

WHITE PAPER

Overcoming Hybrid Cloud complexity

Developing the right Hybrid Cloud
roadmap for your organisation

WELCOME

Overview

In this article Cyberfort Cloud experts discuss the current challenges faced by IT teams when developing the right Hybrid Cloud strategy for their organisation.

We identify the key considerations when reviewing an existing Hybrid Cloud strategy and what to focus on when developing a Hybrid Cloud strategy fit for the future.

Finally, we highlight several key areas organisations may need specialist Cloud Service Provider support to make sure they have the right Cloud transformation roadmap in place.



Introduction to overcoming Hybrid Cloud complexity

For most organisations developing and delivering a Hybrid Cloud strategy is the right approach. Industry figures show Hybrid Cloud is in the middle of a growth cycle, with organisations estimated to spend over \$262bn by 2027 according to Statista (1). Hitachi Vantara's 2024 Cloud survey discovered 79% of UK organisations believe a Hybrid Cloud strategy is the right approach for their organisation (2). So why is the Hybrid Cloud market growing so fast and why are many organisations identifying it as their preferred cloud strategy?

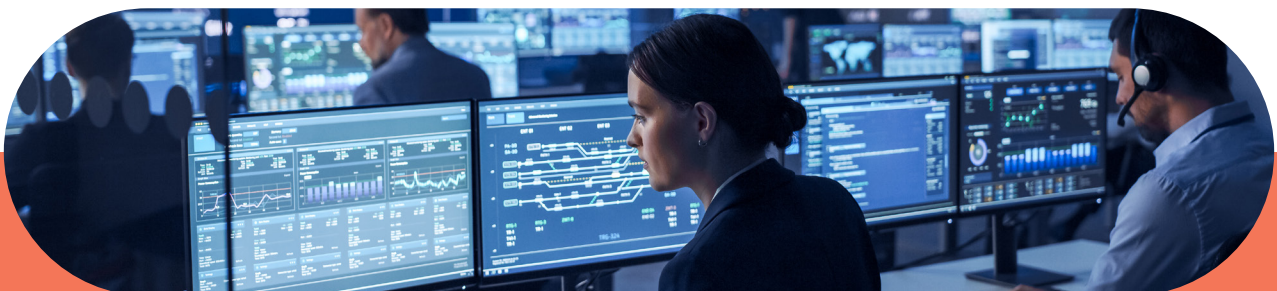
Most organisations will have some workloads, legacy applications and data which requires specific security considerations which needs to be hosted in 'on premises datacentres' or a 'private cloud' and not moved to the public cloud. Many organisations have chosen this approach as they want the best of both worlds. Access to the best features of public cloud (e.g. unlimited storage and compute) whilst keeping control and mitigating risk by using on premise datacentres and private clouds.

Readers of the article will already understand the basics covering Hybrid Cloud; the ability to use both its on-premises data centres and multiple clouds and connecting the environments with shared management, security, and governance policies and simplified data integration.

However, designing and delivering the right Hybrid Cloud strategy for an organisation is no easy task. Many IT teams understand the benefits a Hybrid Cloud strategy can bring:

- **Flexibility** with infrastructure to keep up with fluctuating user demands
- **Agility and scalability** by using a mix of private/public cloud resources
- **Secure access** to data at all times
- **Improved resilience** and operability of a cloud environment
- **A chance** to keep rising public cloud costs under control

But to reach this utopia of a fully functioning Hybrid Cloud which delivers the benefits it promises, it needs the correct strategy, plan, tools and skills in place.



Overcoming the challenges to developing the right Hybrid Cloud strategy for your organisation

At Cyberfort we provide a range of services to customers who are reviewing their Hybrid Cloud strategies. When we talk to customers, we have discovered the most common problems they are facing with their Hybrid Cloud strategies fall into the following categories.

Data management and migration of data



Lack of visibility and control



Security



Putting in place the right provisioning model



Networking



Compliance and Governance



Infrastructure compatibility



Defining the right SLA's with Cloud Service Providers



In the next part of this article, we identify the key challenges organisations are facing in relation to their Hybrid Cloud strategy. Additionally, practical advice for resolving these potential issues is summarised.

Data management and migration of data



Data management and the migration of data from on premises infrastructure to the cloud can be a time consuming and difficult process. Many organisations to try and keep up with storage and compute demands have simply 'lifted and shifted' data, applications and workloads to the cloud. On the surface some data, applications and workloads look ideal to be moved to cloud environments. However, caution should be exercised.

If data, applications and workloads are not correctly migrated and then managed it can lead to issues including:



Sensitive data being moved to cloud environments which may not have the right security measures in place.



Data compliance breaches in regulated industries. Leaving the organisation open to customer and employee complaints and potentially large fines.



Operational and performance issues of applications leading to a poor end user experience.



Overspending on cloud storage and compute as the more data which is stored in the cloud the more it could be potentially costing your organisation. If capacity is available in datacentres this should be evaluated and used first rather than outsourcing to the cloud.



Potential risks with different users having access to and changing data on cloud platforms.

To overcome the data management and migration challenges those who are responsible for cloud in their organisation should:



Identify the different types of data in their organisation, classify by the nature of the data and then decide on what data can safely be migrated to the cloud and managed.



Review the organisations data storage requirements and make a plan for capacity in the cloud.



Understand the provisioning requirements for different volumes of data in the cloud including reviewing the network, storage and applications required and associated costs.

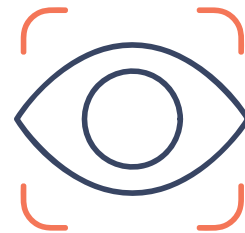


Meet with their Cloud Service Provider to understand how and where their data will be migrated, stored and managed.




Review data management, processing and storage requirements against industry relevant compliance rules and regulations and assess if the cloud data being moved adheres to these rules.

Lack of visibility and control






Hybrid Cloud by its nature if not managed correctly can quickly become difficult to manage due to the range of different platforms, systems and processes involved in the strategy. Many organisations are struggling to view and control all the components of their Hybrid Cloud operating environments due to the range of platforms, systems and processes involved, staff shortages, and current employees not being sufficiently trained and no single reporting platform which can highlight potential issues.

A Hybrid Cloud environment which does not have the right visibility and control platforms in place can result in:

-  Inability to identify issues, which leads to bigger governance and compliance problems in the future.
-  Cloud costs starting to be out of control as usage and spend visibility is not readily available to IT and Finance teams.
-  Constantly being in a reactive mode to cyber security challenges as proactive monitoring and controls around end users is not in place leaving the organisation open to attack.
-  Extra pressure being placed on IT staff for basic cloud access requests and making sure other users outside of the cloud team are using cloud platforms correctly.
-  Data and reporting not being readily available for collaboration across the business. Leaving the business in a non-agile state as it is heavily reliant on manual intervention to create reports.

At Cyberfort we recommended undertaking the following actions to improve visibility and control of cloud operating environments:






-  Review existing visibility and control tools across all cloud platforms and identify where gaps are.
-  Put in place a cloud management system which is automated to take pressure off IT staff.
-  Identify where system management can be simplified and integrated for better visibility.
-  Use DevOps skills for creating centralised management reporting through improved visibility.
-  Review how end users are using the cloud for their work and make sure the right visibility and controls are in place to manage usage effectively.
-  Review existing cloud costs vs business objectives and put in place controls to stop cloud wastage.

Security









Security must be a major consideration when deploying and managing a hybrid cloud environment. Data storage, management and transit, application usage, redundancy in terms of disaster recovery and backup and compatibility between different clouds are all issues which need to be considered and addressed.

The main challenges with security in a hybrid cloud environment include:

-  Creating and maintaining the right encryption and security models with data being used in different cloud environments.
-  Employee access to data and applications which are running in the cloud. Are they storing and managing data correctly?
-  Data in transit between different clouds not securely being transferred. Leading to interception and alteration risks.
-  Resilience of different clouds when come under attack.
-  Identification of data which is considered vulnerable. Failure to identify and properly manage can lead to risk/compliance issues.

To overcome these security challenges with hybrid cloud it is recommended:

-  A full data classification exercise should be undertaken to review where security risks could occur, and mitigation plans put in place.
-  Review the security specifications of cloud service providers and identify where security gaps may be then invest in the right security products to rectify.
-  Understand the data in transit models between clouds, identify vulnerabilities and ensure the right security measures are put in place.
-  Put in place and regularly test a disaster recovery and backup plan to minimise potential loss.
-  Ensure those who are using the cloud for data storage and management have the right levels of training and are aware of the risks.
-  Review industry compliance rules and regulations to ensure data management policies are in place in relation to data being stored in the cloud.

Putting in place the right provisioning model



Cloud provisioning is at the heart of any hybrid cloud strategy. IT teams need to make sure their hybrid cloud operating environments can dynamically scale to cope with different usage patterns and ensure the right self-provisioning is available on a case-by-case basis.

If the right provisioning model is not in place this can lead to:



Inability to scale could environments to cope with increased workloads.



Cost management issues as individuals may be using extra resources which the IT and Finance teams are not aware of.



Applications not being able to scale with usage demand.



A lack of orchestration across clouds for efficient cloud usage.

To overcome provisioning issues with a hybrid cloud strategy IT teams should:



Review which areas of the cloud are being used the most and identify where extra storage and compute power may be needed.



Put in place self service tools for IT teams to react and respond to changing cloud demands.



Review where automation of cloud provisioning could take place across the hybrid cloud architecture.



Develop and use an orchestration tool for improved cost transparency and identify where cloud wastage is happening.



Make sure enough cloud is being provisioned so the organisation can start to take advantage of new technologies such as AI, IoT, and Edge computing.

Networking



Without the right network design hybrid cloud environments can suffer from underperformance. Cloud leaders need to review their network topology on a regular basis to ensure there is little/no separation between virtual and physical components. The network also needs to be reviewed to ensure security and latency between internal and external resources is being managed correctly.

Without the right network design in place hybrid cloud environments can suffer from:



Latency issues between internal and external infrastructure leading to a poor user and customer experience.



Applications not being able to scale usage as end users put more pressure on them.



Security gaps which attackers could exploit.



Branch networks not being in the right place to respond to changing cloud requirements on a seasonal basis.



Inability for the organisation to truly exploit the value of new technologies like AI, IoT, Edge and Quantum Computing.



Network design not being fit for purpose for the wider organisations cloud computing requirements.

To overcome networking issues related to the cloud it is recommended:



IT teams review their network topology and identify where security, performance and integration issues in their cloud operating environments are happening.



Put in place a network management tool which can give visibility and control of the network across public and private clouds.



Collaborate across the business to identify which applications need extra support from the network to remain effective and easy to access for end users.



Review the locations of branch networks and asses if they are causing latency issues due to location.



Understand where network improvements need to be made so new technologies like AI, IoT, and Edge computing can utilise cloud computing effectively.

Compliance and Governance



Maintaining compliance with a variety of ever-changing regulations in a multi cloud environment is difficult. For example, if you are a financial services firm how do you make sure your multi-cloud approach is compliant with PCI DSS? How is your organisation dealing with GDPR? Does it have the right governance and controls in place to make sure compliance is being adhered to?

To maintain compliance with regulations, review if your organisation has:



A dedicated cloud professional who is reviewing the different compliance and governance requirements and assessing if the different Cloud models are adhering to regulations.



The ability to provide standardisation across different cloud platforms for Compliance and Governance purposes.



A Cloud team actively reviewing where cloud could actually speed up compliance procedures.



An end-to-end review process of on premises and cloud infrastructure to assess where IT infrastructure needs to be in place to support the organisations Compliance and Governance requirements?

To make sure your Hybrid Cloud approach is ready for increasingly complex Compliance and Governance requirements Cyberfort suggests:



The IT team reviews the current cloud model both at an individual component level and as a unified system to check all systems are working together in a compliant manner and identify potential issues which could be occurring and put in place a roadmap to remediate.



Review specific regulations related to your organisations industry and make sure it is part of any workload or storage planning.



Put in place a Cloud governance framework which includes staff training on a regular basis to make sure all staff who are using cloud platforms fully understand the compliance requirements and controls which are in place.



Review your SLA's with your Cloud Service Provider to identify if the services they are providing are compliant with rules and regulations in your industry.





Implement a Cloud Management Platform which gives senior leaders visibility and the ability to monitor and manage data usage, security and policies across the hybrid cloud environment.

Infrastructure compatibility








By its nature a hybrid cloud strategy will use a variety of infrastructure technologies to be effective. Multiple infrastructures and technology stacks can cause the IT team an integration headache if not correctly designed, reviewed and managed on a regular basis.

The challenges many organisations need to be aware of with their infrastructure compatibility for hybrid cloud include:

-  Different cloud components not able to be managed easily via a set of common tools and practices.
-  IT teams needing knowledge on different technologies for the hybrid cloud to operational.
-  Tools and processes from Cloud Service Providers not able to be easily integrated into an organisations existing technology environment.
-  Security risks coming to the fore as gaps in infrastructure are available for attackers to exploit.
-  Users and IT teams wasting time having to log in, manage and maintain a variety of systems and processes related to the cloud. Leading to a poor cloud experience.
-  IT architecture not able to respond to changing user demands across different workloads.

When designing a hybrid cloud strategy IT teams need to take the following action to make sure their infrastructure is compatible and can easily be managed and maintained:

-  Review all the different components of the hybrid cloud infrastructure and identify where compatibility issues could be happening today and in the future. Then develop a roadmap to fix.
-  Develop a deep understanding of different Cloud Service Providers tools and processes. Make sure you understand the risks and potential knowledge gaps and then train relevant staff to resolve.
-  Create an 'ideal cloud experience' as part of the hybrid cloud strategy and then review where incompatibility issues may be affecting the user experience.
-  Review how AI, IoT, and Edge computing will have the biggest impact on the existing hybrid cloud infrastructure and plan for coping with the increased workloads these technologies will place on the infrastructure.
-  Invest in management and visibility tools to identify in real time where compatibility issues are occurring and make sure budget is available to fix.

Defining the right SLA's with Cloud Service Providers



As an organisation reviews its Hybrid Cloud operating model it must review existing SLA's with Cloud Service Providers. It goes without saying – not all Cloud Service Providers are the same especially in the Public Cloud. Quite often contracts are signed without the correct amount of time to review all the terms and conditions.

As an organisations Hybrid Cloud model matures this can lead to:



Issues with the Cloud Service Provider contract in terms of system uptime and availability.



Public Cloud environments not reflecting performance and security requirements as reliance on Cloud grows.



Potential security risks as Cloud service providers may not support particular cyber security technologies.



Non compliance with different country and industry regulations in terms of how data is being stored, managed and processed in different cloud environments.



Management and maintenance issues with Clouds outside your organisations control. For example, a Public Cloud Provider may not fix an issue for 48hrs, compared to your own in – house response teams which may be used to 24hr fixes.

To overcome these challenges Cyberfort recommends when signing a contract with a Cloud Service Provider the IT team:



Carefully consider the system uptime and availability of their Cloud services provider and ensure its meets expectations both today and in the future when more workloads, data and applications are moved to Cloud operating environments.



Identify in the contract the security measures and locations of your Cloud Providers datacentres.



Understand where your data from your cloud service provider will be stored, managed and kept safe in transit.



Review the maintenance and management SLA's so if something does wrong how long will you have to wait for the issue to be fixed.



Assess what the extra costs will be as more data, applications and workloads are being moved to the Cloud. How will economies of scale in the contract benefit your organisation as the Cloud is used more by users in your organisation for example.

Helping your business create, manage and deliver Secure Cloud services

Cyberfort Cloud

- Secure multi-tenant cloud
- Infinitely scalable
- Software-defined networking model
- Integrated backup included
- No ingress/egress charges
- Feature-rich optional native capabilities available

Private Cloud

- High performance dedicated platforms
- Compliant to regulatory & security requirements
- Proven technology stacks
- Secure UK Data sovereignty
- Tailored solutions
- Fully managed
- Certified engineers

Public Cloud

- Azure Managed Cloud
- AWS Managed Cloud
- Performance and cost optimised design & management
- Total cost of ownership calculations
- Build validation services
- Multiple billing options
- Flexible support levels from certified engineers

Hybrid Cloud


- Enterprise cloud
- Managed data protection
- Business continuity
- Managed connectivity
- Solution design
- Integrated platform with native Public cloud tooling and services



Cost certainty



Secure and compliant



Tailored cloud



High performance



Managed support



Skills on-demand

Cyberfort Secure Cloud Customers



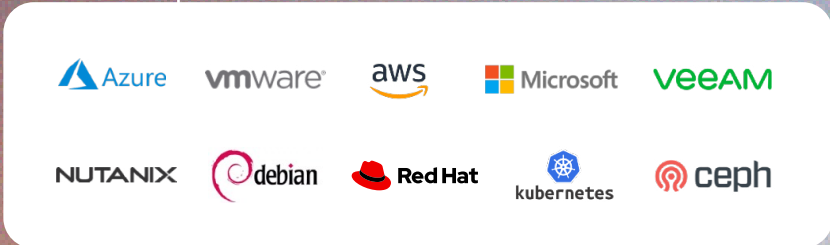
Helping your business create, manage and deliver Secure Cloud services

Market-leading Technology Partnerships

Infrastructure, networking and connectivity



Platforms, data management and storage



Security and management



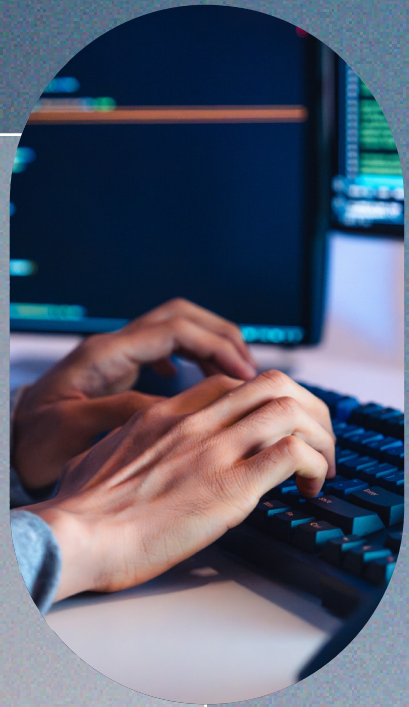
CONCLUSION

Final thoughts

In this article we have identified 8 key areas for review and consideration as part of a hybrid cloud strategy. By taking the time to review your organisations hybrid cloud strategy and assessing its feasibility against the considerations outlined in this article IT teams can really start to take advantage of their cloud investments and be ready for increasing demands on their cloud operating environments.

1 <https://www.statista.com/statistics/1232355/hybrid-cloud-market-size/>

2 <https://technologymagazine.com/articles/how-a-hybrid-cloud-approach-offers-the-best-of-both-worlds>



Discover more about Cyberfort Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.



For more information on our Secure Cloud and Cyber Security services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | <https://cyberfortgroup.com>

We look forward to working with you