Cloud Computing
Navigating the Cloud
Cloud Computing

Navigating the Cloud
Cloud Computing
Navigating the Cloud

Published by PricewaterhouseCoopers AG

By Markus Vehlow and Cordula Golkowsky

With Eiko Ermold, Marius Fetzerberger, Juri Frommer, Martin Glaser,
Andreas Gorholt, Joachim Mohs, Dirk Nippert, Christian Schmidt, Alexia Spieler,
Konrad Wachowiak and Falko Wendt

Telephone survey designed, managed and evaluated by
denkstelle hamburg

Independent market research institute for the telephone survey
C.M.R. Institut für Communication- & Marketing-Research

Layout
Schölzel, Möhring GmbH, Frankfurt am Main

All rights reserved. No part of this publication may be reproduced, photographed on microfilm or
stored or processed electronically without the prior written consent of the publisher.

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.
Preface

Dear reader,

Technology and innovation bring about constant change in our society. They shape how we live in an increasingly digitalised world – a place where technical developments are the foundation for our activities at home and at work. Technology and innovation are also integral parts of modern communication and help make our work processes more efficient and profitable. This is no small challenge. A new player recently joined our business world to help companies successfully rise to this challenge: the name of the game is 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, not without its risks and challenges. Companies need to keep them in mind in order to reap the full benefits of cloud computing.

This survey by PwC identifies the most significant challenges for cloud computing in Germany. These include contracts, data migration, risks and compliance, the protection of data and information security.

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.

The results of the survey make for informative and insightful reading. We hope you enjoy reading them.

Prof. Dr. Georg Kämpfer
Markus Vehlow
Cordula Golkowsky
Contents

Preface .......................................................................................................... 5
List of figures ................................................................................................. 8
List of abbreviations .................................................................................... 11
Summary ..................................................................................................... 12
Methodology ............................................................................................... 15
Cloud service providers .............................................................................. 16

A  Background ............................................................................................. 22

B  The results of the survey ........................................................................ 27
  1  Contract creation .................................................................................... 27
  2  Data migration ........................................................................................ 32
  3  Risks and compliance ............................................................................ 36
  4  Data protection ....................................................................................... 40
  5  Information security ............................................................................... 45
  6  Outlook .................................................................................................. 50

Index ............................................................................................................ 54
Contacts ...................................................................................................... 58
List of figures

Fig. 1 Position of survey participants in their companies ................... 16
Fig. 2 Number of employees in Germany ........................................... 16
Fig. 3 Employees in cloud services ..................................................... 17
Fig. 4 Total net sales in last fiscal year ................................................ 17
Fig. 5 Cloud services as a percentage of total business in
Germany .................................................................................... 18
Fig. 6 Size of cloud services customers in Germany ....................... 18
Fig. 7 Customers according to industry .............................................. 19
Fig. 8 Types of cloud computing services offered by the providers surveyed ......................................................... 19
Fig. 9 SaaS solutions offered by the providers surveyed ................. 20
Fig. 10 Types of clouds supported ..................................................... 21
Fig. 11 Evaluation of customer cloud strategies ................................ 24
Fig. 12 Significant factors affecting customer satisfaction ............... 24
Fig. 13 Challenges in the cloud computing market ......................... 25
Fig. 14 Cancellation notice periods ..................................................... 29
Fig. 15 Additional charges after cancellation ................................. 29
Fig. 16 Service delivery guarantees .................................................. 30
Fig. 17 Cloud chaining – use of sub-contractors .............................. 30
Fig. 18 Data migration support for new customers ......................... 34
Fig. 19 Data migration support after cancellation ............................ 34
Fig. 20 Compliance management .................................................... 38
Fig. 21 Challenges in fulfilling compliance requirements .............. 38
Fig. 22 Location of data .................................................................. 43
Fig. 23 Customer enquiries about data protection and reactions of service providers ........................................................ 43
Fig. 24 Information security guarantees for users ......................... 47
Fig. 25  Aspects of information security ................................................48
Fig. 26  Emergency plans ......................................................................49
Fig. 27  Sales outlook for cloud services .............................................51
Fig. 28  Assessment of market trends .....................................................52
## List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDSG</td>
<td>Bundesdatenschutzgesetz (German Federal Data Protection Act)</td>
</tr>
<tr>
<td>BPaaS</td>
<td>business process as a service</td>
</tr>
<tr>
<td>CATI</td>
<td>computer-aided telephone interviews</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>IaaS</td>
<td>infrastructure as a service</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISMS</td>
<td>information security management system</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>M&amp;C</td>
<td>media and communications</td>
</tr>
<tr>
<td>OCR</td>
<td>optical character recognition</td>
</tr>
<tr>
<td>PaaS</td>
<td>platform as a service</td>
</tr>
<tr>
<td>SaaS</td>
<td>software as a service</td>
</tr>
<tr>
<td>SLA</td>
<td>service level agreement</td>
</tr>
</tbody>
</table>
Summary

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. 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.

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 which 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 which 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.

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.

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
Cloud Computing

Summary

Blue skies ahead for cloud computing

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.

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.
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 August 25th to September 7th, 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 chapter B, “The results of the survey”.

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

The group of respondents was composed primarily of members of strategic management in cloud service 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.
Cloud service providers

Fig. 1  Position of survey participants in their companies

The 51 participants we surveyed worked on the strategic management level of cloud computing providers in the German market.

Fig. 2  Number of employees in Germany

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.
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.

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

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.
Cloud service 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.

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 to companies that had fewer than 500 employees with cloud services.
Which industries do your cloud customers work in?

![Bar chart showing distribution of industries](chart1.png)

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 9). 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.

What type of cloud computing services does your company provide?

![Bar chart showing distribution of cloud services](chart2.png)

Each of the providers surveyed offered an average of three cloud services on 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.

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.
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.
Cloud Computing Background
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 for, 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.

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 things:

• 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.
How developed is the cloud strategy of your customers? What is your general impression?

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.

What are the critical success factors in maintaining customer satisfaction?

Fig. 11 Evaluation of customer cloud strategies

Fig. 12 Significant factors affecting customer satisfaction
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.

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,

![Fig. 13 Challenges in the cloud computing market](image-url)
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 12) 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.

How I see it
“Not every cloud is the same. There are major differences between private clouds and public clouds: pay-per-use and multi-tenancy are two examples of hallmarks of cloud computing. And both are only available in public clouds.”

Mani Pirouz, Head of Product Marketing, salesforce.com Germany GmbH

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

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.

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...
The results of the survey

Cloud Computing

What kind of service delivery do you guarantee your customers contractually?

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.

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

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.
Cloud Computing

The results of the survey
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 structures. 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.

How I see it

“Cloud computing is leading IT to a new type of usability, where electronic business processes can be compared and replaced with the click of a mouse. But for this to happen, the CIO will need to expand the application focus through open information management.”

Stephan Haux, Senior Product Manager – International, Iron Mountain Digital GmbH

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.
Provider support is key

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.

2.2 Survey results

How do you support new customers in transferring their data?

![Fig. 18 Data migration support for new customers](image)

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. 33% of respondents gave no response to this question.

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

![Fig. 19 Data migration support after cancellation](image)

No response 23%

Yes 59%

No 18%
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

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.

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.
Cloud Computing

The results of the survey
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 October 24th 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.

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

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.

Since the amendment to section 11 of the German Data Protection Act entered into force on September 1st 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

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.

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

Does your company have a formal, standard procedure for responding to customer enquiries of this kind?
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 are 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.
How I see it
“The cloud opens up new options to evaluate IT performance and is an impetus for delivering more flexibility and efficiency. The foundation and the future of IT is based on a shared infrastructure that, with automation and simplification, helps to keep up with business.”

Alexander Wallner, Area Vice President Germany, NetApp Deutschland GmbH

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

How well is your company currently able to guarantee information security for your customers?

![Fig. 24 Information security guarantees for users](image)
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.

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.
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.

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.

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

![Sales outlook for cloud services](image)
How do you think the market will develop?

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.

How I see it

"Cloud computing opens up completely new opportunities – for individual companies and also for Germany as a business location. To take advantage of these opportunities, the industry – providers and users – government and science need to work together. The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) is introducing its projects into the programme planned by the German Federal Ministry of Economics and Technology with the goal of promoting increased use of cloud services and developing a competitive industry for cloud services in Germany."

Dr. Mathias Weber, Head of IT Services, BITKOM, Federal Association for Information Technology, Telecommunications and New Media

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, why exactly 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.
# Index

## A

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>20</td>
</tr>
<tr>
<td>Additional charges</td>
<td>29</td>
</tr>
<tr>
<td>Archiving</td>
<td>20</td>
</tr>
</tbody>
</table>

## B

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business intelligence</td>
<td>20</td>
</tr>
<tr>
<td>Business process as a service</td>
<td>19</td>
</tr>
<tr>
<td>Business model</td>
<td>23</td>
</tr>
<tr>
<td>Business portfolio</td>
<td>18</td>
</tr>
</tbody>
</table>

## C

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification</td>
<td>41</td>
</tr>
<tr>
<td>Cloud chaining</td>
<td>30</td>
</tr>
<tr>
<td>Cloud strategy</td>
<td>24</td>
</tr>
<tr>
<td>Commissioned data processing</td>
<td>42</td>
</tr>
<tr>
<td>Compliance management system</td>
<td>37</td>
</tr>
<tr>
<td>Computer-aided telephone interviews</td>
<td>15</td>
</tr>
<tr>
<td>Cancellation</td>
<td>28</td>
</tr>
<tr>
<td>Cancellation notice period</td>
<td>29</td>
</tr>
<tr>
<td>Customer profile</td>
<td>37</td>
</tr>
<tr>
<td>Cloud computing, definition of</td>
<td>25</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>24</td>
</tr>
<tr>
<td>Contract, cancellation of</td>
<td>29</td>
</tr>
<tr>
<td>Contract, creation of</td>
<td>28</td>
</tr>
<tr>
<td>Contract lifecycle</td>
<td>28</td>
</tr>
<tr>
<td>Confidential data</td>
<td>47</td>
</tr>
</tbody>
</table>

## D

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data formats</td>
<td>33</td>
</tr>
<tr>
<td>Data migration</td>
<td>23</td>
</tr>
<tr>
<td>Data protection</td>
<td>23</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>20</td>
</tr>
<tr>
<td>Document recognition</td>
<td>20</td>
</tr>
<tr>
<td>Disaster risk</td>
<td>47</td>
</tr>
</tbody>
</table>

## E

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-commerce</td>
<td>20</td>
</tr>
<tr>
<td>Emergency plans</td>
<td>24</td>
</tr>
<tr>
<td>European Economic Area</td>
<td>41</td>
</tr>
<tr>
<td>European Community</td>
<td>41</td>
</tr>
</tbody>
</table>
Expert interviews............................................................................................................. 15

F

Fee-based services ........................................................................................................... 34
Field phase ....................................................................................................................... 15
Fines .................................................................................................................................. 28

G

Germany ............................................................................................................................. 16
German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) ................................................................. 46
German Federal Data Protection Act (Bundesdatenschutzgesetz) .................... 42
German Telecommunications Act (Telekommunikationsgesetz) ....................... 41
German Telemedia Act (Telemediengesetz) ................................................................. 41
German Social Code (Sozialgesetzbuch) ................................................................. 41

H

Human resources ............................................................................................................. 20

I

Industries ......................................................................................................................... 19
Information security ........................................................................................................ 24
Information security management system ................................................................. 46
Infrastructure as a service ............................................................................................. 19
Integration capacity ....................................................................................................... 24
Internal control systems ............................................................................................... 39
Internet sales .................................................................................................................. 52
ISO/IEC ............................................................................................................................ 46
IT strategy ......................................................................................................................... 24

L

Legal uncertainty ............................................................................................................. 28
Licensing business .......................................................................................................... 53
Licensing model .............................................................................................................. 25
Location ............................................................................................................................ 24
Loopholes ......................................................................................................................... 28

M

Maintenance ....................................................................................................................... 25
# Index

Master of the data ........................................................................................................... 42
Market research institute ................................................................................................. 15
Market trends ...................................................................................................................... 52
Migration tool .................................................................................................................... 34
Monitoring .......................................................................................................................... 31

**N**

Niche strategy .................................................................................................................. 20

**P**

Platform as a service ....................................................................................................... 19
Private clouds ...................................................................................................................... 21
Public clouds ...................................................................................................................... 21
Purchasing .......................................................................................................................... 20

**Q**

Questionnaire ................................................................................................................... 12

**R**

Response rate ................................................................................................................... 15
Return of data .................................................................................................................... 23
Return to operations .......................................................................................................... 47
Risk analysis ...................................................................................................................... 47

**S**

Safe harbour ..................................................................................................................... 41
Sales .................................................................................................................................. 16
Sanctions ........................................................................................................................... 28
Scalability ........................................................................................................................... 25
Scale effects ......................................................................................................................... 25
Security breaches .............................................................................................................. 47
Security concepts .............................................................................................................. 48
Security penetration tests ................................................................................................. 48
Server location ................................................................................................................... 25
Service delivery .................................................................................................................. 24
Service level agreements ................................................................................................. 24
Service quality ................................................................................................................... 25
Software as a service ......................................................................................................... 19
Sourcing governance ......................................................................................................... 23
Standardisation .................................................................................................................. 25
Standard procedure ......................................................................................................... 43
Standard service ................................................................................................................. 31
Sub-contractors ........................................................................................................ 25
Support processes .................................................................................................. 19

T

Telephone interviews ............................................................................................. 15
Total business ......................................................................................................... 18
Total net sales ......................................................................................................... 17
Total sample ............................................................................................................ 15
Trend statements .................................................................................................. 15

U

Unified communication .......................................................................................... 20
Unintended access ................................................................................................. 47
User audits ............................................................................................................... 38
US Department of Commerce .................................................................................. 41

V

Vendor lock-in ........................................................................................................ 33
Vendor management ............................................................................................... 52
With some 9,000 employees and a turnover of around €1,37 billion, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft is one of the leading auditing and consultancy firms in Germany. Experts at 29 locations work on behalf of national and international clients of every size. The focus is on assurance and business advisory services, tax services, and deals and consulting.