge and task. While it's possibly to do much of it inhouse (signing up to Google Drive, AWS, etc is becoming ever more easier), it is usually best to find experts to help you out, due to the depth of the topic.

The 7 Steps to creating a cloud infrastructure within your company are as follows.

1. Service Selection

Finding the services that work best with your current systems and tasks

2. Architecture Design

Designing the infrastructure of your systems, and to see how things will be put together

3. Interconnection of Multiple Environments

Working on the actual interconnectivity of different services and programs so that everything functions seamlessly

4. Implementation and Deployment

The actual roll-out of your cloud systems.

5. Comprehensive Management

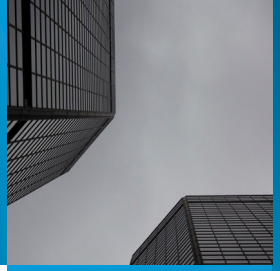
Managing your system to ensure that it works as intended and each and every users is able to do their tasks seamlessly

6. Reporting and Alerts

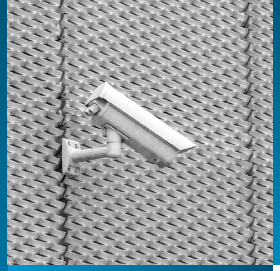
Setting up systems to ensure that you'll be able to resolve any issues, before they cause major issues for your company

7. Ongoing Improvements

Constantly improving your systems where possible. Either improving connectivity, security, integrating more useful services, or



CLOUD SECURITY ALLIANCES



There are 3 alliances that help with the implementation, maintenance, monitoring and security of cloud infrastructures.

CSA - Cloud Security Alliance (https://cloudsecurityalliance.org/)

The Cloud Security Alliance is the world's leading organisation to help with raising awareness and implementing security for the cloud. They use knowledge from experts around the world, to be able to provide accurate, important and up-to-date technical information for cloud services and infrastructures.

TCG - Trusted Computing Group (https://trustedcomputinggroup.org/)

The Trusted Computing Group is very similar to the CSA, but instead of focusing on just the cloud, it focuses on the security and privacy of whole networks. Through open standards and specifications, TCG enables secure computing. Benefits of TCG technologies include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity.

DMTF - Distributed Management Task Force (https://www.dmtf.org/)

The Distributed Management Task Force has set up multiple standards and working groups addressing cloud management, and their Cloud Management Initiative brings this work together for an integrated approach. Focused on achieving interoperable cloud infrastructure management between cloud service providers and their consumers and developers, the Cloud Management Initiative also promotes adoption of these standards by the industry.

ENDNOTES

1 McAfee, *Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security*
https://www.mcafee.com/us/solutions/lp/cloud-security-report.html

2 UK Government, *Government Cloud First policy*
https://www.gov.uk/guidance/government-cloud-first-policy

3 Louis Columbus, Forbes, *2017 State Of Cloud Adoption And Security*
https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/

4 Warwick Ashford, ComputerWeekly, *Business cyber crime up 63%, UK stats show*
https://www.computerweekly.com/news/252433873/Business-cyber-crime-up-63-UK-stats-show

5 Richard Jones, Telegraph, *Flexible working not just for mothers, says largest ever study of UK workforce*
https://www.telegraph.co.uk/women/work/flexible-working-not-just-mothers-says-largest-ever-study-uk/

6 Chris Evans, ComputerWeekly, *GDPR brings serious implications for data storage*
https://www.computerweekly.com/feature/GDPR-brings-serious-implications-for-data-storage

7 Amazon AWS User Guide, *What Is Amazon VPC (Virtual Private Cloud)?*
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

8 Wikipedia, *Middleware*
https://en.wikipedia.org/wiki/Middleware

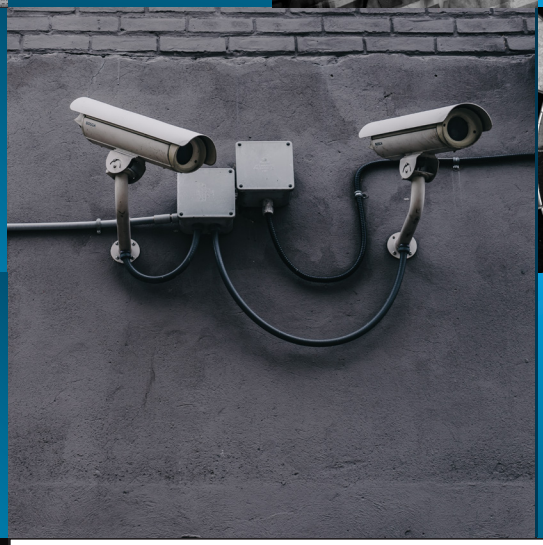
9 TechTarget, *denial-of-service attack definition*
https://searchsecurity.techtarget.com/definition/denial-of-service

10 Peter Bright, ArsTechnica, *Spectre and Meltdown patches causing trouble as realistic attacks get closer*
https://arstechnica.com/gadgets/2018/01/spectre-and-meltdown-patches-causing-trouble-as-realistic-attacks-get-closer/

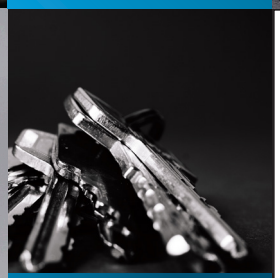
11 Computer Weekly, *Data storage compliance in the UK*
https://www.computerweekly.com/feature/Data-storage-compliance-in-the-UK

KT SECURE










CONTACT US

KT Secure

1 Harewood Row, Marylebone

London, NW1 6SE

+44 (0)207 889 0888

info@ktsecure.co.uk

www.ktsecure.co.uk