

HOW A MULTICLOUD STRATEGY CAN HELP REGULATED ORGANIZATIONS MITIGATE RISKS IN CLOUD

Authors:

Carla Arend
Archana Venkatraman
Massimiliano Claps

March 2021

Sponsored by



IDC #EUR147510821



How a Multicloud Strategy Can Help Regulated Organizations Mitigate Risks in Cloud

Introduction

Cloud in its various forms (on-premises private cloud, public cloud, hybrid, and multicloud) has become the de facto architecture for modern IT and digital transformation (DX) across Europe for business agility, flexibility, scalability, security, and innovation. But cloud adoption is slower in regulated industries like financial services and the public sector due to the complexity of their legacy systems, cultural shifts, and compliance challenges including concerns raised by European regulators. Regulators are, in particular, concerned about concentration risk, vendor lock-in, operational resilience, reliability, and over-reliance on third-party providers.

With COVID-19 recovery a top priority, operational resilience has become ever more prominent across all sectors of the economy, particularly in the regulated industries that need to provide uninterrupted crucial services — and cloud has emerged as an empowering technology to meet this objective. This has resulted in a more aggressive push to the cloud.

The cloud choices organizations make today will need to fulfill their immediate crisis recovery needs but also their long-term strategies and regulatory requirements. Adopting a multicloud strategy that can often be based on open source components offers not only a greater choice but a much more robust approach to guaranteeing resilience, compliance, and business continuity of critically important processes.

Questions on survivability and stability of Europe's economy are underscored in the context of the open strategic autonomy discussions, both in the political and technological context. Having a flexible multicloud strategy and solid foundations for portability and interoperability has never been more relevant, with European authorities aiming to put more control in the hands of the users and create an open, interoperable IT ecosystem to stimulate cross-industry, cross-cloud collaboration for the benefit of all.

European initiatives such as Gaia-X and the European Alliance on Industrial Data and Cloud warn about the perils of locking into individual suppliers. IDC believes that such initiatives will formulate an approach to the sustainable future of cloud in Europe. Providers that participate in these efforts will be the ones that can help regulated organizations build successful multicloud

AT A GLANCE

WHAT'S IMPORTANT

A multicloud strategy is an architectural approach that enables customers to use the best-of-breed cloud components from multiple cloud services but also gives them freedom from a prescriptive architecture of one single cloud provider and makes cloud a two-way street.

Open source technologies such as containers, open APIs, and open source databases are enablers of multicloud as they enable movement of workloads and data to demonstrate portability, compliance, and security for heavily regulated industries.

KEY TAKEAWAYS

A multicloud and open source strategy for organizations in regulated industries can:

- » Reduce reliance or over-dependence on very few third-party providers
- » Demonstrate the capabilities to execute on an exit strategy
- » Boost compliance posture with strong data governance and mobility capabilities

strategies. About a third of financial services organizations surveyed in IDC's *COVID-19 Impact Survey* (Wave 8, July 2020) said they are increasing their public cloud spend on platform and software solutions from what they had planned before the pandemic. The strategy that many financial services organizations are adopting is built on open technologies such as containers, open APIs, and microservices. With this strategy, they can build in application portability, demonstrate a cloud exit strategy, and lay a solid foundation for future-proof innovation.

As for the public sector, IDC research conducted in May 2020 showed that more than half (55%) of government respondents plan to move data and apps to cloud more rapidly primarily for:

- Innovation and customer experience
- Crisis management (business continuity and increasing security)
- Optimized operations to create business resilience (no downtime, availability, and business continuity on an operational level)

Historically, many public institutions have added cloud services on a project-by-project basis without a comprehensive strategy. As a result, they have ended with complex and ad hoc cloud environments. Adopting a long-term multicloud strategy and moving away from the lift-and-shift approach will be beneficial for public sector cloud adoption in the long run.

Cloud is no longer just a destination for workloads — it is an experience, an operating model, and a business enabler. Ensuring a cloud-centric strategy based on open source components and compatible with multiple cloud services can enable businesses in heavily regulated industries and public sector organizations to benefit from faster innovation in compliance with regulatory requirements.

In This White Paper

In this IDC White Paper we discuss how a multicloud strategy can help to alleviate concerns around cloud usage in regulated industries in Europe and accelerate cloud-driven innovation. The paper also highlights the impact of the pandemic on European organizations' cloud strategies.

Multicloud Introduction

As cloud enters the mainstream, it is becoming clear for European organizations that there is no one-size-fits-all cloud model that can meet the cost, security, data, and performance expectations of a heterogeneous set of workloads.

The first era of cloud adoption was to migrate and run some applications in the cloud. This approach then evolved into a hybrid cloud concept that connects private cloud (in-house datacenters) with public cloud solutions. We are now in the second era of cloud-driven innovation where multicloud has become a reality.

A multicloud strategy is an architectural approach that enables customers to pick and choose cloud services from multiple cloud providers. This approach enables organizations to not only

use the best-of-breed technology but also gives them freedom from a prescriptive architecture of a single cloud provider and makes cloud a two-way street.

Open source and open-source-based technologies such as containers, open APIs, and open source databases are enablers of multicloud and often go hand in hand as they support movement of workloads and data across different cloud environments to ensure portability, compliance, and security for heavily regulated industries. IDC estimates that at least 50% of organizations prefer to run databases on a container platform.

Container technology and container orchestration services such as Kubernetes (originally developed by Google, then open sourced and now independently managed by a non-profit organization) are a long-term favorite choice to accelerate DX.

Containers appeal to enterprises for several reasons:

- Developing software faster to improve time to market and compete with digital disruptors
- Making applications portable as multicloud environments emerge as desired outcomes (moving projects across different cloud environments and taking them back on premises if needed)
- Improving abstraction from underlying operating systems (OSs) and other infrastructure software, reducing the potential to break applications when updating or replacing lower-level software layers
- Scaling applications to be highly responsive and to meet increasing application loads
- Modernizing application design by using microservices and DevOps methodologies to suit the cloud world
- Making more efficient use of computing resources
- Finding ways to overcome traditional virtualization licensing fees as IT estates grow

Some organizations also feel that containers make it much easier to collaborate on development across different geographies and public clouds and help accelerate the journey to the cloud. Multicloud also requires a unified management strategy to ensure all the components are integrated and work together, further amplifying the role of open source technologies.

Enterprises' Container Adoption Strategies and Objectives

In conversations with IDC, organizations explain how containerizing legacy applications on a standardized Kubernetes platform brings flexibility to run critical workloads on any infrastructure, thereby bringing huge competitive advantage.

Companies are not looking for day-to-day portability of applications but want the ability to "build once/deploy anywhere" so they can easily adapt as workloads evolve. This strategy enables them to take advantage of all the public cloud services and best-of-breed features according to their needs. Choosing an open, interoperable standard platform is critical to achieve this. Organizations can start small, modernize a few applications, and then templatize the approach.

The second trigger is around data strategy. Organizations are mindful of data compliance, privacy, and management needs, but also want data enablement, sharing, and monetization.

58% of organizations in the healthcare industry cite data monetization as the top priority to meet their digital goals, according to IDC's *2019 Digital Leaders Survey*. Moreover, 59% of European organizations will increase or maintain data-related tech spend in 2020 and 2021, despite overall IT spend going down during the pandemic, according to IDC's *COVID-19 Impact Survey*.

Benefits of an Open-Standards-Based Multicloud Approach

Benefits at a Glance

- Access to cloud-based innovation and capabilities without compromising on security and regulatory obligations
- Complete mobility of applications and data across cloud and on-premises infrastructure
- Demonstrable exit strategies; with containers and open standards, organizations can not only clearly define but also test and demonstrate their ability to migrate applications and data off a cloud provider (either to another provider or back on premises to the in-house datacenters)
- Avoiding the need to invest in the deep technical skills of a single cloud
- Freedom from over-reliance on a single provider to ensure that a cloud provider is not controlling the fate, speed, and IT journey of the enterprise
- Digital resilience, business continuity, and ability to adapt to unforeseen market conditions with a cloud operating model — in particular to protect against the risks of commercial failures and ensure survivability

How Multicloud and Open Source Address Europe's Open Strategic Autonomy Needs

The approach to digital sovereignty and open strategic autonomy has become a key topic for policy makers and organizations, particularly in regulated industries such as the public sector, finance, and healthcare across Europe. Regulated industries are looking to understand how they can achieve more control over data and infrastructure and broader autonomy from their third-party IT providers while continuing to innovate and benefit from cloud-driven transformation. At the same time, European policy makers and regulators are working to develop approaches to define digital sovereignty requirements and provide additional assurances to support the industry's secure and resilient move to the cloud. In this context multiple discussions have evolved across the EU to develop an approach to a trusted cloud, stimulate home-grown innovation, and facilitate European institutions' access to the most secure cloud services.

This approach needs to take into account the benefits of multicloud strategies and open source, which can ensure real portability and interoperability of data and systems in the cloud. It would also guarantee the openness of the European market to all the benefits of global cloud innovation, including those offered by international cloud service providers — as long as they share the core values of the European approach and adhere to the standards of openness, transparency, and security.

IDC believes that successful multicloud strategies are based on the foundation of open source and open standards because it enables organizations to minimize their dependency on third-

party technology providers and be more confident in meeting data sovereignty requirements. For example:

- Customers do not have to choose between retaining the ability to operate on premises autonomously from a cloud provider and accessing the benefits of public cloud. They can choose a combination of a hybrid and public (often multicloud) approach, reducing the overall reliance on one vendor and specific proprietary technology. This also paves the way for a range of technology to choose from.
- The emphasis on interoperability is consistent with the development of third-party competitor services, including in Europe and global markets, which will ultimately support local workforce and economic development.
- Customers can tap into the power of open source to collaboratively build the best and most open cloud environment.

Challenges and COVID-19 Recovery Journey Implications

The COVID-19 pandemic has had a profound impact on businesses and public sector organizations — and their IT spend. Over 90% of European businesses surveyed by IDC said they intend to change their long-term IT strategy in the wake of the pandemic, with many indicating an aggressive push to the cloud to build business continuity, resilience, and financial liquidity into business operations.

Cloud is the foundation of digital infrastructure and the pandemic has only accelerated the journey to the cloud as organizations see it as important for their crisis recovery. 2020 brought a shift in the perception of cloud services, with European organizations appreciating the benefits that cloud architecture provides. 67% of organizations cited maintaining or increasing IaaS investments in 2021 and 69% will increase or maintain PaaS spend in 2021, according to IDC's *COVID-19 Impact Survey* (December 2020).

The immediate crisis response has been focused on boosting digital resilience, starting with IT resilience, ensuring business continuity, and a focus on cost savings, and has often involved a cloud setup to support remote working, resilience, and risk management, as well as real-time automation. Many of these trends that came about in the pandemic (e.g., remote working) are here to stay in the long run.

IDC predicts that by the end of this year, 80% of enterprises will put a mechanism in place to shift to cloud-centric digital infrastructure twice as fast as before the pandemic.

Multicloud Strategies in Financial Services

Rising customer expectations and speed of innovation demonstrated by "challenger banks" create significant pressure on financial services organizations to rapidly transform and stay relevant. Digital experience is a competitive differentiator and a decisive factor in customer retention. IDC estimates that European banks' spending on DX initiatives amounted to \$17.4 billion in 2019 and will grow at 18.8% CAGR from 2018 to 2023. Customer onboarding, personalized and contextualized interaction, cyberthreat prevention, and core transformation are the key areas of investment.

Such enhanced digital services can be delivered on a highly scalable and agile platform such as cloud, which brings speed, logical security, and flexibility to businesses.

Cloud infrastructure (or IaaS) remains a key building block for digital innovation. But there's a growing concern among regulators about relying on a limited number of public cloud environments by financial services organizations as they bring their "crown jewels" applications to the cloud world. This is mainly due to following *perceived* risks:

- Security, data sovereignty, and compliance obligations (particularly GDPR and international regulations such as the CLOUD Act)
- Concerns about vendor lock-in, technology lock-in, and lack of data portability
- Loss of IT control around costs, speed of innovation, and outages
- Cloud concentration risk for the financial services sector — deeper penetration of fewer hyperscalers within financial services could increase dependence on providers and create a single point of failure, raising questions about the company's cyber resilience

While many financial services organizations in Europe still tilt toward an all-in-one cloud approach — citing management simplicity, benefits of deeper integration, and attractive cost structure — this view is increasingly challenged by regulators looking for solutions to avoid cloud concentration risk.

These considerations are prompting financial services organizations to adopt a multicloud strategy and open technology framework from the start, not only to ensure they benefit from the innovation and speed of the cloud, but also to mitigate risks. One of the top priorities for financial services organizations is to move toward a platform-as-a-service (PaaS) model built on containers, open APIs, and microservices to lay a solid foundation for future-proof innovation.

This trend marks a second wave of cloud adoption where organizations consider cloud for not just net-new applications but also to modernize their existing core applications. But the core applications have more robust requirements around security, reliability, availability, and compliance. Taking a platform approach — where existing applications can be modified or redesigned into open source container platforms and hosted on any cloud of choice — is seen as an important mitigant to third-party dependency risks. It also gives companies in regulated industries an alternative to simply "lifting and shifting" their core applications to one public cloud infrastructure and rigidly conforming to one architecture.

This approach equally helps complex financial services organizations bring culture change and encourage IT teams to view features such as automation and orchestration as a glue to DX and IT agility rather than eliminating IT operational tasks. They can adapt their ways of working to develop security guardrails, enable self-services, share app development blueprints and infrastructure best practices, and focus on high-value tasks such as security and data governance.

Case Study: Deutsche Börse Group — How a Multicloud Strategy Helps it Meet Resilience, Security, and Regulatory Requirements

Deutsche Börse Group, an international exchange organization and provider of financial market infrastructure, has adopted a multivendor strategy for cloud usage to avoid dependencies from single partner setups, make use of individual strengths, and have an "exit strategy" before moving to the cloud. It is meeting security and compliance concerns that are specific to the financial services industry, such as audit rights. How? Deutsche Börse Group's IT team has worked with multiple cloud vendors to set new contractual standards in the European financial services industry to make the cloud ready for regulated workloads. This way the company can take business-critical workloads to the public cloud. It is working with the cloud providers to add deeper integrations for an exit strategy, adding more data protection and info-sec features, redesigning its applications, and continuously auditing the approach. It is also adopting an open source container strategy to redesign its applications and optimize their security features.

Source: *Deutsche Börse Press Release, May 2020* (<https://deutsche-boerse.com/dbg-en/media/press-releases/Deutsche-B-rse-and-SAP-set-new-standards-with-cloud-usage-in-compliance-with-regulatory-requirements-for-the-financial-industry-1997312>)

Cloud Strategies in the Public Sector

The public sector across the U.K. and Europe is faced with growing demand for digital innovation to empower a citizen-centric transformation of services. This transformation is enabled by new architectural (e.g., microservices, APIs, containers) and operational (e.g., DevOps, site reliability engineers [SREs]) approaches that empower the sector to decompose legacy applications, connect citizens with digital services, and embed intelligence into core processes.

European public service leaders aim to deliver a new "ETHIC" for public services — efficient, trusted, highly responsive, inclusive, and convenient.

IDC research in 2020 shows that 62% of European governments consider "improving citizen experience, ensuring openness and transparency" as the top business priority. Improving user experience and collaboration, creating new services, and finding cost efficiencies were identified as priorities for the cloud strategy.

Cloud accelerates testing, developing, and deploying services that are natively designed for consumption across multiple channels (online, mobile apps, chatbots). It brings elasticity to meet usage spikes for high-volume services, like intake of tax declarations, student applications, farm subsidy applications, and emergency event management. It scales the ability to ingest data and process events coming from new sources, such as IoT data, or real-time analytics.

With the adoption of new architectural paradigms, the public sector must modernize its IT infrastructure with speed, elasticity, and automation, but at the same time ensure that security and data sovereignty are embedded in system design. This is especially a concern for those public sector organizations that have sensitive, personal information, or official secrets data.

IDC research reveals differences among European countries:

- **The U.K.**, as an early adopter of a cloud-first policy, cloud service provider certification guidelines, and cloud procurement frameworks and marketplaces (e.g., G-Cloud), leads the way with more than 30% of government organizations adopting public cloud.
- The two largest members of the European Union, **Germany and France**, have strict data sovereignty requirements. In particular, the French cybersecurity agency (ANSSI) mandates strict cloud certification guidelines, such as SecNumCloud. France is also developing a comprehensive national cloud of trust strategy. In Germany, the complexity comes from the high level of autonomy of regional and local governments that tends to fragment IT demand across levels of government. As a result of these governance and policy characteristics, the level of public cloud adoption in the public sector in the two countries has remained below 20%.
- Others, including **Spain, Italy, the Netherlands, and the Nordics**, have learned lessons from the U.K. and then cautiously followed a similar model of creating cloud policies, supplier certification guidelines, and governmentwide cloud contract frameworks. In **education**, cloud adoption has grown faster, with 35% of education institutions across Europe adopting public cloud and a further 20% planning to adopt it as an immediate priority. Source: *IDC European Tech and Industry Pulse Survey 2019–2020 (for more details, see [European Public Sector IT Infrastructure Transformation](#), IDC #EUR145685319); IDC European Multicloud Survey, 2020.*

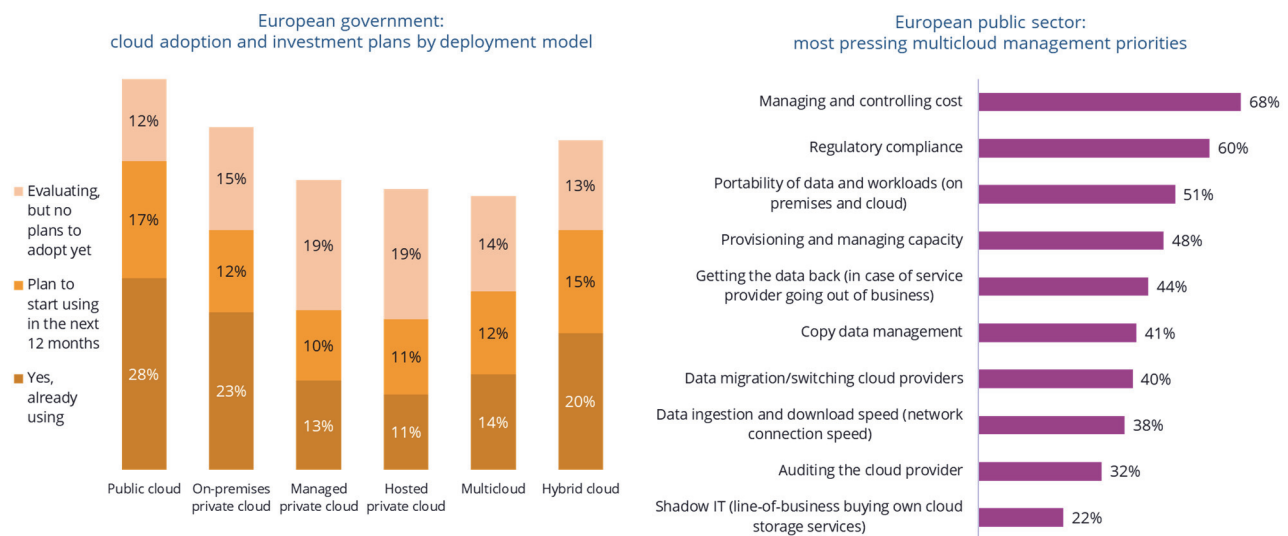
Cloud adoption in the European public sector remains well below the usual cloud penetration of 30%. The top barriers are:

- **Architectural constraints.** Government executives want data and workload portability across providers and the ability to integrate cloud with legacy systems. Overcoming the complexity of legacy architecture can bring business and technical benefits. At the technical level, it can minimize the legacy debt. On the business side, it can bring in speed, agility, and self-service.
- **Skills and culture shift.** Cloud is not just a technology but an operating model, and it underpins DX. As a result, it challenges traditional norms around IT architecture, nature of services, speed of business workforce, and skills. Navigating change management is a critically important component of cloud transformation.
- **Organizational barriers.** Government entities are local and have limited budgets. Their procurement policies differentiate between capital expenditure to acquire systems and operating expenditure to run them. And IT operating models often rely on a centralized function that manages IT assets and services. Cloud services require a shift toward operating expenditure, opex planning, and comprehensive transformation strategy.
- **Regulatory concerns.** Public sector executives need to comply with ever-evolving and complex EU and national regulations aimed at protecting privacy of personal data and resilience of critical digital services and infrastructure. Public sector organizations with little experience can risk security or network misconfigurations or not do proper due diligence.

In this context, multicloud has become a desired outcome in the public sector. However, governments have grown their multicloud adoption organically rather than strategically. They have acquired services from different providers, which helped them innovate rapidly. But to achieve the full benefits of multicloud, they now need to better integrate workloads and orchestrate services in a cost-effective manner. This will require stakeholder buy-in and a paradigm shift in people, process, and technology.

FIGURE 1

European Public Sectors Organically Building Multicloud Environments but They Need a More Strategic Approach to Address Management, Portability, and Compliance Challenges



Source: IDC European Tech and Industry Pulse Survey, 2019–2020 (n = 464, of which government 291 and education 173); IDC European Multicloud Survey, 2019 (n = 63 public sector)

Case Study: U.K. Department for Transport Embraces Cloud First

Governments have started to use cloud services for selected workloads, such as collaborative tools and web hosting. The migration of core systems to the cloud has proceeded more slowly because of architectural, regulatory, and organizational barriers. However, institutions like the U.K. Department for Transport (DfT) demonstrate that a full migration to cloud is possible. Prior to moving to the cloud, DfT had to maintain many servers, manage backups, and secure siloed systems, which resulted in simple utilization and querying tasks often requiring days to complete. The legacy infrastructure also made it difficult to scale innovative data sharing and analysis solutions.

To speed up the migration to the cloud, DfT worked with a number of global and local cloud service providers and partnered more closely with Google Cloud to deliver on a road map for a large proportion of its applications and underlying databases. To fully realize the benefits of such a cloud migration road map DfT went beyond lifting-and-shifting applications from on-premises to public cloud. It replatformed its systems and reimagined the business and IT service delivery processes. Source: <https://www.cloudpro.co.uk/cloud-essentials/public-cloud/8305/department-for-transport-turns-to-google-to-be-cloud-first-by>

Profile: Google Cloud's Anthos Open Platform

Enterprises have applications and data in a variety of locations, and they want the freedom to keep them there — or move them as needed. Flexibility reduces business risk, but it's only possible if applications are portable. Anthos, the managed platform based on open source technologies like Kubernetes, Knative, Istio, and Tekton that extends Google Cloud services and engineering practices to hybrid and multicloud environments, delivers that portability so customers can modernize apps faster and establish operational consistency across them.

Anthos is the heart of Google Cloud's hybrid and multicloud strategy. Google Cloud intends for Anthos to provide a single management console to deploy, secure, and manage all workloads in a consistent and unified manner across hybrid and multicloud infrastructure. The Anthos console and management API provide a central control point for unified analytics, operational practices, and policy-driven automation. IDC believes that this flexibility to build, run, and manage applications on any chosen infrastructure, without IT or developers needing to learn different environments and APIs, can truly make multicloud operational. This is especially advantageous for financial services and public services organizations, which typically have many custom apps and are heavily regulated industries.

Customer Voice

"As a provider of financial markets infrastructure we need to fulfill the high regulatory requirements of the financial industry. Our infrastructure needs to be fault tolerant, highly resilient, run 24 x 7, and meet stringent regulations of where data is, what info-sec standards are attached to it, what the exit strategy is — these are all considerations in our cloud migration journey. Together with GCP we are contributing to enhance security features and regulatory readiness, to the benefit of the financial sector." Lars Bolanca, EVP, Head of Corporate IT, Deutsche Börse

Customer Voice

"Our goal is to create an integrated and compliant banking platform that puts customers at the center of what we do. With Google Cloud and Anthos, we've gained powerful functionality and operational efficiency on the back end of our software to give customers the best possible experience. With Anthos, scaling our Kubernetes clusters up and down is really easy. On an average day, we handle 1 million logins, while during the national holidays, it can be four or five times that amount. Today, we never have to worry about meeting demand. We're saving time and money by using Anthos because it scales easily and takes care of security and upgrades. We've redeployed two full-time employees who were previously managing peak times to more value-added roles, and we believe that more opportunities like that are on the way." Dilek Duman, Chief Operating Officer, DenizBank

Conclusion and Recommendations

Policy makers and regulators want to create the right framework for cloud adoption in Europe among key industries such as financial services and the public sector because these are critical to the economy and are home to a lot of sensitive and personal data. Operational resilience and data sovereignty are key considerations that can be addressed with a multicloud and open source strategy, including container technologies.

Recommendations for Regulated Industries

- Adopt best practice for cloud operational models and usage patterns in collaboration with industry providers and share practices across different organizations. Bringing in expertise from trades and establishing a system of cloud ambassadors might be a useful practice, as well as creating multistakeholder forums to discuss adoption in the regulated sectors.
- Pivot to PaaS (and a platform-based approach more broadly) as a strategic cloud adoption model. Assess the application portfolio to determine which workloads to use and how to refactor/reengineer them and make them cloud ready rather than simply opting for a lift-and-shift approach that doesn't help realize full cloud benefits.
- Build a cloud center of excellence or embed cloud in the DevOps center of excellence to drive cultural change and build multicloud skills. To make the CoE strategy impactful, there are four areas the squad needs to focus on around cloud adoption — best practice (or patterns of cloud usage), DevOps centers, competency centers, and innovation centers. Ultimately, cloud needs to become a function within a business unit, rather than a separate IT entity.
- Evolve from accidental multicloud to intentional multicloud with open standards and a container-based approach. Nearly 70% of European organizations are already running multicloud environments, but management complexity, the ability to support all types of workloads, and inconsistency are key challenges. Addressing all the challenges and facilitating a build once/run anywhere vision along with core application modernization using open, container-based platforms will yield results. Organizations need to be mindful when selecting the container platform and opt for an industry-standard (CNCF-certified) container management platform to avoid any proprietary software-layer lock-in in the cloud. It also means enterprises don't necessarily have to invest in developing skills in the nuances of each cloud vendor to optimize their workloads.
- Address the main cloud-related risks in your industry through a multicloud approach. Aim to focus on business outcomes and skills development in the multicloud journey and demonstrate how it can also bring operational resilience and eliminate concentration risk, vendor lock-in, third-party dependencies, and single point of failure. In the financial sector these expectations are consistent with the regulatory requirements for exit planning under the EBA, ESMA, and EIOPA Outsourcing Guidelines.
- Given the emphasis on security, data protection, and governance as key challenges for enterprises and public sector organizations, evaluate how the platform helps overcome the complexity of data migration. Data has gravity and moving data frequently along with

the security policies can be difficult. The container platform that financial services or public sector organizations adopt needs to accommodate stringent data security measures such as encryption and anonymization, and enable federated access controls. Importantly, given the critical focus on security, data protection, and governance, organizations need to ensure that their platform can maintain consistent security and compliance controls across different environments.

Recommendation for Policy Makers

Multicloud is a long-term journey requiring commitment from multiple internal and external stakeholders. Ensuring organizations from regulated industries have access to all the modern technologies to improve their competitive edge and relevance in the digital world is of paramount importance to the region's economy.

Policy makers should:

- Endorse and stimulate cloud-driven innovation and portability, interoperability and openness through affirmative cloud-first policies.
- Lead by example — embrace multicloud and an open-source-based approach in their own organizations in the government sector and regulatory authorities that are moving to the public cloud.
- Clearly communicate the objectives of data regulations and the obligations of heavily regulated businesses.
- Work hand in hand with companies and technology providers to ensure proper audit channels are in place and share best practices or blueprints for success in multicloud strategies.
- Encourage use of open source and multicloud strategies through the relevant policies and by creating skills and talent development/support programs across the region.
- Work together to make data protection and regulatory compliance a competitive differentiator and not an innovation bottleneck.

Regulated organizations' adoption of cloud is guided by a range of regulatory requirements and standards. It is important to drive best practices to risk assessment to reduce fragmentation at the departmental level and make the process effective, outcome-based, and focused on understanding and mitigating risk.

It would be beneficial to create common frameworks to monitor cost-saving targets and long-term improvements achieved with the help of cloud through value-based assessment in regulated sectors. KPIs on the impact of improving public services and reduction of the costs of these services as a result of their digitization should be central to this approach, rather than just price-based validation.

Definitions

Microservices is an architectural approach to system and application design where applications are made up of several components. These small components can communicate with each other and enable the business to break away from monolithic apps. The basis for building

microservices is simple — every service needs to have just a single function and execute that function efficiently and securely. This means the application components have only a few hundred lines of code, so they are easier to understand, manage, and tweak. Microservices require considerable organizational and cultural adjustment to execute successfully.

Cloud Definitions

Public Cloud

IDC defines one major model for the public cloud world called, not surprisingly, public cloud. Public cloud services are shared among unrelated enterprises and/or consumers, are open to a largely unrestricted universe of potential users, and are designed for a market, not a single enterprise. Underneath this big umbrella, there are a growing variety of options available relating to public/private/VPN network connection, geolocation of data, options for dedicated data storage devices, and so forth. IDC considers all these features and potential future submarkets within the public cloud world.

Private Cloud

Private cloud represents a pool of resources that are shared within a single enterprise or an extended enterprise, with restrictions on access and level of resource dedication, and defined/controlled by the enterprise, beyond the control available in public cloud offerings. In the private cloud market world, there are three major options:

- **Hosted private cloud.** In this deployment model, service providers typically stand up a private cloud system that is fully dedicated to the customer for an extended duration. The hosted private cloud is a service provider owned and operated cloud IT service that is dedicated to one enterprise (or an extended enterprise) for a period of time that is typically months or years. In contrast with the public cloud models such as bare metal compute, hosted private cloud offerings are relatively static, with less automated deployment (longer time to deploy), longer-term contract commitments, slower scaling, and resources tightly bound to one customer (not easily redeployable) and not tied to the public cloud enhancement cycles.
- **Local cloud as a service.** In this deployment model, cloud service providers deliver a cloud system (hardware and software) that is fully dedicated to the customer for an extended duration and located on the customer site (or a colocation provider's site). This model is essentially a dedicated version of a publicly available cloud offering, modified to run in on-premises or a specially certified colocation environment, including outside of a traditional datacenter environment (edge). The cloud service provider retains full ownership of all underlying infrastructure hardware and software and is completely responsible for delivery, maintenance, updating, and ultimate disposal of the asset when the subscription is terminated.
- **Enterprise private cloud.** In this private cloud scenario, an enterprise typically either acquires a preintegrated cloud services system or integrates component software and hardware elements and operates the cloud service for its own use. The enterprise sometimes contracts with a third party for integration and/or operational services. An

enterprise private cloud may be run in the enterprise's own datacenter or may be colocated in a third-party facility where the enterprise has a direct facilities contract with the colocation operator. IDC sizes this market as the sum of the revenue for the cloud-enabling hardware and software products that make up the cloud services system plus any related spending on third-party services (e.g., integration, operation/management, and colocation). Enterprise private clouds — as they are owned/operated by enterprises for their own internal use — are not included in IDC's tracking of cloud IT services revenue. However, technologies used to build these enterprise private clouds are covered in their respective markets.

Hybrid Cloud

IDC defines hybrid cloud as the usage of IT services (including IaaS, PaaS, SaaS apps, and SaaS-SIS cloud services) across one or more deployment model using a unified framework. The cloud services used leverage more than one cloud deployment model. Hybrid cloud services include "public-public," "public-private," and "private-private" combinations. Cloud and non-cloud combinations (sometimes referred to as hybrid IT) where the non-cloud applications are front ended with cloud services interfaces (e.g., RESTful APIs) are also included. Examples include:

- A customer using a public cloud IaaS service while also consuming the same IaaS portfolio on a dedicated local cloud-as-a-service (LCaaS) platform in the customer's datacenter or edge location
- A customer using a hosted private cloud system while also consuming a dedicated LCaaS platform in the customer's datacenter
- A customer using a common cloud automation/operating environment (open or proprietary) across more than one public cloud and/or on an LCaaS, a hosted private cloud, or an enterprise private cloud

IDC is closely watching the continuing evolution of hybrid-cloud-enabling tools and technologies, such as those that provide much more real-time, dynamic deployment of cloud services across diverse private and public cloud models. Truly dynamic cloud service portability will likely require further refinement in how IDC categorizes cloud services. But this vision is currently still much more in development than actual deployment. IDC will wait until at least the next cloud taxonomy version (or whenever there's a significant amount of adoption of real offerings) to address this emerging approach.

Because hybrid cloud services are defined as combinations of (already sized and categorized) private, public, and non-cloud resources, from a market sizing standpoint (e.g., "how big is the hybrid cloud services market?"), IDC considers hybrid cloud services as an overlay of existing cloud services and traditional (non-cloud) markets — not as a separate market distinct from the public and private cloud services markets. IDC sizes hybrid cloud services adoption by researching what percentage of public and private cloud services (and non-cloud resources) is part of an integrated and/or coherently managed hybrid cloud environment. IDC's perspective is that the percentage of cloud services that is part of a "hybrid" environment will steadily rise to a majority in the coming five to seven years.

Industry Cloud

IDC defines industry clouds (ICs) as cloud platforms that enable multiple organizations in an industry to transact or collaborate toward common goals, such as improving industry insights, efficiencies, and/or capabilities. ICs can be controlled by multiple organizations/participants or by one primary owner. An industry cloud often resides on a public cloud but may reside in a private cloud environment when there's a smaller number of participants. Some ICs are open platforms or services that organizations may join freely, while others are commissioned and controlled by a group of named enterprises (occasionally called community clouds in some industries).

Industry clouds are designed to create broad industry value through initiatives like aggregation of cost reductions, operational benefits, risk mitigation, insight creation via pooling data/information, intra-industry digital capabilities, and increased access to markets. Participants may share technology, operations, and/or information. A cloud-based industry application would not be considered an industry cloud by IDC's definition unless it involves sharing or collaboration beyond shared public cloud infrastructure. Industry clouds can be segmented by how users participate through arrangements of communities, workspaces, industry marketplaces, and distribution hubs.

Conclusion

Operational resilience and data sovereignty are key considerations that can be addressed with a multicloud and open source strategy, including container technologies. Organizations, especially those in heavily regulated industries, should evaluate Google Cloud infrastructure and Google Cloud's Anthos open platform when building multicloud strategies.

About the Analysts

[Carla Arend](#), Senior Program Director, Lead Analyst, Cloud in Europe, IDC



Carla Arend is a senior program director with the European software and infrastructure research team, and heads up IDC's European cloud research. She provides clients with key insight into market dynamics, vendor activities, and end-user adoption trends in the European cloud market. She covers topics such as how European organizations are adopting cloud, how cloud drivers and inhibitors are evolving, cloud management, cloud security, data management in the cloud, IoT and cloud, AI and cloud, DevOps and cloud, as well as GDPR impact on cloud and cloud code of conduct. She also works on custom consulting projects, identifying opportunities in the European cloud market, and has authored white papers on subjects such as cloud management, cloud security, and data management in the cloud.

[Archana Venkatraman](#), Associate Research Director, Cloud Data Management, IDC Europe



Archana Venkatraman's primary research coverage is cloud data management. She covers multiple topics, including data protection, edge to cloud data trends, application and data availability, compliance, data integration, intelligent data management, DataOps, data quality, and multicloud priorities and trends. She also co-leads IDC's Cloud Practice and is an active contributor to IDC's European DevOps and AI research practices.

[Massimiliano Claps](#), Research Director, European IDC Government Insights



Massimiliano Claps is research director for the European IDC Government Insights team. His research empowers technology suppliers and professionals to embrace disruptive technologies, including artificial intelligence, edge computing, and augmented and virtual reality, to realize the benefits of strategic initiatives such as smart cities and citizen-centric government services.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.