Keeping cloud computing competitive

How multi-cloud solutions benefit the public & private sectors

Roland Berger

IEF

Preface

This year marks the 30th anniversary of the birth of the World Wide Web, but the concept of "cloud computing" – the sharing of servers or computing space – even predates the Internet. While the first waves of mass digitalization were driven by the personal computer and on-premise technology for business, now, after massive advances in computing power, capacity and connectivity, we are truly ready for the cloud computing age. A vast range of products and services are all being delivered via "the cloud", creating an enormous and fast-developing market.

As this study will illustrate, "cloud" actually has several meanings and levels, from infrastructure to software applications, presenting potential customers with a wide range of possible combinations. But whether a customer deploys a "single", "hybrid" or "multi cloud" solution, this trend is now unavoidable, not only for businesses, but also for public sector institutions.

As we highlighted in our previous study *Fair Play in the Digital Arena,* the digital economy can not only create global players seemingly overnight; it can also give dominant market positions to a few. And in some cases, e.g. search engines or mobile operating systems, this can lead to critical bottlenecks or even competitive abuse. The hypergrowth and dynamism of cloud computing is already starting to form a small group of main market players at several operating levels, which must raise the question: could we soon see another digital market sector produce dominant, duopoly or monopoly players?

With this study, we want to examine the cloud computing ecosystem, its potential impact on business and the public sector, and vice-versa. How can governments prevent strategic dependencies, increase cyber resiliency and – at the same time – foster innovation and competition? Further, how can the public sector wisely adopt this technology, especially given the diverse range of missions that governments have regarding data – some of which have to be made open by law, and some of which are top secret?

We would like to thank ORACLE for their support of this study and hope that its exploration of cloud computing's impact will help inform the debate about this crucial component of the digital economy. Our wish is that when the Internet turns 40, we don't look back and regret not having done more to safeguard competition in the wild days when cloud computing was young.

Prof. Dr. Friedbert Pflüger
Chairman,
Internet Economy Foundation

Clark Parsons
Managing Director,
Internet Economy Foundation

SIX KEYS TO INNOVATION AND DIVERSITY IN CLOUD COMPUTING. AS BOTH BUYER AND REGULATOR, THE PUBLIC SECTOR MUST LAY THE FOUNDATIONS FOR FAIR COMPETITION IN THE CLOUD.

IN THEIR CAPACITY AS BUYERS, GOVERNMENTS MUST ...

1. ... align their use of the cloud with strategic objectives
2. ... minimize lock-in effects by deploying multi-cloud solutions
3. ... create contractual obligations for interoperability and portability

IN THEIR CAPACITY AS REGULATORS, GOVERNMENTS MUST ...

1. ... drive the development of Europe-wide security standards for cloud computing
2. ... support self-regulation by cloud service providers
3. ... pursue the statutory regulation of cloud service interoperability as a last resort

Contents

1
TIME FOR ACTION TOWARD HEALTHY COMPETITION IN CLOUD COMPUTING

Sunny days in the clouds: Ever since Amazon began selling cloud-based storage solutions under the name Amazon Web Services (AWS) in 2006, the market for cloud computing has grown at a frantic pace. The volume of data handled by cloud-based data centers is currently eleven times higher than that handled by "traditional" means. In the next two years, the ratio will probably leap to 19:1. The market for cloud computing is already valued at around USD 200 billion – roughly twice what it was worth four years ago.

Scalability is the main reason why this technology is growing. Storage and computing capacity can be accessed and scaled (up or down) at short notice, letting everyone respond flexibly to changing needs. Cloud computing is not restricted solely to providing distributed IT infrastructure, however: It also lets market players use entire platforms to develop and/or operate digital services and applications that can be sourced directly in the cloud. Text files, for instance, can be processed in the cloud without users having to install an application on their local computer.

The diverse array of services made available via cloud computing is reflected in the varied landscape of cloud service providers: Alongside Amazon, Internet titans such as Google, Microsoft, IBM and Oracle likewise sell cloud computing services. They in turn are complemented by large cloud specialists such as Salesforce and a phalanx of niche providers. Now that the cloud is no longer pie in the sky, everyone – to mix our metaphors – wants a larger slice of the cake. But that, precisely, is becoming more and more difficult, as market share is increasingly concentrated in the hands of only a small number of cloud service providers. In infrastructure and platform services especially, there are signs that a handful of providers could dominate. Monopolization similar to what we have witnessed in the markets for operating systems, e-commerce and search engines is a real threat. Yet in the cloud sector too, that would deal a fatal blow to market diversity and competition. Customers – be they businesses, public authorities or private individuals – would have fewer offerings to choose from. Moreover, a lack of competition would stifle innovation and erode financial value.

There is still time to act! The market power of individual players is not yet as heavily concentrated as it is in other digital markets. In the latter too, though, the

Monopolization in the cloud market similar to what we have witnessed in the market for operating systems is a real threat.

"I am convinced that real and fair competition has a vital role to play in building the trust we need to get the best out of our societies, and that starts with enforcing our rules, actually just to make the market work for everyone."[1)]

Margrethe Vestager
European Commissioner for Competition

current dominance of Microsoft, Amazon and Google in their respective sectors did not emerge overnight. It was a gradual process, and competition regulators are now struggling to contain the impact of this market power. Would it not be far simpler to prevent such a concentration of power from accruing in the first place?

In this respect, governments must assume a dual role. The public sector is itself a major customer for cloud computing services. In this capacity, public administrations must support a balanced cloud portfolio as part of a multi-cloud strategy. In other words, they should source the most suitable cloud solution for each individual task area. True, such a policy requires more control and coordination than one-stop shopping for a single-cloud solution. But it also reduces dependency on individual providers. Multi-cloud strategies thus sharpen competition between different cloud computing players and help prevent individual companies from dominating the market.

In their second role – as legislators – governments establish the market conditions. Here, they must press ahead with pan-European standards to govern the security and interoperability of cloud services. Uniform security standards would enable smaller cloud computing providers in particular to sell their products across borders throughout Europe. Introducing common industry standards in cloud computing would also make it easier for customers to combine the services of different providers, or to "take their data with them" when switching providers. These common standards to reinforce interoperability and portability should be hammered out autonomously by self-regulating stakeholders. Statutory intervention in regulating the interoperability of cloud services must remain a last resort but cannot be precluded a priori.

This study is essentially an appeal for healthy competition to be upheld in cloud computing – especially in the public sector. We begin by analyzing the cloud computing market and describing the observable trend toward concentration. We then discuss the benefits and challenges of cloud computing and explain why companies are well advised to commit to multi-cloud portfolios rather than single-cloud solutions. This is followed by a detailed analysis of the public sector as a source of demand for cloud solutions, demonstrating how it can benefit handsomely from multi-cloud solutions. The study ends with a set of recommendations for political and administrative decision-makers. And it is here that the dual role of governments we have already mentioned comes into play: governments as buyers of cloud services, but also governments as lawgivers in the cloud market. Our study is based on interviews with cloud users and providers and with experts from both public administrations and the corporate sector. These interviews were augmented with analysis of extensive data and study materials.

2
TREND TOWARD CONCENTRATION IN CLOUD COMPUTING
A FAST-GROWING MARKET DOMINATED BY A HANDFUL OF PROVIDERS

2
Trend toward concentration in cloud computing

Intensive use is today made of cloud services, which have become a standard-issue strategic IT tool. This chapter traces the surge in usage in recent years, describes the provider landscape and identifies a growing trend toward market concentration. Before examining the cloud computing market, though, let us first make it clear what we are talking about. To do so, we will define cloud computing, outline the various provision and service models and explain the ways in which users can put together a cloud portfolio.

There is no single definition of cloud computing that is unanimously accepted by all users and experts. The latter often point to the definition promulgated by the US National Institute of Standards Technology (NIST), which the EU's ENISA (European Network and Information Security Agency) has also taken on board:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models and four deployment models.

The NIST definition was also used for the purposes of this study. The five essential characteristics of a cloud service are:

1. On-demand self-service
A consumer can tap and use resources (such as server time and network storage capacity) automatically whenever they are needed. No human interaction with the service provider is needed.

2. Broad network access
Services are made available over the network and accessed through standard mechanisms that support use by heterogeneous device platforms.

3. Resource pooling
The provider's computing resources are pooled to serve multiple users. Customers generally have no knowledge of the location of the resources provided, but may be able to contractually specify the location (e.g. a given region, country or data center).

4. Rapid elasticity
Resources can be provisioned elastically – in some cases automatically – and can therefore quickly be scaled up or down. To users, the resources appear to be unlimited.

5. Measured service
Resource usage can be monitored and controlled. Monitoring and control allow the use of resources to be managed and optimized, while also providing transparency for both the provider and the user.

Cloud services can be made available to users in four different ways, referred to here as "deployment models":

- A **private cloud** operates the cloud infrastructure for a single organization only. The infrastructure may be managed and operated by the organization itself or by a third party. Similarly, it may physically exist on or off the organization's premises.
- In a **public cloud,** services are made available to the general public or a large group of users.
- In a **community cloud,** the infrastructure is shared by a group of users with similar interests. It may be operated by a member of the community or by a third party.
- Lastly, a **hybrid cloud** is a composition of several cloud infrastructures for which standardized interfaces create data portability for shared use.

Cloud computing is made available via a variety of service models, most of which can be assigned to three rough categories: →A

- The **Infrastructure as a Service (IaaS)** model delivers individual IT resources – usually data storage capacity, computing capacity and networks – as a service. Customers can use this infrastructure to run their own services (such as operating systems and application programs). One benefit is that the infrastructure provided can be scaled up quickly as requirements grow.

- The **Platform as a Service (PaaS)** model goes a step further, letting customers use a self-contained cloud infrastructure as a platform. The platform includes standard interfaces and supplies customers with a broad spread of tools (such as databases and programming languages) for use in their own applications.

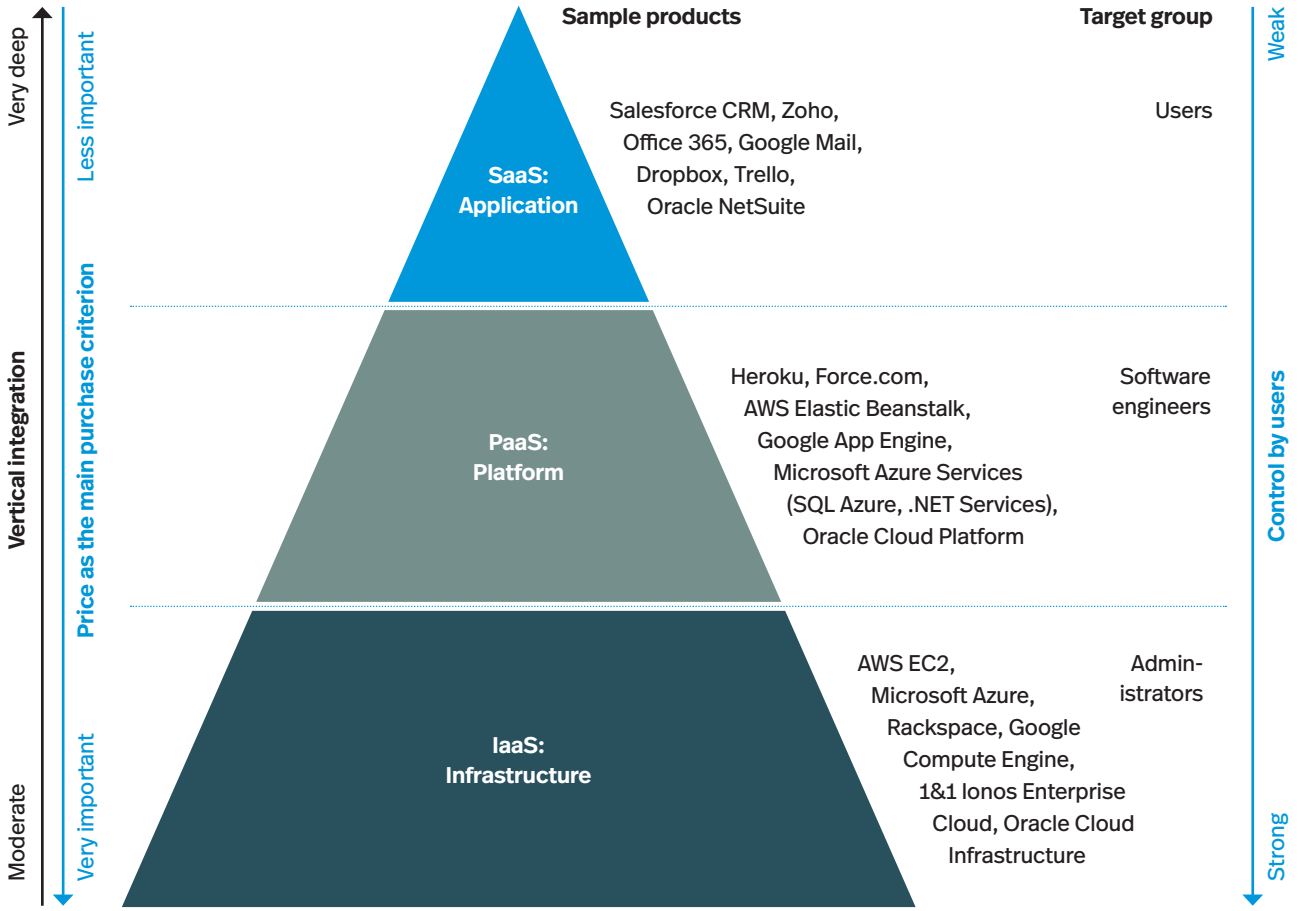
- The **Software as a Service (SaaS)** model focuses on the provider's applications, which customers can use in the cloud. In this case, the cloud infrastructure is merely a means to an end. The spectrum of applications is vast, ranging from contact data management to full-service financial accounting.

Price, the level of vertical integration and the degree of user control are the criteria that distinguish between these three service models. IaaS supplies users with infrastructure that they can use on demand. Cloud users retain comparatively substantial control: Physical capabilities and the price of the service are the key criteria determining the choice of a provider. Customers' control decreases as the level of vertical integration increases. So too does the importance of price in the purchase decision. SaaS services, for example, are tailored to specific applications. Accordingly, once customers have opted for this or that SaaS service, there is little they can then do to influence the design of the application. Price becomes only a secondary criterion in the decision process: The important thing is that the application in question meets the customer's specific needs.

Distinguishing between the various service models is important as we seek to understand how the individual segments of cloud computing market have evolved and how providers' market shares have shifted within these segments.

A The cloud service pyramid: Each successive layer – from Iaas to PaaS to SaaS – adds more value for the user

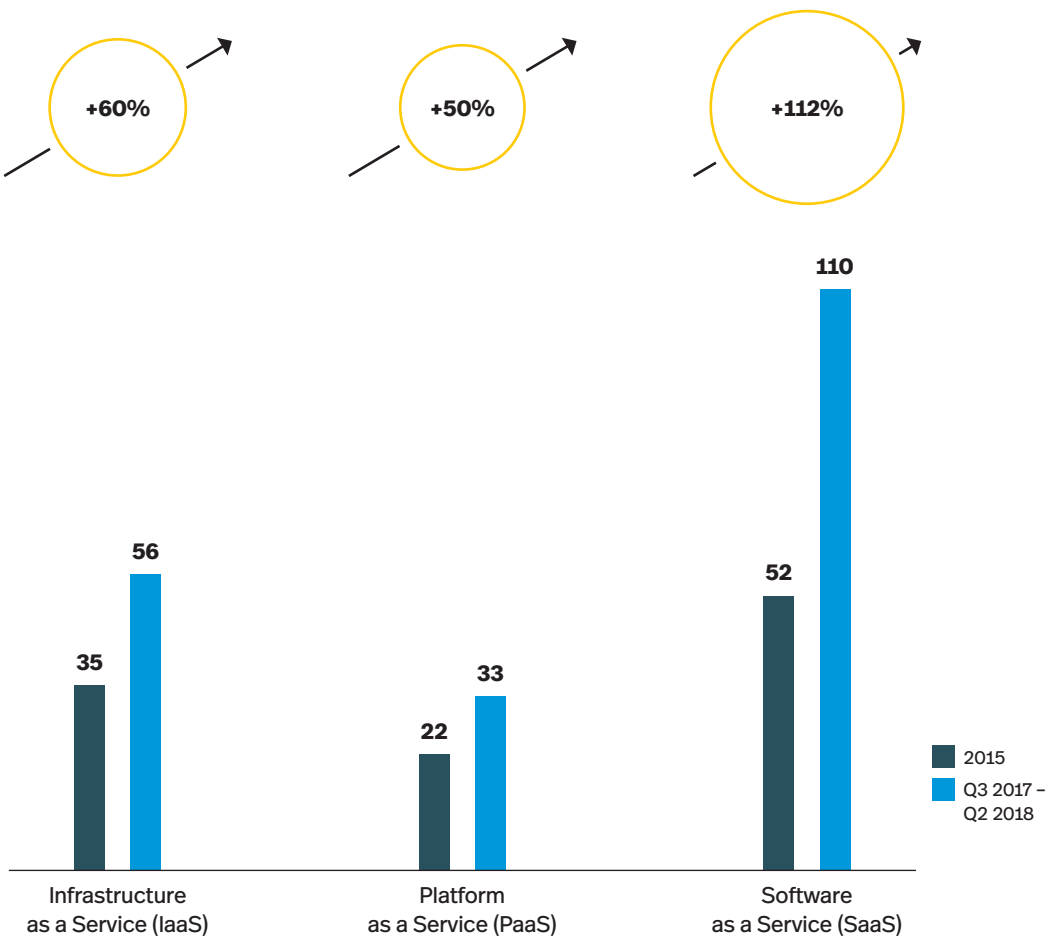
Characteristics of the different service models



Source: Roland Berger

B Surging growth in the cloud: Software as a Service in particular has seen revenue increase strongly in recent years

Global revenue in the market for cloud computing, by segment, 2015-2018 [USD bn]



Source: ITCandor, Statista

Global revenue in the three segments IaaS, PaaS and SaaS totaled USD 56 billion, USD 33 billion and USD 110 billion respectively in the four quarters from Q3 2017 through Q2 2018. →B SaaS is by far the largest segment and, in recent years, has also experienced the fastest growth. This is because incumbent software providers are shifting to cloud-based business models and successfully selling products as SaaS applications. Between 2015 and the period from Q3 2017 through Q2 2018, the SaaS market grew by 112%, the IaaS market by 60% and the PaaS market by 50%.

The processing of data is migrating from traditional to cloud-based data centers.

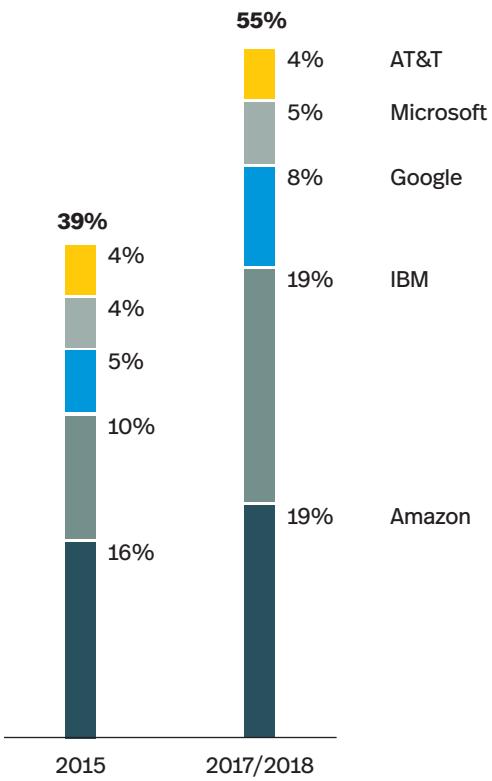
Rapid revenue growth in the cloud market reflects two developments. One is a sharp increase in the volume of data traffic handled by data centers (including traffic between data centers and users, between two data centers and within data centers) and the volume of data stored by data centers. According to the Global Cloud Index published in 2018 by Cisco, data centers handled 6,819 exabytes of data traffic in 2016. Annual growth of 24.7% is forecast to raise this figure to 20,555 exabytes by 2021. An exabyte is a thousand billion megabytes – 500,000 billion pages of text. The volume of data stored in data centers is projected to soar from 286 exabytes in 2016 to 1,327 exabytes in 2021, equivalent to an annual growth rate of 36%.

At the same time, the processing of data too is migrating from traditional data centers (i.e. the ones operated by companies and other institutions themselves) to cloud-based data centers. In 2016, the data traffic handled by cloud-based data centers (5,991 exabytes) was roughly seven times more than the volume handled by traditional data centers (828 exabytes). The ratio was already 11:1 (10,606 exabytes to 952 exabytes) in 2018 and is expected to increase to a factor of about 19 in 2021 (19,509 exabytes to 1,046 exabytes). From 2016 through 2021, the annual rate of growth in the volume of data handled by cloud-based data centers is put at around 27%. For the data volume handled by data centers not in the cloud, the rate of increase is just about 5%.

Across the market as a whole, global heavyweights such as Amazon, Microsoft and IBM line up against a plethora of small providers selling specialized products in clearly delineated markets. The firms that provide cloud computing also come from a variety of industries. The spectrum ranges from telecommunication companies (such as NTT, Vodafone and United Inter-

C Way ahead of the competition: Amazon and IBM lead the market in the IaaS segment

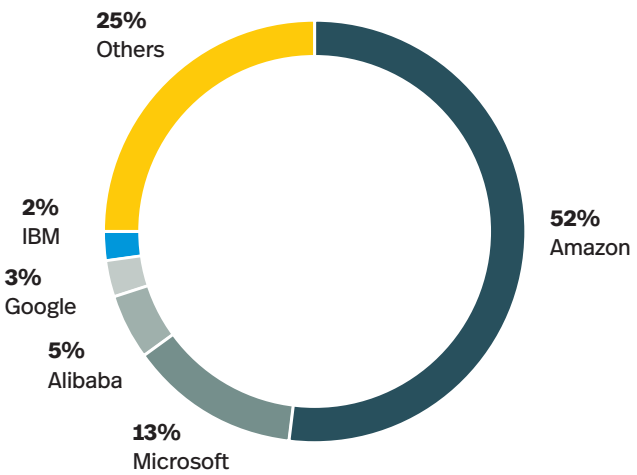
The top five providers' global share of revenue in the cloud-based IaaS segment [%]



Source: ITCandor, Statista

D Dominant Amazon: More than half of public cloud IaaS revenue in 2017 went to Amazon

The top five providers' global share of public cloud IaaS revenue in 2017 [%]



Source: Gartner

net) through IT service providers (such as IBM, Microsoft and Oracle) to companies set up expressly to sell cloud computing (such as Salesforce) and even online retailers (Amazon). Some of the smaller niche providers started out as spin-offs from larger IT companies. French provider Outscale, for example, was spun off from Dassault Systems in 2010.

The focus varies even among the big players. For instance, Amazon and Google lean very heavily toward infrastructure, whereas Salesforce concentrates on selling software and platforms via the cloud. Corporations such as Microsoft, IBM and Oracle are all-rounders whose strength lies in providing integrated end-to-end solutions across all segments. These different focal areas are reflected in the companies' shares of the market segments for IaaS, PaaS and SaaS.

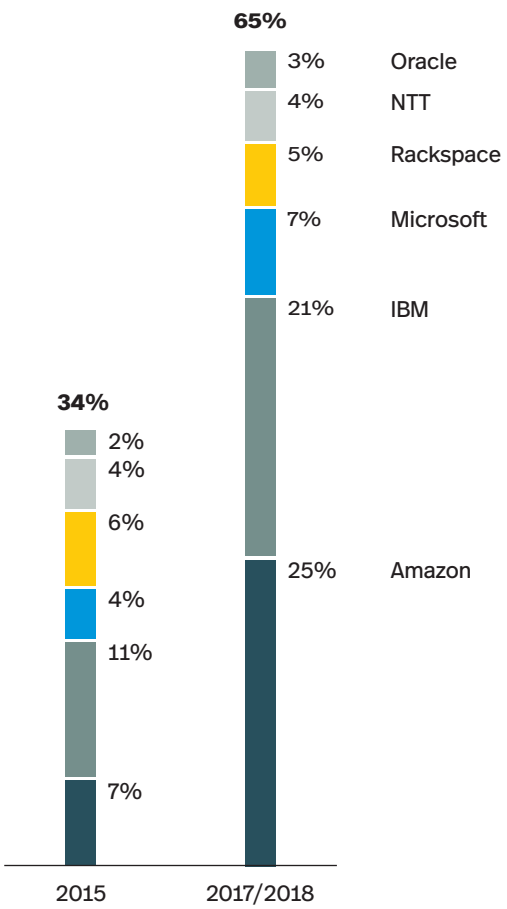
Infrastructure as a Service

Amazon and IBM have established themselves as the market leaders in the Infrastructure as a Service (IaaS) segment. Together, they accounted for a good 38% of global revenue in the four quarters from Q3 2017 through Q2 2018. →C Although both companies have lost market share since 2016, they are still miles ahead of Google in third place (with 7.6%). Microsoft (5.2% with Microsoft Azure) and AT&T (4.2%) follow on behind.

Amazon's strong position in the IaaS segment can be attributed to its dominant role in the market for public cloud IaaS. In 2017, more than half of the total revenue realized in this market went into Amazon's pocket. →D

E Out in front again: Amazon and IBM also dominate the PaaS market – Amazon has reached pole position in a very short time

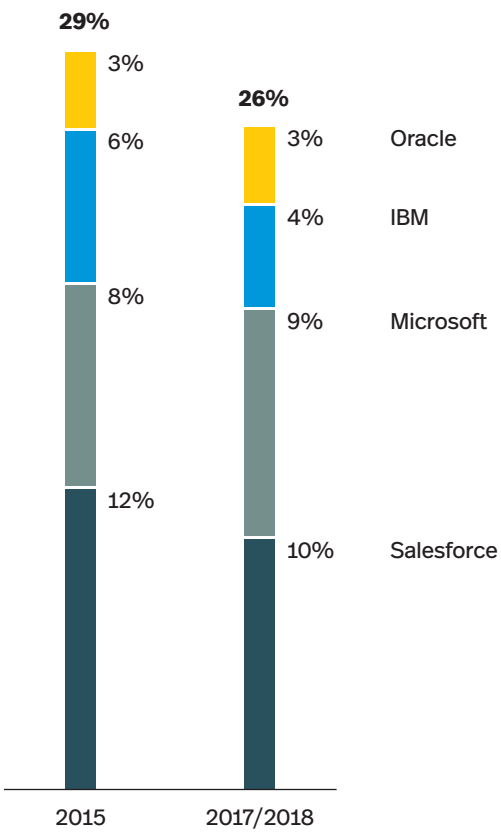
The top five providers' global share of cloud PaaS revenue [%]



Source: ITCandor, Statista

F Most fragmented segment: In the market for SaaS solutions, no one provider had a share of more than 10% in 2018

Top providers' global share of cloud SaaS revenue [%]



Source: ITCandor, Statista

Platform as a Service

The picture in the Platform as a Service (PaaS) segment is similar to that of the IaaS market. Here again, Amazon and IBM have carved up a large chunk of the market between them. Together, the companies netted more than 46% of total revenues in the four quarters from Q3 2017 through Q2 2018 . →E In a very short time, both players have succeeded in opening up a large lead over their competitors. To put that in perspective: IBM held a market share of just 11.3% and Amazon 7.3% as recently as 2015. IBM has seen its market share decline of late (from 28.0% in 2016 to 21.3% in the period from Q3 2017 through Q2 2018), while Amazon has virtually doubled its share of the market (from 13.3% to 25.5%), thus securing pole position in the PaaS market.

Software as a Service

Software as a Service is the most heavily fragmented of the three segments. As things stand, no one player has yet cornered more than 10% of the global market. →F The biggest provider is Salesforce (Q3 2017 through Q2 2018: 9.6%), closely followed by Microsoft (9.1%). Some distance behind, IBM (4.0%) and Oracle (3.3%) occupy third and fourth place respectively.

Our market analysis confirms what the experts we talked to said: While the provider landscape is still very diverse, a trend toward concentration is apparent, especially in the IaaS and PaaS segments.

This trend toward concentration could threaten the diversity of the provider landscape. In a worst-case sce-

nario, it could lead to the kind of market domination we have long experienced in the realms of software (Microsoft), online retail (Amazon) and search engines (Google) – and that in one of the key disciplines of the future at the hands of companies that already dominate other digital sectors!

In the chapters that follow, we explain how multi-cloud solutions can combat these concentration tendencies while at the same time empowering customers to put together the best solutions for each requirement. We also show that, above and beyond the corporate community, governments too play an important role – both as customers and as legislators. It is very much easier to prevent the monopolization of individual markets in the first place than to regulate their repercussions when they are already a fait accompli.

The trend toward concentration in the cloud market could threaten the diversity of the provider landscape. In a worst-case scenario, it could lead to the kind of market domination we have long experienced in the realms of software, online retail and search engines.

3 DIVERSITY AND FLEXIBILITY

MULTI-CLOUD SOLUTIONS CAN MITIGATE THE DRAWBACKS OF INDIVIDUAL CLOUD SERVICES

The history of the global economy is also a history of growing interdependencies between companies, industries and regions. In the last ten years, complexity has increased significantly as digital technologies have continued their triumphal march. The digital transformation has replaced inflexible value chains with dynamic value networks. The real-time availability of virtually all information of relevance to value creation enables processes to become more efficient. Capturing and analyzing the data generated by production machinery allows outages to be forecast, for example. Maintenance planning can thus be improved and production downtime minimized. At the same time, the omnipresence of data opens the door not only to more efficient processes, but also to entirely new data-driven business models. In the latter, value creation is rooted solely in collecting, connecting and analyzing data. Search engines such as Google and online brokers such as Airbnb are successful examples of these exclusively data-based business models.

Modern organizations depend on powerful infrastructures to cope with huge volumes of data

If companies are to derive benefits from mass data, they must be able to store and process that data. All data users, be they humans or machines, must have access to the data they need for the task at hand. A logistics department, for example, needs real-time access to stock levels, the status of current orders and production's material requirements. It must be able to integrate all this data in its own logistical processes. At the interface to the customer, too, this data is critical for showing customers delivery times before they place orders, for instance. Data generated at the customer interface must then in turn be fed back into the business processes. One benefit is that production can be optimized in light of recurrent patterns of demand.

Companies have long made use of central IT resources

Powerful infrastructures are needed to stay in control of these large volumes of data. Since the 1950s, businesses have turned to central IT resources that are shared by the users. The concept of sharing computing capacity via remote access has long been in operation via everything from mainframes to client/server architectures in local area networks to the rise of web-based applications at the end of the 1990s. In the last ten years, cloud computing technologies have gained a foothold as important elements in modern corporate IT landscapes, as attested by recent figures published by Eurostat:

- More than every fourth company in Europe made use of cloud computing services in 2018. The proportion has risen by 37% since 2014.
- More than half (56%) of all large companies (with more than 250 employees) used cloud computing services in 2018, an increase of 60% since 2014.
- Cloud computing is used primarily for communication (e-mail) and data storage. Two thirds of the companies that use cloud computing utilize these services.

“Cloud providers have understood that IT security is a selling point that users see as increasingly important to master the challenges of digitalization.”[2)]

Arne Schönbohm
President of the German Federal Office for Information Security (BSI)

Cloud computing delivers scalable IT resources via outsourced infrastructures …

The users of cloud computing technologies benefit by outsourcing all (or selected) IT services to a third party. This party could be part of the same organization – for example if the IT department operates as a separate profit center, providing services to the other departments on the basis of a private cloud. Alternatively, cloud computing services can also be sourced in the public clouds operated by external providers.

In either case, the IT infrastructure is outsourced, in return for which required services such as storage, computing power and e-mail are purchased. Since payment is linked to the services used, cloud computing gives companies greater flexibility: If the need to deal with occasional peak workloads demands more substantial IT resources than those needed for routine operations, the cloud can make extra capacity available at short notice. Peak demand periods can thus be accommodated flexibly without customers having to buy the necessary infrastructure. In periods of slack demand, less capacity is sourced in the cloud.

This arrangement can yield benefits for both the providers and users of cloud computing services. Cloud users can save on capital spending and running costs, as they do not have to keep IT infrastructure available that is only needed to handle occasional peak loads. Cloud service providers can make their infrastructure available to all kinds of internal and external customers to ensure that capacity is well and evenly utilized. The performance and security of their systems is pivotal to their business model, so cloud service providers constantly invest in their infrastructure. Here again, cloud users reap the benefits without having to commit to heavy investments of their own.

Above all, cloud computing can help make companies more agile as they develop and launch new products. New projects can be tackled without first having to create a dedicated IT infrastructure. Startups, for example, can respond to fast-growing customer numbers without difficulty thanks to cloud computing. In the first year after it was founded, users uploaded more than 100 million photos to the social media app Instagram. The company was only able to cope with this astronomical growth by using cloud computing, harnessing the resultant flexibility and drawing on practically unlimited scalability. →G

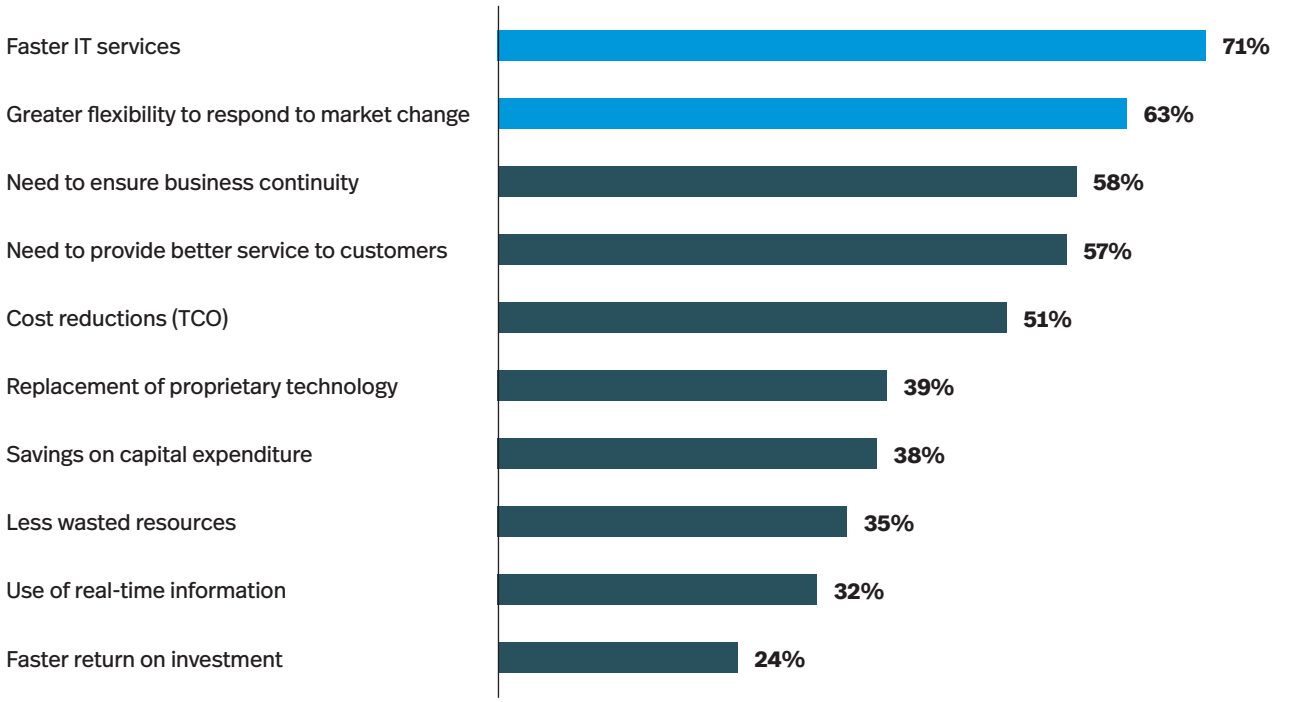
… but also harbors risks with regard to security and cost

In the context of digital data security, a distinction is drawn between information security and data protection.

Information security concerns the protection of data against unauthorized access or loss. Since they are so highly specialized, cloud service providers can guarantee a very high level of security and extremely robust reliability – usually what is known as a monthly uptime percentage of at least 99.5%. Given that this level of availability still admits the possibility of more than 3.5 hours' downtime per month, availability levels of over 99.9% can also be purchased. Additionally, cloud service providers can

G Speed and flexibility: Companies see investing in the cloud primarily as a way to become more agile

Corporate goals as drivers of cloud investments and initiatives in 2018 [% of respondents]



Source: IDG Research

offer powerful protection against data loss by creating redundant system structures and replicating data across several data centers. Cloud service providers therefore normally deliver very high levels of availability and data security. Yet even cloud applications can experience large-scale failures: In 2017, an operating error by leading cloud infrastructure provider AWS triggered outages at 54 of the 100 largest online retailers in the world.

Besides the issues of availability and data security, though, the protection of confidential and personal data is another important aspect for companies. Especially in the case of cloud service providers with a global

reach, cloud users need to check very carefully under whose jurisdiction their data falls. Based on the EU-US Privacy Shield, European companies can transfer personal data to US companies in compliance with the EU's General Data Protection Regulation, provided the American companies possess a valid Privacy Shield certificate. At the same time, what is known as the US CLOUD Act states that US government authorities can access data on EU citizens in the context of criminal investigations if this data is processed by a US company, irrespective of where the data is physically stored. Notwithstanding, the disclosure of personal data on the basis of the CLOUD Act may be found to violate the provisions of the General Data Protection Regulation. This situation can create a dilemma for US cloud service providers, who run the risk of infringing either US or European law. European cloud service providers do not have this problem.

The cost of cloud computing services is another source of risk. When opting for or against the purchase of one or more cloud services, it is important to know how long it will take to actually migrate the applications and data concerned to the cloud. The longer it takes, the later the customer company will realize the benefits associated with the cloud. On top of upfront investments, running costs too can be a serious risk factor. The fact that cloud computing resources can be accessed at short notice and without complications also implies that the associated costs must be monitored very closely. In large organizations where numerous departments independently make use of cloud computing resources, it is often hard enough to simply find out how much money is spent on cloud computing. Companies are aware of this problem, though, and cite the cost of cloud computing as one of their most important challenges. →H

Integrated single-cloud ecosystems could create a lock-in effect

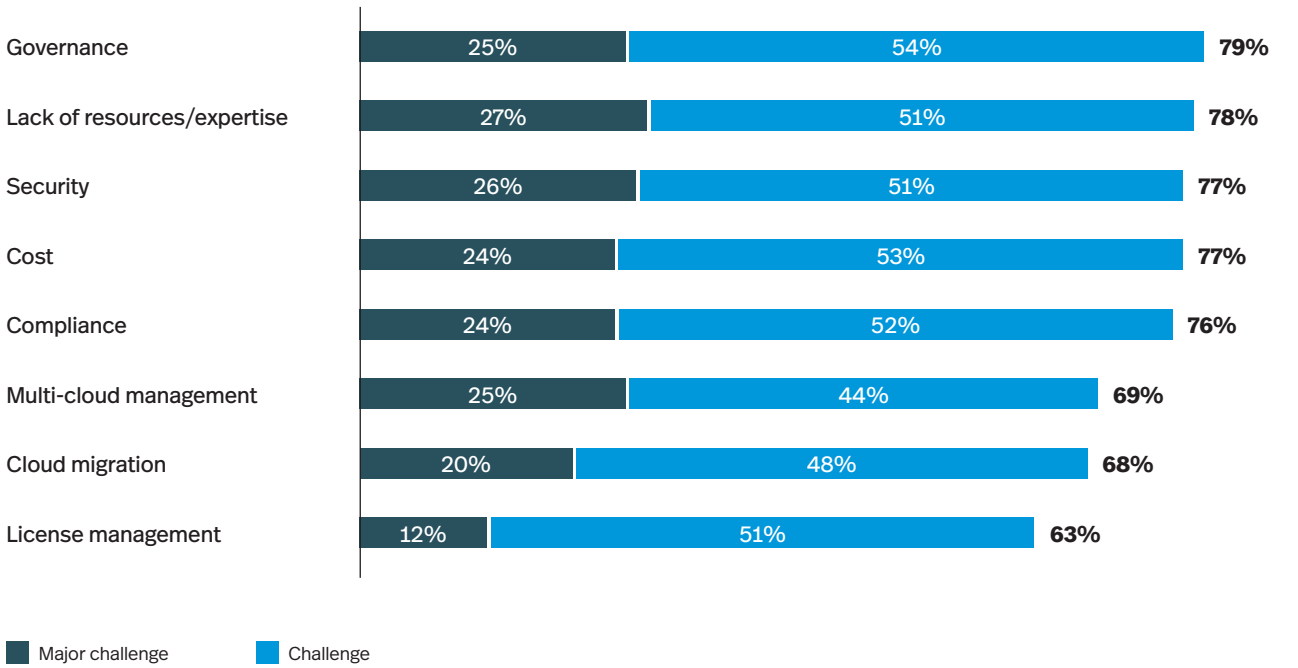
Aside from privacy and cost concerns, the biggest threat arising from the use of cloud computing services is what is referred to as the lock-in effect (see box). This effect materializes when customers stay loyal to a given cloud service provider not because they are satisfied with its performance, but because high barriers prevent them from switching to an alternative provider. Market mechanisms in the cloud sector are similar to those in the context of digital platforms. Like Google and Facebook, for example, cloud service providers set up entire ecosystems within which customers can access a whole raft of different and mutually compatible cloud services.

As with digital platforms, these ecosystems generate tangible benefits for customers by bringing all relevant cloud applications together in a one-stop shop. Most also have their own interfaces to third-party applications. These allow providers to incorporate third-party developments in their own platform to further boost the utility to customers while also making themselves indispensable as customers' interface to third-party suppliers.

For customers, the downside of this kind of cloud ecosystem is the lock-in effect. Because the proprietary standards used by the provider are the easiest way to combine the various applications (databases, containers, search functionality, content management) and data in the cloud, customers who want to change their cloud

H The risk factors: Companies consider personnel, security and cost to be among the main challenges

Challenges to companies that use cloud computing [2019, %]



Source: RightScale 2019 State of the Cloud Report

service provider face high costs to migrate their applications and data.

Another consideration is that the first step into the cloud is always the most difficult one. Applications and data are only ever migrated to the cloud at the end of a lengthy process of selecting the right cloud strategy. This alone creates a stronger incentive to also use the same cloud solution for other applications (completely new ones, for instance), even if a different cloud service provider has a solution that fits better for a given application. This effect – where more data follows the initial data migration to a certain cloud – is labeled "data gravity". It causes companies to quickly store large volumes of data with a single cloud provider. However, if they then want to migrate that data to another cloud, physical con-

straints are quickly reached: Even if a company has stored only 100 terabytes in a cloud – equivalent to the storage capacity of just 100 modern business notebooks – it would take more than 90 days (more than 13 weeks!) to physically transfer that data to another cloud, even if a 100 Mbit/s line were used to full capacity.

Precisely these mechanisms induce customers to develop close ties to a specific cloud service provider – and thus to fall into a dependency trap that can have serious consequences: If customers are no longer happy with the price or availability of new applications at their existing cloud service provider, moving to a competitor will prove very expensive. The danger is therefore that customers will shy away from this expense and simply put up with a suboptimal cloud solution. This erodes the flexibility that cloud computing delivers in principle and undermines customers' potential to quickly develop and launch new products. If the worst comes to the worst, the cloud provider's application landscape and capacity could end up defining the limits of customers' ability to innovate and grow.

Lock-in effects can be reduced with the aid of multi-cloud solutions

The cloud computing risks outlined above can be substantially reduced by combining several cloud solutions. What are referred to as multi-cloud solutions are based on the idea of picking the best provider on the market for each different cloud-based application. A company's applications and data are then spread across a number of providers. That improves overall security by allowing higher levels of security (which are more expensive) to be chosen for sensitive data than for non-sensitive data. A multi-cloud strategy also guards customer companies against lock-in effects. Dependencies can still arise in the case of highly specialized applications, where a suitably specialized cloud service provider is indispensable. The company as a whole nevertheless retains sufficient flexibility to commission different providers for different applications and projects. Another benefit is that multi-cloud strategies enable companies to benefit more from price competition between different cloud service providers.

Multi-cloud solutions will succeed only if users can cope with the complexity of a multi-cloud strategy. Customers must therefore possess a very thorough knowledge of what the market has to offer in the individual segments, including the benefits and drawbacks of each. Only then can the best cloud service provider for each application be selected. On top of that, a multi-cloud solution inherently adds to the burden of control and coordination: To keep costs from spiraling out of control, companies must keep a close and constant watch on how much cloud computing capacity they are using. If they fail to do so, they run the risk of having different departments source similar applications with different cloud service providers – or of concluding parallel contracts with one and the same provider. That would both generate unnecessary costs and, possibly, lead to security headaches: Where there is confusion about what data is in which cloud and who can access it, data can be lost or abused, and privacy violations are a real threat.

The comparison of the benefits and drawbacks of single and multi-cloud solutions shown in Figure I makes it

CAUGHT IN THE CLOUD – THE CONSEQUENCES OF CLOUD LOCK-IN

Lock-in effects occur when a customer becomes so closely tied to a product that high barriers must be surmounted in order to switch to a rival product. Such close ties to the products of a given vendor often result from the use of proprietary (i.e. non-open) or patent-protected standards. That, for example, is what happens with self-contained operating systems that offer good compatibility with other systems from the same vendor, but that are scarcely compatible with the products of competitor firms. Initially, customers reap benefits from using a product with proprietary standards, for instance because compatibility across all the vendor's products supports a single sign-in feature, customer service from a single source and a more predictable user experience. Conversely, though, high barriers to migration also allow the vendor to demand higher prices or keep customers loyal even though rival products may be of a better quality.

The same kind of effects can be seen in cloud computing, where they are called cloud lock-in. Here, cloud users refrain from switching to a cheaper or more suitable competitor product because it would cost them so much to change their cloud service provider. Once they have opted for a cloud, they effectively find themselves caught in it. One reason for this phenomenon is the use of proprietary cloud services with no open interfaces to migrate data to other providers.

The social media platform Instagram experienced this situation at first hand: After its inception in October 2010, it was able to master rapid growth in user numbers only by using cloud computing. Specifically, the company used EC2, a highly scalable solution from Amazon Web Services (AWS). When Instagram was acquired by Facebook, the latter wanted to migrate the data to its own data centers. Due to a lack of standardization, however, that turned out to be a tricky undertaking. In fact, it was only possible at all by taking a detour through a virtual AWS private cloud. It took almost a year.

Cloud lock-in can also be problematic if the cloud service provider files for insolvency. US cloud service provider Nirvanix, for example, announced in 2013 that it was pulling out of the business. Customers had only 30 days in which to back up their data. The problem in such a situation is that, if customers have stored large data volumes in excess of 100 terabytes in the cloud, transferring that data over the Internet will itself take several weeks. At the same time, another (compatible) cloud solution must be ready and waiting to take all the data. Failing that, customers will have to store the data on their own servers. Assuming they have the capacity: One reason why data is stored in the cloud in the first place is so that customer companies do not have to keep suitably dimensioned infrastructure available themselves.

These examples show that cloud lock-in is not just a theoretical danger: It can lead to very real difficulties and costs for users. On the SaaS level in particular, technical constraints mean that portability and interoperability can be implemented only to a very limited degree. This being the case, companies should mitigate the danger of cloud lock-in by adopting a strict multi-cloud strategy that keeps them from becoming dependent on a single provider.

clear that – all things being equal – multi-cloud solutions are the better option. →I Single-cloud solutions certainly score points for their ability to provide an ecosystem of integrated applications, consistent support and a single sign-in feature for a wide array of services. However, the ecosystem constellation is also the biggest downside to single-cloud solutions as it leads to serious lock-in effects. The risk of information losses or violations of privacy laws by the provider are also concentrated in this scenario. Lastly, single-cloud solutions generally fail to do justice to all of a company's applications: They are at a disadvantage compared to specialized solutions.

Multi-cloud solutions are better able to deliver innovation

Multi-cloud solutions have the edge with their best-of-breed approach: Each application gets the cloud solution that is best suited to it. This strategy sidesteps the a priori restrictions imposed on new developments and innovative products by a single-cloud provider's portfolio. The development and implementation of innovative ideas does not have to be watered down to fit the capabilities of the existing single cloud. Instead, the best cloud solution is purchased to fit each individual innovation. →J

I Advantage multi-cloud: Opportunities and risks inherent in single and multi-cloud solutions

	Single-cloud solution	Multi-cloud solution
Opportunities/ benefits	• Single sign-in (central access) • Single point of customer service • Less control and coordination	• Flexibility – best solution for each application • Innovation • Spreading risk improves security • Less dependency on individual providers • Performance
Risks/ drawbacks	• Vendor lock-in • Cluster risk – all your data with one provider • One-size-fits-all approach does not do justice to all applications	• More control and coordination

Source: Roland Berger

"While the transition to cloud services offers many tangible advantages, such as business efficiency and technical flexibility, the migration to cloud environments does also come with challenges, from a legal, technical or security standpoint." [3)]

Mariya Gabriel
European Commissioner for
Digital Economy and Society

A further consideration is that multi-cloud solutions are a good way to ensure greater security for the customer company's data. That begins with the fact that multi-cloud solutions automatically involve storing data with more than one cloud service provider. The risk of information losses is thus spread, and the likelihood that all cloud-based applications might fail across the board is vastly reduced. Multi-cloud solutions also allow applications and data to be split up according to their varying security needs. Non-critical applications, for example, can run in a cloud offering regular levels of security. For sensitive applications that process personal data, for instance, a private cloud with a high level of security might be a better option.

J Strength through diversity: Using multi-cloud solutions opens up many and varied benefits

Flexibility

- The best solution on the market can be purchased for each application
- Especially for new applications, the most suitable cloud can be added flexibly

Innovation

- An innovative cloud solution can be sourced for innovative applications
- The cloud thus follows the organization's innovations, not vice versa

Security

- Risks can be spread across several clouds and a number of providers
- Sensitive data can be protected in specially developed clouds

Multi-cloud computing

Independence

- Dependency on individual vendors is curbed
- That gives customers greater freedom and makes it easier to switch between cloud providers

Performance

- A cloud as close as possible to the user's physical location can be chosen for latency-critical applications, for example

Source: Roland Berger

The resultant multi-cloud flexibility likewise pays dividends in terms of the performance of individual cloud services: Latency-critical applications, for example, can be entrusted to a high-performance cloud in close physical proximity to the users.

Open standards make cloud computing more flexible

Using multiple clouds lets companies reduce their dependency on individual cloud service providers. However, to achieve this end, it is important to avoid the use of proprietary cloud architectures in the form of interfaces, database systems and containers, and instead to go the way of open standards – as far as this is possible. Proprietary standards make it easier to work across different applications within one cloud, but they make it harder to migrate those applications to another cloud. Using open standards simplifies the task of moving individual applications back and forth within a multi-cloud environment. That explains why it is increasingly attractive for users to back open solutions such as OpenStack, whose technology makes them more open to different platforms and thus gives the user greater freedoms.

The majority of companies commit to multi-cloud solutions

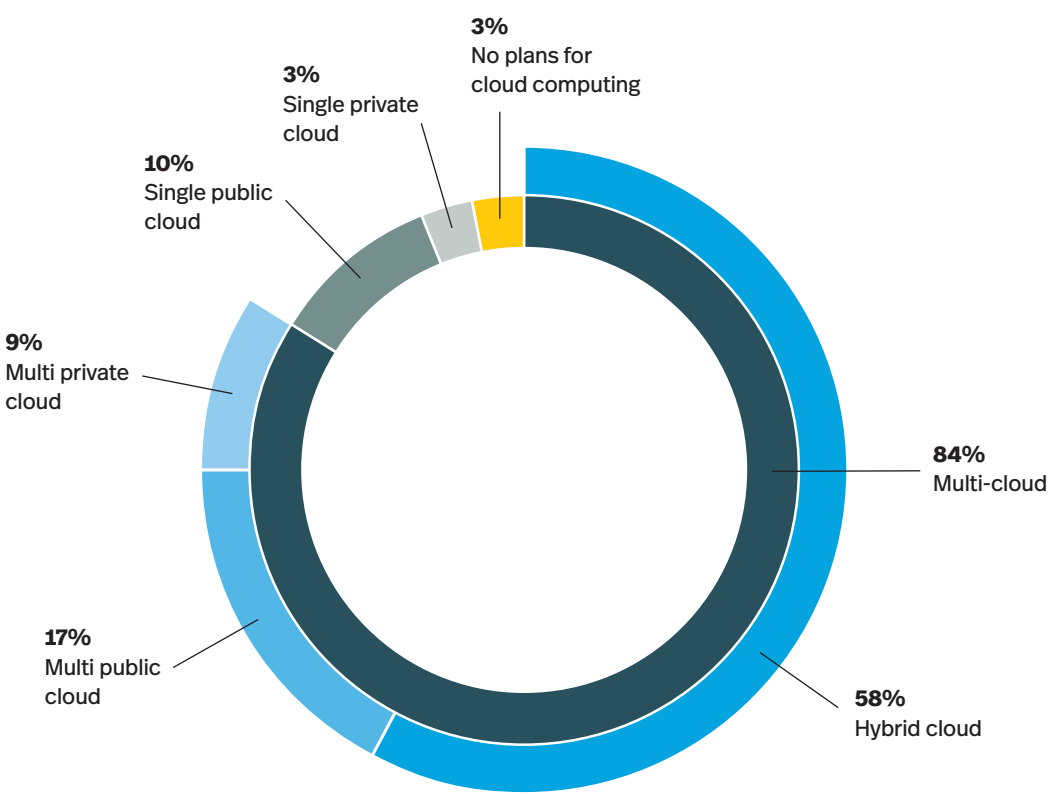
Using multiple clouds is already common practice at most companies. Surveys show that only a small proportion of companies use single-cloud solutions. →K More than half of the respondent companies prefer a combination of public and private clouds. Every sixth company uses more than one public cloud, and every tenth company has several private clouds.

Overall, then, multi-cloud strategies offer more than just theoretical benefits compared to single-cloud solutions. Many companies already rate them as more advantageous in day-to-day practice. Lock-in effects can still occur in a multi-cloud context – for example where business-critical tasks are based on the proprietary applications of just a single cloud service provider. That said, using – and intelligently managing – multiple clouds can combat many of the drawbacks of single-cloud solutions.

Alongside private and corporate users, public administrations too have increasingly moved over to cloud computing in recent years. Cloud services can benefit government organizations above all where efforts are being made to ramp up e-government. The chapter that follows discusses the requirements the public sector places on cloud computing and looks at how they can be met by multi-cloud solutions.

K Business community shows the way: Four out of five respondent companies worldwide operate multi-cloud strategies

Cloud strategies at companies with more than 1,000 employees [2019, %]



Source: RightScale 2019 State of the Cloud Report

4

MULTI-CLOUD SOLUTIONS AS THE WAY FORWARD FOR PUBLIC ADMINISTRATIONS

COMPLEX NEEDS DEMAND VERSATILE SOLUTIONS

It's not just private sector companies that generate huge volumes of data every day; public authorities and whole governments do too. Some of this data can, for instance, take the form of traditional case files. Taken together, Germany's local courts completed over 662,000 sets of criminal proceedings in 2016 – more than 2,600 per working day. Added to that is the data increasingly churned out by machines. Sensors for traffic control systems and in weather stations are constantly generating data that all has to be stored and analyzed. Something like 1,000,000 reports from ground stations, shipping vessels, aircraft, radar stations and weather satellites arrive at the German meteorological service DWD every day, with the consequence that the service measures its data volume in terms of petabytes (millions of gigabytes).

In light of such vast quantities of data, of which this is only one example, public administrations face challenges of at least the same magnitude as the corporate community. Large amounts of data have to be stored, processed and exchanged between different organizations and organizational units, not to mention the need for compliance with statutory documentation regulations. It follows that the benefits of cloud computing described so far also apply to public authorities: Using cloud technologies is an excellent way to place vast IT capacity at the disposal of public-sector agencies and organizations on a flexible basis.

There are nevertheless three major differences between companies and public administrations that lead to the special requirements for cloud computing in the public sector described in this chapter.

1. Public authorities operate in a complex cosmos of political stakeholders, government agencies and individual citizens, all of whom have varying needs that they can assert – or at least express – on the basis of legal norms, service orders and/or applications.

2. This heterogeneous stakeholder landscape combines with a broad spectrum of activities to force public administrations to work with all kinds of different data types. Some of these – the raw data from government reports, for example – have to be made available to all citizens in line with the open data principle. At the same time, authorities also work with personal data and other information ranging from confidential to top secret.

3. IT systems used in the public sector must satisfy the highest standards because, as well as safeguarding personal data, they must also uphold the security and reliability of the system of government as such. Security agencies in particular therefore depend on IT resources that maximize protection against unauthorized access – even from other countries.

To meet these specific requirements, cloud computing can play an important part in the IT portfolios of public authorities. The public sector does, however, place higher demands on cloud solutions than the private sector. Ultimately, this means that multi-cloud solutions are even more important to public administrations than to private enterprise.

Public authorities are faced with a complex assortment of players and processes

The public sector as a whole and each individual agency or authority operates in a very diverse stakeholder landscape. As expressions of government, public administrations are responsible for performing public duties but are also accountable to the legislature. At the same time, the dictates of "customer orientation" mean that public authorities are also answerable to citizens. The way individual authorities discharge their duties is naturally overseen by the next-highest authority. And they themselves may be required to supervise lower-level authorities. →L

Additionally, many countries have a federal structure, a decentralized administrative structure or – as in the case of Germany – both at the same time. To properly depict the public sectors in this kind of state, the chart shown in Figure L would have to be replicated on every political level.

Public authorities thus find themselves in a position between numerous stakeholders. As such, individual agencies are called on to fulfill an assortment of functions that in turn necessitate a large number of internal processes (personnel management, accounting, document management, internal communication) and interfaces to the outside world (information, the acceptance of applications/requests and the transmission of replies/assessments).

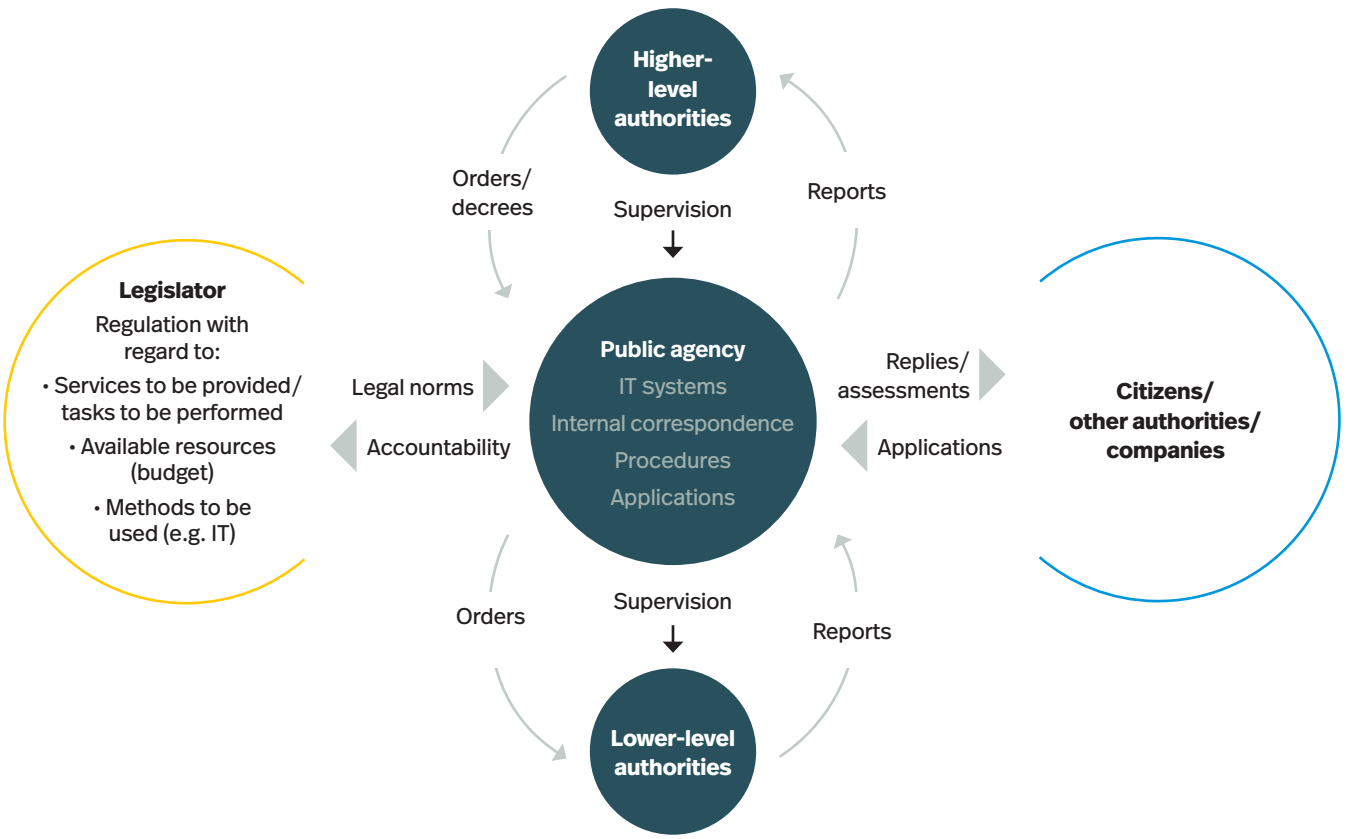
In public administrations, IT must model the diversity of stakeholders and processes

A smooth-running IT system must be capable of modeling all these different processes. At the same time, the information technology deployed across different authorities must reflect consistent standards to facilitate data exchange between them and guard against a breakdown into an unmanageable clutter of individual systems. The situation today, however, is that data resources are indeed heavily fragmented across German administrations. The Federal Statistical Office has identified no fewer than 214 separate databases (known as registers) at federal, regional and municipal government agencies. And this piecemeal IT landscape has tangible consequences: Data on convicted foreign criminals, for example, is maintained both in the central register of foreign nationals and in the systems operated by regional police forces. As a result, one and the same person may be registered under different names and thus not found in the databases in the event of criminal investigations. Conversely, innocent persons might wrongfully be targeted by the authorities.

Digitalization of the public sector demands new, user-friendly customer interfaces

Future-proof IT must be able to do more than merely model processes and interfaces across individual agencies and departments, however. The digitalization of public administrations also harbors tremendous potential especially at the interface to the public at large and the corporate community. If everyone can deal with their personal, pro bono and professional administrative

L Diversified landscape: Public administrations must accommodate the demands of various stakeholders



Source: Roland Berger

affairs online, that vastly simplifies processes for individuals, companies and public agencies themselves. Citizens can save themselves the time and trouble of waiting in line at the authority in question. Companies can more easily transfer data and applications to the relevant agencies via standardized interfaces. And ad-

ministrations themselves can benefit from more heavily automated internal processes: With relevant data and applications arriving in digital form, these can be channeled seamlessly and immediately into the corresponding specialist procedures. The EU Commission estimates that introducing e-government solutions throughout Europe would save over EUR 50 billion a year.

Public administrations place heavy demands on cloud solutions…

If the potential of digitally transformed administration is to be fully exploited, it is imperative to put cloud solutions to good use. For instance, the extensive scalability of cloud resources enables authorities to deliver digital administration services reliably even when demand is very strong. The exchange of data between agencies and/or departments is likewise faster and simpler with the aid of cloud computing.

However, the cloud solution deployed must be capable not only of coping with the stakeholders and processes described above: Public authorities also work with a very large number of different data types that are governed by different rules and regulations. Open data laws are one example; they prescribe that administrations must place the raw data they gather in the public domain (except where confidential or personal information is concerned). Additionally, public administrations work with highly sensitive personal data – in areas such as tax and healthcare – that require a very high level of security. The same goes for information that is strictly confidential and that, if it were disclosed to unauthorized parties, could threaten the security and interests of whole nations.

…which in turn necessitates the use of multi-cloud solutions

Integrated single-cloud solutions do not do justice to the broad spread of requirements incumbent on public administrations. True, a single-cloud solution could make it easier to integrate a number of specialist procedures on a single platform. The trade-off, though, is that all specialist procedures must then be aligned with the cloud architecture of just one provider. Yet this kind of cloud strategy can never optimally model the diverse array of procedures in place, because for each procedure a compromise would have to be found between its software components and the architecture of the chosen cloud.

Instead, the weakness of a single-cloud solution can be overcome by combining several clouds. In a multi-cloud strategy, an administration can choose those cloud solutions and/or those services that are best suited to each different specialist procedure. Databases designed to help fight crime, for example, need fast mobile access and minimized latency so that police officers in the field can access the information they need without delay. On the other hand, a cloud solution for fiscal administration needs to be scalable enough to handle peak periods of demand before and on the closing dates for tax returns.

Multi-cloud solutions combine strong information security with robust data protection

According to the "Branchenkompass [Sector Compass] Public Services 2018" published by Sopra Steria Consulting and the F.A.Z. Institute, 95% of decision-makers in

Germany's public authorities see the security of IT infrastructures and data as the pivotal challenge in the years ahead. For public administrations, a multi-cloud solution has the huge advantage that individual cloud solutions can be tailored specifically to the security needs of each application and the data they use. For example, cloud-based open data platforms need to be protected from data loss but do not require any special security measures to guard against data theft or the violation of informational autonomy. This kind of platform could therefore be operated in a public cloud. On the other hand, data from security agencies does indeed require effective protection against unauthorized access. That could, for instance, be accomplished via a private cloud whose physical infrastructure is right on the agencies' premises.

Besides adjusting cloud security levels depending on the needs of the type of data to be processed, multi-cloud solutions provide a higher level of security in general. While individual clouds also deliver very high security levels, system outages and unauthorized access to the data can never be completely ruled out. As rarely as that happens, a single-cloud solution implicitly means that any security-critical incident could affect all the data and applications stored in that cloud. The cloud thus becomes what is termed a single point of failure – a weak link that, in the event of an outage, could bring down the whole system.

Using multiple clouds allows security risks to be spread around more evenly. If one system within a multi-cloud solution is compromised by a cyber-attack, say, the other clouds remain unaffected. In other words, multi-cloud solutions are better than single clouds at satisfying the single most important requirement of public administrations. If the public sector wants to harness the benefits of the cloud without simultaneously jeopardizing the interests of the citizens it serves, using multi-cloud solutions must effectively become the gold standard.

On top of the benefits to citizens and the administration itself, governments can also generate important external effects by deploying multi-cloud solutions. In their capacity as major market players, governments that use multi-cloud solutions make a powerful public statement in favor of diversity and variety in the cloud computing market. At the same time, public administrations that adopt multi-cloud solutions strengthen competition between different cloud service providers. Similarly, regular calls for tender for new cloud projects likewise promote dynamic development and innovation in the cloud computing market. The bottom line, then, is that governments reap dual benefits by using multi-cloud solutions: While public authorities get to exploit the potential of digitalization securely and efficiently, they also benefit from a diversified and innovative cloud provider landscape.

5
BUYERS AND REGULATORS
HOW GOVERNMENTS CAN DRIVE DIVERSITY AND COMPETITION IN THE CLOUD COMPUTING MARKET

Cloud computing is becoming the solution of choice for the flexible, on-demand provisioning of centralized, scalable and pay-per-use IT resources not only in the corporate community, but increasingly also in the public sector. In the public sector in particular, the numerous advantages of cloud solutions must be carefully weighed against strict requirements for information security and data protection. Moreover, single-cloud solutions also heighten the risk of vendor lock-in, which could lead to high costs and suboptimal performance.

On the macroeconomic level, the use of single-cloud solutions could play a part in perpetuating the trend toward concentration in the market for cloud services that is already becoming apparent. In the long term, that would weaken competition and possibly even undermine innovative capabilities in the cloud computing market.

To ensure that fair competition remains possible in cloud computing, governments must therefore play a proactive role as both buyers and regulators. →M

As buyers (i.e. customers), they must support a varied provider landscape and avoid lock-in effects by giving precedence to multi-cloud solutions over single-cloud solutions. As regulators – especially at the European level – they must drive "soft regulation" in the shape of common standards and codes of conduct.

Governments must act as buyers

Decisions to use cloud solutions must be strategic decisions that serve the purposes of the organization

Thanks to the specific benefits it offers, cloud computing is a sensible solution that is rightly becoming established as standard practice for meeting IT requirements in the modern age. That said, cloud computing is not an end in itself, but merely a means to an end. It is thus all the more important that public authorities – who have a reputation for adopting technical innovations more hesitantly than private enterprise – do not fall into the trap of always seeing cloud computing as the only solution for any and every specific IT requirement. Rather than asking how to get into the cloud as quickly as possible, organizations must consider the extent to which a cloud solution may or may not help them achieve certain defined goals faster, more efficiently and in a better way.

Balanced multi-cloud portfolios should take precedence over single-cloud solutions

The advantages that single-cloud solutions unquestionably offer as integrated cloud ecosystems are – all things being equal – nevertheless outweighed by the benefits of multi-cloud solutions. Especially with a view to avoiding lock-in effects, public administrations should give their backing to balanced cloud portfolios in the context of multi-cloud strategies. This strong recommendation carries even greater weight given that public authorities must safeguard their own ability to act in the long term. Spreading risks across a number of providers is therefore a sensible way to contain the effects of putative system outages.

"The cloud is one of the pivotal areas in the digital transformation of government." [4)]

Mounir Mahjoubi
Former French Secretary of State for Digital Affairs

Contracts with cloud service providers must factor in the portability and interoperability of data and applications

Not all types of data and applications can be migrated from one cloud to another. That is precisely why it is crucial to identify the extent to which interoperability and portability are possible for all the cloud solutions deployed. Above all, the use of recognized industry standards such as the Open Virtualization Format for virtual appliances helps ensure interoperability between a selected cloud solution and other cloud services.

Governments must act as regulators

The development of Europe-wide security standards for cloud computing must be driven forward

Today, security standards and certification/audit programs for cloud service providers vary from country to country. Although the standards are similar, compliance in each country must be proven based on the certification/audit programs that apply in each jurisdiction. Security and audit standards that are valid throughout Europe could play a decisive role in fostering a single European market for data and cloud services. Within this market, cloud service providers across the continent would have to contend with each other, thereby safeguarding competition and innovation.

In December 2018, the European Commission, the European Council and the European Parliament reached political agreement on a cyber-security regulation. The first reading of the regulation commenced at the European Parliament in March 2019. One aim is to introduce pan-European certifications for IT products. This standardization is to be targeted for cloud computing in particular in order to strengthen competition and counter the advance of market concentration. In this context, data portability must also be specified as an aspect of relevance to security. In its "C5" catalogue of requirements for cloud computing, for example, Germany's Federal Office for Information Security (BSI) makes it clear that portability and interoperability are valid criteria with which to assess the information security of cloud services.

Self-regulation by cloud service providers must be supported and the outcomes evaluated over time

EU Regulation 2018/1807 came into force at the end of 2018 and stakes out a framework for the free flow of non-personal data in the European Union. It prescribes that stakeholders in the European cloud computing market, operating under a regime of self-regulation, are to agree to a code of conduct for interoperability with due provision for open standards. This promising approach requires political support, flanked by active efforts to ensure implementation – as envisaged in the regulation itself – by the end of May 2020.

As a last resort, statutory provisions may be needed to regulate the interoperability of cloud services

The code of conduct agreed under self-regulation must be evaluated quickly, as soon as it takes effect – preferably ahead of the end of November 2022 deadline stipulated in the EU regulation. If the code of conduct proves ineffective in its attempts to guarantee the necessary interoperability, statutory provisions must then be considered. This path should, however, be followed only as a last resort to ensure that predefined standards do not put the brakes on cloud service providers' innovation.

M Buyers and regulators: Governments must utilize both levers to uphold competition and innovation in the cloud computing market

Governments must act…

…as buyers

Base cloud usage on a strategy aligned with the goals of the organization/authority

Give precedence to the use of balanced cloud portfolios as part of multi-cloud strategies

Draw up contracts that make due provision for portability and interoperability

…as regulators

Promote EU-wide security standards for cloud computing in the context of the cyber-security regulation

Support the self-regulation of cloud service providers regarding the development of codes of conduct for data portability and interoperability

Evaluate self-regulation and implement statutory provisions where necessary

Source: Roland Berger

Innovation and competition on the European market for cloud computing are essential prerequisites for the successful digital transformation of companies and public authorities alike. Governments in particular play a vital dual role as buyers and regulators of cloud solutions. They must proactively leverage both of these roles in order to curb the nascent market dominance of individual cloud service providers.

Imprint

Publishers

Internet Economy Foundation (IE.F)
Uhlandstrasse 175
10719 Berlin
www.ie.foundation
Prof. Dr. Friedbert Pflüger
Chairman

Roland Berger GmbH
Sederanger 1
80538 Munich
www.rolandberger.com
Stefan Schaible
CEO Germany & Central Europe

Authors

IE.F
Clark Parsons
c.parsons@ie.foundation
Amelie Drünkler
a.druenkler@ie.foundation

Roland Berger
Klaus Fuest
klaus.fuest@rolandberger.com
Dr. Christian Krys
christian.krys@rolandberger.com
Dr. David Born
david.born@rolandberger.com

Contacts

IE.F
Clark Parsons
Managing Director
Internet Economy Foundation (IE.F)
c.parsons@ie.foundation
+49 30 8877 429-400

Roland Berger
Claudia Russo
Press Officer
Roland Berger GmbH
claudia.russo@rolandberger.com
+49 89 9230-8190

Publication date

May 2019

Picture credits

Cover: Zenobillis/iStock; **Page 3:** IE.F; **Page 8:** Jasper Juinen/Bloomberg/Getty Images; **Page 10:** Zenobillis/iStock; **Page 20:** Zenobillis/iStock; **Page 22:** Ulrich Baumgarten/Getty Images; **Page 28:** Zenobillis/iStock; **Page 30:** Emmanuel Dunand/AFP/Getty Images; **Page 40:** Artulina1/iStock; **Page 42:** Joel Saget/AFP/Getty Images

Quote sources

1) TEDGlobal Talk New York City, September 20, 2017 (minute 15:06); **2)** Federal Office for Information Security press release, August 15, 2017; **3)** European Commission press release, September 4, 2018; **4)** Channel Business Partners press article, July 5, 2018