Cloud Computing
Navigating the Cloud

Strategy, Organisation,
Processes and Systems

pwc

PwC works with technology companies around the world to help them fulfill the promise of their great ideas. Whether it's driving innovation to meet the growing consumer opportunity of the global markets or adopting new "digital" business models, our strong relationships and track record of delivering value have made us the trusted adviser or auditor to the majority of the technology companies in the Global Fortune 500 and Global Financial Times 500.

Given our significant client base and considerable resources, our technology professionals work from an exceptional base of experience. We're in touch with your industry—and ready to work with you. For more information on how PwC's technology industry practice can help your company, or to get in touch with a technology industry partner in your area, please visit us at www.pwc.com/ technology or contact one of the professionals listed at the end of this publication.

Cloud Computing
Navigating the Cloud

Innovative technology brings constant change to our society, shaping how we live and work in an increasingly digitised world—a place where technical developments are the foundation for our activities both at home and at work. Technology and innovation are also integral parts of modern communication, making our work processes more efficient and profitable. This is no small challenge. A powerful tool has emerged to help companies meet this challenge: cloud computing.

Cloud computing allows users to procure their IT services on a flexible basis according to their needs, putting companies in an ideal position to meet the dynamic demands of their markets. This enables IT to be flexible and react quickly to accommodate the needs of the business world, which results in cost savings and a more effective use of available capacity. This lucrative opportunity is, however, like many things, not without its risks and challenges.

In order to identify the most significant challenges faced by cloud computing providers, PwC Germany surveyed a number of German-based cloud providers. The results illustrate how cloud providers are meeting the current demands of the market. The survey also provides an overview of the risks and challenges that cloud providers are facing and shows what they need to do to make the use of cloud services successful and profitable for their customers.

It is important to note that while this survey was conducted exclusively in Germany, the challenges and opportunities are pertinent to cloud providers around the world. I would like to recognise my colleagues in Frankfurt, Germany who organised this study and conducted the analysis:

Dr. Georg Kämpfer   Markus Vehlow   Cordula Golkowsky

I hope you find the study informative and insightful reading. If you'd like to discuss the challenges and opportunities cloud computing presents for your company—whether as a provider or user of cloud services, please don't hesitate to reach out to me or any of my colleagues listed in the back of this report.

Raman Chitkara
Global Technology Industry Leader

Table of contents

List of figures

List of abbreviations

BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
BPaaS	Business process as a service
CATI	Computer-aided telephone interviews
EC	European Community
EEA	European Economic Area
IaaS	Infrastructure as a service
IEC	International Electrotechnical Commission
ISMS	Information security management system
ISO	International Organization for Standardization
M&C	Media and communications
OCR	Optical character recognition
PaaS	Platform as a service
SaaS	Software as a service
SLA	Service level agreement

Summary

Motivation and approach

Unimaginable just a few years ago, but now an attractive implementation and operating model for many companies and their IT departments, cloud computing is essentially a wall socket for your IT services. Cloud computing offers a number of clear advantages, including increased flexibility and business agility, reduced complexity, payment according to actual use of services and a high degree of scalability. Providers and users are nevertheless faced with a host of questions, and while views held by users on this topic have already been examined in a number of German and international studies, little attention has been given to how providers see things.

This survey reveals the perspective of providers in Germany, focusing on what they consider the current challenges in cloud computing to be. A market research study was used to identify the key topics to be addressed by the survey. These focal points were then confirmed via questionnaire through preliminary interviews with representatives of selected providers. The 51 participants were primarily from the strategic management level in their provider companies.

Cloud service providers

Our survey interviewed small, medium and large providers. The percentage of cloud services compared to total business varied widely from provider to provider. Some companies, mostly young enterprises, specialise exclusively in cloud services. The majority of these are small providers. Large companies, in contrast, tend to offer a wide spectrum of solutions, with cloud services generally comprising a small percentage of total services.

On average, each participant surveyed offers three cloud services in the German market. More than three quarters offer software as a service (SaaS); half offer infrastructure as a service (IaaS) and two out of five offer platform as a service (PaaS). Traditional support processes such as purchasing, sales, human resources and accounting are already represented by SaaS solutions. The overwhelming majority of the solutions are commercially relevant. Business process as a service (BPaaS) plays the smallest role and is only offered by one quarter of the participants surveyed.

Half of the participants offer their solutions exclusively as private cloud plans; one quarter offer public cloud plans and one quarter offer both types of implementation.

Cloud service users

Notably, the size of the user has little effect on the amount of services they procure; the providers interviewed reported that they provide practically the same amount of cloud services to companies of all sizes. Cloud services seem to be in demand in all industries at the moment. This makes sense, since the existing cloud services focus on secondary processes and can therefore generally be used across all industries.

According to the providers surveyed, comprehensive cloud strategies have still not been fully developed for users, despite a high level of interest. Instead, users tend to look for solutions to individual, concrete problems, creating references and/or pilot applications in the process. At this point, very few users have established a comprehensive cloud strategy in harmony with their IT strategy.

Information security, data protection and compliance are important for users and providers

Three issues in particular stood out in the survey: information security needs to be guaranteed, data protection ensured and compliance achieved. According to those interviewed, finding solutions for these issues represents a significant challenge for the providers and is an important factor in achieving customer satisfaction.

Providers listed a detailed risk analysis as the most important task in guaranteeing information security for customer data. The second-most important task was certifying their own information security, followed closely by security penetration tests, adapting security concepts and having external third parties conduct user audits. More than half of those surveyed had agreed upon a user emergency plan to put into effect if some breach in security or data protection should occur. Almost one third of respondents had no emergency plan in place.

We also talked with providers about the second challenge they named—data protection. We asked them where they store and process the customer data that is entrusted to them and what measures they take to protect it. A good half of the respondents use data centres in Germany; however, just under one third of the providers store their data exclusively in Germany, which simplifies data protection. Some providers give their customers the option of choosing whether or not they want their data stored exclusively in Germany or also abroad, although larger providers tend to do this more often than smaller ones. A little over half of all providers have been asked by their customers about the technical and organisational measures they have taken to protect their data (enquiries relating to section 11 of the German Federal Data Protection Act [Bundesdatenschutzgesetz]). The same number of providers said that they have a formal, standard procedure for responding to this type of data protection enquiry.

Four out of five providers have established their own compliance management system to keep risks and compliance under control. The providers also said that the most important compliance challenge was being able to identify the compliance requirements of the user to begin with. Other major challenges listed were fulfilling industry-specific needs, furnishing proof of compliance and implementing an internal control system.

Into the cloud, out of the cloud

Two out of five providers sold additional services to securely and seamlessly transfer customer data into the cloud, while only one out of five offered free migration tools or functions. Just three out of five respondents had a contract that arranged for the return of the data. In this instance, smaller providers were in the majority.

Know your contract!

The survey revealed some interesting information about contracts in the cloud: half of the providers interviewed offered contracts with a fixed number of months and a fixed cancellation notice period. Just one provider released customers from their contracts within 24 hours. Although flexibility is promoted as one of cloud computing's main selling points, providers still often have long cancellation notice periods. A good one third of those surveyed deliver public cloud solutions, which have the most technical potential to offer customers short cancellation notice periods.

One quarter of respondents bill their customers for additional charges after the cancellation of the contract. Surprisingly, the same amount of respondents said that they had no contractual agreement regarding service delivery. Overall, smaller providers guarantee a lower level of service delivery than large providers.

About two out of five providers use sub-contractors. Less than one tenth of providers do not have any resources for cloud services and rely exclusively on sub-contractors to provide their services. Practically all providers who use sub-contractors inform their customers of that fact. We also asked the respondents how flexibly they react to service level agreements (SLAs). The vast majority of companies offer their customers individually configured services in addition to standard services.

Blue skies ahead for cloud computing

Just under three quarters of providers thought that the percentage of cloud services in their total business will increase in Germany in the medium term. None of those interviewed expected a decrease. The majority of providers expected that cloud computing will pose new challenges for vendor management and related provider control systems. In particular, the heavily specialised providers believed that internet-based work will become the norm and that the ability to integrate and combine cloud offers will become increasingly important. It will be necessary to standardise the various services in order to integrate individual cloud services with one another.

Background

Cloud computing enables companies to procure their IT resources over the internet—on a flexible basis, cost-efficiently, almost limitlessly, and effectively with payment based on consumption. This means that companies no longer need to keep a certain amount of computer capacity or data storage space free, or constantly run applications. This leads to a reduction of necessary capacity, investments and costs for companies, and, most importantly, allows them to structure their specialist departments in new ways.

Cloud computing is a paradigm that will change business models, processes and IT in companies

While the underlying technologies are not new, the effects of their further development are likely to have an immense impact on both the providers and the users of IT services. Right now, cloud computing forms a basis for completely new sales and use channels for IT services, but it is also preparing the ground for completely new processes and business models. There is no doubt that these prospects appear to be extremely lucrative. At the same time, both providers and users need to overcome a variety of challenges before they can successfully take advantage of all that cloud computing has to offer. Of course, users and providers need to consider different questions.

Users need to ask the following questions:

• For which purposes, processes or applications would it make sense to use cloud services?

• Does the company know of all the potential risks of the services?

• How should the cloud provider be managed and monitored (sourcing governance)?

• Which conditions need to be met in order to integrate the cloud services into existing IT?

• Which criteria are decisive in choosing the ideal cloud provider?

Providers need to consider these core issues:

• Which user compliance and security requirements should providers fulfil?

• How can data protection be guaranteed when data is stored abroad or in different countries?

• How should data migration, archiving and the return of data to the client be arranged?

• Which contractual implications do our approach and business model entail?

In short, providers and users have identified the potential and the challenges inherent in cloud computing and are currently working on integration concepts and strategies to deliver solutions. We asked the providers for their opinion—based on customer requests they had received—on how well prepared users were to implement cloud services.

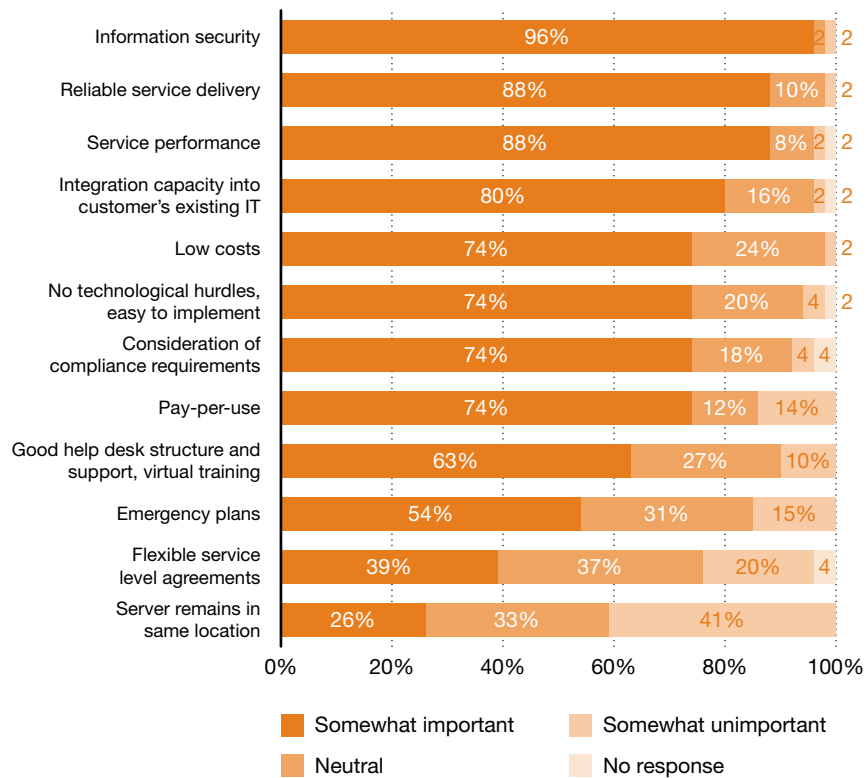**Figure 1: Evaluation of customer cloud strategies**

Q: How developed is the cloud strategy of your customers? What is your general impression?

Legend:
- Applies frequently
- Applies rarely
- Not applicable
- No response
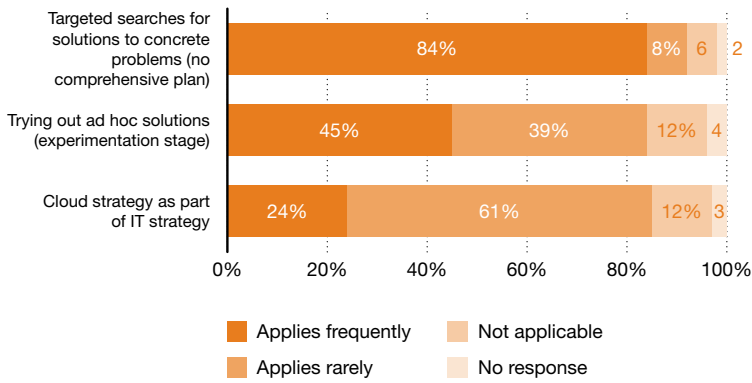
The providers surveyed did not think that the cloud strategies of their clients were very well developed. In many cases, users only searched for solutions to concrete, individual problems. In general, the larger providers tended to experience this scenario more than the smaller ones. Only the providers who primarily worked for large companies said that their clients had already developed a cloud strategy.

Figure 2: Significant factors affecting customer satisfaction

Q: What are the critical success factors in maintaining customer satisfaction?

	Somewhat important	Neutral	Somewhat unimportant	No response
Information security	96%		2	2
Reliable service delivery	88%		10%	2
Service performance	88%		8% 2	2
Integration capacity into customer's existing IT	80%		16%	2 2
Low costs	74%		24%	2
No technological hurdles, easy to implement	74%		20% 4	2
Consideration of compliance requirements	74%		18% 4	4
Pay-per-use	74%		12%	14%
Good help desk structure and support, virtual training	63%		27%	10%
Emergency plans	54%		31%	15%
Flexible service level agreements	39%		37%	20% 4
Server remains in same location	26%		33%	41%

From the providers' point of view, information security and reliable service delivery were the most significant factors in maintaining customer satisfaction. Other important factors were service performance, low costs, easy installation and the capacity to integrate cloud services into existing IT, compliance, and pay-per-use billing. Emergency plans, flexible SLAs and a constant server location were considered the least important criteria. Aspects that are often mentioned as benefits of cloud computing, such as low costs and pay-per-use billing, were not among the most important factors in customer satisfaction. Also of interest is the fact that aspects such as emergency plans and a constant server location came in last, however, it must be noted that these factors are related to information security, which tops the list.

Figure 3: Challenges in the cloud computing market

Q: What are the biggest challenges for providers right now?

Challenge	More of a challenge	Moderate challenge	Less of a challenge	No response
Data protection and compliance requirements	60%	22%	18%	
Standardisation of internal processes	53%	24%	23%	
Individual service level agreements	49%	24%	25%	2
Information security	49%	12%	39%	
Customer satisfaction	47%	27%	26%	
Definition of cloud	47%	20%	33%	
Recruitment of qualified employees	32%	41%	27%	
Identification of appropriate sub-contractors	31%	27%	38%	4
Departing from the licensing model	30%	24%	44%	2
Guaranteed service quality	28%	18%	52%	2
Dispelling reservations about cloud computing	28%	18%	50%	4
Maintenance and scalability	26%	20%	54%	

■ More of a challenge   ■ Less of a challenge
■ Moderate challenge   ■ No response

The two biggest challenges in the German cloud computing market were listed as data protection and compliance and the standardisation of internal processes. The latter is surprising, given the provider-side scale effects that are associated with cloud computing. After these two challenges, the other aspects were weighted almost equally: the arrangement of SLAs, and data information security, followed closely by customer satisfaction and, somewhat surprisingly, the need to establish a concrete definition of cloud computing. This probably stems from the fact that one can currently find an extraordinary number of sometimes contradictory definitions on the internet and in industry publications. The lack of standards in the market, as well as the complexity of the topic, make it even more difficult for providers to give their customers a clear description of cloud computing.

The providers surveyed considered departing from the licensing model, guaranteeing service quality and German customers' general reservations against cloud computing to be lesser challenges. Maintenance and scalability bring up the rear in the challenges category. This suggests that providers appear to be staying on top of the technological challenges.

It is interesting that the critical success factors for customer satisfaction (see Figure 2) are not identical to providers' own challenges. Flexible SLAs, for example, are less important for customer satisfaction, but are definitely seen as a major challenge. The same goes for the reliability of service delivery versus guaranteeing service quality. Information security, data protection and compliance are considered both important for customer satisfaction and as major challenges. Providers should therefore give them the highest priority.

The results of the survey

1. Contract creation

While contract management forms a basis for business management decisions, it is a complex task with many different aspects that require consideration. Contract management generally follows the contract lifecycle, starting with the decision to establish a contract and tendering process, followed by the creation of the contract and negotiation of its terms, managing any changes that may come up and finally, the termination of the contract. Experience shows that, in practice, there are often a number of weak spots that arise during the creation of contracts. The consequences can be drastic. Loopholes create legal uncertainty, ineffectual clauses increase risk, and infringement upon the rights of third parties can potentially result in claims or legal disputes. On top of that, non-compliance with regulatory requirements can lead to fines, detention or sanctions levied by the authorities.

How I see it

"To be successful, a provider needs to act on two fundamental criteria: first, develop custom services that reflect the size and industry of your customers; and second, build up a functioning ecosystem of industry partners whose complementary services fit together to form one comprehensive custom solution."

Michael Rosbach, board member, Scopevisio AG

1.1. Contract creation and cloud computing

The innovative technology that forms the basis for cloud computing makes contract creation difficult. It is a formidable task to define the rights and obligations of the contractual partners in detail. Crucial aspects of contracts for cloud computing services include cancellation conditions, ensuring service provision and the use of sub-contractors. If a cloud user is not aware of cloud-specific contract risks, such as licensing pitfalls, before concluding the contract, and is instead focused solely on cutting costs, then he may end up being saddled with considerable extra costs after all. The danger of concentrating solely on costs is well known from IT outsourcing and needs to be considered by both providers, who draft standard contracts for cloud computing services in line with general terms and conditions—which may need to be negotiated—and by potential users, who need to know all contract-related risks in order to properly evaluate the proposed contracts.

This survey asked the participating providers about what they included in their contracts. The following section presents the results in detail.

1.2. Survey results

Figure 4: Cancellation notice periods

Q: What is the length of your cancellation notice period?
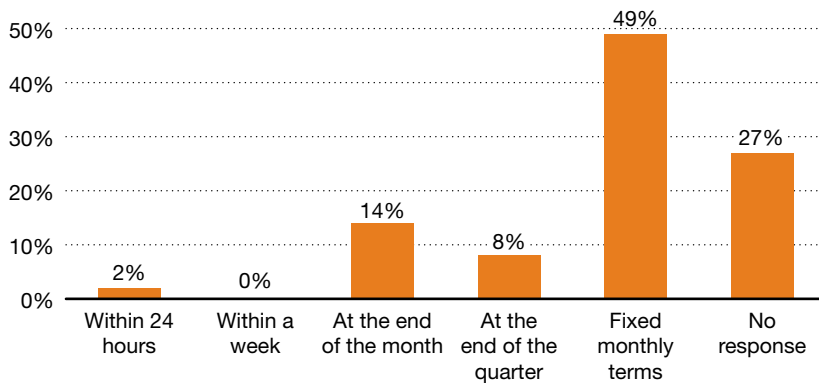

Half of the providers interviewed offered contracts with a fixed number of months and a fixed cancellation notice period. Just one provider released customers from their contracts within 24 hours, and no providers allowed cancellation at a week's notice. Even though flexibility is promoted as one of cloud computing's main selling points, providers still have cancellation notice periods that predate cloud computing. A good 27% of the providers surveyed did not respond to this question.

To qualify these figures, we have to note that just under 38% of the respondents offered public cloud solutions, which have the most technical potential to offer customers short cancellation notice periods, particularly with IaaS.

Figure 5: Additional charges after cancellation

Q: Do customers have to pay additional charges after cancellation?

- No
- Yes (compliance reasons)
- Yes
- No response

14%
16%
10%
60%
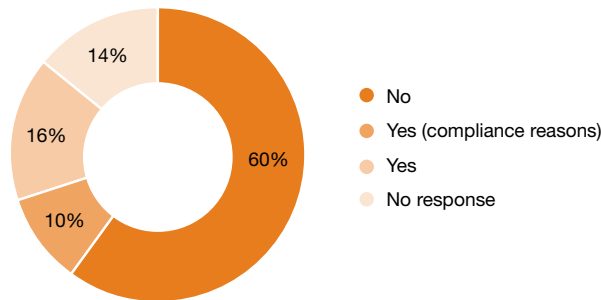
The majority of cloud providers (60%) said that there were no additional charges for their customers after the cancellation of the contract. Only about one quarter of the companies had additional charges. Almost 40% of the companies who charged additional fees after cancellation emphasised that these costs mainly arose as a result of statutory obligations to keep the data on record for a certain period of time. Smaller providers and providers with smaller customers charged additional fees much less often than larger providers and providers that predominantly served large companies.

Figure 6: Service delivery guarantees

Q: What kind of service delivery do you guarantee you customers contractually?

	Not stipulated contractually	< 99%	99,1–99,8%	> 99,9%	No response
	24%	8%	25%	29%	14%
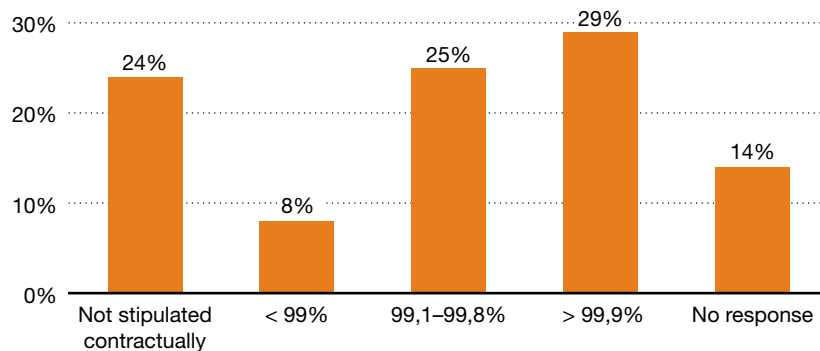
Of the providers surveyed, 29% contractually guaranteed their users a service delivery rate of at least 99.9%. Just 8% of providers guaranteed less than 99% service delivery; these were smaller companies with fewer than 500 employees in Germany who mostly provided services to middle-market customers.

Larger and specialised cloud providers generally guaranteed their clients a higher level of service delivery than smaller providers and those for whom cloud services made up only a small percentage of their total business. The latter often guaranteed between 99.1% and 99.8% service delivery in comparison with the larger and/or specialised providers, who mostly guaranteed 99.9% or more service delivery. Surprisingly, one quarter of the respondents did not guarantee a specific level of service delivery in their contracts.

Figure 7: Cloud chaining – use of sub-contractors

Q: Do you use services from other cloud providers to guarantee the provision of your own services?

- No
- Yes, for some things
- Yes, for all cloud services
- No response

4%
8%
33%
55%
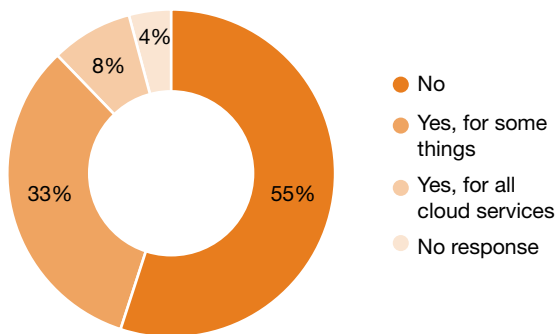
More than half of the providers offered all the services themselves. Just over 40% of providers used sub-contractors to offer their services and 8% provided services without having any resources of their own. This could be seen as a harbinger of integration as a service (IaaS), where the actual service consists of providing a combination of different services. According to providers, IaaS will grow in the coming years, but because of the high level of interdependence involved, users need to be particularly careful about governance aspects, such as monitoring and managing the providers, when creating and negotiating contracts. On a positive note, practically all providers that use sub-contractors inform their customers of this fact.

We also asked the participants about how flexible they are in terms of SLAs. On the one hand, providers generate large scale effects by using standard versions of SLAs, but, on the other hand, it is more attractive for customers when the provider is able to offer customised contractual arrangements. Three out of four companies offered their customers both standard services and individually configured services. Providers that mostly served large companies tended to offer individually configured services more often than providers that served smaller companies. The volume purchased seems to be the decisive factor here.

2. Data migration

The introduction of new technologies, architectures and systems or organisational restructuring often requires a company to reorganise its databases. Companies have to transfer their data from old applications to new ones, or reorganise data in an existing application according to the new organisational structure. The latter might be necessary, for example, after a merger. The challenge in all these cases lies in guaranteeing complete and accurate migration of all data, or, in other words, ensuring that no data is lost, placed in the wrong location or altered in the course of the migration process.

How I see it

"Cloud computing does not represent a revolution in IT use or provision, but rather an evolution that is based on the further development and combination of existing technologies. Nevertheless, I am convinced that we will see a paradigm shift comparable to that from mainframes to customer servers, or the emergence of the internet."

Frank Strecker, Director of Cloud Computing, IBM Deutschland GmbH

2.1. Data migration and cloud computing

One of the biggest challenges for users of cloud computing solutions is the outsourcing of applications that had previously been used and operated internally. As a rule, outsourcing applications is accompanied by the migration of data from the company's internal IT department to the cloud. The uniform transfer of data to the provider requires the technical standardisation of transfer processes, interfaces and data formats. If this does not occur, there is a risk that the data will need extensive processing after migration, which may require considerable time and effort both from the user and provider. In particular, when transferring data related to accounting, companies must be able to guarantee that the migration will be complete, understandable and accurate.

When users cancel their cloud services, they need to know how they are going to get their data back or have it competently transferred to the cloud of another provider. In principle, this entails the same requirements as the initial transfer into the cloud. On top of that, the confidentiality of the data needs to be protected by irreversible, complete deletion so that no data may be reconstituted or remain in the original cloud. In general, users tend to worry about what is known as the vendor lock-in effect, where there is a delay in the return of data after cancellation.

The situations described above make it clear that successful data migration into or out of the cloud depends upon the support of the providers and the measures they put in place. However, to what extent do providers actually support their customers during the transfer of data into the cloud and the return of data from the cloud? PwC asked the respondents to share their thoughts on this issue.

Provider support is key

2.2. Survey results

Figure 8: Data migration support for new customers

Q: How do you support new customers in transferring their data?

- Migration tools/ free functions — 22%
- Additional fee-based services — 41%
- Not compatible with the products — 4%
- No response — 33%
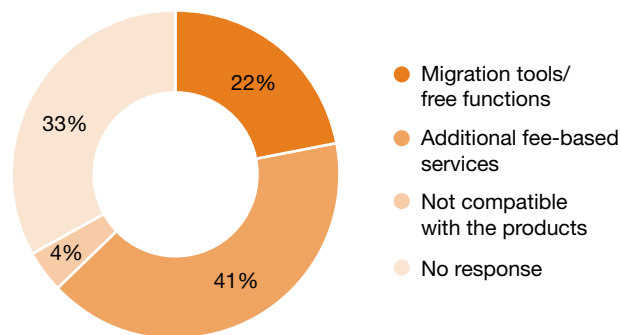
A good 20% of providers offered migration tools or free functions as part of their product. About 40% of providers offered additional fee-based services to support new customers in the transfer of their data. Large and small providers offered the same amount of support. Thirty-three percent (33%) of respondents gave no response to this question.

Figure 9: Data migration support after cancellation

Q: Do your contracts stipulate when and how the data will be returned after cancellation of the contract?

- Yes — 59%
- No — 18%
- No response — 23%
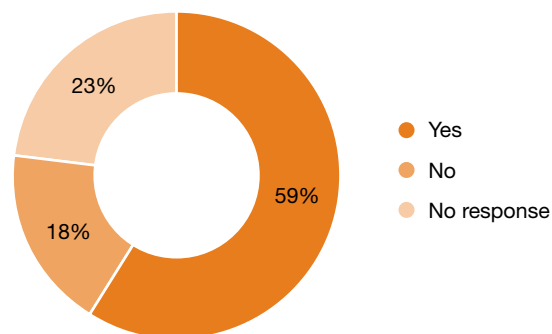
Around 60% of the providers reported that they and their customers had contractually arranged when and how the data would be returned after cancellation. Smaller providers are in the majority here. Surprisingly, just under 20% of providers said that they had no contractual arrangement regarding this point. In these cases, the risk of the aforementioned vendor lock-in is particularly high, as is the risk of violating data protection laws. It was also surprising that just under one quarter of respondents could not or did not want to provide a response to this question.

3. Risks and compliance

Compliance is the mechanism responsible for ensuring that a company's activities do not violate society's laws, values, morals or ethics, and also for making sure that the company adheres to its own internal rules and regulations. The individual measures that are required in each case are determined by the type and size of the business, its sales channels and its customer profiles. As such, a compliance approach needs to be developed specifically for each company to ensure that all of the requirements of those involved can be fulfilled.

How I see it

"The new challenges that cloud computing brings with it call for an intelligent data centre architecture where the network is a platform for transparency, management and security."

Viktor Hagen, Data Centre Architect, Cisco Systems GmbH

3.1. Risks, compliance and cloud computing

When a company begins to source its IT services with a cloud computing solution, it can no longer use internal control measures to monitor them. At the same time, the user company is still responsible for fulfilling all of the compliance requirements. In this case, the user must make sure that all risks are identified early on and that the IT services are appropriately monitored. The challenge here lies in determining whether or not the provider has implemented measures for risk assessment and control that can adequately handle the risks that the user faces. This, however, turns out to be quite difficult since, for example, the virtualisation technology that underlies cloud computing opens up a number of new and changing IT risks. What percentage of providers use an appropriate compliance management system to help them and their users meet compliance requirements? Which aspects are most important? PwC asked the survey participants about their thoughts on the matter.

How I see it

"The decision-makers in IT should use the cloud as a chance to reduce complexity and to focus on the further development of business technologies. People should already be working on cloud readiness and pilot projects. Many areas still lack integration technologies, pioneering standards and best practices. What we are seeing now is that both users and providers are working hard to develop them."
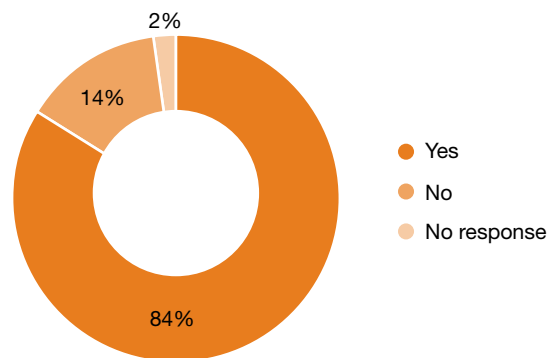
Jörg Hastreiter, Head of Business Technology, T-Systems Multimedia Solutions GmbH

3.2. Survey results

Figure 10: Compliance management

Q: Does your company have a compliance management system?
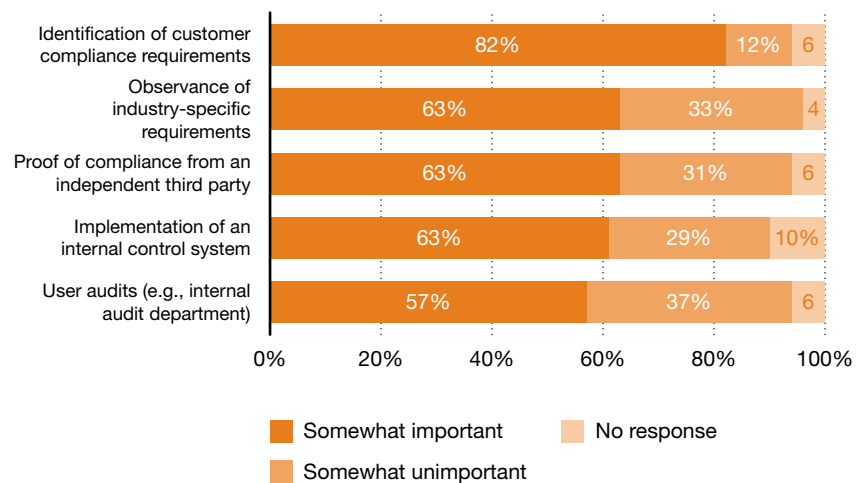

- Yes
- No
- No response

2%
14%
84%

A compliance management system ensures that company-specific compliance requirements are fulfilled. As part of risk management, a compliance management system combines the principles and measures that are intended to ensure that the behaviour of the legal representatives and employees of a company is consistent with its rules and regulations.

Only 14% of the providers surveyed said that they had no compliance management system. These respondents were almost without exception smaller providers.

Figure 11: Challenges in fulfilling compliance requirements

Q: Which challenges does your company currently face in fulfilling compliance requirements?

	Somewhat important	Somewhat unimportant	No response
Identification of customer compliance requirements	82%	12%	6
Observance of industry-specific requirements	63%	33%	4
Proof of compliance from an independent third party	63%	31%	6
Implementation of an internal control system	63%	29%	10%
User audits (e.g., internal audit department)	57%	37%	6

- Somewhat important
- Somewhat unimportant
- No response

Given that 84% of the participating providers said that they had a compliance management system, it was particularly surprising to find out that more than three quarters of those surveyed considered identifying the compliance requirements of their customers to be their most important challenge. After all, identifying customer compliance requirements is an elementary part of compliance management systems and is usually the chief concern. What also stands out is that all of the other challenges listed were given a similarly high level of priority.

There were several clear trends: obtaining proof of compliance with customer requirements from an independent third party seemed to be more important for providers serving large companies than for those serving users mostly in the middle market. The same can be said for user audits, internal control systems and the observation of industry-specific requirements. These three compliance aspects are considered more important by the larger providers than by their smaller counterparts.

4. Data protection

The negative press surrounding recent incidents in the business world has put the spotlight on the issue of data protection. Both the general public and business executives are thinking more about data protection than even just a few years ago. Violations of data protection regulations can result in sanctions, fines and lasting damage to a company's reputation. More than ever before, decision-makers need to make sure that their companies are complying with statutory requirements. Data protection law is intended to protect individuals against the misuse of their personal information and also to protect their basic right to decide which personal information should be communicated to others and under what circumstances. The scope of this law covers, for example, the user as an individual, or an employee of the user. In Germany, the Federal Data Protection Act (Bundesdatenschutzgesetz) is the main law that regulates the handling of personal data. Data protection is also addressed in other laws, such as the Telemedia Act (Telemediengesetz), the Telecommunications Act (Telekommunikationsgesetz) and the German Social Code (Sozialgesetzbuch). These laws apply to both users and providers.

How I see it

"One of the most significant tasks for providers is to clearly present their services—transparently, sustainably, and supported by the appropriate measures and certifications—and thus gain the trust of their customers. This starts with the creation of the contract and progresses throughout the entire contractual relationship along different areas, all the way to information security and data protection issues."

Michael Kranawetter, Chief Security Advisor, Microsoft Deutschland GmbH

The European Community (EC) has long recognised the need for a uniform level of data protection. The Data Protection Directive 95/46/EC was approved on 24 October 1995 to protect individuals with regard to the processing of personal data and the free movement of such data. All member states have since transposed this legislation into national law.

One of the basic principles of European data protection law is that personal data may only be transferred outside of the European Economic Area (EEA) if the recipient of the data has an adequate, legally regulated level of data protection. This condition is considered fulfilled when the country in which the recipient is located has an adequate level of data protection, as for example, Switzerland does. The United States does not have an adequate, legally regulated level of data protection; however, American companies can still fulfil this condition if they agree to abide by the "safe harbour" framework developed by the US Department of Commerce.

This obligates the recipient of personal information to uphold standards which are equivalent to those laid down in European data protection legislation. This makes the recipient a "safe harbour" for data in a country which is otherwise inadequate from a data protection point of view. Contracts can also be used to achieve an adequate level of data protection, for example, through standard contractual clauses. Nevertheless, regardless of the recipient country, or the existence of a safe harbour or standard contractual clauses, European data exporters must constantly verify whether they are allowed to transfer data to a third party.

4.1. Data protection and cloud computing

Cloud computing providers in Germany also process personal information (e.g., information about customers, employees, suppliers and contracts) in the cloud. Depending on the workload, providers may send personal information to different server systems in different data processing centres—regardless of location or country—in order to process it more efficiently. Normally, providers have a data processing contract with the user (commissioned data processing). In this case, users that are not in the public sphere must comply with the requirements of section 11 of the German Federal Data Protection Act. This means that when a provider is commissioned to collect, process or use personal data, the user is still the "master of the data", i.e., he retains sole responsibility for compliance with the Data Protection Act. As such, if data is to be processed outside the EEA, the user may only make it available to the provider if an adequate level of data protection exists. The provider may only process or use the data as instructed by the user.

Data traffic knows no bounds

How I see it

"The integration and orchestration of a vast array of solutions comprising on-premise components and different cloud services will need to be a core competence of IT departments in the future. The IT department will take on a completely new role, and, at the same time, become more important—also for business in general."

Dr. Bernd Welz, Senior Vice President OnDemand Services Unit, SAP AG

Responsibility rests with the owner of the data, security guarantees with the provider

An essential factor in the protection of personal information is the adequate technical and organisational measures that providers are required to implement by section 9 of the German Federal Data Protection Act. An annex to section 9 specifies its goals in detail. Among them are protecting the confidentiality, availability and integrity of personal information. Protective measures include access controls to physically protect the systems and input controls to monitor and regulate any modification, deletion or storage of personal information.

Amendment to Data Protection Acts defines requirements in detail

Since the amendment to section 11 of the German Data Protection Act entered into force on 1 September 2009 users have been required to confirm that the providers to whom they will entrust their data for transfer to the cloud have taken adequate technical and organisational measures to ensure the protection of personal information. The contract for commissioned data processing must also include certain basic information, such as the use of sub-contractors. For the duration of the contractual relationship the user must continually confirm that the data given to the provider is secure, and also document the results of the inspections. How do providers organise data processing today and where do they process user data? In practice, do cloud users actually verify whether their providers are fulfilling all data protection requirements? When this is the case, how do providers react to these enquiries? PwC asked the survey respondents about their experiences in this area.

4.2. Survey results

Figure 12: Location of data

Q: In which countries does your company currently have data processing centres and/or servers that are used to store user data?
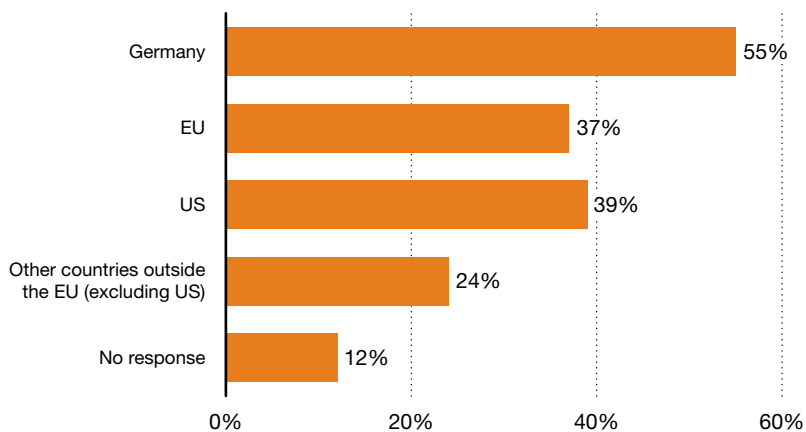
A good half of the providers used servers or data processing centres in Germany. As expected, the larger providers tended to store their data in more locations than smaller providers.

Just 30% of the providers stored their user data exclusively in Germany. This means that for 25% of the providers, data transfer outside Germany cannot be ruled out. Larger providers tend to allow their customers to decide whether they want their data to be stored exclusively in Germany more often. This could be due to the fact that smaller companies with a higher percentage of cloud services may use more sub-contractors who are not able to offer a choice of specific locations.

One third of cloud providers and one half of the large providers stored their data in a country outside the EU (excluding the United States). Of the companies surveyed, there were also large providers that stored their customer data exclusively outside the EU.

Figure 13: Customer enquiries about data protection and reactions of service providers

Q: Have customers asked you which measures you have implemented in accordance with section 11 of the German Federal Data Protection Act?

Q: Does your company have a formal, standard procedure for responding to customer enquiries of this kind?

	Yes	No	No response
Customer enquiries regarding § 11 Federal Data Protection Act	57%	27%	16%
Standard procedure for responding to customer enquiries about data protection	57%	27%	16%
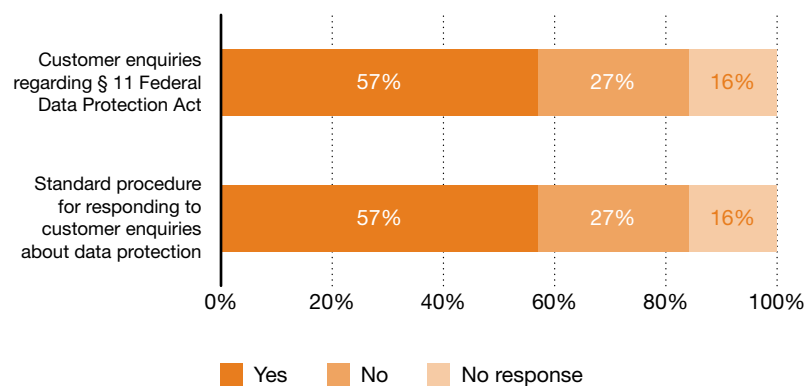
Of the providers surveyed, 57% said that their customers had already enquired about data protection measures taken in accordance with section 11 of the German Federal Data Protection Act, and 57% also reported having a formal, standard procedure for responding to customer enquiries of this type. The corresponding figures suggest that only those companies who have received customer enquiries have established a standard procedure. This implies that the other providers have yet to prepare any standard response to customer enquiries.

5. Information security

It is just about impossible to imagine a company without an IT system these days. IT systems have become essential for the successful management of most companies and public institutions. In some companies, parts of manufacturing or other areas that directly create value rely on IT delivery. For companies whose competitive advantage is based on maintaining an information edge (e.g., research and development), the confidentiality and integrity of all electronically processed information must be guaranteed. A breach in IT security can result in considerable economic damages. As such, all IT systems containing sensitive data must be protected on all levels.

How I see it

"Cloud computing is a feasible option for managing local IT. In particular, desktop as a service with hardware independence helps globally active companies reduce heterogeneity and cut costs."

Dr. Roland Schütz, Chief Operating Officer, Lufthansa Systems AG

Information security is not an end in itself, but needs to be considered with economic factors in mind. Companies need to achieve an adequate level of security and continually ensure it is aligned with their needs. This is precisely what an information security management system (ISMS) does. The ISMS provides a framework for taking measures to protect sensitive data from potential threats and concrete dangers. This allows companies to avoid fines and damage to their reputation and also to minimise operational risks. In practice, information security management is based on the ISO/IEC 2700-series standards, on ISO/IEC 15408 and/or on a country's own recommendations. In Germany, the IT basic protection guidelines (IT-Grundschutz-Kataloge) published by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) outline measures for implementing an effective information security management system.

5.1. Information security and cloud computing

When companies place data in the cloud, they surrender their ability to exercise control over it. At the same time, the confidentiality, integrity and availability of information must continue to be guaranteed. In contrast to other conventional outsourcing solutions, protection and control measures have to extend beyond local servers and data processing centres to various server systems (logical security) and data processing centres (physical security) that are located across the world. Up until now, providers have installed firewalls to keep the user data stored in their data processing centres safe from attacks and unauthorised access internally and externally. But this measure does not offer adequate protection in a cloud with locations in different countries and providers. The only thing that can guarantee the protection of sensitive company data is a comprehensive, global ISMS.

New risks require new measures

Many public cloud solutions deliver services to a number of users at the same time. In order to use the resources of a physical system in the most efficient manner possible, the applications of various users are run at the same time (multi-client capability). In this environment, confidential data, such as personal information, product information or upcoming innovations, are particularly endangered by the potential for unintended access (e.g., by another client) and security breaches (hacker attacks). This cloud-specific feature alone makes clear how important risk analysis and the continuing re-evaluation of security risks are.

The risk of disaster or insufficient capacity is another issue that cannot automatically be ruled out in the cloud. Who is able to guarantee that the physical resources available will always be sufficient for a number of often changing users to use simultaneously? To prepare for the event of a disaster, it is also wise to define suitable alternatives and agree on the return to operations so that business operations can be maintained.

PwC asked the providers surveyed about their information security situation and which aspects they found particularly important. We also wanted to know if they had arranged emergency plans with their customers so that they would be prepared for a potential disaster.

5.2. Survey results

Figure 14: Information security guarantees for users

Q: How well is your company currently able to guarantee information security for your customers?
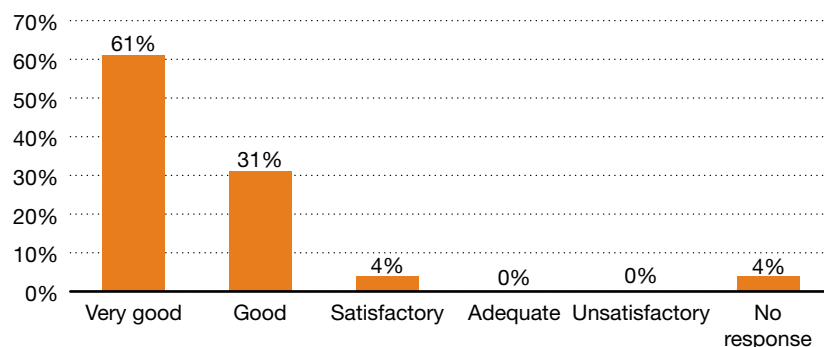
Almost two thirds of those surveyed said that they were currently doing very well in terms of guaranteeing information security for their customers; however, it must be assumed that considerations of values and external expectations influence answers about information security to some extent. Positive answers to questions regarding socially desirable behaviour are more common than negative ones. One clear trend was that the assessments of larger providers were better than those of smaller ones, and that the assessments of companies that mostly supplied large customers were better than those with smaller customers. The most important aspects of guaranteeing information security were having a detailed risk analysis as a basis for planning security measures and the certification of information security (e.g., through ISO/IEC 2700-series standards). Considered only slightly less important were security penetration tests (simulated hacker attacks), the adaptation of security concepts and customer-commissioned audits by an external third party.

Figure 15: Aspects of information security

Q: What role do the following aspects play in guaranteeing the protection of customer information?
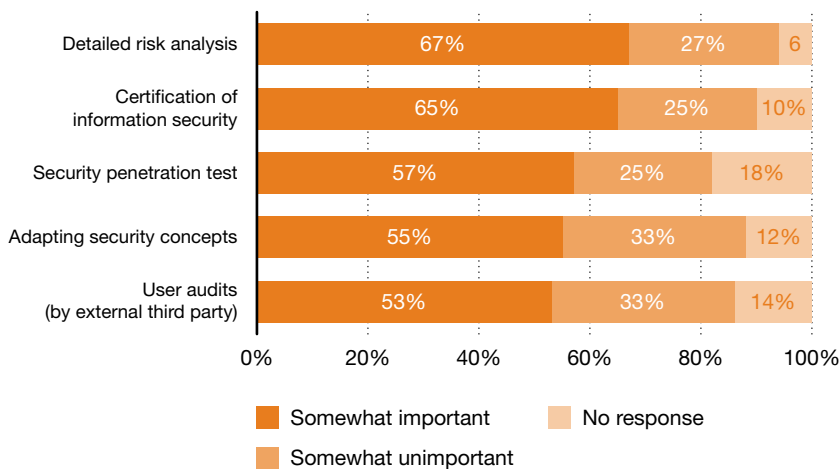
Detailed risk analyses, certifications of information security and external audits seemed to be more important for the providers that mainly served large companies than for those that mainly served small companies.

External audits, certifications and penetration tests were more important for larger providers than for smaller ones.

Only one aspect was more important for smaller providers: the adaptation of security concepts.

Figure 16: Emergency plans

Q: Does your company contractually arrange emergency plans with its customers?

Yes, in case of disasters	55%
Yes, for data protection or security incidents	55%
No	27%
No response	12%
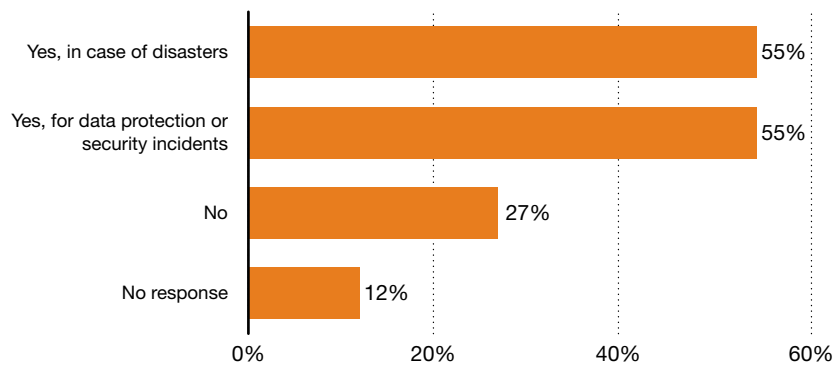
More than half of the participating providers contractually arranged emergency plans for disasters or breaches of data protection or security. There was no contractually arranged plan among 27% of the providers. These companies were almost exclusively smaller cloud providers with fewer than 500 employees in Germany.

6. Outlook

We asked the participating providers about different trends they expect to see in the German cloud computing market. We were interested in how they expected sales to develop over the next five years and also how the cloud computing market itself will develop.

Figure 17: Sales outlook for cloud services

Q: How will sales for your cloud services develop in the next five years?

Will increase	73%
Will remain the same	27%
Will decrease	0%
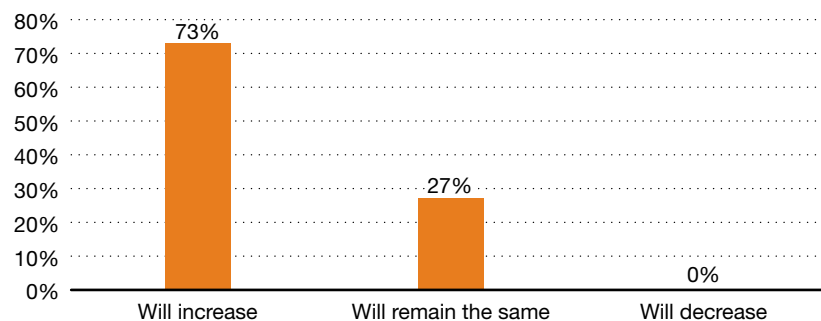
Just under three quarters of the providers surveyed expected that the percentage of cloud services in their German total business would grow. The respondents that did not expect any difference in sales were almost all smaller providers. None of the respondents expected sales to drop.

Figure 18: Assessment of market trends

Q: How do you think the market will develop?

	Somewhat agree	Somewhat disagree
	Neutral	No response

The more specialised providers thought that internet-based work would become normal, and that this future scenario would also mean that the ability to integrate and combine cloud services would become more important. Larger providers and providers that mostly served large companies seemed particularly convinced of this last point.

The majority of providers expected that cloud computing will pose new challenges for vendor management and related provider control systems.

The question of whether culture-based reservations against cloud computing would persist in the long term in Germany proved divisive; less than half of the respondents believed that the negative view of cloud computing would last for long.

Opinions also varied widely concerning the question of whether cloud computing will make IT departments less important or change current sales models. In particular, the smaller providers believed that more cloud providers would focus on internet sales in the future. It remains unclear, however, exactly why providers think that sales models won't change. It is surprising given the fact that more than 80% of the survey participants offered SaaS solutions, so, as licensing business drops off, it is precisely these companies that will be forced to rediscover or increase use of internet sales.

The results of the survey have shown that cloud computing is a dynamic type of IT service that can be adapted to fit users' needs. It combines different technical developments and opens up fascinating new opportunities for both providers and users. While the underlying technologies are not new, their further development holds immense innovation potential for providers and users of IT services. With that, cloud computing forms a basis for completely new sales and use channels for IT services, and simultaneously prepares the ground for completely new processes and business models.

Methodology

This survey was conducted in three stages. In the first step, eight telephone interviews were conducted to optimise the questions in the survey. The subsequent field phase consisted of 51 telephone interviews. These were conducted by an independent market research institute as computer-aided telephone interviews (CATI). The anonymity and personal data of the respondents was strictly protected by the market research institute. The field phase took place from 25 August to 7 September 2010.

In addition to the telephone survey, PwC conducted 10 expert interviews with providers selected from the German cloud computing market. Excerpts from these conversations have been used to illustrate different aspects of the survey in "The results of the survey" section.

The conversations with the experts were held from 22 September to 5 October 2010.

The group of respondents was composed primarily of members of strategic management in cloud services provider companies.

After the data was collected, it was analysed to define approximate qualitative trend statements according to the following aspects:

- Providers with up to 499 employees in Germany were compared to providers with 500 and more employees. In the results, these groups have been referred to as "smaller providers" and "larger providers."

- Information about the providers' customers was also evaluated. Providers that primarily served smaller companies were differentiated from providers who primarily served larger companies with more than 2,000 employees in Germany.

- In terms of the ratio of cloud services to the total business of the provider, larger providers whose cloud services sales were less than 10% of their total business were compared with smaller providers with a higher percentage of cloud services in their portfolio.

The sample in the study comprised providers in the German cloud computing market. Our survey had a response rate of 71%.

The figures used to illustrate the results of the study have been based on a total sample of n=51 unless otherwise noted.

Demographics: Cloud services providers

Figure 19: Position of survey participants in their companies

Q: What is your position in your company?

- Head of sales/communications/marketing
- Head/manager of IT
- Board/managing director
- Other (e.g., chief security officer, vice-president)

34%
31%
29%
6%
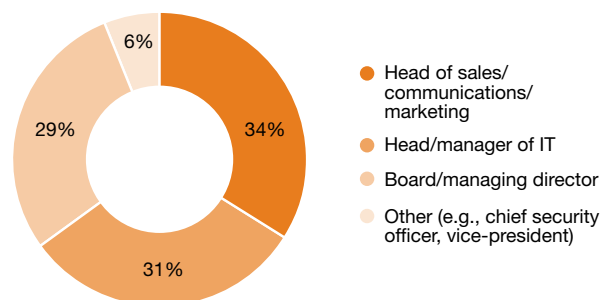
The 51 participants we surveyed worked on the strategic management level of cloud computing providers in the German market.

Figure 20: Number of employees in Germany

Q: How many employees does your company have in Germany?

- ≤ 50
- 51–499
- 500–5.000
- > 5.000
- No response

31%
29%
22%
16%
2%
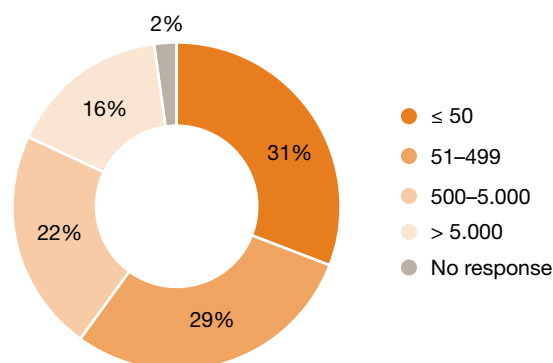
To define company size, we asked each respondent how many employees their company had in Germany: 60% of the cloud providers surveyed employed fewer than 500 people in Germany. Just under 40% of respondents employed more than 500.

Figure 21: Employees in cloud services

Q: How many employees does your company have working in cloud services in Germany?
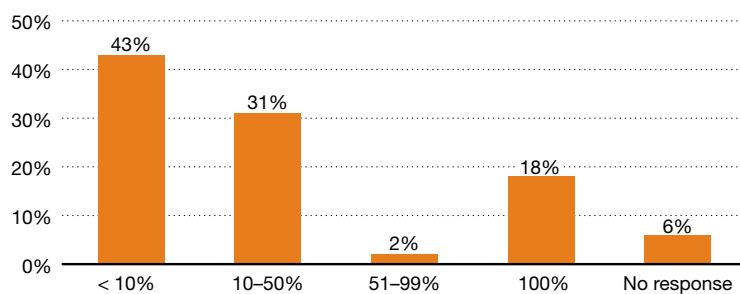
We also asked what percentage of employees worked in cloud services in Germany. The answers varied widely: for 43% of the providers, less than 10% of their employees worked in cloud services. Just under a third of companies had 10% to 50% of their staff working in cloud services. It is not surprising that the smaller providers employed proportionally more people in cloud computing than the larger providers. Currently none of the larger providers is 100% specialised in cloud services.

Figure 22: Total net sales in last fiscal year

Q: How high were the total net sales in Germany for your company in the last fiscal year?

- < 20 Mio. €
- 20–499 Mio. €
- ≥ 500 Mio. €
- No response
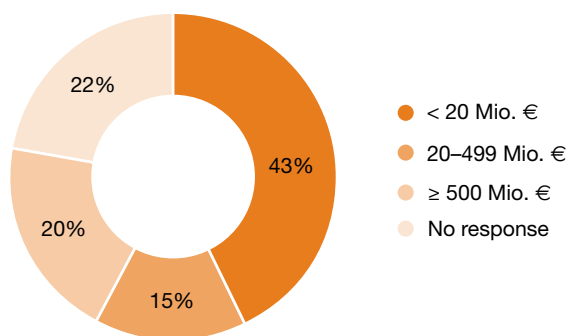
Last year's total net sales in Germany surpassed €500 million for one fifth of the providers surveyed, while 15% recorded sales of between €20 million and €500 million. Sales of less than €20 million were listed by 43% of respondents. The majority of participants who gave no response to this question were smaller providers. The following figure shows cloud services as a percentage of total sales.

Figure 23: Cloud services as a percentage of total business in Germany

Q: What percentage of your total business in Germany comes from your cloud services?
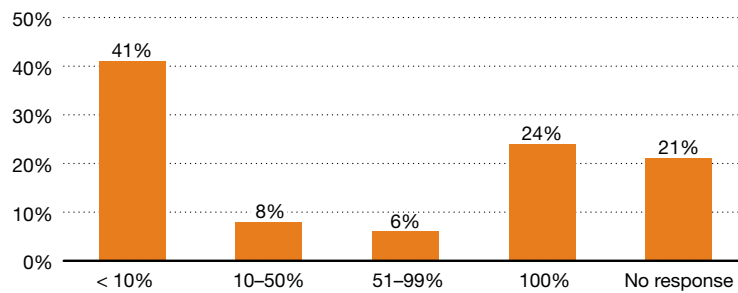
Cloud services providers also proved to be a very heterogeneous group in terms of the percentage of their total business coming from cloud services. Some respondents offered 100% cloud services, while others had a share of less than 10% of their business portfolio. Only seven respondents answered with a share of between 10% and 99%. Just under one quarter of providers reported that cloud services made up 100% of their business portfolio. Only the smaller providers focused exclusively on cloud computing.

Figure 24: Size of cloud services customers in Germany

Q: How big are the companies that you provide cloud services to?

Company (> 2,000 employees)   Company (< 500 employees)
Company (500–2,000 employees)   No response
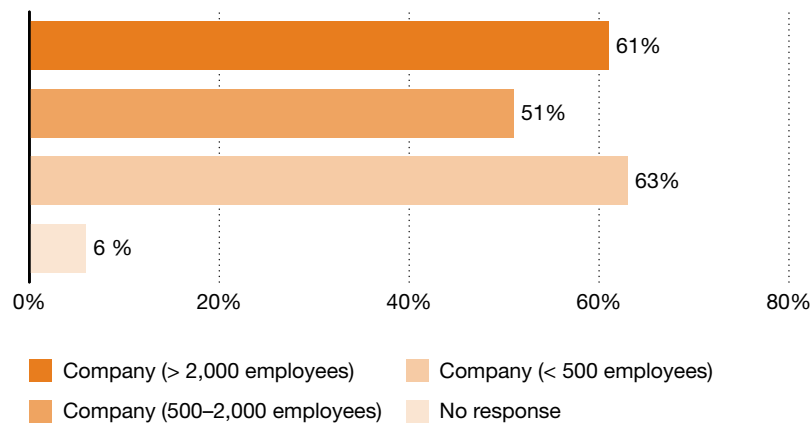
Interestingly, the providers interviewed reported that they provided practically the same amount of cloud services to smaller and larger companies. This is surprising since it is often said that cloud computing pays off for the middle market and that larger companies will only join in later.

In response to the question about the size of their main customer group, 42% of providers said they served companies with more than 2,000 employees, while 23% of participants said that their main customer group was companies with between 500 and 2,000 employees. One third of respondents supplied companies that had fewer than 500 employees with cloud services.

Figure 25: **Customers according to industry**

Q: Which industries do your cloud customers work in?

Industry	Percentage
Chemicals, pharmaceuticals, health care	63%
Financial sector	63%
Industrial manufacturing	63%
Technology, M&C	61%
Retail and consumer goods	59%
Automotive industry and suppliers	59%
Energy industry	57%
Transport and logistics	57%
Public sector	39%
No response	12%
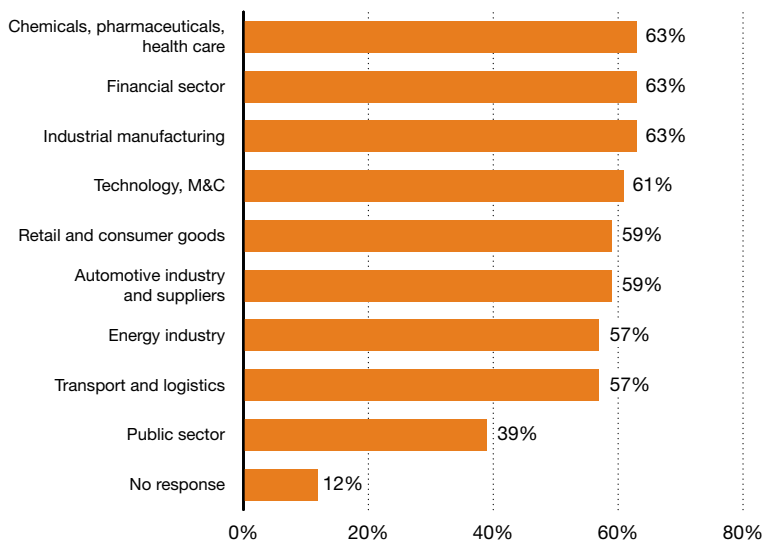
On average, the respondents listed five industries that they worked for. This can be traced back to the fact that a number of cloud services can be implemented across most industries (mainly in the area of support processes, see also Figure 27). This statement is supported by an almost equal number of mentions across all industries. Our sample shows that there seems to be very few purely industry-oriented solutions on the market right now.

Figure 26: Types of cloud computing services offered by the providers surveyed

Q: What type of cloud computing services does your company provide?

Service	Percentage
Software as a service	83%
Infrastructure as a service	53%
Advisory services for cloud computing	51%
Platform as a service	39%
Business process as a service	27%
Other cloud services (e.g., desktop as a service)	21%
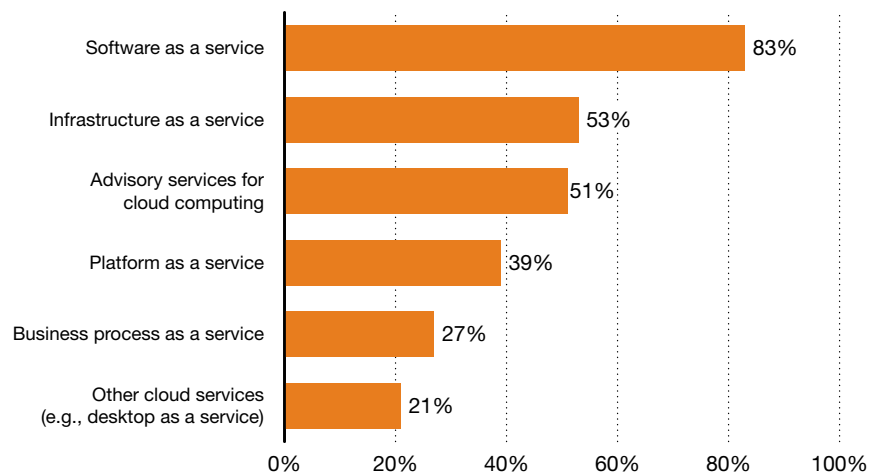
Each of the providers surveyed offered an average of three cloud services to the German market. There was a clear emphasis on software as a service. Half of the respondents offered services related to infrastructure as a service, and half also offered general advisory services related to cloud computing. Business process as a service, however, was only found in the portfolios of one out of four providers.

As expected, software as a service, platform as a service and infrastructure as a service played the most important roles in terms of sales. None of the respondents listed business process as a service as their best-selling service, however, an increase in sales is expected in the coming years.

Figure 27: SaaS solutions offered by the providers surveyed

Q: Which SaaS solutions does your company offer?

Solution	Percentage
Collaboration	64%
Back-up and archiving	60%
Customer relationship management	57%
Content management systems	50%
Enterprise resource planning	48%
Office software	36%
Financial accounting	31%
Human resources	31%
Supply chain management	26%
Payment systems (e.g., for credit cards)	21%
Other	52%
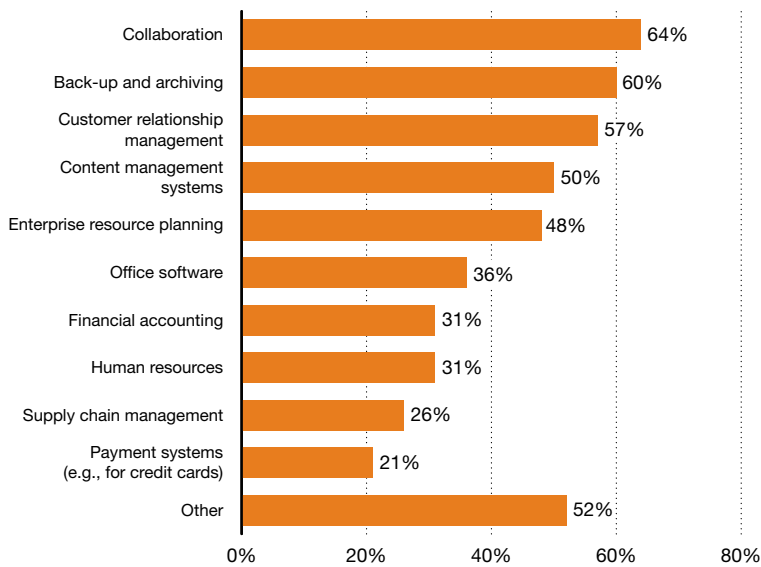
The providers who offer software as a service offer five different solutions on average. Interestingly, a number of traditional support processes (purchasing, sales, human resources, accounting, etc.) are already captured by SaaS solutions. More than half of the SaaS providers had other services in their portfolios as well. Of these, the most significant were unified communication (approximately 29%), business intelligence (approximately 23%), security (approximately 18%) and e-commerce (approximately 11%). There were also individual mentions of marketing, document recognition (optical character recognition, or OCR), disaster recovery and compliance. The results made clear that smaller providers tend to follow a niche strategy.

Figure 28: Types of clouds supported

Q: What type of cloud solutions does your company offer?

- Private clouds only
- Public clouds only
- Both public and private clouds

50% · 25% · 25%
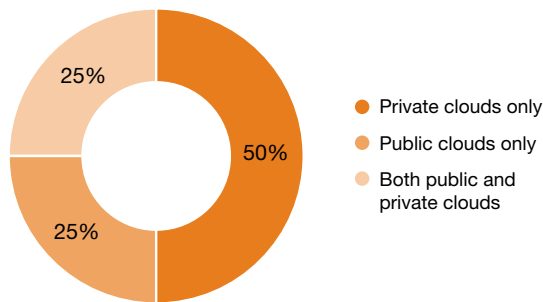
One quarter of cloud solutions are offered over the internet (public cloud). Half of the cloud services used are implemented and operated by either the customers themselves or by a provider in an environment provided exclusively for the customer (private cloud). The remainder of the solutions are offered as private clouds and as public clouds.

Index

Of further interest

PwC offers a number of viewpoints relating to cloud computing. Below you will find a sampling of available thought leadership. Click on any of the titles to visit the web page and read or download the pdf files.

10Minutes on the cloud

Cloud computing is resolving typical IT barriers to agility: complexity, solid infrastructures and long lead times for changes. It holds the potential to change the way companies do business. Those who integrate a cloud strategy with their business imperatives will benefit the most. For example:

- Companies can use cloud computing to accelerate the experimentation cycle and improve on time-to-market for the successes.

- The inherent flexibility of cloud architecture allows enterprises to meet changing needs of end customers with agility.

- Cloud-based systems that can be integrated seamlessly and rapidly are making companies better orchestrators across their network of suppliers, time zones and cultures.

A view on cloud computing: Is it important and is it secure?

This whitepaper, written by Dr. David Jacobson, director of the Emerging Technologies practice at PwC Canada, clarifies the differences between cloud computing models such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). It also discusses how some of Canada's software CEOs feel about the technology, using the results of the 2010 PwC Survey of Canadian Software Company CEOs.

Embracing the power of the cloud

A brief article on how and why cloud computing is causing a fundamental shift in how technology solutions are being delivered to support business.

Protecting your brand in the cloud: Transparency and trust through enhanced reporting

This paper explores how cloud risks could negatively impact companies' brands. Many cloud providers are working to address risks with strong controls, but these providers lack a trusted way to demonstrate the adequacy of their infrastructures to potential customers. Third-party assurance may be the answer for both cloud users and providers. With third-party assurance, a trusted third party evaluates and reports on a cloud provider's ability to deliver promised levels of service and protection from risk.

Security among the clouds

Cloud computing promises significant cost savings, diminished IT complexity and increased flexibility in managing IT and responding to market changes. However, CISOs must consider the risks associated with these new computing models, possibilities of data loss, data leakage, downtime of service providers, regulatory constraints and risk of intellectual property theft.

Technology forecast: Issue 4 2010 – Driving growth with cloud computing

This series of articles looks beyond better and cheaper IT to a step or two ahead. How will cloud computing impact the enterprise more broadly? What does cloud computing mean for business strategy? What does it mean for the finance organisation? After cloud computing has "reformed" IT, does it have an answer to these concerns?

Contacts

PwC delivers value with a global perspective through local implementation. Please contact any of the leaders listed below to discuss the challenges facing your company and how we can help you.

Report authors

Dr Georg Kämpfer
+49 69 9585 1333
georg.kaempfer@de.pwc.com

Markus Vehlow
+49 69 9585 2293
markus.vehlow@de.pwc.com

Cordula Golkowsky
+49 69 9585 5022
cordula.golkowsky@de.pwc.com

Cloud computing leaders

Australia
Dave Bostock – Brisbane
+61 7 3257 8405
david.bostock@au.pwc.com

David Moore – Sydney
+61 2 8266 3313
david.e.moore@au.pwc.com

Austria
Andreas Plamberger
+43 1 501 88 2837
andreas.plamberger@at.pwc.com

Brazil
Ricardo Neves
+55 11 3674 3250
ricardo.neves@br.pwc.com

Canada
Albert Silverman
+1 416 869 2990
albert.silverman@ca.pwc.com

China/Singapore
Greg Unsworth
+65 6236 3738
greg.unsworth@sg.pwc.com

Shong Ye Tan
+65 6236 3262
shong.ye.tan@sg.pwc.com

Germany
Markus Vehlow
+49 69 9585-2293
markus.vehlow@de.pwc.com

India
Rajesh Rajan
+91 80 40794008
rajesh.rajan@in.pwc.com

Ireland
Richard Day
+353 1 792 8573
richard.day@ie.pwc.com

Japan
Maki Matsuzaki
+81 80 2079 9278
maki.matsuzaki@jp.pwc.com

Netherlands
Adrie Briene
+31 8879 25241
adrie.briene@nl.pwc.com

Poland
Tomasz Bejm
+48 22 746 6750
tomasz.bejm@pl.pwc.com

Russia
Doug Downing
+7 495 223 5196
douglas.downing@ru.pwc.com

Switzerland
Yves Holenstein
+41 0 58 792 1337
yves.holenstein@ch.pwc.com

United Arab Emirates
Taha Khedro
+971 4 304 3300
taha.khedro@ae.pwc.com

United Kingdom
Philip Shepherd
+44 20 7804 9366
philip.a.shepherd@uk.pwc.com

United States
Mike Pearl
+1 408 817 3801
michael.pearl@us.pwc.com

Techology industry leaders

Australia
Rod Dring
+61 2 8266 7865
rod.dring@au.pwc.com

Brazil
Estela Vieira
+55 21 3232 6069
estela.vieira@br.pwc.com

Canada
Chris Dulny
+1 416 869 2355
christopher.dulny@ca.pwc.com

China
Alison Wong
+86 21 2323 2551
alison.cy.wong@cn.pwc.com

France
Xavier Cauchois
+33 1 56 57 10 33
xavier.cauchois@fr.pwc.com

Germany
Werner Ballhaus
+49 211 981 5848
werner.ballhaus@de.pwc.com

India
Hari Rajagopalachari
+91 80 4079 4002
hari.rajagopalachari@in.pwc.com

Japan
Shigeru Shiina
+81 3 3546 8480
shigeru.shiina@jp.pwc.com

Korea
Yong-Won Kim
+82 0 2 709 0471
yong-won.kim@kr.pwc.com

Netherlands
Marcel Jakobsen
+31 0 104075354
marcel.jakobsen@nl.pwc.com

Russia
Natalia Milchakova
+7 495 967 62 40
natalia.milchakova@ru.pwc.com

Singapore
Greg Unsworth
+65 6236 3738
greg.unsworth@sg.pwc.com

Taiwan
Andy Chang
+886 4 2328 9191 ext. 25216
andy.chang@tw.pwc.com

United Kingdom
Jass Sarai
+44 1895 522 206
jass.sarai@uk.pwc.com

United States
Rob Gittings
+1 408 817 3730
robert.gittings@us.pwc.com

The results of this survey and the contributions from our experts are meant to serve as a general reference for our clients. For advice on individual cases, please refer to the sources cited in this study or consult one of the PwC contacts listed at the end of the publication.

Statements titled "How I see it" represent the opinions of their authors.

www.pwc.com

BS-11-0300-A.0311.JL