



Cloud Risk & Control

A KPMG Service for G-Cloud 14

May 2024

kpmg.co.uk



Introduction to KPMG's Cloud Risk & Control

Service Description:

KPMG has developed a proven Cloud framework which helps organisations across industries accelerate operational, technical and compliance with standards and guidelines across key Cloud risks in a safe and cost effective way.

Cloud Risk & Controls underpins the cloud transformation process as we support our clients in navigating complex cloud risks, standards and regulations to ultimately accelerate their cloud journey by supporting internal organisational and cross-HMG discussions, and minimising challenges in a secure, cost effective and agile manner.

What are the benefits of KPMG service?

- Accelerates Cloud adoption without deviating from established controls
- Provides increased assurance over Cloud to stakeholders, HMG / the Cabinet Office and customers
- Supports compliance with standards
- Fully auditable and can be used for internal control assurance
- Helps you to continuously manage and proactively mitigate Cloud risks, as well as articulating and realising Cloud benefits
- Enables informed decisions around Cloud risks and performance
- Increases certainty and transparency on compliance with Cloud good practice and control effectiveness
- Drives improvements in controls processes
- Helps to engage with the Cabinet Office, 2nd Line Risk & Assurance and Head of Audit
- Provides intuitive Data & Analytics visualisations to help deliver a coherent message

Our service features:

- Well proven framework and approach, applied at major clients globally
- Mapped to industry standards such as COBIT, ISO 27001/2, the Cloud Security Alliance, PCI/DSS
- Service can be utilised at any stage of your cloud journey including:
 - Strategy & Roadmap
 - Mobilisation
 - Design & Build
 - Go-live
 - Run & Maintain (and Exit)
- Identify key cloud risks in current control environment and controls to manage these
- Provides audit traceability between controls and built environment for BAU
- Provides technical guidelines for cloud architects and engineers to meet the control requirements
- Technology agnostic
- Provides clarity around roles and responsibilities between your organisation and your Cloud Service Providers for control design and operation
- Utilising analytics and visualisations to enable reporting
- Aligned to common HMG and regulatory guidelines and proven best practice

Client Challenges

How do we move to the cloud **safely and securely**?

How do we **respond to and engage with oversight and other HMG bodies** during our cloud migration?

How do we maintain and assess our **Cloud security, resilience and operations**?

How do we **build a clear Cloud Exit strategy and approach**?

How do we **integrate cloud controls** into our existing control frameworks and **assess effectiveness of these controls**?

How do we use **automation to drive efficiencies** in our Cloud controls operation and monitoring?

Focus Areas & Hot Topics



Migration Planning

Uncertainty around workload sequencing and inconsistent approach for grouping applications to be migrated to cloud



3LOD Assurance

Limited assurance by three lines of defence over key aspects of the cloud migration; from procurement to risk and controls assessment to migration testing



Cloud Risk & Controls Framework

Cloud Control Framework not yet defined, implemented and tested



Third Party Oversight

Ineffective controls over monitoring of cloud suppliers in line with shared responsibility model

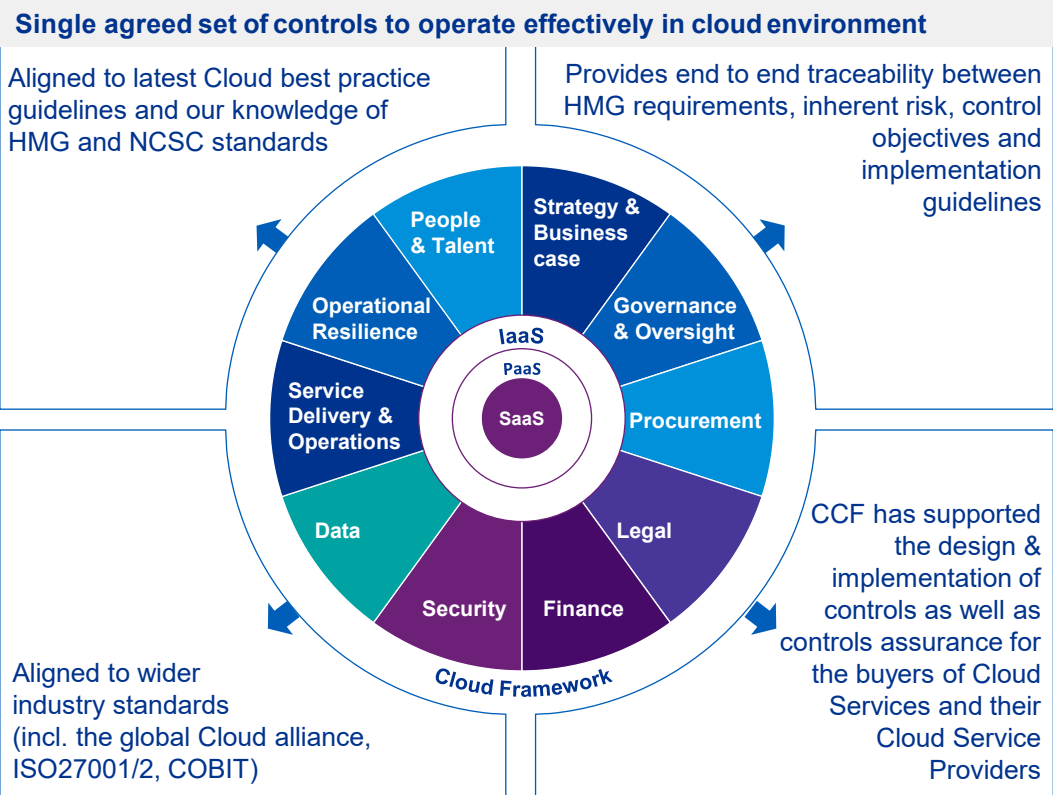


Cloud Exit Planning

Immature exit strategies and plans for both stressed and managed exit scenarios

KPMG Cloud Controls Framework

The KPMG Cloud Controls Framework (CCF) is used as an accelerator to support in the development of organisations’ Cloud control frameworks; either from scratch or to help evaluate existing controls and identify key improvements. It provides traceability between an organisation’s risk appetite and how controls can most effectively help reduce risks.



The KPMG Cloud Controls Framework is a significant accelerator for safe cloud adoption and compliance with standards and best practice as it balances the need for speed and safety.

This is especially pertinent in Government where there are significant benefits (cost, agility, resilience and performance) for migrating to the cloud from legacy platforms, but also the need to safeguard critical national infrastructure, sensitive data and secure processes.

We support organisations in all aspects of their end-to-end Cloud transformation journey. We have highlighted our key propositions under the 5 areas below.

01 Strategy & Roadmap



- Cloud strategy definition – alignment to business, IT strategy & success factors
- Cloud risk & control framework
- Cloud risk appetite definition
- Cloud risk assessment of business case & strategy

02 Mobilisation



- Cloud risk assessment approach definition
- Programme & governance structure: business engagement
- Programme planning
- Cloud MI and reporting

03 Design & Build



- Operating model & tooling
- Control by design implementation
- Control automation
- Cloud Risk & control review
- Contracting / assurance with CSPs
- Exit strategy & planning
- Scenario testing

04 Go-Live



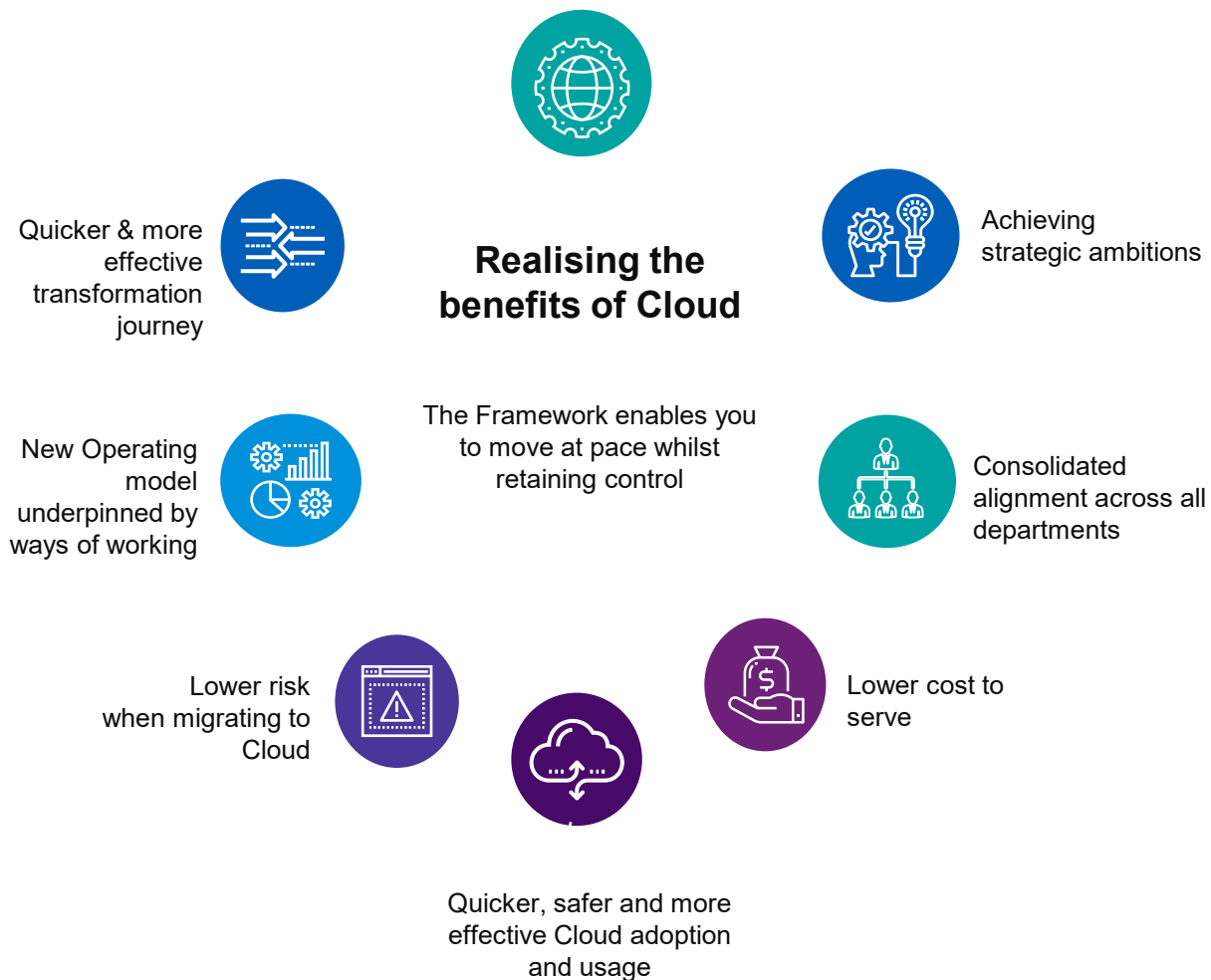
- Pre and post- implementation testing
- Business sign-off and risk acceptance criteria definition
- Cloud control effectiveness review
- Governance and oversight submissions

05 Run & Maintain



- Cloud control monitoring & continuous compliance
- Remediation support for cloud solutions

Key Outcomes



A Case Study



Financial services retail bank



The challenge

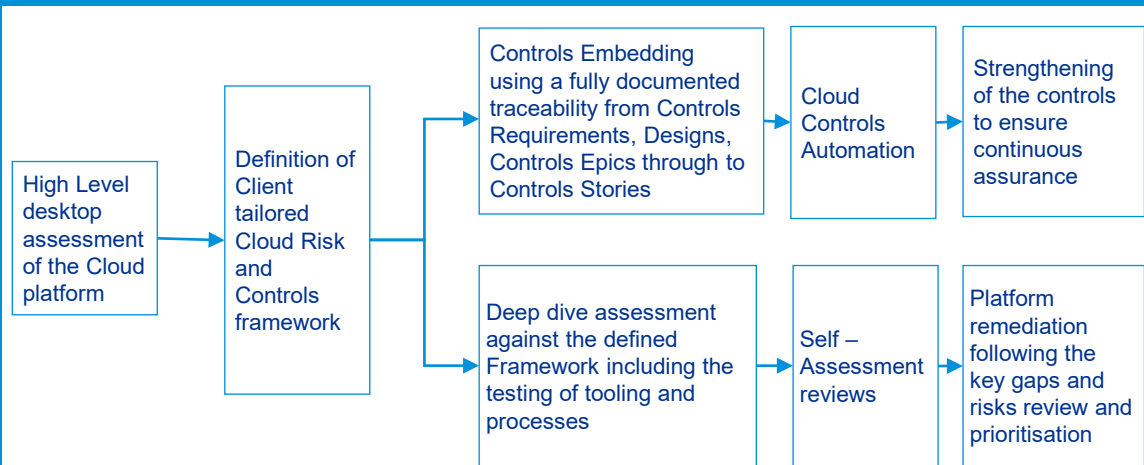
- We worked with one of the UK's leading banks to develop and enhance their Cloud platform.
- Our Client wanted to reduce the cost to serve and be more responsive to customer needs & demands
 - Our multi-disciplinary team worked collaboratively with a Client's Cloud Centre of Excellence (CCoE) and Cloud GRC (CGRC) to support their migration to Cloud
 - To mitigate the risk of the Cloud Centre of Excellence not meeting wider strategic goals we supported them in developing a tailored Cloud Risk and Controls Framework with a clear RACI defining roles, responsibilities and reporting lines
 - In addition, we helped them assess and mitigate risk exposure across personnel responsible for existing Cloud platforms. The objective was to identify, prioritise and remediate gaps in their strategy and delivery and to determine the future roadmap and investments



KPMG supported the Client end to end on their journey to Cloud Best Practice, focusing on the key deliverables as follows:

Approach

BAU support



Client benefits

- We enabled the Client to meet the wider strategic goals and the Cloud Business case by:
- Partnering with our Client, and by applying our Cloud knowledge, risk & compliance and technology infrastructure expertise
 - Achieving higher certainty and transparency on Cloud compliance, control effectiveness and risk exposure enabled through Controls definition, embedding and strengthening
 - Building and developing their Cloud platform, but also implementing controls automation and supporting continuous compliance with applicable standards and frameworks



CONTACT US

KPMG G-Cloud Services Team

T +44 (0) 207 311 5767

E uk-g-cloud@kpmg.co.uk

www.kpmg.com

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 endeavour 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.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.