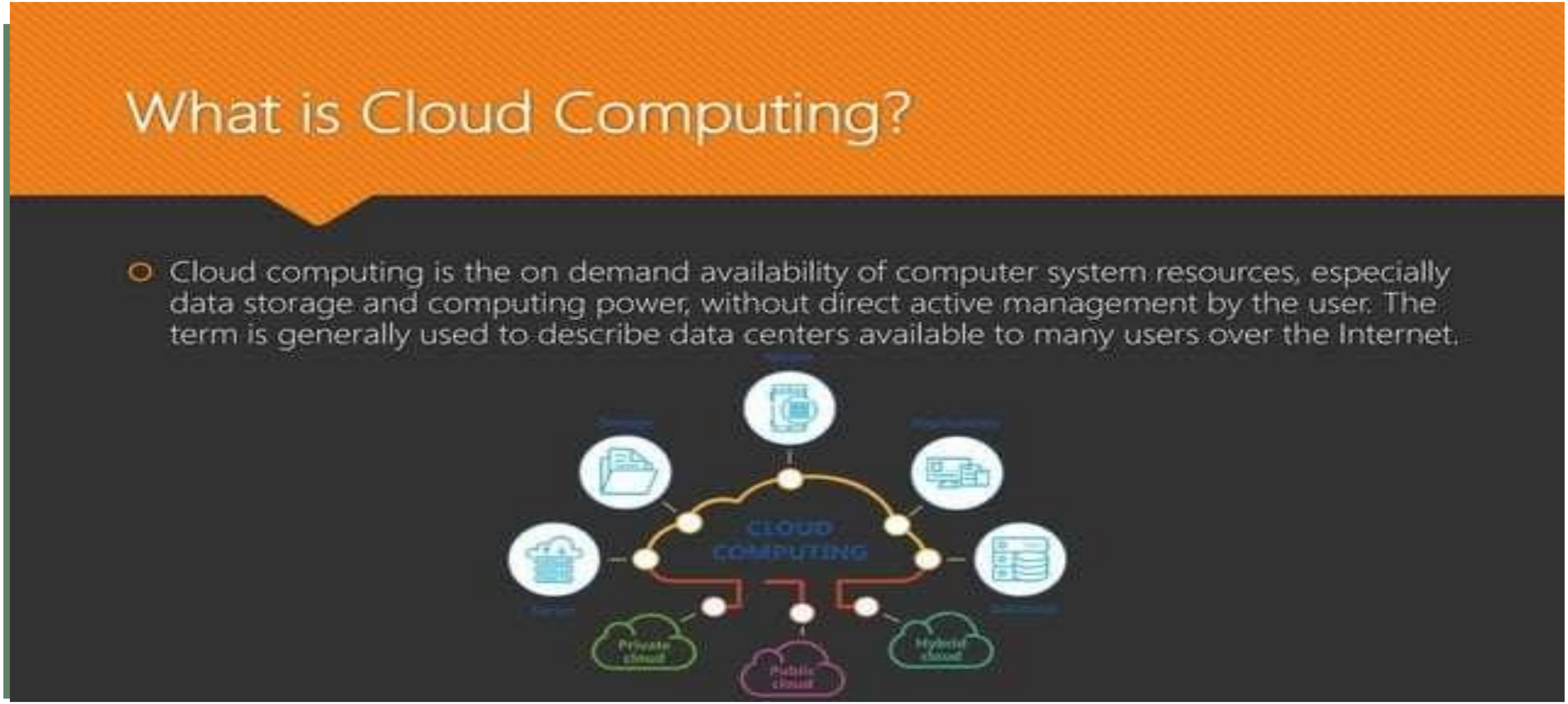
SNS College of Technology

Department of Information Technology

COMPUTER NETWORKS

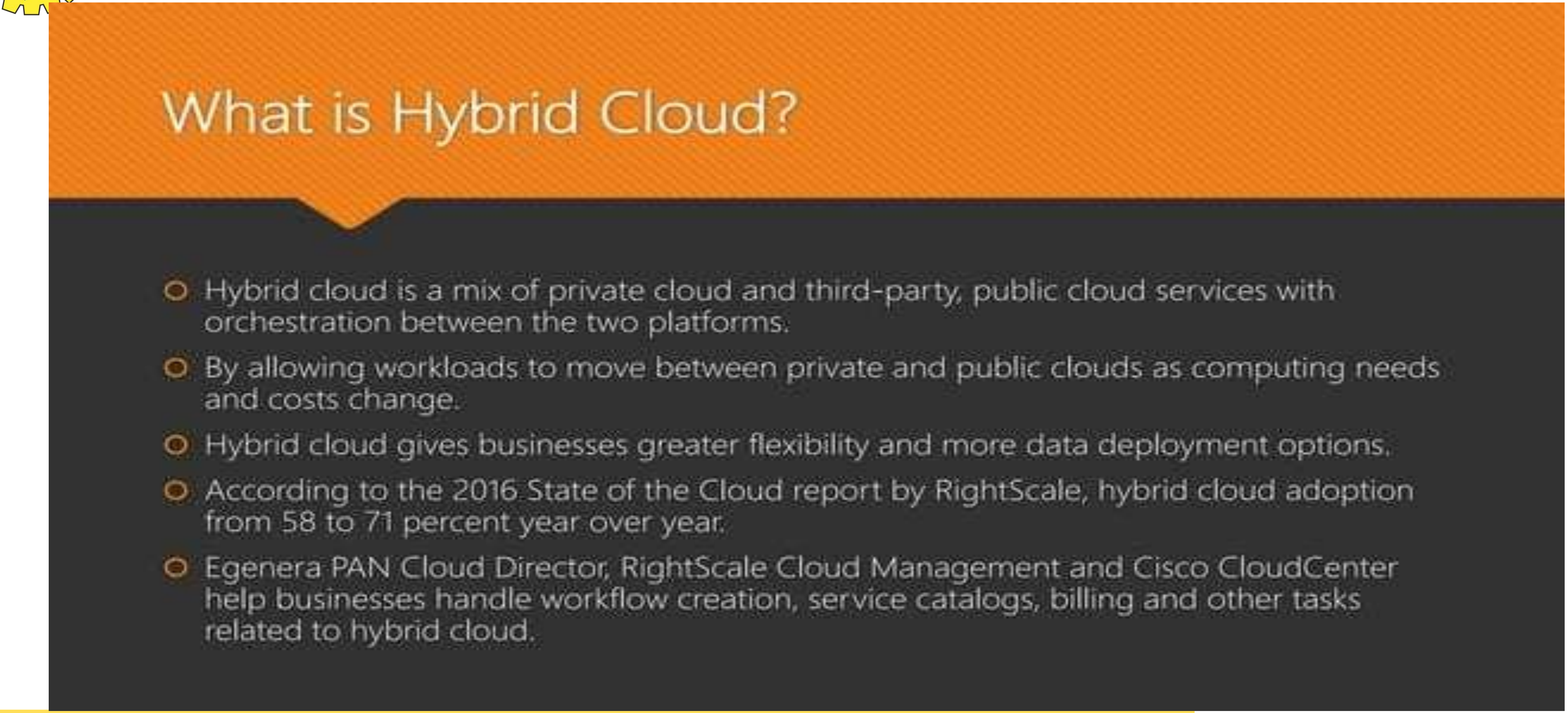
Case study - Hybrid cloud Networking

K.S Mohan
AP/IT
SNSCT



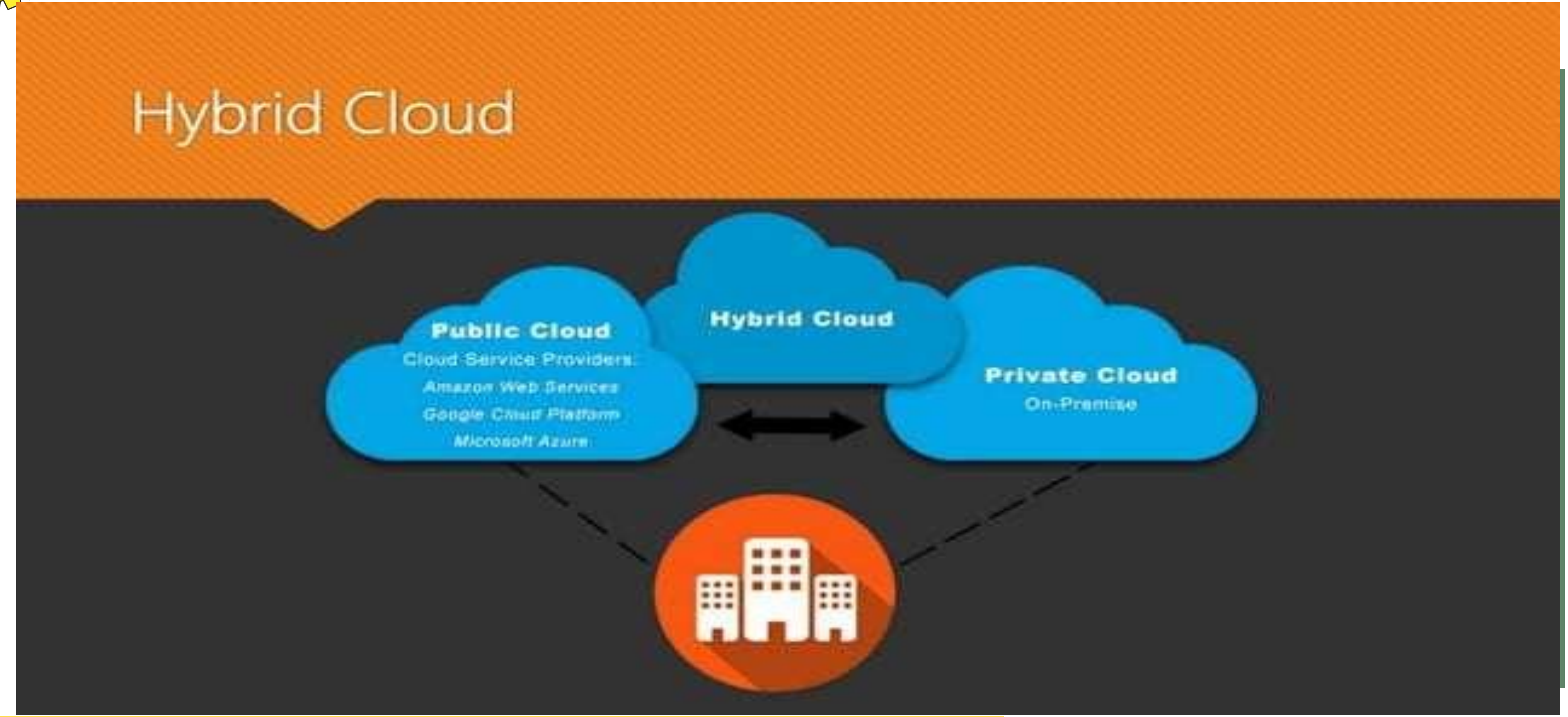
What is Cloud Computing?

- Cloud computing is the on demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet.



What is Hybrid Cloud?

- Hybrid cloud is a mix of private cloud and third-party, public cloud services with orchestration between the two platforms.
- By allowing workloads to move between private and public clouds as computing needs and costs change.
- Hybrid cloud gives businesses greater flexibility and more data deployment options.
- According to the 2016 State of the Cloud report by RightScale, hybrid cloud adoption from 58 to 71 percent year over year.
- Egenera PAN Cloud Director, RightScale Cloud Management and Cisco CloudCenter help businesses handle workflow creation, service catalogs, billing and other tasks related to hybrid cloud.



Hybrid Cloud

Public Cloud

Cloud Service Providers:

Amazon Web Services

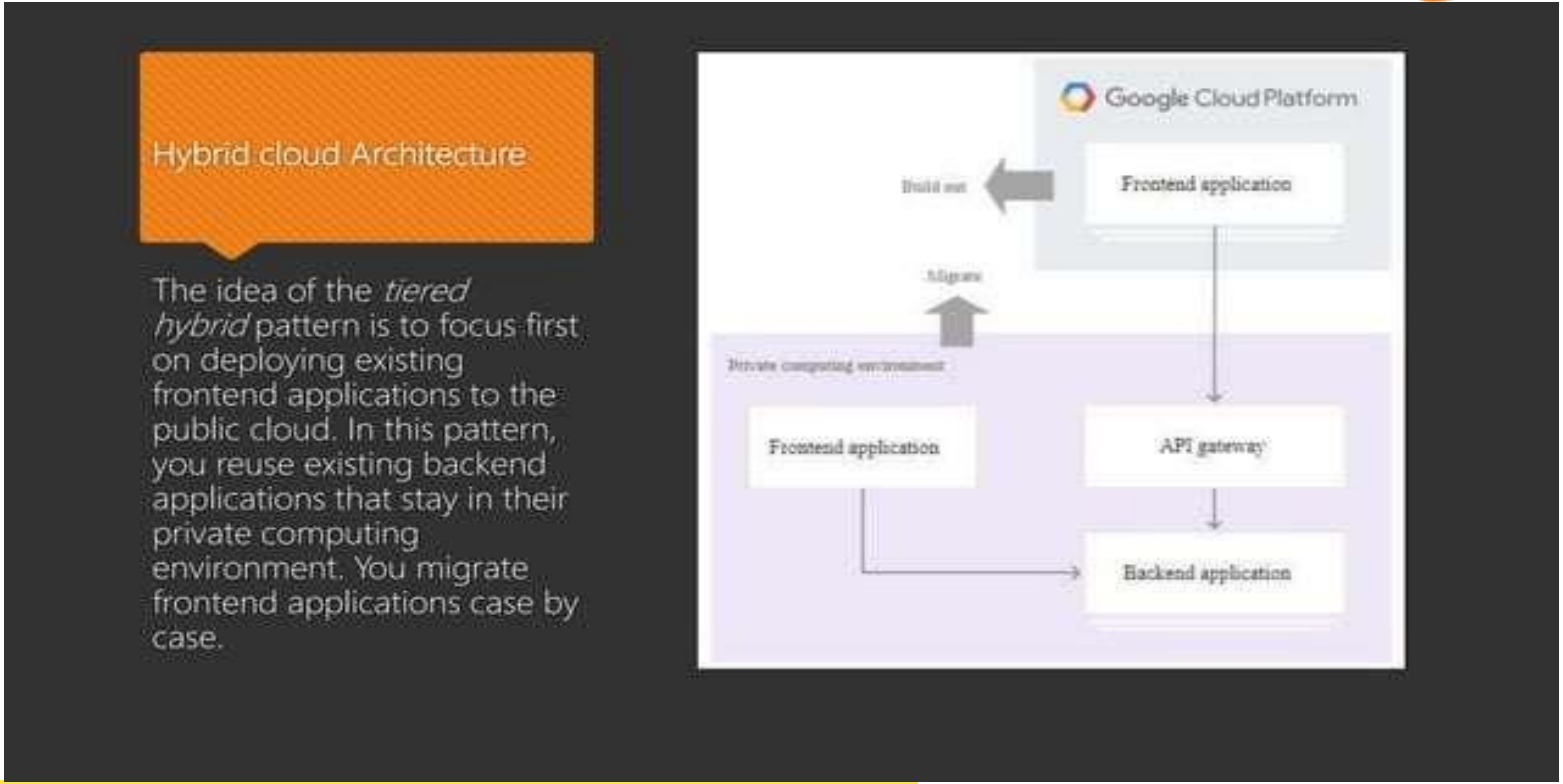
Google Cloud Platform

Microsoft Azure

Hybrid Cloud

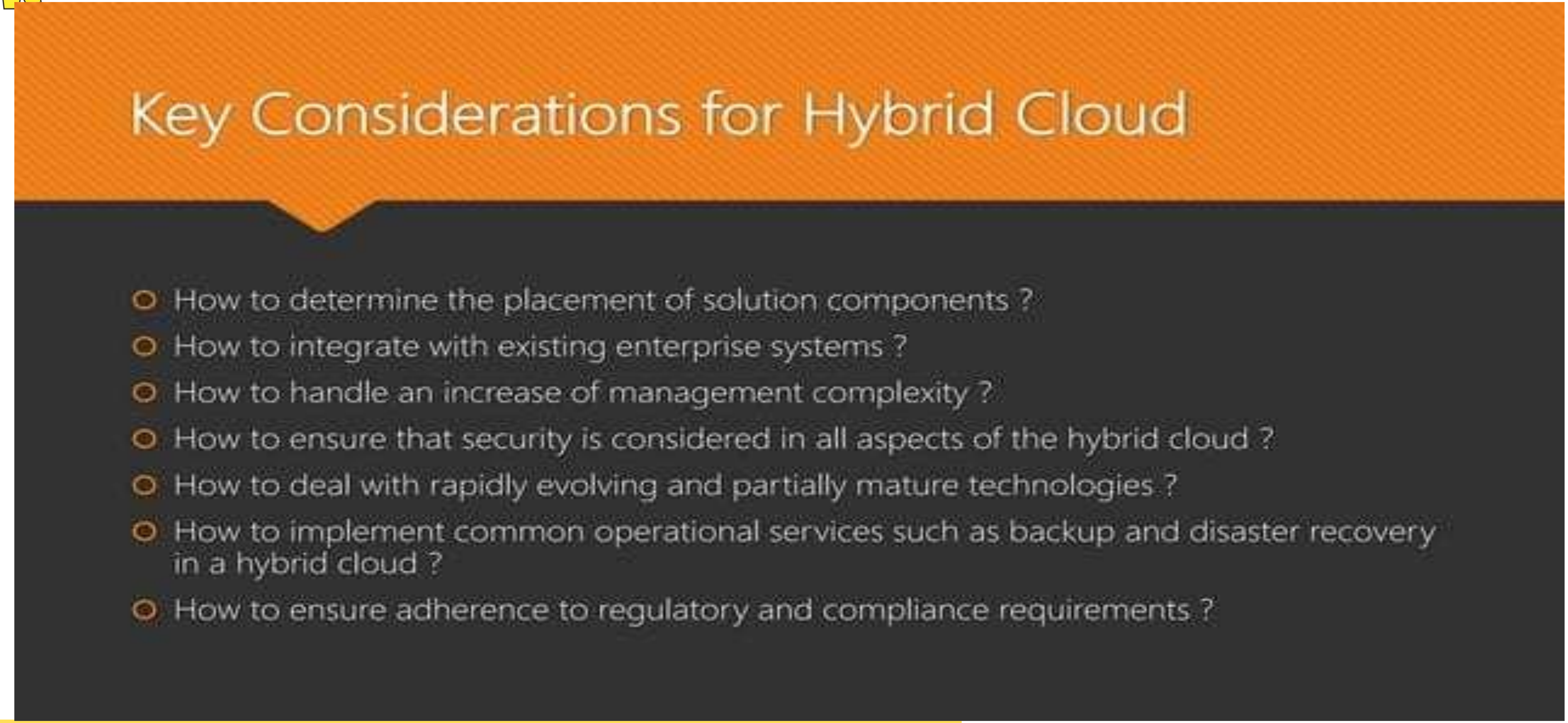
Private Cloud

On-Premise



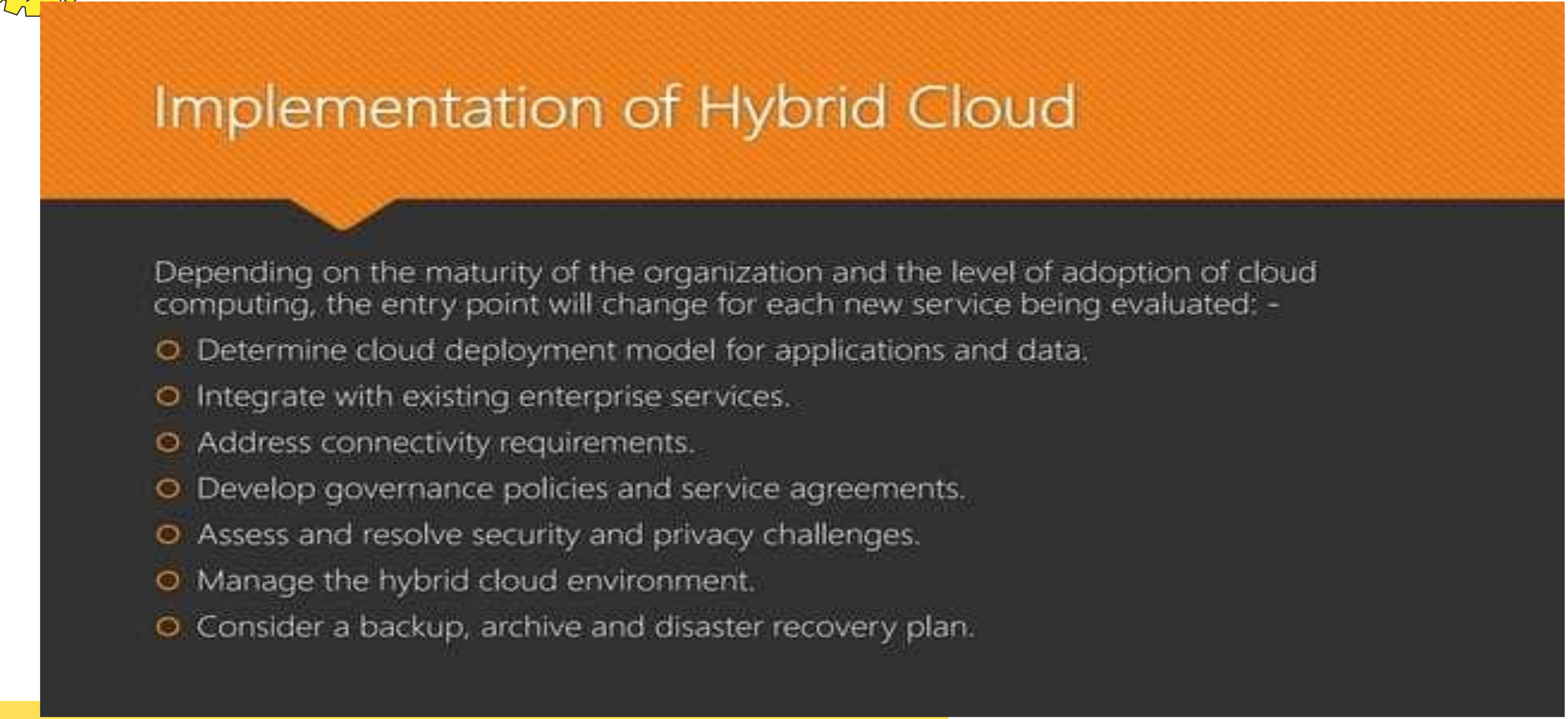
Hybrid cloud Architecture

The idea of the *tiered hybrid* pattern is to focus first on deploying existing frontend applications to the public cloud. In this pattern, you reuse existing backend applications that stay in their private computing environment. You migrate frontend applications case by case.



Key Considerations for Hybrid Cloud

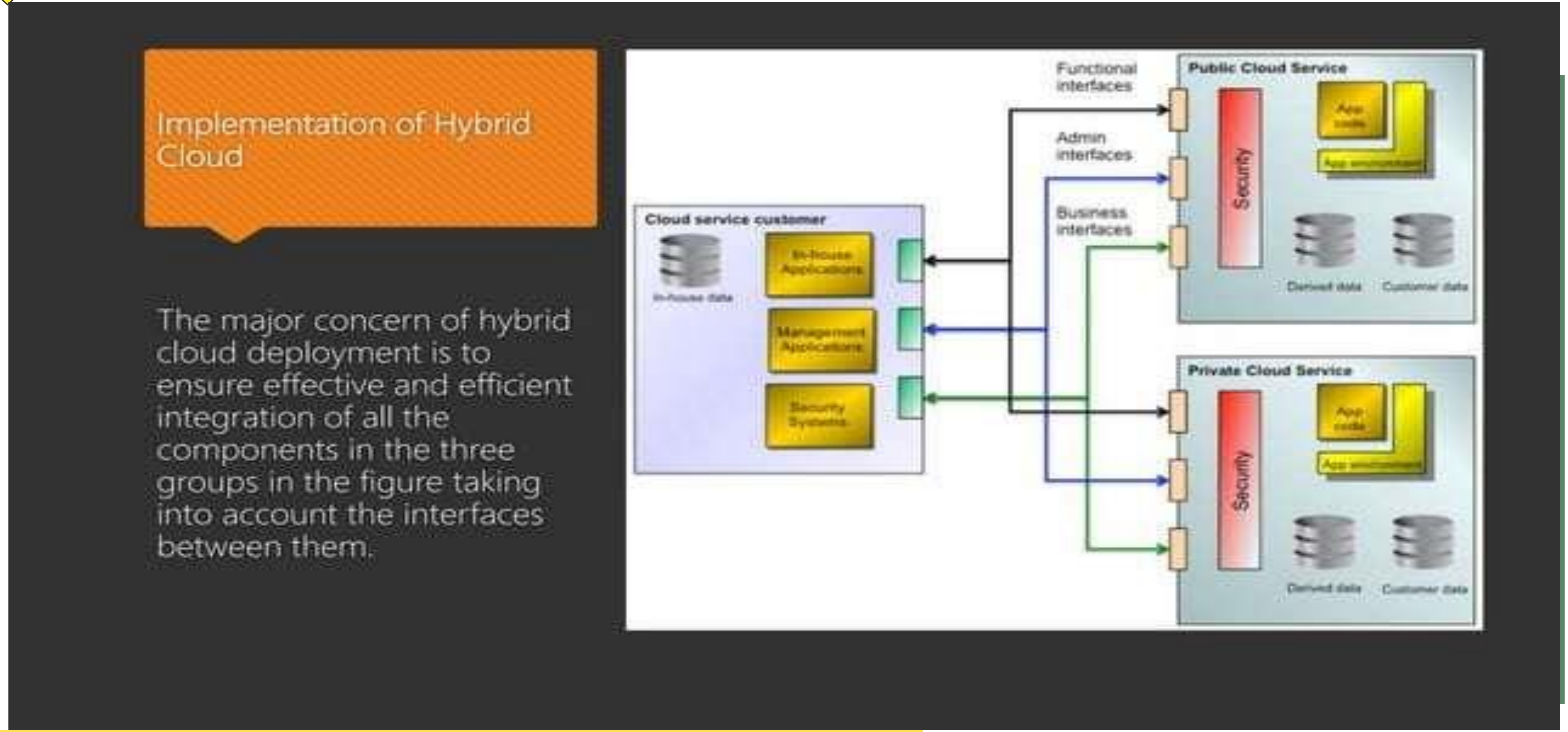
- How to determine the placement of solution components ?
- How to integrate with existing enterprise systems ?
- How to handle an increase of management complexity ?
- How to ensure that security is considered in all aspects of the hybrid cloud ?
- How to deal with rapidly evolving and partially mature technologies ?
- How to implement common operational services such as backup and disaster recovery in a hybrid cloud ?
- How to ensure adherence to regulatory and compliance requirements ?



Implementation of Hybrid Cloud

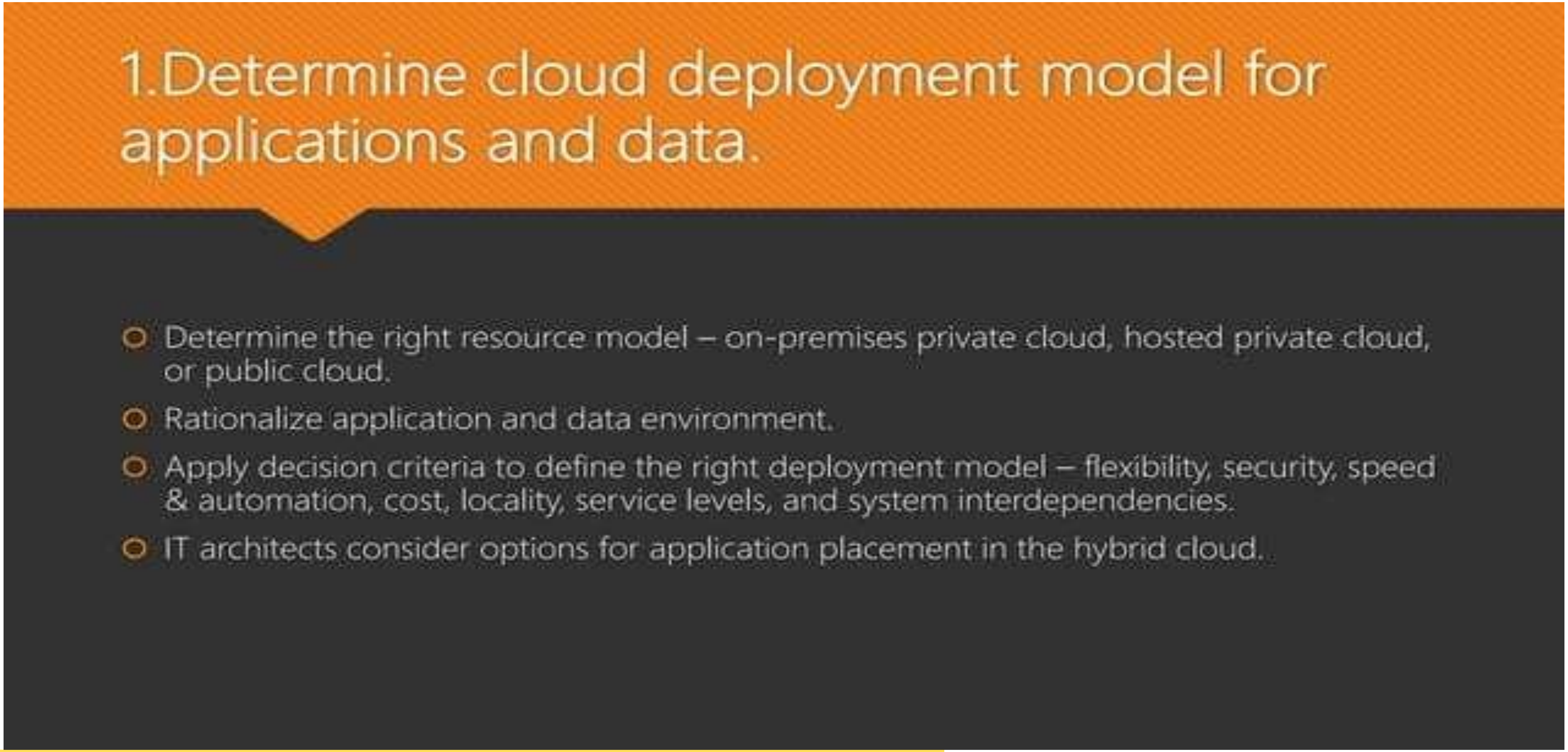
Depending on the maturity of the organization and the level of adoption of cloud computing, the entry point will change for each new service being evaluated: -

- Determine cloud deployment model for applications and data.
- Integrate with existing enterprise services.
- Address connectivity requirements.
- Develop governance policies and service agreements.
- Assess and resolve security and privacy challenges.
- Manage the hybrid cloud environment.
- Consider a backup, archive and disaster recovery plan.



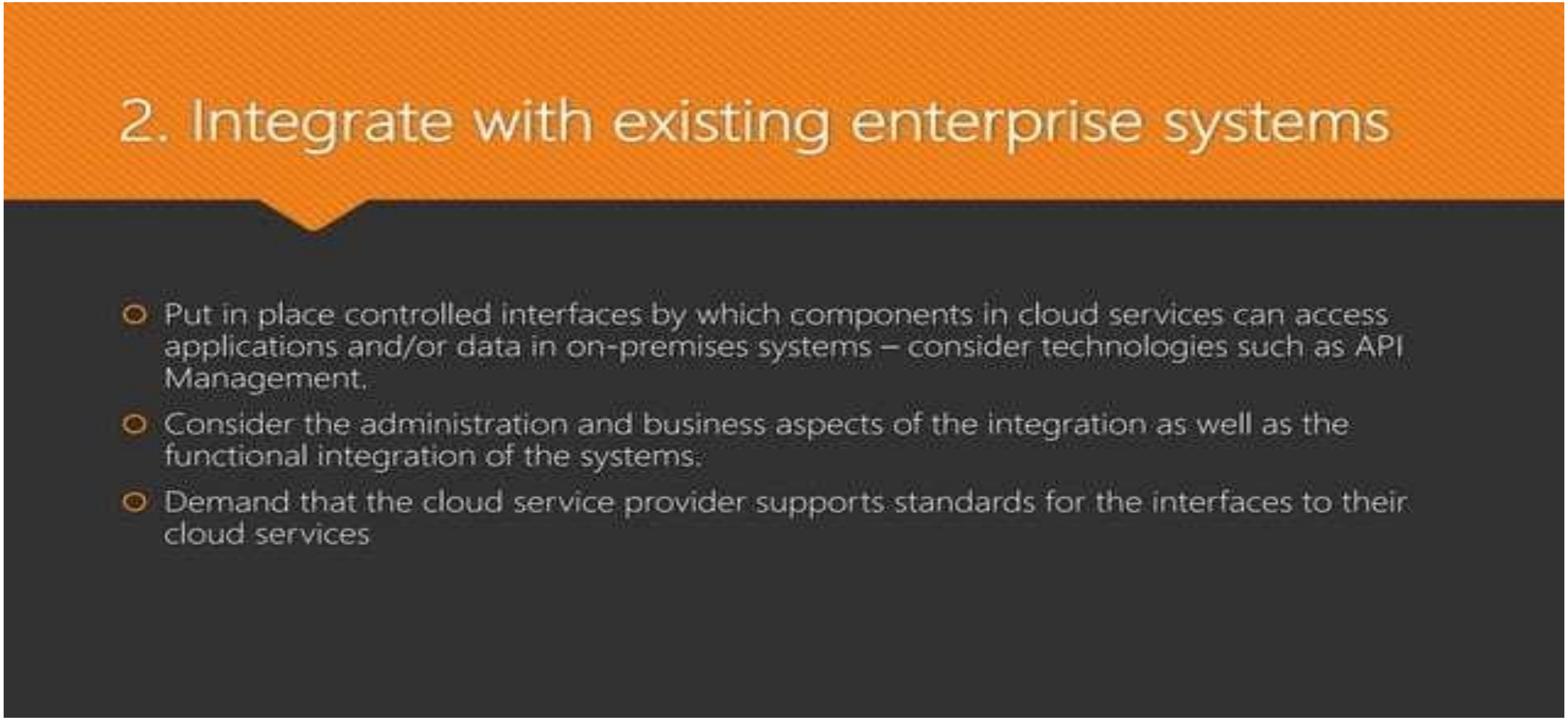
Implementation of Hybrid Cloud

The major concern of hybrid cloud deployment is to ensure effective and efficient integration of all the components in the three groups in the figure taking into account the interfaces between them.



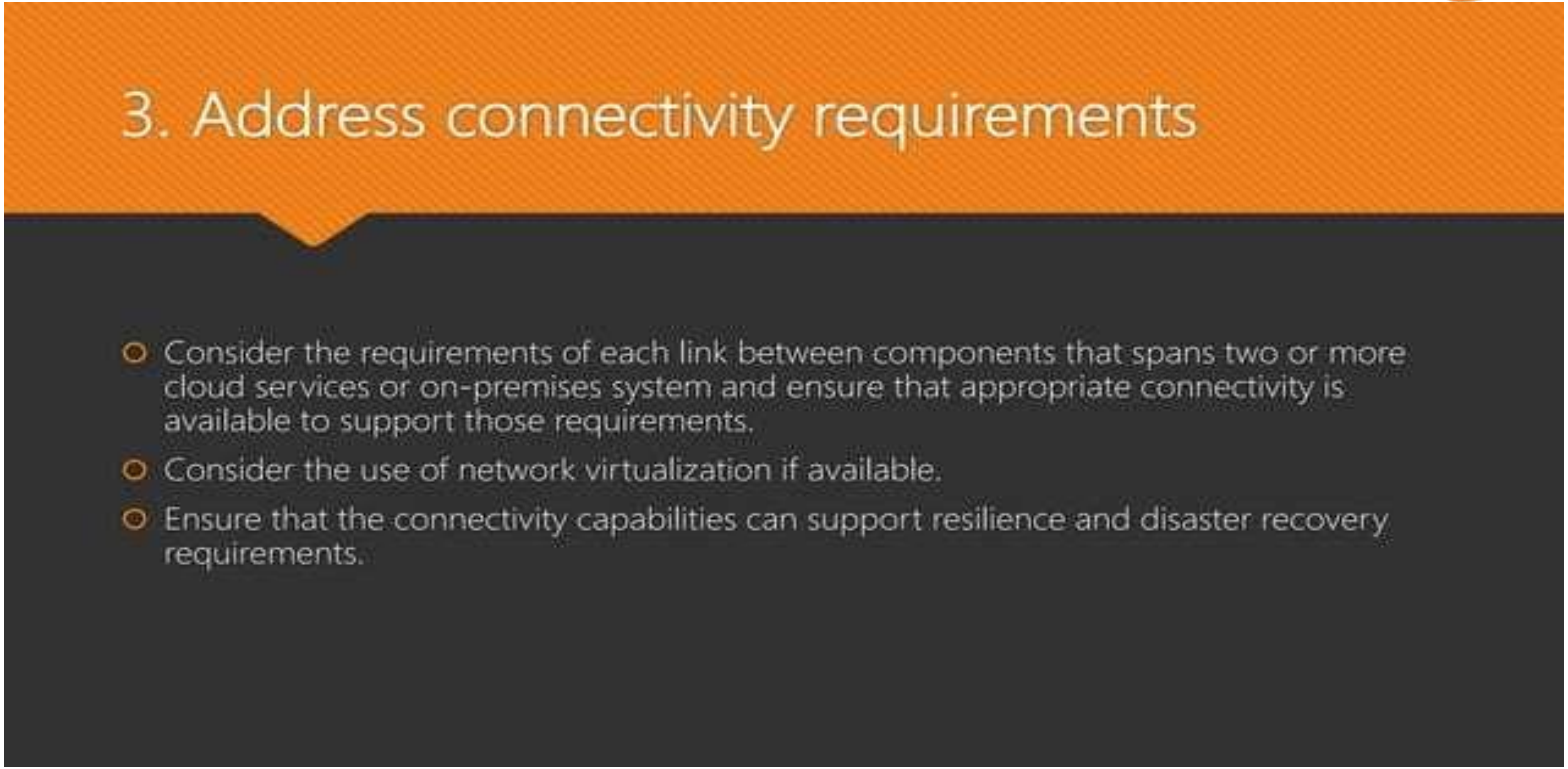
1.Determine cloud deployment model for applications and data.

- Determine the right resource model – on-premises private cloud, hosted private cloud, or public cloud.
- Rationalize application and data environment.
- Apply decision criteria to define the right deployment model – flexibility, security, speed & automation, cost, locality, service levels, and system interdependencies.
- IT architects consider options for application placement in the hybrid cloud.



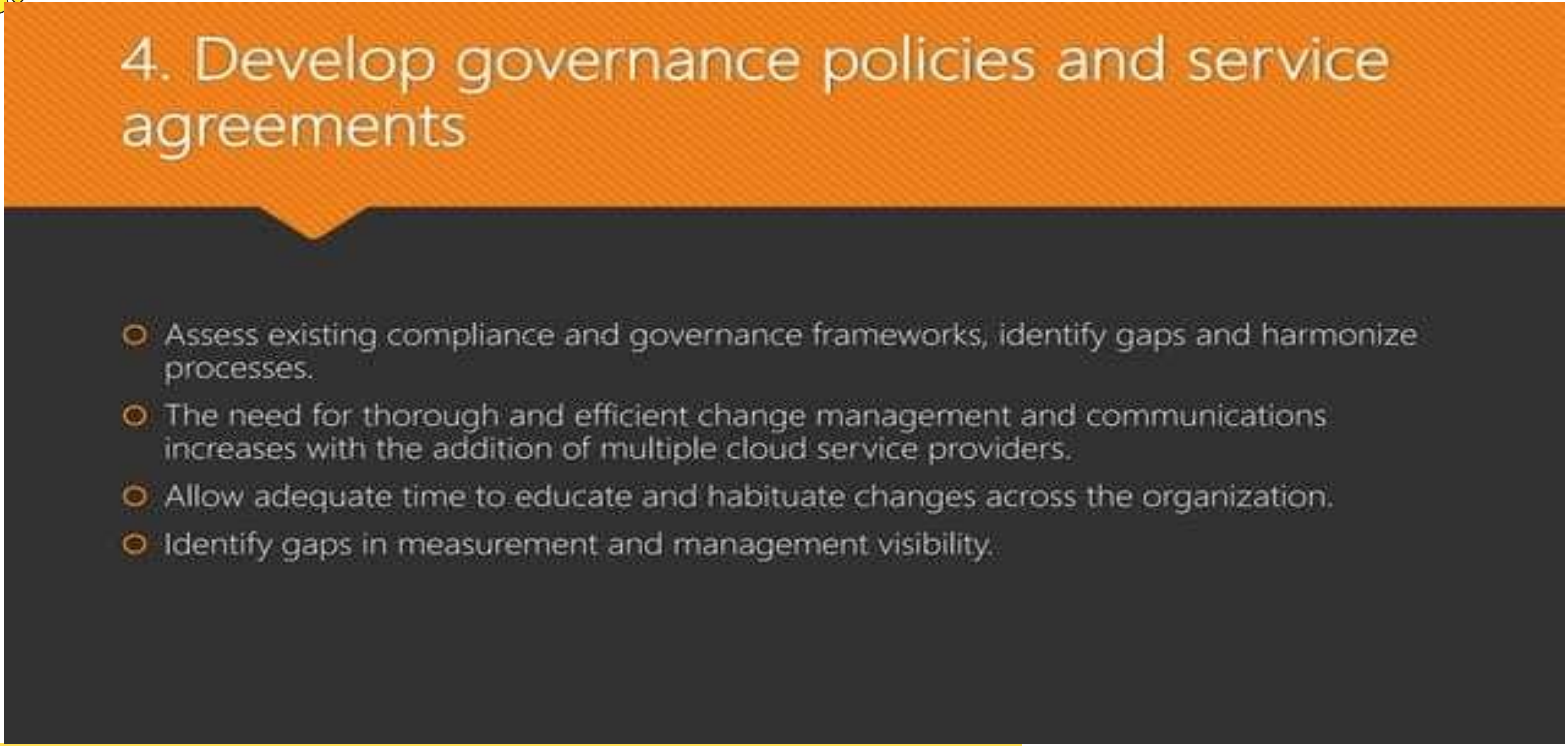
2. Integrate with existing enterprise systems

- Put in place controlled interfaces by which components in cloud services can access applications and/or data in on-premises systems – consider technologies such as API Management.
- Consider the administration and business aspects of the integration as well as the functional integration of the systems.
- Demand that the cloud service provider supports standards for the interfaces to their cloud services



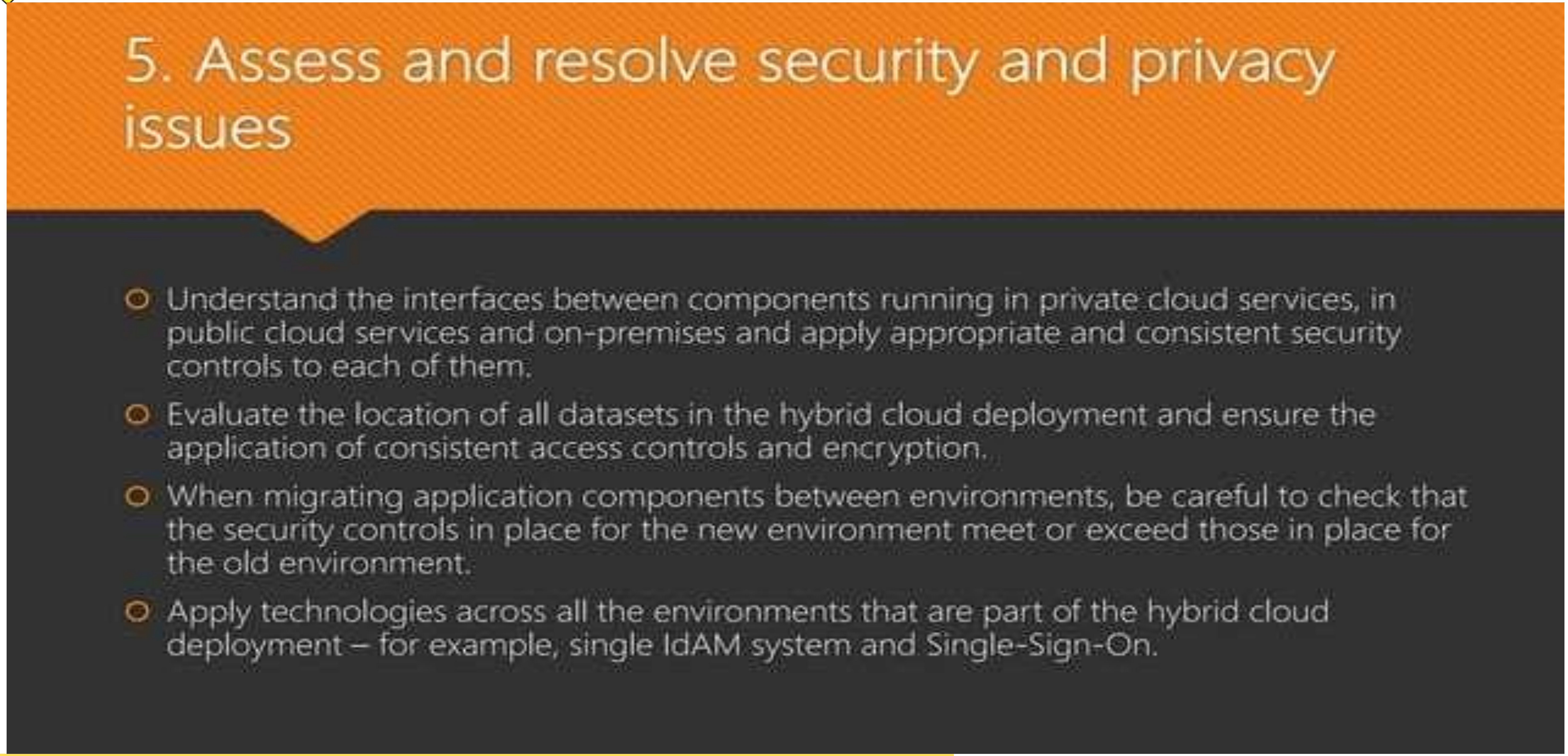
3. Address connectivity requirements

- Consider the requirements of each link between components that spans two or more cloud services or on-premises system and ensure that appropriate connectivity is available to support those requirements.
- Consider the use of network virtualization if available.
- Ensure that the connectivity capabilities can support resilience and disaster recovery requirements.



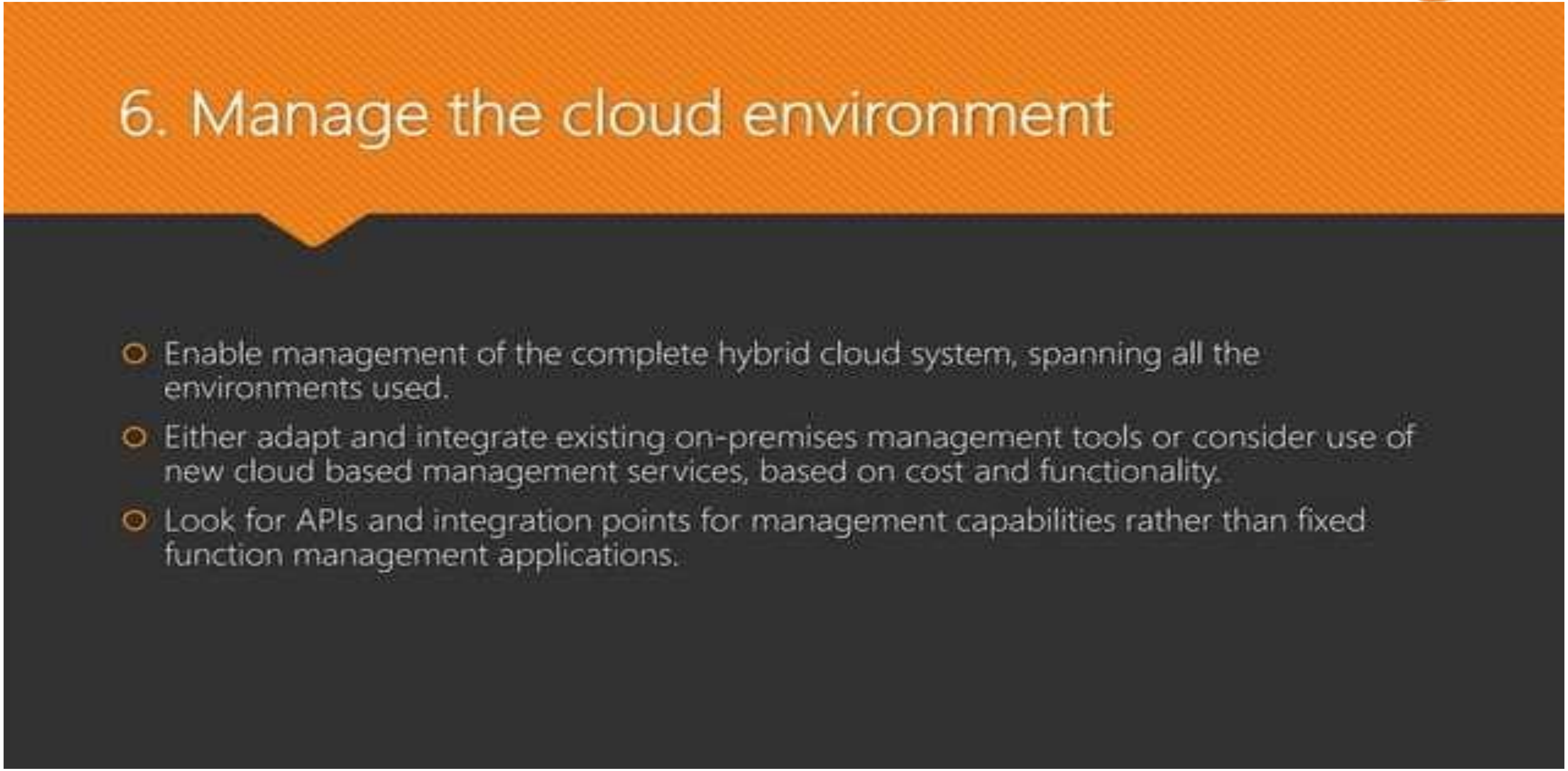
4. Develop governance policies and service agreements

- Assess existing compliance and governance frameworks, identify gaps and harmonize processes.
- The need for thorough and efficient change management and communications increases with the addition of multiple cloud service providers.
- Allow adequate time to educate and habituate changes across the organization.
- Identify gaps in measurement and management visibility.



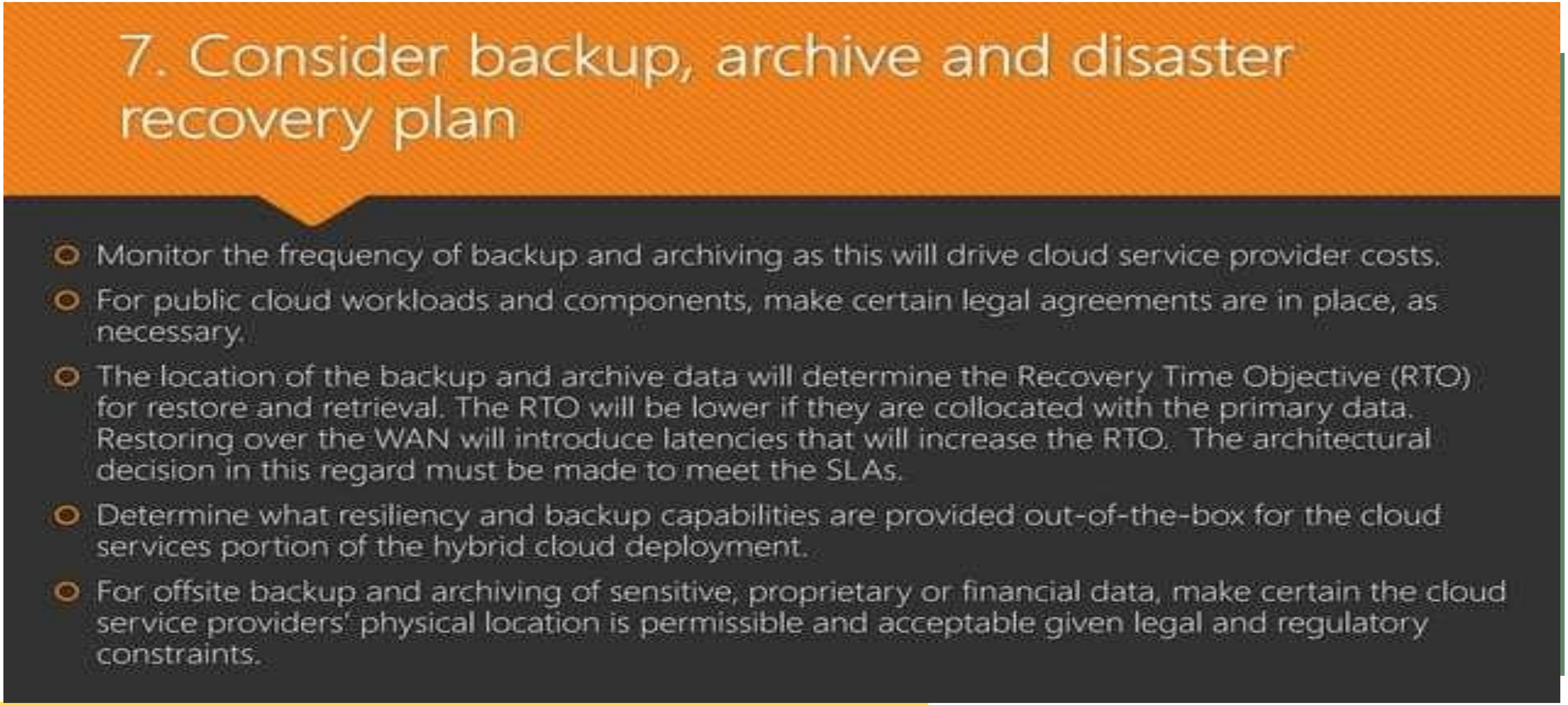
5. Assess and resolve security and privacy issues

- Understand the interfaces between components running in private cloud services, in public cloud services and on-premises and apply appropriate and consistent security controls to each of them.
- Evaluate the location of all datasets in the hybrid cloud deployment and ensure the application of consistent access controls and encryption.
- When migrating application components between environments, be careful to check that the security controls in place for the new environment meet or exceed those in place for the old environment.
- Apply technologies across all the environments that are part of the hybrid cloud deployment – for example, single IdAM system and Single-Sign-On.



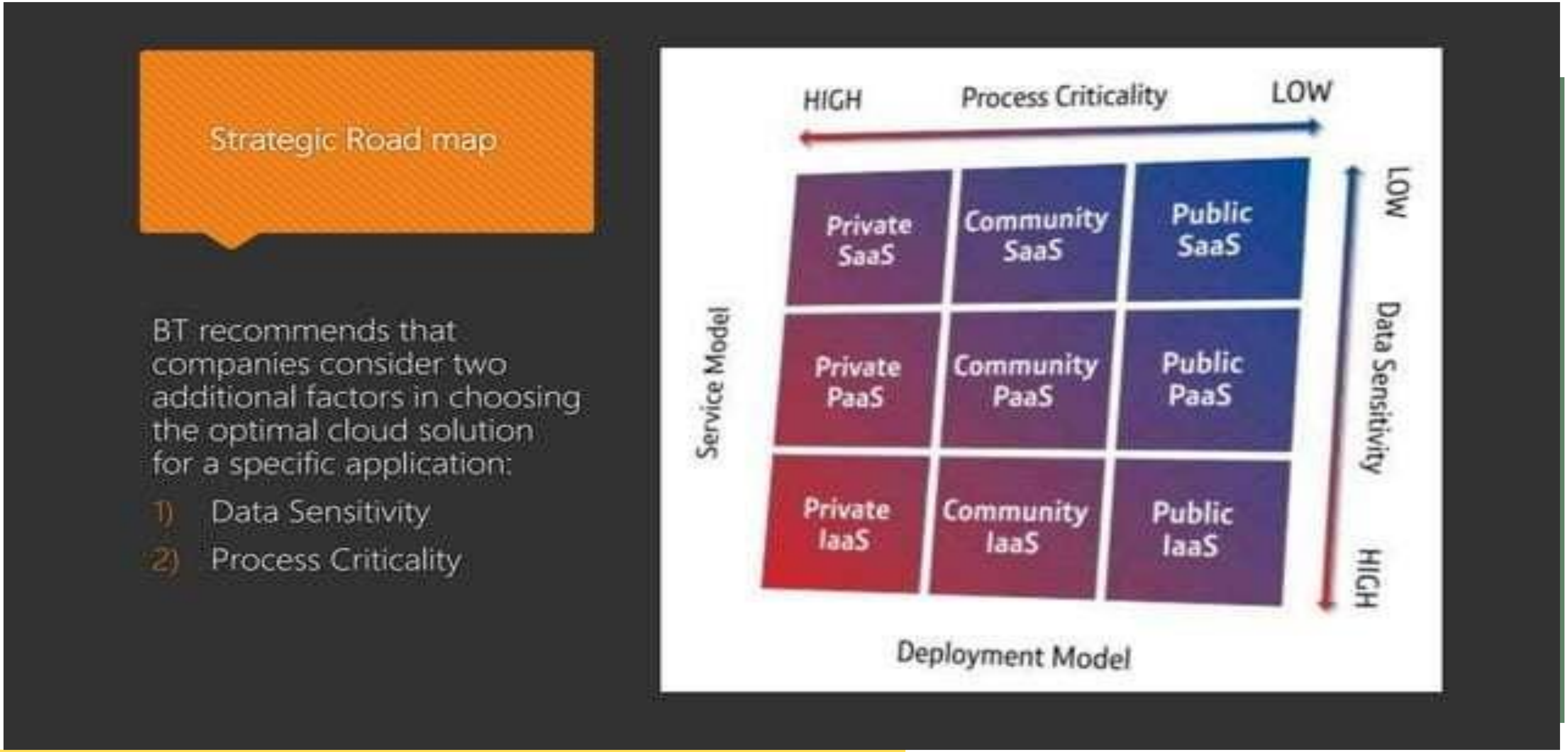
6. Manage the cloud environment

- Enable management of the complete hybrid cloud system, spanning all the environments used.
- Either adapt and integrate existing on-premises management tools or consider use of new cloud based management services, based on cost and functionality.
- Look for APIs and integration points for management capabilities rather than fixed function management applications.



7. Consider backup, archive and disaster recovery plan

- Monitor the frequency of backup and archiving as this will drive cloud service provider costs.
- For public cloud workloads and components, make certain legal agreements are in place, as necessary.
- The location of the backup and archive data will determine the Recovery Time Objective (RTO) for restore and retrieval. The RTO will be lower if they are collocated with the primary data. Restoring over the WAN will introduce latencies that will increase the RTO. The architectural decision in this regard must be made to meet the SLAs.
- Determine what resiliency and backup capabilities are provided out-of-the-box for the cloud services portion of the hybrid cloud deployment.
- For offsite backup and archiving of sensitive, proprietary or financial data, make certain the cloud service providers' physical location is permissible and acceptable given legal and regulatory constraints.



Strategic Road map

BT recommends that companies consider two additional factors in choosing the optimal cloud solution for a specific application:

1) Data Sensitivity
2) Process Criticality

HIGH Process Criticality LOW

Service Model

Data Sensitivity LOW … HIGH

Private SaaS	Community SaaS	Public SaaS
Private PaaS	Community PaaS	Public PaaS
Private IaaS	Community IaaS	Public IaaS

Deployment Model

Thank You