



# Cloud Governance

Managing your cloud risk exposure



Technology Risk Series



Increased use of cloud services

May 2023

The use of cloud services has increased over the last number of years and continues to rise as businesses everywhere accelerate their pursuit of increased digital capabilities. Cloud governance is vital for managing your cloud risk profile.



**Cloud computing** is often at the core of digital disruption today. While cloud computing comes with great benefits such as reduced costs, flexibility and scalability, it also introduces a unique risk profile including information security, data protection, service availability and increasing regulatory requirements.



**Striking a balance** between managing this risk and leveraging the power of cloud is crucial. Effective cloud governance, that promotes optimisation and does not create barriers for innovation, can help organisations strike this balance.

## Key drivers of the increased use of cloud services

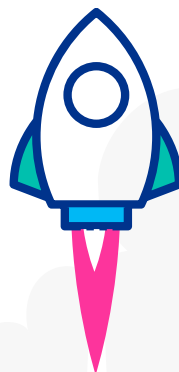
Digitalisation and resilience are two of the key strategic pillars we see at many organisations. This is a reflection of the rapidly advancing technological environment that we operate in, which was further accelerated by the pandemic.

The use of cloud to support these strategic objectives is key and the choice of a Cloud Service Provider (CSP) is becoming a strategic decision that needs to be carefully considered. It is important to understand some of the benefits (below) offered by cloud services to strike the balance between reaping the reward and managing the risk.

### Benefits of cloud:



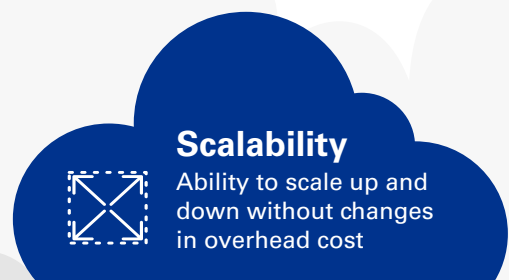
**Reliability & Availability**  
More reliable and available services



**Security**  
Cloud Service Provider may have better security and technical controls



**Flexibility**  
Provides real time resource sharing and the ability to access data from anywhere



**Scalability**  
Ability to scale up and down without changes in overhead cost

# Navigating the key risks of cloud computing

**While cloud computing provides many benefits, it also presents risk to your organisation.**

These risks need to be governed and managed to ensure that your cloud technology is being used responsibly and in compliance with regulatory expectations. As a result, it is more important than ever to understand and mitigate these potential risks in order to safely leverage cloud computing.

Your first step to determining your cloud risk exposure, is understanding the following six potential risk categories:



## People

Lack of available resources with the right skillset.



## Compliance

Failure to meet regulatory compliance requirements (including across multiple jurisdictions).



## Financial

Failure to perform proper Cloud Spend Management around unplanned spikes in transaction volume and traffic.



## Data security

Failure to implement sufficient and appropriate security controls to protect data and prevent data loss through unauthorised access.



## Operational

Failure to implement cloud processes, systems and controls that are aligned to current policies.



## Third party

Lack of third party oversight including failure to acknowledge increased risk of cloud vendor lock in, vendor unreliability and dependencies.



# The challenges that you may face

Navigating these risks is no small challenge and you may face a variety of obstacles that you will need to overcome.

## Key challenges of cloud:



Increasing number of cloud applications in use



Different controls and operating models to what is currently in place



Limited cloud maturity and skills



Difficulty embedding cloud controls across your organisation



No single 'golden' standard for cloud risk and controls

# Approaching cloud governance

## Cloud-focused governance bodies



Cloud governance bodies will be required to **develop, monitor and evolve** cloud governance over time by leveraging existing governance forums or establishing new ones to have responsibility for:

- **Cloud governance** – **formulating** initial cloud governance **policies**, monitoring **compliance**, and reviewing **exceptions** and proposed changes.
- **Cloud operations** – managing day-to-day cloud operations, **service provision** and related issues.

## Management of CSPs



The approach to **managing Cloud Service Providers (CSPs)** should be formalised and include processes for:

- Ensuring CSP's have **adequate controls** in place.
- **Onboarding and offboarding** of cloud services from CSPs.
- **Monitoring of performance** in line with Service Level Agreements (SLAs).
- Oversight of outsourcing arrangements carried out by CSP (i.e. **sub outsourcing**).
- Ensuring **exit strategies** are in place for termination of services (both expected and unexpected).

## Cloud strategy



A cloud strategy should be **developed**, or at least, be considered as part of the technology and outsourcing strategies. The cloud strategy will need to remain **aligned to the strategic objectives** of the business and be **reviewed and updated** on a **periodic basis**.

## Data privacy and security



Your data privacy and security policies and processes should be **updated** to **consider the use of cloud and additional controls** that may need to be implemented as a result of this, such as:

- Sensitive data **ownership** and **classification**.
- **Data flows** and requirements for **data transfer**.
- **Data loss prevention** and **rights management for cloud data** at rest, in transit and in use.

## Cloud capabilities



Mechanisms should be put in place to ensure ongoing **availability of resources** with the **right expertise and skill set**.

## Regulatory compliance



**Regulatory horizon scanning** mechanisms should be in place to identify the regulatory **compliance landscape** and expectations for cloud services relevant to your organisation. This may include the implications of using cloud in relation to General Data Protection Regulation (GDPR) and Network and Information Security (NIS) Directive); financial services regulations in relation to ICT and outsourcing; or more specific cloud regulations such as EIOPA Cloud Outsourcing for the insurance industry.

## Cloud policies & processes



Cloud policies and processes should be **developed** to define **how cloud is managed and monitored**. These policies and processes should be **communicated** to appropriate **stakeholders** across your organisation to support ongoing compliance.

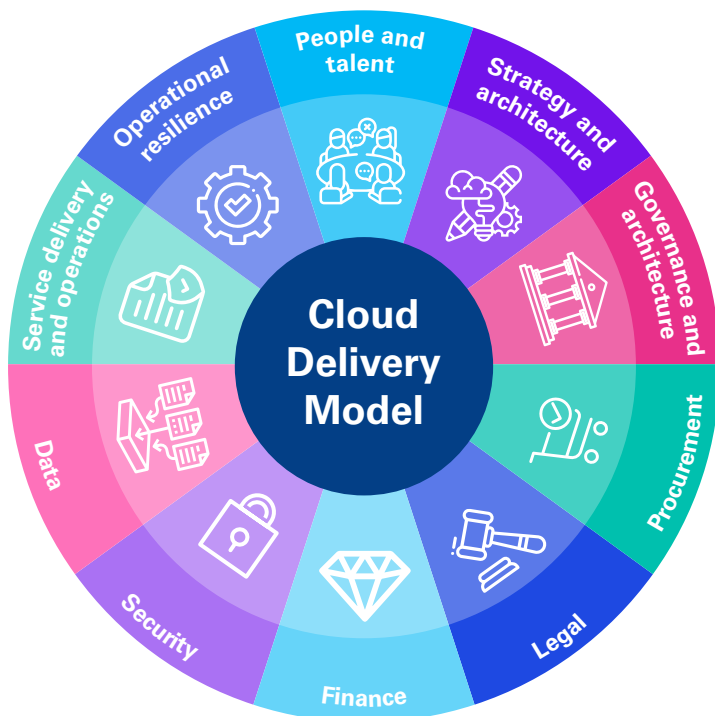


# The KPMG Cloud Risk Framework

We have helped clients effectively manage risks across the technology risk landscape as it has evolved significantly over the last number of years.

KPMG have developed a Cloud Risk Framework to help client's understand, mitigate and effectively manage risks in the cloud. This covers assessing cloud related risks along with assessing governance, operating models and tools to strike the balance between the risk and creating business value.

## KPMG Cloud Risk Framework:



## Key outcomes:



Continuous monitoring of cloud risks



Cloud controls in place

# Contact us

Our Technology Risk team have strong technical capability in the development of risk management frameworks, risk identification and assessment, performing regulatory compliance gap analyses, as well as reviewing, designing and implementing IT controls.



**Jackie Hennessy**  
Partner  
Technology Risk  
**t:** +353 87 050 4171  
**e:** Jackie.Hennessy@kpmg.ie



**Michelle Byrne**  
Associate Director  
Technology Risk  
**t:** +353 87 111 6985  
**e:** michelle.byrne@kpmg.ie



**Carmen Cronje**  
Associate Director  
Technology Risk  
**t:** +353 87 050 4455  
**e:** carmen.cronje@kpmg.ie



**Clarke Ellis**  
Associate Director  
Technology Risk  
**t:** +353 87 111 6974  
**e:** clarke.ellis@kpmg.ie



**Kate Mulhall**  
Manager  
Technology Risk  
**t:** +353 87 744 4530  
**e:** kate.mulhall@kpmg.ie



**Sandani Luvhengo**  
Manager,  
Technology Risk  
**t:** +353 87 111 5978  
**e:** sandani.luvhengo@kpmg.ie

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



[kpmg.ie](https://www.kpmg.ie)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG, an Irish partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks of KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

Produced by: KPMG's Creative Services. Publication Date: May 2023 (9295)