



White Paper Security in the cloud.

Securely harnessing the benefits of cloud computing.

.....T...Systems.....

Contents.

3	1. Introduction.
5	2. Security requirements: cloud computing vs. conventional environments.
6	2.1 A shift in security risks.
8	2.2 Potential problems.
9	3. Security measures for the cloud.
9	3.1 Three cloud models.
10	3.2 Security impacts of different models.
11	3.3 Data availability through failure safety.
11	3.4 Data storage location.
12	4. Implementing cloud computing.
12	4.1 Define requirements.
13	4.2 Selecting the right provider.
15	4.3 Migration.
17	5. Legal requirements and other compliance issues.
18	6. Conclusion.
19	7. Glossary.
20	8. Bibliography.
21	9. List of figures.

1. Introduction.

The cloud is an enduring new computing paradigm driven by greater specialization and industrialization in the ICT space. Cloud adoption rates have risen rapidly on the back of the tremendous economies of scale that ICT service outsourcing unleashes for users and providers. This helps to cut costs, boost availability and enhance quality and security. And these economies of scale increase dramatically with greater ICT industrialization.

Cloud computing is defined as a flexible delivery model for ICT services that uses powerful systems and networks with high transfer rates. It typically leverages distributed hardware and software resources and shared, redundant, multitenant platforms that deliver a high degree of scalability.

The cloud is essentially the next link in the evolutionary chain after software as a service (delivery of software over the Internet) and grid computing (central pooling and sharing of high-performance resources). It takes these concepts to the next level with high bandwidth, virtualization and other tried-and-tested technologies. Unlike its predecessors, though, clouds are more like comprehensive computing environments assembled from various ICT modules.

For personal and business users, cloud computing offers a way to run software (e.g. business applications and e-mail security) or utilize infrastructure (e.g. storage) dynamically over the Internet on an as-needed basis. Users typically pay only for the services they consume (pay per use).

Containing risks – reaping rewards.

Since providers centrally pool services such as e-mail, database applications or security solutions for a large number of users, they tap into vast economies of scale and can pass these savings on to customers. Users appreciate the simplicity and efficiency of cloud computing. They merely plug right into a sophisticated system – there is no need for capital investment on their part. Not that cloud computing is entirely effort-free: organizations still need to define the specifications for their business and lay them out in a contract with the provider. Overall, the cloud offers compelling business benefits, provided rigorous security is in place.

Projected spending on cloud computing in the next two years.

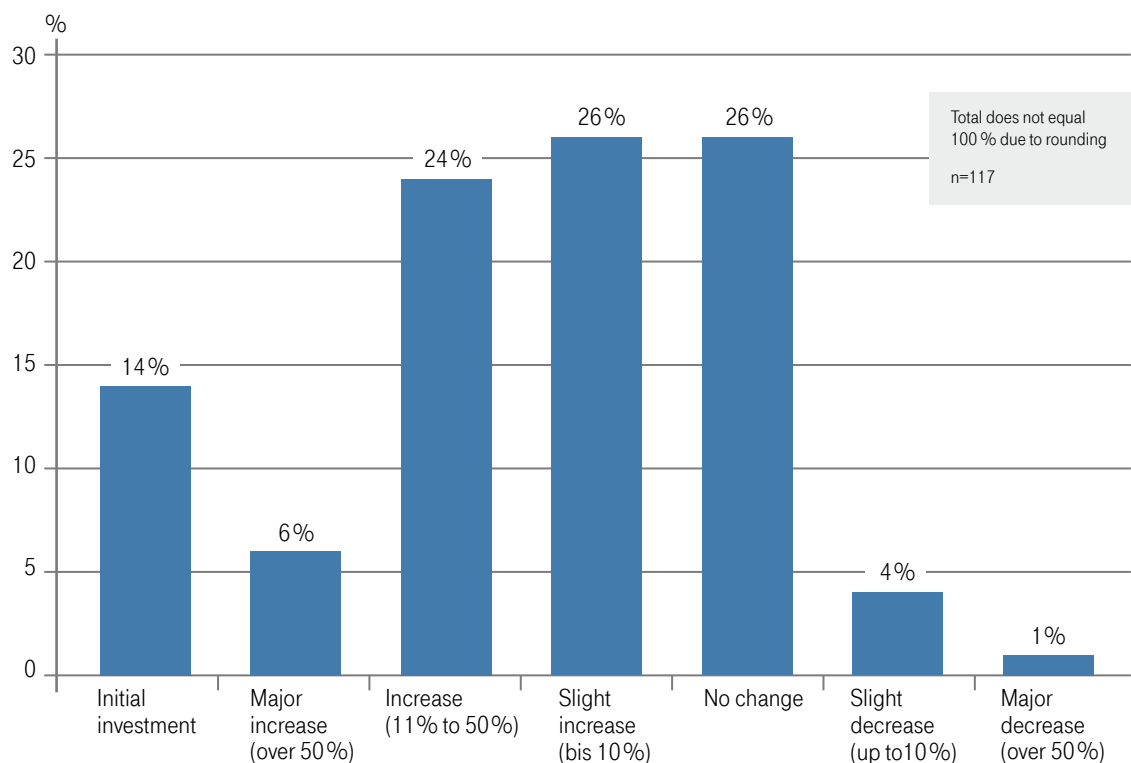


Fig. 1. [Source: IDC, Cloud Computing and services: the current picture and trends in Germany in 2009 (German only)]

Every ICT service model involves risk, especially when data and applications are entrusted to an outside provider. A particular risk may or may not be acceptable; it depends on the organization's security requirements. In cloud computing, where users share systems and platforms, the risk sources, types and forms will vary depending on the user's business model and how the ICT service is produced and provided. To remain protected, cloud users will have to maintain a solid repertoire of techniques for containing risk and enforcing security.

Experience shows that consuming ICT services in the cloud can improve security significantly. Many users, for instance, are unwilling to take all the necessary security precautions on a regular basis or invest the time and energy needed to maintain top quality. The cloud is an excellent choice for them, since established ICT providers have much more experience and highly trained personnel. Their core business is ICT services, and they will only survive if they provide services securely, reliably and effectively.

2. Security requirements: cloud computing vs. conventional environments.

Before moving ICT services to the cloud, organizations should clarify their security requirements. They may wish to compare the risks in conventional IT environments with those in cloud computing. There is an instinctive tendency to equate less control over the ICT environment with higher data security risks. This is misleading, though, as a comparison of security scenarios will show. Another factor is a threat's impact. Organizations are only exposed to a business risk if a threat can exploit a vulnerability and cause damage (its "business impact"). That makes it essential to manage risk and identify vulnerabilities, ideally through close cooperation between responsible users and competent providers.

Vulnerability management.

The first step in evaluating IT or business risks is to identify threats in terms of opportunities and impacts. What specifically or generally could happen in a cloud context? Next, the organization should probe for vulnerabilities, such as inadequate data backups or weak authentication before accessing data and ICT resources. The service provider should then integrate security processes. Vulnerabilities cannot be identified without analyzing the infrastructure and how it is used, while security risks can only be evaluated if users quantify the potential financial damage and business impact.



Security varies depending on the requirements.

Many medium-sized and some large organizations are lax about security. They may have defined procedures and assigned responsibility, but security policies are still not rigorously enforced day-to-day. Requirements are becoming more challenging, too, outstripping organizations' technical and procedural capabilities.

In these cases, organizations enjoy tighter security if they move IT resources to the cloud. A professional provider offers IT security as part of its core business. With its experience, more powerful infrastructure and highly trained workforce, it is much better poised to protect a high-performance data center against outside threats and run stable applications.

Comparison of potential risks in cloud computing and conventional delivery models for ICT services.



Failure due to overloading.

Privacy problems.

6

Hardware loss or theft.

Most people would cite unauthorized data access as a key threat. Conventional environments, however, have another, very real loss path for intellectual property: employees carrying mobile devices or USB flash drives with confidential or critical data. If they are lost or stolen and land in the wrong hands, the damage can be severe. After all, how many users have really encrypted and backed up the data on their systems? Cloud computing eliminates the risk of data loss through central data storage and the use of thin clients.

Availability problems due to server failure.

In a traditional IT environment, hardware breakdowns can inflict enormous damage if there is no failover capability. And few organizations have the funds in their budgets to build redundancy into every system. Cloud computing, by contrast, keeps availability high with various methods that stay affordable through economies of scale. Failures are kept under control.

Compliance problems due to distributed data storage.

Unlike in conventional IT environments, users do not always know where in the cloud their data and applications may be. Some providers also use subcontractors. These issues can pose legal problems, particularly in processing personal data (see sec. 5 “Legal requirements and other compliance issues”). There are, however, providers who can restrict data storage to, say, Germany or the European Union and confirm this commitment in a contract.

Out-of-date software.

Organizations that host their own IT environments will also maintain their software themselves. Maintenance is essential: every type of software has bugs and vulnerabilities that, once identified, can be fixed with patches. However, it is also complicated, potentially disruptive and can produce new errors. In cloud computing, this work is done by the provider, who applies patches centrally in order to preserve system stability and failure safety.

Liability issues.

Disagreements over liability occur in all ICT delivery models, including the cloud. In one example, a service level agreement is breached due to technical problems. There are two possible culprits: the network or the hosted IT systems. However, it is impossible to identify which one caused the problem. This does not happen with cloud providers with network capabilities who can supply and manage an end-to-end solution.

Virus threats.

Antivirus programs are commonly used in traditional IT environments. Some new malware can still slip under the radar, however, due to sluggish processors and infrequently updated antivirus software. In the cloud, this task can be centralized, enhancing its effectiveness and update frequency. All of the provider’s customers automatically enjoy the same level of protection.

Hackers.

Hackers could theoretically attack any system, data or application in any environment whatsoever. In conventional IT environments, the user is directly responsible for security and has to plan, implement, monitor and update security precautions such as firewalls, intrusion detection, virus scanners or server isolation from the public Internet. In the cloud, these activities fall to the provider.

Changing providers.

Switching to the cloud or changing providers means moving the entire application environment. Vast volumes of data and entire work environments will have to be ported. Business continuity can be assured, however, by migrating the data correctly and allowing employees to use the old and new environments simultaneously for a certain period of time. Experience is needed to maintain availability and avoid data loss during the transition.

2.2 Potential problems.

Legal issues figure prominently in the current debate about cloud computing's pros and cons. Many organizations need to know the location of the server hosting their data and applications. If they do not, they may run afoul of regulatory requirements such as the German Federal Data Protection Act. Especially financial service providers, life, health and casualty insurers – even institutions and government agencies that use personal data for social security programs – are best served by a provider who can contractually guarantee strong security and fulfillment of disclosure obligations (also see sec. 5 “Legal requirements and other compliance issues”).

Data segregation and data protection.

Corporate clients in other industries also believe cloud computing holds legal, technical and organizational risks of varying severity. These companies or government agencies place a premium on keeping data and transactions strictly segregated and thus protected from unauthorized access or manipulation. They are concerned, among other things, about ceding control of their corporate data, insecure or incomplete deletion of data residing on servers, vulnerabilities in tenant segmentation and open user interfaces. Legal certainty may be added to the list if the data is stored outside the European Union's reach and jurisdiction.

This is not to imply, however, that data protection and security requirements limit the use or spread of cloud computing. Organizations simply need to define their specific security needs and then assess providers' capabilities and services against them. That calls for a detailed understanding of the cloud model (see sec. 3).



Professional providers can contractually guarantee strong security and fulfillment of disclosure obligations.

If organizations need to know where their data is stored, they can choose providers that operate data centers within a particular territory, such as Europe. The organizations may be domestic and expanding to another country, or foreign-based and looking for a secure location to store their data.

Identity management.

Permission management is one of cloud computing's main challenges. Managing users and permissions for applications installed “out there” in the cloud requires a different solution from traditional IT systems. Professional providers have the expertise and ability to implement large-scale security systems without weakening cloud computing's cost argument.

To improve security, organizations can replace their static passwords with hardware tokens such as standard smart cards or USB flash drives. Whatever their form factor, these tokens come with microprocessors that support powerful encryption keys, stopping many exploits in their tracks. Users enjoy secure access to data and applications, and can even add another layer of protection with an optional PIN.

Conclusion.

Cloud computing is no less secure than traditional IT service models. However, its risk profile is different, since it faces threats of a different source, type and form. To account for these risks, organizational and technical security measures are updated continually. These updates should always reflect the user's security needs as based on his business model. Security problems only arise if providers cannot satisfy these needs.

3. Security measures for the cloud.

Every new IT trend forces users to weigh the risks and opportunities and learn to trust the new technology. In the case of cloud computing, trust is absolutely pivotal. The cloud is an abstract structure; how it is accessed, and who can access it, will determine how much users trust it.

Trust can be strengthened with reliable verification mechanisms. They can include transparent security, certifications, active documentation of compliance and specified server locations. Other options include regular audits, suitable liability contracts and service level agreements, and clear processes with built-in monitoring and effective reporting.

Cloud computing is often evaluated based on three criteria: data availability, legal issues with data storage locations and the unique security profiles of the three cloud models.

3.1 Three cloud models.

The three models of cloud computing.

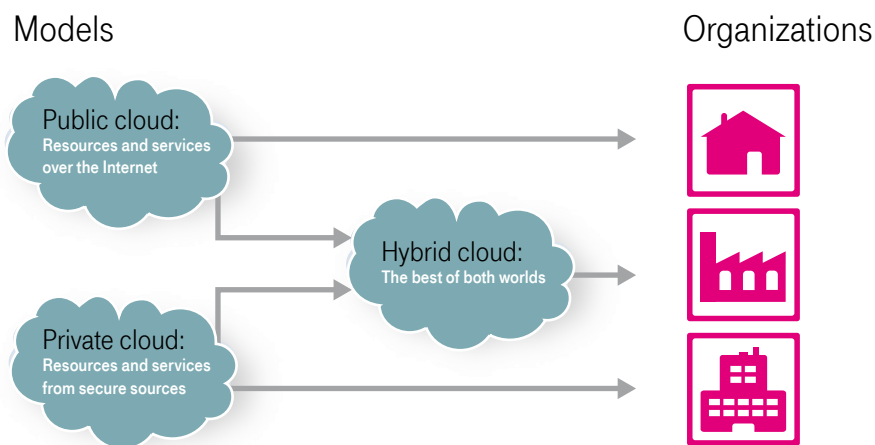


Fig. 3.

Cloud computing has no official definition, but it does have three distinct models: public clouds, private clouds and hybrid clouds. Each one has different security implications.

Public cloud.

ICT services in the public cloud are highly standardized, provided like a product and generally charged per use. Examples include e-mail, productivity applications or storage. They are freely and publicly available and used over the Internet.

The degree of virtualization can vary – even including dedicated systems. Public clouds are, however, mass-market offerings. They generally fall short of the standards of business users and are not suited for critical data whatsoever.



The security characteristics vary between cloud models. The hybrid model combines the best of both worlds.

Private cloud.

Private clouds can involve pooling computing resources within the enterprise and allocating them dynamically to internal users. Normally, though, dedicated private clouds are provisioned and managed by an outside service provider. These clouds are designed to satisfy the specific needs of corporate customers and to provide ICT services on the fly.

Specialized providers with network capabilities can supply private clouds as one-stop, end-to-end solutions. They cover the full range of ICT services and systems, from mobile and stationary devices to connectivity and bandwidth to the integration of ICT in the customer's business processes. They also guarantee service levels through binding SLAs, giving customers maximum peace of mind.

Hybrid cloud.

It appears likely that the hybrid cloud – a combination of public and private clouds – will dominate cloud computing in the enterprise space. Providers are already mixing and matching private clouds and public services to create end-to-end offerings. They integrate public clouds mainly to capture certain functions or capitalize on economies of scale. The combination can even enhance security. A public directory service, for instance, lets users easily use and send encrypted or signed e-mails between secured private domains. Essentially, public cloud services connect private clouds and utilize the integrated security technology.



Once organizations decide to move ICT services to the cloud, they should start classifying their data. Critical data needs to stay in the enterprise or a private cloud.

3.2 Security impacts of different models.

Since each cloud model is different, organizations have to decide what services they want to use, and how, based on their security and business requirements. Once an organization has decided to move ICT services to the cloud, it should start classifying its data; highly critical data ought to stay in the enterprise or a private cloud. The classifications are made as part of the organization's risk management process and reflect the information's potential business impact. Several factors figure into the classifications, including the organization's service portfolio or product range, ICT's role in it, the importance of the workflows, the organization's overall risk tolerance and the sensitivity of the data.

That said, some general recommendations can be made. First, a cloud strategy should begin by entrusting the provider with applications that are not deeply integrated with internal processes. For example, batch jobs that require no further user interaction. This can include e-mail or data backup applications. Other good springboards: web applications, information services and e-collaboration systems. These are all low-risk introductions to the cloud.

3.3 Data availability through failure safety.

Availability requirements and their fulfillment differ widely from model to model. Public clouds are mainly intended for the mass market, and do not lend themselves well to business applications. Their data security and availability assurance measures are geared toward consumers, for whom data unavailability may be inconvenient, but hardly life-threatening. Not so with corporate users: they could be destroyed or financially crippled, suffer irreparable damage to their brand and reputation or lose sensitive business data.

A private cloud, by contrast, is designed for business users. It ensures availability with a host of systems and activities: redundant standalone systems, synchronous replication of entire data centers, data backups and automatic system recovery after a certain downtime threshold. The provider guarantees availability, meets all data retention requirements with secure archiving systems and also offers an end-to-end service.

3.4 Data storage location.

“Cloud computing” is an umbrella term comprising different business models for decentralizing and outsourcing ICT services. In some models, such as the public cloud and some hybrid clouds, it is not always clear which data and applications reside on which servers at a specific moment, nor when and where certain ICT services are provided. That raises difficult questions: How do you maintain an audit trail? How do you perform forensic investigations? What data can you even process under the applicable privacy laws? And what country’s laws govern service delivery and dispute resolution?

The simplest solution is to hire a cloud computing provider who can reliably document that it only stores and processes the data on servers located in a particular territory, such as the European Union. This restriction provides legal certainty. Providers can inspire even more trust from organizations if they can operate their own network and do not have to outsource services.



Providers should be able to contractually guarantee that their servers are located in a particular territory.

Likewise, organizations should look for providers who institute controls and ongoing monitoring for data processing under an outsourcing arrangement, as required by laws such as the German Federal Data Protection Act of September 1, 2009.

A capable cloud provider will understand the differences between legal systems. And these differences can be much more profound than one might expect. Some governments give their agencies sweeping powers to procure and process data. Yet other countries require providers to release information or hand over entire datasets. Differences also abound in attitudes toward security, intellectual property and critical data. Users should talk through these important issues with their ICT provider or knowledgeable advisors.

4. Implementing cloud computing.

Once an organization has decided to embrace the cloud, it should move to the next step: execution. This begins with an analysis of the provider and its services, technical expertise and trustworthiness. Preferably, it should follow a road map: first, define the organization's unique security requirements; next, select the best-fit provider; finally, migrate all or part of the ICT environment to the cloud.

Steps for implementing cloud computing in the enterprise.



Fig. 4.

4.1 Define requirements.

In cloud computing, users hand off their data and applications to providers. In so doing, they also delegate their responsibility for security. But an organization can only determine whether the cloud offers adequate security if it has clearly laid out its own security requirements. They generally flow directly from its strategy, business activities and the role played by ICT and certain applications and data in business processes. After defining the requirements, the organization can evaluate service offerings against them. Security does not live in a technological vacuum, though. That is why its ICT specialists should be familiar with the latest technology and best practices so the organization can work with its future provider on an equal footing.

In the cloud, security is a blend of new and familiar mechanisms and challenges. Physical and building security protects data centers. IT security locks down the systems, applications and platforms hosted at the data center. All these systems have to be securely networked within the data center and be able to securely communicate with the outside world. Data and applications belonging to different customers should be reliably segregated to prevent unauthorized access to enterprise data (multitenancy). Which segregation method is chosen depends on the underlying virtualization technologies and methods or other solutions.



Users should be familiar with security technology and best practices to be able to negotiate with the provider and evaluate its effectiveness.

The ICT architecture, data center locations and service models all have legal, strategic and functional implications. Headcounts and staff skills are also important, as are ICT service and security management processes at the provider's data center. Organizations should ask the provider how it would adapt security measures to their unique needs and what business continuity management and disaster recovery plans are in place. Additionally, they should evaluate the provider's policies and practices for monitoring and managing security incidents.

Since the user is always outside the cloud, data should be protected not just within the cloud, but also when it is transferred between the user and the provider. This can be done with access and collaboration models and role, permission and digital identity management (organizational, technological and procedural identity and access management).

Users tend to underestimate the significance and effectiveness of some security mechanisms. Take data encryption. Not only does it safeguard communications over public networks, but it can enable several tenants to share a single "virtualized" database management system (DBMS). Encryption can also render data unintelligible to unauthorized parties – including the service provider. Payroll data, for example, can be encrypted in the database so the system administrator cannot read it. Encryption can even be restricted to specific fields if not all the data is sensitive. It takes special methods, however, to securely and reliably encrypt user data while enabling all database operations to continue running without encryption. Encryption and decryption are transparent to the user and the application. And only the user has access to the cryptographic keys needed to unlock the data.



Security is a matter of trust.

4.2 Selecting the right provider.

Clearly defined requirements give organizations a useful list of criteria for evaluating and selecting a provider. The final choice depends on the provider's capabilities, reliability, trustworthiness and ability to satisfy the security requirements.

Providers can be assessed along six dimensions of essentially equal importance:

Dimensions of measuring provider trustworthiness.

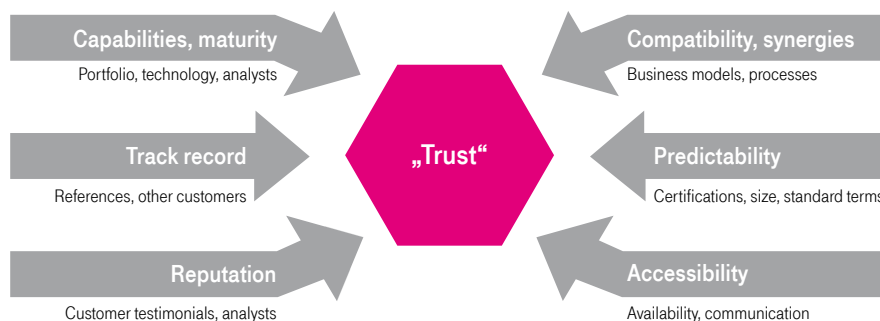


Fig. 5.

The first dimension addresses the provider's capabilities and process maturity. They can be evaluated based on its service portfolio, its proficiency in certain technologies and the opinions of market observers and analysts. The provider's track record is another dimension. It can be checked by looking up references or talking to other customers. Information on the provider's reputation, by contrast, can be obtained from user associations, business magazines or trade journals.

The assessment should also look at how well the provider's services mesh with the organization's business model (compatibility) and what efficiencies and advantages can be realized. It can help to examine and evaluate the various ICT service models. Provider reliability – i.e., whether it will meet its obligations – is illustrated by certifications and other seals of quality. Other good indicators are company size and financial strength.

Finally, the provider's accessibility and communication practices should figure into the equation. In ICT outsourcing relationships, users often stay in close touch with providers. Both sides have to communicate, and not just when there are contracts to sign or problems to resolve. After all, the services support the user's business. And as the business model and operating environment change, so too should the ICT services.



The main question is this: do the provider and its products match the user's requirements in terms of features, service levels, other key parameters?

The organization is essentially conducting due diligence. For its part, the provider should clearly demonstrate that it can satisfy the customer's needs better than the competition.



4.3 Migration.

Selecting a cloud provider can have a large strategic impact that goes beyond simply picking a security system. The organization has to spot optimization opportunities and hive off processes for outsourcing. It then awards the contract and begins with migration.

Security has to be planned from a ‘big picture’ perspective.

Migrations tend to comprise five phases that should be tightly linked with risk management.

The five phases of migration.



Fig. 6.

Strategy development.

The strategy should reflect global or country-specific conditions. For example, organizations may not be legally allowed to merge formerly separate databases that contain personnel data. Other key factors include the type of data, the business and potential threats, including those specific to the country.

Requirements definition.

Next, the organization identifies its security and compliance requirements. Service- and provider-specific requirements are defined separately. The organization takes all relevant company parameters into account in estimating the potential impact of incidents.

Market analysis.

After preparing a requirements specification, the organization draws up a provider profile and service definition and solicits bids, generally through competitive tenders and RFPs. Many organizations consult analysts and advisers when evaluating the bids. Security issues play an important role in the selection of a cloud model. This is the phase where organizations list special technical and other security requirements and define the statutory, regulatory or industry standards to be complied with.



An experienced provider helps to deeply integrate the ICT services and supports the customer's risk management processes.

Negotiations and contract.

The organization and provider start negotiations on various issues, including security. The organization should go into the negotiations with very clear priorities. That will help it decide where it can compromise, and where it cannot. Otherwise, it may not give security its due. The parties should also make arrangements to maintain a strong security posture during the transition. This is commonly a sensitive phase: the production environment's security measures are not fully accessible, while scarce resources and looming deadlines may cause carelessness.

Operation.

The partners lay out the parameters of their relationship and resource provision (especially personnel) during the operational phase. They clarify details such as preferred communication channels or service and contract management. And they define quality control procedures, compliance with service level agreements (SLAs), escalation paths and penalties. In addition, their plans address practical operational issues such as employee training or incident management. Many of these issues only affect security tangentially at first. However, it may be difficult or impossible to respond promptly to incidents if the resources are inadequate or the communication channels ill-defined.

5. Legal requirements and other compliance issues.

Cloud computing differs from conventional IT environments not just in terms of security, but also in terms of legal compliance. Various issues in ICT outsourcing and decentralization have been settled in the courts, including the use of service level agreements to guarantee uninterrupted service availability or term licenses to grant access and usage rights for specific periods of time. Judges have also issued rulings on limitations with respect to transferring personal data to an external provider for processing.

Not knowing where data is located in the cloud introduces new legal concerns, particularly regarding compliance with national laws. Organizations may also be bound by their own policies, by contracts with customers, suppliers or partners, or by other obligations that they have explicitly or implicitly undertaken.

These requirements tend to be imposed by either statutes (data privacy requirements and reporting obligations) or regulations (accounting directives, due diligence and obligations to produce supporting documents). The German Federal Data Protection Act, for example, bans transfers of personal data to countries outside Europe. Any organization covered by the Act needs to ensure that its provider only uses servers based in the European Union. And then there is a more fundamental issue: what data can be processed in the cloud under German law? That puts much the same legal burden on insurers and healthcare organizations that financial service providers face in protecting personal privacy.

Tax law also puts restrictions on efforts to shift enterprise data to global networks and server environments. In some countries, taxpayers must give their internal revenue office immediate access to data on request. They also have to disclose the location of their data-processing systems to tax officials. Neither requirement can generally be satisfied properly if servers are located outside the European Union.

Trust in guaranteed services.

Contracts can address many issues, but trust matters more. The provider should cement the user's trust by disclosing who is actually supplying the ICT services. If it subcontracts work, the user should know. A provider of genuine end-to-end solutions can maintain seamless security and pursue an all-in-one approach that protects the customer from nasty surprises.



Providers should proactively address compliance issues and propose solutions.

The partners should discuss compliance at an early stage, covering everything from regulatory and statutory provisions to internal policies and contracts with business partners.

Compliance can be achieved more easily in the cloud if the organization has prior experience with traditional outsourcing. However, the user's usual monitoring and management tools will be of limited usefulness in the cloud. An experienced provider can compensate by proactively addressing compliance issues and proposing solutions.

Users also benefit from specialized certification bodies and professional security auditors. The providers can furnish certifications documenting compliance with a particular standard. The user no longer needs to perform its own audits, and the provider reaps rewards from using only a few certification organizations. Certifications have long been commonplace and essential for payment systems. They are now gaining acceptance for other ICT services, too. There is, however, no one-size-fits-all test for whether a cloud service is compliant; that depends on the organization's unique situation. After all, IT risks are business risks, and so any compliance review requires an integrated approach and a judicious assessment of the organization's requirements. The trend towards division of labor in the ICT space is unstoppable and brings many benefits. Appropriate security measures and technologies ensure that these benefits are sustained long-term.

6. Conclusion.

Cloud computing has a certain strategic component. It is a high-efficiency model: organizations can consume dynamic ICT services when and as they need them, but do not have to invest in complex systems or infrastructure. It also has the same effect as regularly modernizing legacy ICT infrastructure since, to compete effectively, providers have to keep their ICT environments state-of-the-art.

Maintaining uninterrupted operations and protecting the data and applications are top priorities in any environment. However, cloud computing's security profile differs from that of traditional ICT environments. With its elasticity, it avoids failures due to overloading or availability issues. It is less exposed to threats such as the loss or theft of (laptop) computers since data is stored centrally in the cloud. Instead, more attention must be paid to matters such as reliably segregating data and applications for different organizations or tracking where data is processed in the cloud. Each organization's security requirements depend on the theoretical business impact of a security incident. This makes it essential to evaluate and classify data and applications and pursue an integrated approach to risk management. Provider selection and migration are also important.

Three different models address use cases with different performance and security requirements: public, private and hybrid clouds. They offer resources and services over the Internet or in an ICT environment protected by the provider in accordance with special contracts and operating procedures. The hybrid cloud combines these two scenarios. Before selecting a model, users should classify their data and analyze the risks. Highly critical data should remain in the enterprise or a private cloud.

Data storage and processing locations are legally very sensitive. Organizations often do not know which server is hosting which data and applications at any given time – nor the country where the server is located. As a result, they do not know which legal jurisdiction applies or if they are in compliance with national data privacy laws.

Every stage – from defining the sourcing strategy to operating ICT in the cloud – should address security issues and IT governance (effective management and monitoring). By outsourcing services to specialized providers, organizations can focus on their core competencies, cut costs, and improve quality. That makes the cloud a powerful driver of long-term success.

Given these considerations, organizations are well-advised to select a cloud provider who can meet high quality standards with respect to technical expertise and capability, trustworthiness, reliability and the ability to satisfy all the organization's requirements, legal or otherwise.

7. Glossary.

Term	Definition
Audits	Audits are reviews of action taken. They are conducted by independent experts.
Business continuity	Business continuity refers to strategies, plans and activities designed to keep ICT resource management operational. It includes scenario planning, quota management (resources) and disaster and crisis management, including resumption of regular business operations (disaster recovery).
Business impact	Business impact refers to the consequences and effects of an error / incident on business operations and the organization as a whole.
Disaster recovery	Disaster recovery is the ability to resume business operations or, ideally, to maintain them without interruption after an adverse event or a disaster (earthquake, terrorist attack, etc.).
Due diligence	Due diligence is the examination of a cloud provider's reliability. It covers factors such as the provider's reputation as well as its profits and financial statements.
E-collaboration	E-collaboration is electronically supported collaboration.
Hardware token	Hardware tokens are items such as USB flash drives and smart cards with microprocessors used instead of, or in addition to, passwords or PINs in order to securely identify users in ICT systems.
ICT environment	ICT environment is an umbrella term for all computer and communications hardware and software that supports all ICT-based tasks and processes in an organization. It comprises the following components: clients, servers, applications, routers, switches and connections.
Incident management	Incident management involves fixing service malfunctions and handling service requests.
Migration	In this context, migration refers to transferring business processes to the cloud.
Reporting	Reporting involves the communication of system states, errors and other relevant events. Good reporting involves precise, timely notifications.
Roadmap	A roadmap is a plan that describes the way forward. In this context, a roadmap lays out the steps for successfully migrating to the cloud.
Thin clients	Thin clients are devices that only support user interactions (input / output) and use computing resources or often entire applications in the network. These clients are used to minimize the damage a user can potentially cause within the cloud.
Trust	Trust refers to the confidence shown in a cloud computing provider. The level of trust depends on various factors (provider reputation, capabilities, etc.).

8. Bibliography.

Source	Title
[IDC]	Cloud Computing und Services - Status quo und Trends in Deutschland 2009; Cloud Computing and services: the current picture and trends in Germany in 2009; Kraus, M.; Benner, J.; 2009 (German only)

9. List of figures.

No.	Name
<hr/>	
Figure 1:	Projected spending on cloud computing in the next two years.
Figure 2:	Comparison of potential risks in cloud computing and conventional delivery models for ICT services.
Figure 3:	The three models of cloud computing.
Figure 4:	Steps for implementing cloud computing in the enterprise.
Figure 5:	Dimensions of measuring provider trustworthiness.
Figure 6:	The five phases of migration.
