JUMPSEC

NAVIGATING CLOUD ADOPTION MYTHS AND MISCONCEPTIONS

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

Cloud computing is the vehicle with which modern enterprise organisations drive their digital transformation initiatives.

Despite the clear advantages of cloud adoption, many organisations, or factions within organisations, have resisted cloud adoption at a management level.

Part of the resistance to cloud adoption is due to misinformation. To tackle the confusion, we discuss some of the most prevalent misconceptions that organisations have concerning the cloud.

Introduction

Cloud computing is the vehicle with which modern enterprise organisations drive their digital transformation initiatives to deliver increased value for end-customers faster, with lower operational overheads.

Businesses today are increasingly defined by the digital infrastructure through which they operate and the digital services they can provide to customers.

Cloud adoption provides an opportunity for organisations to progress their digital transformation initiatives, scale rapidly and develop their digital service offerings with reduced time and cost overheads, resulting in more agile and efficient working practices and increased value to customers.

Organisations recognise that they can realise greater value for money by migrating their business workflows to the cloud, resulting in:

- Reduced lead time from months or weeks to hours to deploy digital environments when compared to on-premise provisioning of physical server space
- Reduced time-to-market for digital products and services to improve market competitiveness
- Reduced manual overheads by leveraging automation and digital services, enabling a leaner operating model
- Reduced infrastructure costs through economies of scale and removal of maintenance overheads

Cloud adoption challenges

Despite the clear advantages of cloud adoption, many organisations, or factions within organisations, have resisted cloud adoption at a management level influenced by a variety of factors, such as:

- Lack of understanding on what the cloud is and how it delivers the intended benefits
- Unclear guidance from regulators and policy-makers on how to safely utilise the cloud (for example, when tackling data protection and residency requirements)
- Concerns relating to outsourcing and the lack of direct control over underlying data storage and security
- Fear of change or disruption to the status quo
- Personal risk, such as where the team is negatively impacted by the efficiencies created by cloud adoption

While some of these points present valid concerns which should be carefully managed as part of the cloud adoption decision-making process, concluding that the cloud should be avoided entirely is often futile.

Part of the resistance to cloud adoption is due to misinformation. Overuse of 'cloud' has granted it buzzword-like status, as IT service providers contribute to the 'cloudwashing' of the industry – whereby vendors questionably tout their products and services as the cloud in a me-too fashion to profit from the hype.

Similarly, the cloud is often seen as either good or bad depending on the business context. Frequently, cloud adoption becomes a proxy battleground for wider politicking within an organisation, obfuscating the meaning and masking both the positives and negatives of the cloud.

Myths and misconceptions of the cloud

To tackle the confusion, we have shortlisted some of the most prevalent misconceptions that need clarifying. Some of the key truths that you should know when considering the adoption of cloud technologies and services are covered below.

The cloud is not inherently insecure and organisations moving to the cloud do not have an increased risk of being breached.

While high-profile data breaches have adversely affected confidence in the cloud, the majority of organisations have come to accept that such events can be avoided through effective management on the customer's side. Furthermore, cloud service providers are doing more than ever to support organisations in securing their environments.

Concerns persist amongst some that cloud computing is inherently less secure than traditional approaches. This misconception is due largely to the fact that the approach itself *feels insecure*, with data stored on servers and systems not owned or controlled by the data owner. However, third-party managed infrastructure is nothing new (see IBM, HP, Fujitsu, etc.) and does not have to be less secure than on-premise infrastructure managed by an in-house security team.

In reality, cloud platforms themselves benefit from an unrivalled level of security investment, with cloud providers proving to be highly effective in the quick identification and remediation of vulnerabilities affecting their infrastructure, without incurring operational disruption. This contrasts with many local patch management processes, which can take significant time between the release of a patch and its implementation due to the need to carefully manage the update so as not to threaten system uptime.

For many organisations, outsourcing some elements of infrastructure security management to a third-party provider will not only yield reduced costs, but increase the level of security investment. In fact, avoidance of cloud services may even lead to unnecessary security risks, as organisations continue to rely on ageing in-house systems. As the security posture of cloud deployments hardens over time, these legacy estates will become a more viable target. Placing workloads into the cloud does not mandate a security trade-off – **Gartner have predicted that, through 2020, public cloud IaaS workloads will suffer at least 60% fewer security incidents than those in traditional data centers.**[1]

Gartner predicts that by the end of 2020, 95% of cloud security failures will be the result of customer mismanagement of the cloud deployment. The cloud itself is not less secure, but the way that organisations deploy, configure, administrate the cloud may introduce security risk.

Real-world examples substantiate this claim. For example, in the 2019 Capital One attack the attacker was able to breach the network through a misconfigured web application firewall, as Capital One had failed to configure privileged access authentication tokens on their cloud deployment (a feature which Capital One was responsible for managing).[2]

[1] https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/cloud-strategy-leadership.pdf
[2] https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/

The cloud will not automatically help to save money on operating costs.

As with any transformation project, there is a cost of change associated with migrating to the cloud, and transitioning to the cloud does not immediately result in cost savings.

Migrating workloads to the cloud offers significant reduction in operating costs over the longer term, from removing the overhead associated with managing and maintaining an internal data centre, to enabling storage capacity to be optimised to usage.

However, cloud migration can often incur significant hidden costs. Where services are transferred to the cloud without undertaking required architectural changes, or best practice configuration and management principles are not applied, the organisation can expose itself to a number of hidden costs later – such as rebuilding or refactoring problem applications, suffering service downtime as a result of applications no longer working as intended, or losses due to security or data breach. Performing these tasks requires investment in professional and technical skills development in both cloud and DevOps-related technologies, further impacting the cost of change.

Therefore while a fully functional, well managed, and securely configured cloud asset is likely to deliver significant cost savings over on-premise, considerable investment is required to achieve this state.

Not all assets are likely to be suitable for direct migration to the cloud – for example, those with extensive legacy components associated with them. Instead, organisations may look to redevelop using cloud-native technologies and methodologies in the longer term.

Despite cost savings being reported as the main motivator for cloud adoption (61% of respondents)[3], a recent report suggests that only 42% of organisations successfully manage to optimise cloud spending. 75% of participants noted that their primary concern was managing cloud spend, and average cloud capacity waste was reported at 35%.[4]

Organisations migrating only select workloads to the cloud will fail to realise economies of scale, and those utilising predominantly private cloud will incur greater data storage without the ability to optimise capacity to usage in the same way as with a public cloud model.

Using a cloud service provider does not mean that all responsibility for security is outsourced.

Under a cloud outsourcing model, businesses often (incorrectly) assume that all operational and security management tasks are the cloud provider's responsibility. In reality, the division of responsibilities is more nuanced, and the customer retains all risk ownership and accountability for the compliance of the model.

[3] http://datometry.com/resources/surveys/cloud-data-warehousing-survey/
[4] https://medium.com/@jaychapel/multi-cloud-hybrid-cloud-and-cloud-spend-statistics-on-cloud-computing-ba4c194d2e10

Responsibility will vary based on the type of deployment model and the specific nature of the contractual agreement between the customer and service provider; it is crucial to assess each supplier's terms. Organisations must build an understanding of the **shared responsibility model** between cloud vendor and consumer to ensure that appropriate action is taken to manage areas of responsibility, build oversight of vendor dependencies, and consequently manage the risks associated with the outsourcing process.

At a high level, the provider will typically operate, manage and control components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates, while the customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as firewall configuration. In addition, organisations must consider any additional requirements or responsibilities based on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

The belief that cloud providers are entirely responsible for their customers' security means that enterprises continue to fail to implement appropriate controls and safeguards to prevent data from being inappropriately shared with other employees, external parties and sometimes the entire internet.[5] The parts of the stack under customer control can make cloud computing a highly efficient way for inexperienced users to implement poor practices, leading to security or compliance failures.

The cloud does not represent a regulatory or compliance risk if managed appropriately across the business.

Within enterprise business risk and compliance management functions, concerns persist in some areas around how to maintain compliance with internal governance and external regulation and audit when using the cloud. These typically pertain to data handling and storage, responsibility and accountability, and performing audit and review.

The reality is that the major cloud service providers are required to regularly demonstrate compliance with a range of standards to provide services to highly regulated entities. Part of this process is committed to supporting organisations in evaluating and managing their business risks posed by cloud adoption. In addition, regulatory authorities (such as the European Commission with its Digital Operational Resilience Act (DORA) initiative[6] and the UK FCA's recent consultation on operational resilience[7]) are committed to evolving the understanding and management of risks with technology adoption and facilitate safe third-party provision of critical business services.

For example, Amazon has 3 lists for compliance services that cover certifications/attestations; laws/regulations/privacy; and alignments/frameworks, while Microsoft goes further in providing a granular breakdown of global, government, industry, and regional.

[5] https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/cloud-strategy-leadership.pdf
[6] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1685
[7] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

Cloud service providers have experience of complying with a range of classifications and policies including ISO 27017[8], ISO 27018[9], ISO/IEC 27701[10], NIST 800-53[11] and GDPR,[12] PCI DSS[13], and have welcomed the coming regional implementation of the NIS Directive for European Digital Service Providers[14].

While cloud service providers are able to meet a range of compliance requirements, it is the responsibility of the customer to define the controls and configurations required to achieve compliance. Proper due diligence should be standard for any outsourcing initiative to understand the key risks and embed controls into the contract – e.g. assessing whether the cloud service provider can comply with physical audit requirements, ensuring that an exit strategy is in place, and verifying and validating the security controls implemented by the third-party.

Effective control over the use of cloud computing is not about saying "no"; rather, it is the ability of the business to maintain oversight of cloud usage, and demonstrate understanding and visibility to managers, board members, auditors, regulators and partner organisations alike that cloud computing is being used effectively and appropriately.

Given the ease with which groups within an organisation can (and likely already have begun to) adopt cloud, those who attempt to quash or disrupt adoption are shouting into the wind. Where a long-term change plan can be put in place to ensure business processes are adapted to cloud requirements of the cloud, and the requirements for safe and secure adoption can be defined, usage can be managed, tracked, and governed to control risk.

Cloud adoption is driven primarily by developers, but the rest of the business has a vital role in secure and beneficial cloud usage.

The primary reason that cloud adoption fails to deliver the expected benefit and introduces risk is due to a lack of transparent business strategy and commitment to change for the project. Cloud adoption is central to wider digital transformation and should be a business-wide matter. Even organisations hesitating to adopt cloud more widely should look to create a mechanism to oversee and manage cloud adoption with clear visibility and accountability across the business.

Because cloud strategy usually lags behind cloud use, many organisations have unsanctioned, unknown public cloud usage. Most organisations start with the ad hoc adoption of cloud services, often outside of IT governance – which can expose the business to significant cyber and compliance risk.

---

[8] https://aws.amazon.com/compliance/iso-27017-faqs/ and https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27017

[9] https://azure.microsoft.com/sv-se/blog/

[10] https://azure.microsoft.com/en-gb/blog/azure-is-now-certified-for-the-iso-iec-27701-privacy-standard/

[11] https://aws.amazon.com/compliance/nist/ and https://azure.microsoft.com/en-gb/blog/new-azure-blueprint-simplifies-compliance-with-nist-sp-800-53/

[12] https://aws.amazon.com/compliance/gdpr-center/

[13] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/ and https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-pci-dss

[14] https://www.microsoft.com/security/blog/2016/01/25/whats-next-for-eu-cybersecurity-after-the-nis-agreement/

Especially when sensitive or regulated data is involved, unapproved clouds create unnecessary risk exposure and are the primary cause of security breaches in the cloud to date.

Because of the widespread nature of cloud services and technologies today, organisations looking to avoid cloud use entirely are likely to struggle to enforce this stance. Cloud use will instead be invisible and unknown to business functions such as central IT and security, which must be aware of cloud use to be able to adapt their approach to manage and mitigate cloud risks – as traditional approaches security monitoring and threat detection are not typically effective in the cloud without significant tuning.

With cloud technology intertwined with modern business operations, unsafe use of the cloud will become more common unless a cloud strategy is implemented, and historically siloed business departments become more integrated and collaborative to ensure effective cloud management and oversight. The most significant step an organisation can take to ensure appropriate levels of cloud security is for the corporate leadership to reach a consensus on cloud adoption to enable safe implementation through planning and policy.

Moving to the cloud changes the role of IT within the business but does not eliminate conventional IT operations.

There is a concern in many IT departments that transitioning to the cloud is likely to make the current role that they play within a business redundant.

There is an element of truth to this; as core business services are procured as SaaS applications, the role of traditional IT in managing, developing and administering systems is somewhat diminished. The typical security controls that can be applied – creating or linking accounts, password maintenance, access controls, and activity monitoring – are almost exclusively performed through web-based dashboards and interfaces and are less demanding of technical expertise. The employees managing SaaS processes may be in IT operations, but they are generally not the same people responsible for system internals or network protocols.

That said, the basic deployment and operational framework of IaaS usage is broadly the same as the processes and skills used in traditional IT network management. For example, the foundation for the well-managed use of the cloud is identity governance and administration, requiring the integration of external cloud user management (often across providers) with the internal user directory service (e.g. Active Directory) to ensure that only authorised users have permission to access sensitive data. This is a core requirement of on-premise systems administration and remains so in the cloud.

However, the professionals completing these tasks will need to learn and develop virtualisation and cloud-service-specific knowledge – especially regarding DevOps-style automation of virtual infrastructure, IAM, workload protection, network security, and encryption.

To fill knowledge gaps, organisations will have to consider the upskilling of existing personnel in specific cloud services and technologies (often across cloud service providers) and investment in new teams or capabilities to meet emerging requirements. One solution could see IT teams shifting from a provider of services to a facilitator – taking on the role of a centre for excellence to establish cloud management best practice. This would enable central IT to retain its oversight of cloud usage by centrally supporting dispersed business units and teams – reducing the risk of insecure cloud services being exposed to the internet as part of the development process.

For example, at present, 59% of firms do not maintain an approved service catalogue[15]– reducing business control over what is deployed.

While it is clear that the function of IT management within the business is changing in the context of the cloud, which may require them to adapt and skill-up in certain areas, it is also evident that IT teams still have an important role to play, particularly in the governance and brokerage of third-party services.

Organisations looking to benefit from the cloud don't have to pick any one service provider or solution.

When looking to define their cloud strategy, many businesses state that they are "moving to AWS" or "moving to Azure". Many more insist that they will, for example, only use private cloud offerings for perceived better security and control.

In reality, the choice between cloud vendors, platforms and services does not have to be so binary, and there are many advantages to a multi and hybrid cloud strategy (respectively, using more than one cloud service provider and both public and private cloud offerings).

According to a 2019 report, 91% of businesses used public cloud and 72% used a private one. Most enterprises actually utilize both options – with 69% of them opting for a hybrid cloud solution. Just 22% use the public cloud exclusively, and only 3% use a private one exclusively.[16] Further, 62% of cloud adopters are using more than one cloud platform / provider, and 74% describe their strategy as multi-cloud.[17]

The primary blocker to effectively using a range of cloud services offered by different providers is the lack of internal expertise in the particular technologies used. The major cloud platforms (AWS, GCP, Azure) have little in common, often differing significantly in terms of:

- The mechanics of the platform and the bespoke tooling used to configure and orchestrate services as part of a deployment.
- The terminology used to describe components, services and functions is not rooted in any standard "cloud language" and is custom to the service provider.
- While the functionality provided by the platforms is typically similar, there are differences in what and how certain desired outcomes can be achieved using the building blocks made available by the provider.

Therefore while it can be advantageous for the organisation to build expertise in a single platform (initially, at least), organisations should not lock themselves to a single vendor long-term.

---

[15] https://medium.com/@jaychapel/multi-cloud-hybrid-cloud-and-cloud-spend-statistics-on-cloud-computing-ba4c194d2e10
[16] https://hostingtribunal.com/blog/cloud-adoption-statistics/#gref
[17] https://medium.com/@jaychapel/multi-cloud-hybrid-cloud-and-cloud-spend-statistics-on-cloud-computing-ba4c194d2e10

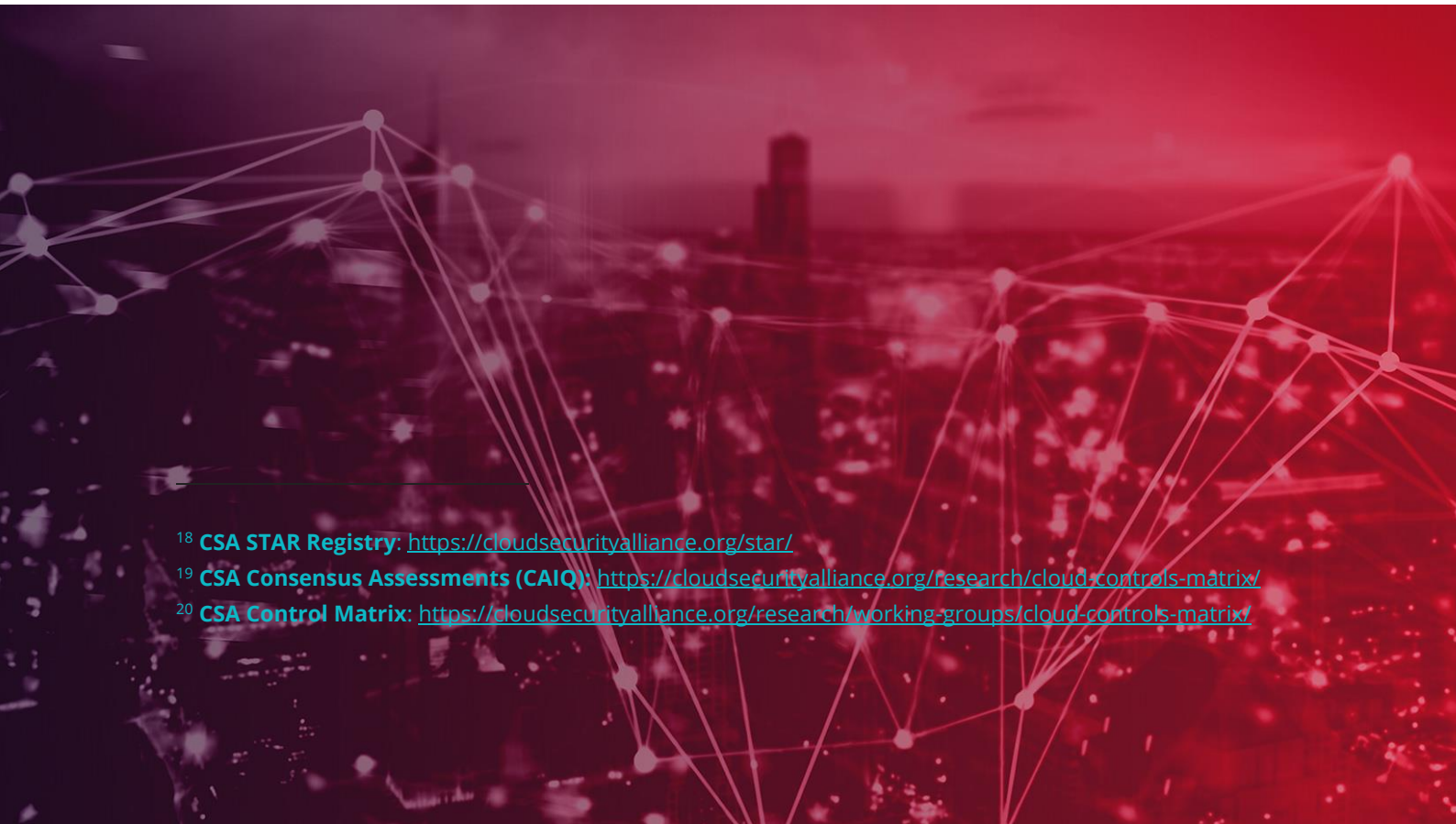
At a minimum, organisations should consider having multiple cloud deployments from a single vendor to ensure data is segregated, and dedicated cloud deployments can support the differing requirements of each business function. **By tailoring deployments, the cloud can meet a range of security, risk and compliance requirements.**

Understanding and communicating their requirements to a third-party service provider is often the biggest challenge facing organisations when looking to move securely and safely to the cloud. While some vendors offer pre-configured deployments to meet specific standards (e.g. PCI DSS), many more do not. In this case, it falls to the customer to define which controls and checks must be implemented to meet compliance requirements. For organisations who are only partially aware of their needs and lack knowledge of the controls offered by the provider, this can be hugely challenging.

Organisations like the Cloud Security Alliance (CSA) are leading the way in making due diligence easier for cloud customers. They provide a registry of the security and privacy controls provided under popular cloud computing offerings[18] using vendor responses to a "Consensus Assessment"[19] – a set of Yes/No questions a cloud consumer or auditor may wish to ask of a cloud provider to ascertain their compliance, informing a control matrix[20] composed of 133 control across 16 areas. This can be used as a tool to identify which security controls can be implemented by the major service providers, and therefore which CSP provides the best services for a particular environment and set of requirements.

Finally, organisations that limit themselves to only using private cloud deployments will not take full advantage of the benefits offered by a public cloud model.

Private cloud deployments will typically lack the scale of computing resources available through public cloud – with this scale comes greater potential for efficiency and optimisation of resources. Therefore, organisations that limit themselves to private cloud only will see reduced returns and lesser performance than organisations that fully embrace the advantages of public cloud.



[18] **CSA STAR Registry**: https://cloudsecurityalliance.org/star/
[19] **CSA Consensus Assessments (CAIQ)**: https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[20] **CSA Control Matrix**: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

Conclusion

Most organisations will leverage cloud technology as part of their digital operations in future. Those who fail to prepare and adapt will invariably expose themselves to unnecessary security and compliance risks. Equally, those organisations which patently refuse to entertain the possibility and opportunity of cloud adoption are likely to severely impair their operations in comparison to their competitors in future.

Organisations that are yet to establish their cloud adoption strategy should do so as a matter of priority – those who think they are currently not 'in the cloud' may be surprised, especially when assessing their adoption of platforms and their third party (and sometimes integrated) suppliers.

While some organisations see the cloud as less secure than their existing arrangement, this often means overlooking the deficiencies with their current operating model. **In reality, this is rarely the case.**

Organisations that continue to resist cloud adoption should ensure they are suitably informed; cloud adoption should not be regarded as an inherent risk, and challenges can be addressed through ensuring clarity of the division of responsibilities between the customer and the cloud service provider, communicating any specific requirements, and establishing contractual safeguards to de-risk the arrangement.

Clearly, the greatest challenge affecting organisation when looking to adopt cloud services is in inward one; prior to cloud adoption, organisations must look to understand their existing security, data protection, and compliance requirements, and how they are managed through the current operating model. With this information, organisations moving business-critical assets or data with strict control requirements to the cloud can engage in an informed dialogue with the service provider(s) to ensure their needs are met and the introduction of unnecessary risks are avoided.

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com