KPMG

Maximising the value of on-premise IT infrastructure

What is Private Cloud and what are the typical challenges organisations face when they transform their hosting platforms?

—

June 2023

Introduction

As we emerge from the tail-end of the public cloud goldrush, organisations are taking a more balanced and mature approach to developing their hosting strategies. Many organisations with public cloud-centric technology strategies have either struggled to achieve their stated objectives or have discovered that public cloud is not the low-cost, no-maintenance hosting platform originally envisioned. Meanwhile, tried-and-tested technologies remain active and effective for hosting critical applications in their data centre. Furthermore, the regulatory requirements[1] and the economic and technical challenges of a full data centre exit conspire to support local hosting as a long-term strategy.

As a result, hybrid cloud and multi-cloud approaches are now the mainstay of any enterprise hosting strategy with a best of breed approach: use public cloud where it provides features and value not achievable locally while providing on ongoing investment stream to maintain and improve the local presence.

Accelerating business change drives consumers of technology services to have ever-increasing expectations of the capability and consumability of on-premises infrastructure. Private cloud adopts desirable features from traditional IT (Information Technology) such as bespoke hardware configurations, transparent supply chains, and managed data centre hosting, and marries them with consumer-focused features traditionally only seen in public cloud, such as self-service interfaces for humans and applications alike, itemised billing, and automated scaling.

Numerous organisations, from central government to banks and insurance companies, are either building their own private cloud data centres or transforming their current infrastructure and data centres to provide private cloud services. According to Technavio, a market research agency, the global private cloud market is growing with the Compound Annual Growth Rate (CAGR) of 26% and is projected to grow by more than £200bn by 2027.

To understand what a private cloud is, let's look into the key characteristics, benefits and challenges companies face when deploying private cloud solutions and how KPMG can help on their private cloud journey.

[1] For example, recent data protection regulations, such as the United Kingdom (UK) Data Protection Act (DPA), the European Union (EU) General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) or the China Personal Information Protection Law (PIPL)

What is private cloud?

Based on the hosting location, hardware ownership, and capabilities offered by IT infrastructure, there are four main IT infrastructure deployment types[2]:

	Traditional on-premises	Private cloud on-premises	CSP on-premises extensions	Public cloud
Ownership/ Hosting	Dedicated customer-acquired hardware within customer DC (or in a third-party facility)	Dedicated customer-acquired hardware within customer DC (or in a third-party facility)	Dedicated CSP-owned hardware (single tenant) within customer DC (or in a third-party facility)	Shared CSP hardware (multi-tenant) within CSP-owned DC
Capabilities	Manual virtualisation platform	Fully automated virtualised platform, offering self-service capabilities to consumers	Packaged automated and self-service environment, managed by Cloud Service Provider	On-demand availability of scalable resources provided over the public internet

In our view, private cloud is a cloud infrastructure environment dedicated to a single organisation, both virtually and physically. In addition, an infrastructure platform can be considered a private cloud if it meets the following two criteria:

- Digital Sovereignty (incl. data, hardware, and software); and
- Automation and Self-Service.

[2] There might be other unique examples that can be considered private cloud based on organisational requirements, for example dedicated hosts (physical servers owned by a CSP and located within the CSP data centre, but dedicated to a single organisation)

Therefore, in the private cloud market, there are two major options:

Private cloud on-premises

- Dedicated customer-acquired hardware within customer Data Centre (DC) or in a third-party facility.
- Leverages automation and virtualisation on top of customer-owned hardware to offer infrastructure resources such as compute, storage, and network services.
- Typically hosted within a company's private internal network, either on-premises or in third party data centres.
- The underlying IT infrastructure is dedicated to a single organisation.
- Portals and Application Programming Interfaces (API) available to allow consumers to self-service infrastructure patte9rns without manual intervention from IT operations
- For example, below vendors provide private cloud on-premises solutions:
  - Infrastructure management tools: OpenStack, Apache CloudStack, Eucalyptus, VMware Cloud Foundation, Nutanix Enterprise Cloud
  - Container management tools: Kubernetes, Red Hat OpenShift Container Platform, Docker

CSP on-premises extensions

- Dedicated Cloud Service Provider (CSP) owned hardware (single tenant) within customer DC or in a third-party facility.
- CSP extending their capabilities for deployment outside their DC, reducing latency and bandwidth usage by bringing computation and storage closer to the data.
- CSP on-premises infrastructure acts as dedicated private platform, bringing the benefits of public cloud combined with the isolation and security of on-premises infrastructure.
- Note, the management of CSP on-premises extensions is done via CSP-controlled APIs and hence creates a dependency on CSP availability.
- For example, below are the CSP on-premises extensions products, provided by major Cloud Service Providers:
  - AWS (Amazon Web Services) Outposts
  - Microsoft Azure Stack
  - Google Anthos
  - OCI (Oracle Cloud Infrastructure) Dedicated region
  - IBM Cloud Satellite

Potential use cases

What are the drivers for using private cloud?

Companies may consider developing private cloud infrastructure in multiple scenarios, for example:

Existing investments

When the company has its own data centre and exiting the data centre is not feasible from an economic perspective.

Economies of scale

Where the economies of scale allow operating on-premises at a lower cost than public cloud hosting.

Uptime and latency

Where the service availability (uptime) and/or latency levels offered by public cloud are not sufficient.

Regulated industry

When the company is operating in a regulated industry[3] and needs to host critical workloads.

Business agility

When the company needs to increase their pace of change while still operating an on-premises infrastructure

Controlled environment

Other scenarios where the company needs to retain full control and ownership of the technology estate (incl. hardware, software, and data).

[3] For example: Financial Services, Energy, Transport, and Telecommunications sectors

Key Private Cloud benefits

Private cloud combines the consumability and agility of public cloud with the customisability and ownership of on-premises infrastructure in order to deliver greater value than either solution can on it's own.

What are the key benefits of private cloud over traditional on-premises infrastructure?

Automation and Self-Service:

As with public cloud, the advantage of private cloud is the capabilities offered by advanced automation tooling: Self-Service, Continuous Integration (CI) / Continuous Deployment (CD) pipelines, Infrastructure-as-Code (IaC) and Platform-as-a-Service (PaaS) services are all available in a private cloud.

Elasticity:

Virtualised and automated infrastructure allows organisations to automatically scale up/down resources in near real-time to meet user demands and other organisational priorities.

Security:

Automation of the network allows organisations to be more proactive in their approach to security by automatically detecting, responding, and recovering from cyber incidents.

What are the key benefits of private cloud over public cloud infrastructure?

Enhanced Trust:

Banks and other companies operating in regulated industries have heavy governance requirements from regulators and associated business partners in terms of data localisation, hosting, and movement. Private cloud brings greater trust by offering the best of both worlds, enabling organisations to control precise locations to collect, process and store their data while offering the benefits of self service and automation.

Transparent Recovery opportunity:

Digital sovereignty means organisations can directly control any part of the technology stack (incl. data, software, and hardware), which in turn enables them to drive recovery from a cyber or operational incident.

Stability of Costs:

Private cloud capabilities enable sweating of IT assets; this can particularly beneficial when the organisations have already invested in best-in-class hardware. By amalgamating already procured hardware with latest advancements in software virtualisation and automation, organisations can control costs and have more clarity around future expenditures (whether it is CapEx or OpEx).

Application-specific Optimisation:

In private cloud infrastructure, it is possible for the operator to select specific host operating system versions, device driver and kernel optimisations, and purpose-built Software-Defined Networking (SDN) solutions. This level of flexibility enables multiple use cases, for example, ultra-low latency for cloud robotics applications and multimedia processing capabilities for telecoms.

Hardware Performance:

Hardware ownership means that organisations can build to custom specifications for compute farms, rack switches, and storage arrays ensuring a highly optimised platform for hosting technology services and business applications.

What are the options available to deploy Private Cloud?

We believe there is no one-size-fits-all approach when it comes to private cloud deployments. Instead, organisations should consider multiple options before adopting private cloud.

	Private cloud on-premises	CSP on-premises extension
	Dedicated customer-acquired hardware within customer DC (or in a third-party facility)	**Dedicated CSP-owned hardware (single tenant) within customer DC (or in a third-party facility)**
Investment/ ownership options	Client acquired – CapEx Client acquired – OpEx (Lease)	Cloud Service Provider (CSP) acquired – OpEx (pay-as-you-go)
Hardware sharing option	Dedicated hardware (single tenant)	Dedicated hardware (single tenant)
Location options	Customer DC Colocation/third party	Customer DC Colocation/third party
Access options	Private network	Private network Internet (for management interface)
Virtualisation and Orchestration options	Client proprietary Open/Standardised across DC	CSP proprietary
Operations & Maintenance options	Customer managed Original Equipment Manufacturer (OEM) managed	CSP managed

Deployment Options:

Investment/ownership options

Client acquired – CapEx

Organisation requires upfront investment to own hardware and licensing. Organisation is responsible for all associated direct platform costs including building, running, and maintaining the environment. This will provide elasticity up to limit of resource pool deployed.

Client acquired – OpEx (Lease)

Organisation does not require upfront investment but rather they finance the hardware and associated licensing from the Original Equipment Manufacturer (OEM), Cloud Service Provider (CSP) or another vendor via monthly payments. The cost will be spread over the defined finance period.

Cloud Service Provider (CSP) acquired – OpEx (pay-as-you-go)

This is typically offered by CSP where equipment can be reprovisioned for other clients when rental is terminated. This model is based on “pay per use”.

Hardware sharing option

Dedicated hardware (single tenant)

A private cloud is used by a single organisation or customer. Whether this is in a dedicated data centre, in a co-location data centre or elsewhere, the hardware is not shared with other organisations or entities.

Location options

Customer Data Centre

On-premises private clouds are hosted within an organisation’s own data centre. On premise private clouds are typically used by large organisations with significant IT resources and expertise.

Colocation/third party

Private clouds can also be hosted in a third-party data centre operated by a service provider. A secure and dedicated area will be provided, often in a physically segregated space. Similarly, hosting CSP on-premises extensions in the customer data centre may come with provider stipulations, such as being in a physically segregated space.

Access options

Private network

The private network is dedicated to the organisation's environment (i.e., not shared). The accountability for the private network sits within the organisation. Access can be provided through customised security measures, such as zero-trust network access (ZTNA), built in layers of security, or more traditional VPN (Virtual Private Network), dedicated leased lines, and private network connections. Note, the management interface of CSP on-premises extensions is typically routed via CSP-controlled APIs (over public internet).

Virtualisation and Orchestration options

- **Client Proprietary**

  The customer is responsible for maintaining the environment.

- **Cloud Service Provider (CSP) Proprietary**

  Virtualisation and orchestration vendor lock-in needs to be taken into consideration for cross-provider mobility and exit strategies.

Operations & Maintenance options

- **Customer-managed**

  Complete control over the underlying infrastructure and management of the cloud environment by the customer. In this model, the customer owns and operates the hardware, software, and networking components of the cloud environment, allowing them to tailor the infrastructure to meet their specific needs. The customer is also responsible for the day-to-day management activities (security, upgrades, maintenance).

- **Original Equipment Manufacturer (OEM) / vendor managed**

  The IT infrastructure of the cloud is hosted internally but is operated by an external provider, where OEM (or the vendor) provides maintenance and support (mixed support, contracted to the client).

- **Cloud Service Provider (CSP) managed**

  CSP is solely responsible for running managed single tenant services on behalf of the customer and the CSP is responsible for the day-to-day management and responsibility of the environment (upgrades, patches, security). The software may be deployed and configured by a third-party provider/vendor. Managed private cloud may also employ fixed contracts and require more local support and maintenance staff.

Services hosted on Private Cloud

Organisations investing in private cloud infrastructure typically host Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) services. Below are some example types of services that can be used on a private cloud:

IaaS

Virtual Machines

PaaS

Containers

Serverless

Infrastructure as a Service (IaaS)

a form of cloud computing environment that provides virtualised computing resources (e.g., servers, data bases) over the network. It gives developers full control of the operating system.

- **Virtual Machines** (VMs) emulate the functionality of physical servers and host an operating system on a virtualised environment.

Platform as a Service (PaaS)

a form of cloud computing environment, where developers are provided with a platform to develop, run, and host applications.

- **Containers** offer both efficiency and speed compared with virtual machines. Containers are typically smaller that virtual machines and have improved performance and flexibility, which helps to host microservices on them.
- **Serverless** goes one step further than containers, eliminating the need for server and Operating System (OS) management.

Architecture and chargeback

Private cloud architecture:

Private cloud infrastructures use ‘software-defined’ compute, network, and storage resources. This enables on-demand resources and provides a high level of automation throughout the entire operational lifecycle. A wide range of open source and vendor-supported software solutions can turn traditional datacentres into private clouds that provide flexibility and all the key features as listed above. With orchestration tools like Terraform, organisations also have the choice to operate a multi-cloud environment, easily manage multiple private clouds, or combine services across private and public clouds. Standardised orchestration solutions are currently in development for managing private multi-cloud infrastructures, for example ETSI OpenSource MANO, which is driven by the telecommunications sector.

Infrastructure management and service orchestration solutions facilitate the implementation of a Zero-Trust security model where users are granted least privilege access and operate within sandboxes, where they are only allowed to perform specific actions. Orchestration is also used to create end-to-end network slices across several cloud infrastructures using software-defined networking. This enables communication between the distributed components of cloud-native applications irrespective of their location - potentially spanning large geographical regions.

Infrastructure as Code (IaC) leverages orchestration by using service and infrastructure ‘descriptors’ that contain blueprints for application deployment and platform configuration. These descriptors allow for quick deployment (and duplication) of virtual infrastructures and hosted applications, thus reducing time-to-market, facilitating agile development, and enhancing business continuity.

Cost of resources and chargeback model:

Organisations offering private cloud services to their business units can maintain the ability to charge back for the consumption of the private cloud services in a similar fashion as public cloud consumption.

This is achieved by calculating total costs involved in running and maintaining private cloud services (incl. software licensing and DC maintenance costs) and then dividing them by the consumption units using organisation-defined accounting principles.

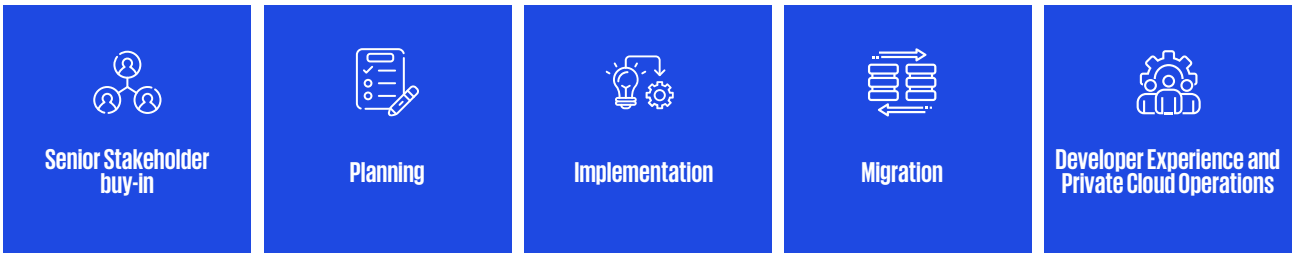
To derive the individual resource costs, it is important to track consumption in 2 dimensions:

- the amount of resources consumed by each business unit (CPU, memory, storage, network); and
- the consumption duration (from a few minutes to days).

The approach will help organisations define internal costs distribution and mature their FinOps and Chargeback capabilities.

Key Private Cloud challenges

Our clients face a wide spectrum of challenges when moving from a traditional on-premises data centre to a fully virtualised private cloud environment. These challenges can be categorised by the below sections:



Senior Stakeholder buy-in

With the prevalence of public cloud, it can be challenging to get funding for implementing a private cloud from senior stakeholders. Public cloud is still a significant industry trend and executives want to be seen to be promoting it while anyone proposing building a data centre is automatically seen as an advocate of legacy infrastructure.

To help the leadership team to make an informed decision, it is important that a clear business case is formulated, explaining what private cloud is and what cost-benefit analysis has been conducted. The long and short-term benefits must be clearly communicated and aligned with the business objectives. In addition, run costs, new product development, and vendor fees need to be factored into the private cloud strategy.

Once the decision has been made, it is vital to get a long-term commitment from senior leadership to support the strategy.

Planning

Private cloud planning is a strategic process and comes with several challenges. Some of the key challenges that need to be considered are regulatory requirements, product offering standardisation, operating model, controls, and governance.

- **Regulatory requirements:** Different regulations require certain characteristics to be present in a private cloud that do not necessarily exist in the current environment. A regulatory compliance strategy will need to cover all aspects of the private cloud from infrastructure design to the support functions which surround it.
- **Product offering standardisation:** It is essential that the product offerings for consumers are standardised across the platform to allow self-service consumption, automation, and to benefit from economies of scale. By increasing standardisation, companies would lower the overhead of technical product management, thus decreasing costs and improving the fulfilment of currency obligations.

- **Operating Model:** Long-term support and maintenance of the private cloud is challenging, and the support model must be part of strategic planning. In-house teams can be upskilled to support private cloud; alternatively, we have seen several of our clients engaging with specialised third-party vendors to support their private cloud. Often the growth of the IT organisation may be required, since large teams with diverse skillsets are needed to manage demands of backup, regulatory compliance, and the management of both physical infrastructure and virtual compute, storage, and network infrastructure. We have also seen that a decentralised approach giving greater control to autonomous functional units working well in a private cloud environment, provided a proper governance process exists, ensuring changes align with the strategic view of the platform.

- **Controls:** As consumers get greater autonomy through cloud offerings, the applications on the platform become prone to non-standard, non-compliant code. To combat this, it is essential that adequate controls and guardrails are in place ensuring non-compliance can be checked and flagged. It is also important that a continuous improvement approach is taken to the platform ensuring that it is offering the latest features, maintaining parity with other technology solutions where possible, and pro-actively reducing the accumulation of technical debt. Software ownership and responsibility between the platform operations team and consumers especially around currency and patching can be a potential challenge if not defined clearly and upfront.

- **Governance:** With technology rapidly evolving, private cloud platforms can very quickly get misaligned with their strategic purpose. To help prevent this, it is important to have a proper governance structure in place that ensures major changes align with the platform strategy and roadmap. Proper measures also need to be in place to ensure capacity is smartly managed and demand can be forecasted. In addition, application change governance should also evolve, providing a similar experience to consumers as public cloud.

Implementation

A private cloud can be implemented by virtualising and enhancing existing on-premises infrastructure or building new infrastructure from scratch. Both approaches can present major challenges, and a successful implementation will depend on understanding the six factors below:

- **Consumption model:** Achieving autonomy is hard, and the way users interact with the infrastructure matters. This can be achieved by offering self-service capabilities to consumers. Therefore, interactions with customers should move to strategic conversations around future needs, rather than discussing reactive operational tasks.

- **Financial model:** Building a private cloud requires investment. Whether this is OpEx or CapEx, the private cloud implementation and running costs need to be linked to a usage level (as is possible with public cloud) and require careful planning for chargeback mechanisms. Organisations need to mature their FinOps and chargeback tools to provide public cloud-like experience and to define how much to charge internally and to whom.

- **Current infrastructure:** Age of the current kit is a key driving factor in the implementation plan. Rapid technological changes in the application layer may not be supported by an out-of-date hardware kit. To derive full benefits of a private cloud, it is important that the underlying layer is modern and can support business requirements. For example, an existing storage platform with new infrastructure around can provide a good cost-benefit balance.

- **Location:** Business requirements may determine the hosting location of a private cloud. For example, as part of the regulatory requirements, data may need to be kept at certain location or outside of certain jurisdictions. This will present a challenge to a co-location strategy and will have to be factored into the choice of location.
- **Recovery:** Private cloud also reinforces the need for good Disaster Recovery (DR) strategy and planning. Often in public cloud, an organisation will design their workloads to take advantage of the resilient nature of multiple availability zones and regions. In private cloud, this may be more difficult to achieve, and a more traditional DR approach will be required.
- **Demand and Capacity management:** Cost savings are normally achieved by hosting thousands of virtual servers onto a minimum amount of high-performance high-grade hardware infrastructure, which requires comprehensive planning and management of demand versus capacity.

Migration

One of the major challenges faced by our clients when migrating apps into private cloud is developing a reliable migration strategy. Most of the time existing workloads are not compatible with the latest technologies on offer from the private cloud, so clients end up migrating the apps “as-is” using a “lift-and-shift" strategy. This is the quickest migration route; however, it does not always realise the full potential of the private cloud platform and limits benefits in the longer term.

We have seen many of our clients set up specialised programmes to carry out migration projects and to perform rearchitecting and refactoring of legacy applications. These projects are delivered by carefully considering the business requirements, application features, and the new platform tooling available (such as containerisation), as well as decentralising components by using modern messaging platforms. Rebuilding the application using a cloud-native approach requires a major upfront investment in terms of time and money, but it is the most successful strategy in realising the long-term benefits of moving to private cloud.

Organisations adopting private cloud are likely to have considerable experience in the development of a standardised virtual machine image. However, the mindset needs to shift from developing traditional VM images to developing cloud-type images. Availability of these reusable templates and technologies within a migration project is key to enable automation, high visibility of operations, and ease of management, which will require significant time and investment before the migration.

Long-term maintenance and support of migrating applications need to be carefully planned as well. Conventional teams might not be adequately trained to support the application in the new environment, and proper upskilling and training plans should be factored into the migration strategy.

Developer Experience and Private Cloud Operations

The service offerings need to be presented as a singular product to the consumer; however, they are often composed of tools from multiple vendors which creates complexity when building a platform.

The use of multiple vendors can also cause confusion amongst users trying to consume services within the private cloud, as they often compare the private cloud services to their equivalents in public cloud and expect similar functionality. To mitigate this, an effective training and communications plan should be in place to ensure consumers understand the differences of public and private cloud. Regular product offering updates should also be clearly communicated to users using multiple channels. This is especially relevant for organisations operating a hybrid cloud environment where both public and private cloud co-exist.

User expectations in these cases need to be set clearly, and a proper adoption mechanism must be developed to make it easier for users to choose the right platform for their applications. Services provisioned in private cloud can be made consistent with those in public cloud, allowing reduced friction for migrating between hosting locations.

How KPMG can help with Private Cloud

At KPMG in the UK, we are experts in Cloud Transformation, including legacy data centre transformation, private cloud, and public cloud. We have a team of over 200 experienced consultants, architects, and delivery managers who can help you to understand the complexities of your private cloud environment and assist with an end-to-end solution. No matter where you are on your journey with private cloud, whether it be a technology refresh to deal with currency or the distribution of a brand-new private cloud solution, KPMG have the skills and expertise to assist in the journey.

Our service propositions address all your challenges:

Client Challenge	KPMG Service Offering	Description
Senior Stakeholder Buy in	• Cloud strategy / private cloud strategy • Hosting and DC strategy • Roadmap	We will help you derive value from IT infrastructure by determining where, when, and how to effectively use cloud products and services through new models such as PaaS, and IaaS.
Planning	• Current State Assessment • DC facility audit • Sustainability planning • Private cloud design and architecture • Data Centre design • Operating Model design • Decommissioning approach and plan	With a clear strategy defined, KPMG will work with your teams to transform the strategic vision into the high-level architecture and realistic roadmap for implementation and/or migration to ensure you achieve maximum value from your cloud infrastructure investments.
Implementation	• Implementation delivery • Implementation programme assurance	Selecting a delivery and implementation team capable of working to the specific needs enables a people-centric approach to the technology and transformative changes required.
Migration	• Migration delivery • Migration programme assurance	Our Cloud Migration Framework consists of five sequential stages, each having a defined purpose, key objectives and work products/deliverables enabled by KPMG accelerators. The framework is agnostic in that it describes a high-level approach that does not specifically reference (or rely upon) third-party services from any of the leading Private cloud vendors.
Developer Experience & Private Cloud Operations	• Private Cloud Operations support • Cost optimisation • Footprint optimisation • Currency Level Model and Maintenance Planning • Sustainability Impact Assessment	We will help you optimise your current private cloud delivery and operations capabilities to ensure consistent developer experience across your technology estate.

KPMG private cloud capabilities enable our clients to effectively integrate and manage hosting and related infrastructure whilst realising opportunities to consolidate and optimise their infrastructure landscape.

We have a proven set of tools which help guide you in delivering your cloud transformation programme. Using a collection of KPMG Accelerators will improve delivery at pace and help not just the technology transformation but also to bring your employees with you on the journey. There is a range of services that can be enabled on a private cloud, and it is important to make consumption of these services as seamless as possible for your end users, platform/product, and application owners. This will assist in the adoption of your private cloud and provide a better return on your technology investment.

KPMG Contacts

For any questions on private cloud, please do not hesitate to contact:

Tom Bragg

Senior Manager, Cloud Transformation, KPMG in the UK

Email : tom.bragg@kpmg.co.uk
Phone : +44 (0) 7738 040 649

Tom has over 25 years of experience in Banking, Insurance and Automotive sectors, working across a broad range of IT disciplines, holding technical and managerial roles with a strong technical architecture focus. He has extensive experience developing IT strategies for SME and large enterprises, focused on enabling business change in organisations on a global scale coupled with practical knowledge of delivering radical transformation programmes.

Iakov Fedoseenko

Senior Manager, Cloud Transformation, KPMG in the UK

Email : iakov.fedoseenko@kpmg.co.uk
Phone : +44 (0) 7581 121 767

Iakov is a cloud architect within the KPMG's Connected Technology function specialising in Technology Strategy & Architecture, IT Governance, Infrastructure transformation, Cloud Security and Resilience. He has led global diverse teams and managed complex digital transformation projects for clients across financial services, private and public sectors.

Contributors

We would also like to thank the following authors for their contribution to this white paper:

Adnan Ajmi, Neil Adams, Tim Sneath, Shariq Syed, Shahraiz Huda, Fragkiskos Sardis, Erdal Cetin, and Anthony Sabin.

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

kpmg.com/uk

Document Classification: KPMG Public

CREATE: CRT143124A