BearingPoint® Institute

BearingPoint Institute Report

Issue 002

In Cloud we trust ?

Stefan Pechardscheck
Christoph Schiefer

Stefan Pechardscheck
Stefan is a Partner within the IT Strategy and Transformation practice of BearingPoint Berlin

Christoph Schiefer
Christoph is a Senior Manager within the IT Strategy and Transformation practice of BearingPoint Berlin

In Cloud we trust?

Driving trusted cloud computing as a foundation for business

Trust matters in business – so it matters in cloud computing

Cloud computing is becoming the de facto IT service approach for the digital enterprise – but there can be no business without trust!

We are seeing a major shift in the technology landscape, as organisations look to use both opportunistically hosted services delivered via the internet – an approach known as "public cloud computing" – and dynamically managed, "private cloud" solutions to deliver a large part of the company's IT portfolio. Cloud-based IT service delivery builds on principles of IT outsourcing and hosting, creating disruptive models with the potential to standardise and even industrialise how organisations use IT.

IT service providers, analyst firms, governments and indeed end-user organisations see huge potential in transferring IT services to the cloud. The benefits are striking: increased flexibility coupled with more efficient service delivery, freeing the IT department to focus on innovation and the creation of business value. Who could ask for more?

Enterprise adoption of cloud is hampered as potential benefits are outweighed by reticence from business leaders

The use of cloud services continues to grow particularly in the consumer space, however enterprise adoption is hampered as potential benefits are outweighed by reticence from business leaders. In our experience, the main concerns are that cloud services lack maturity and do not align fully with IT and/or business requirements; security as well as data privacy issues; and migration costs, in terms of both time and skills.

While some concerns are valid, they are equally based on a sense of unease whose source is difficult to pinpoint but whose impact on adoption is clear. Gartner forecasts 17.7% growth in public cloud services worldwide between 2011 and 2016: this average increases in Latin America (26.4%) and North America (19.1%). The picture is very different in Western Europe, with growth amounting to only 11.8% – Germany is slightly higher at 12.9%.[1] Clearly, Europe remains far less confident about the cloud than the Americas.

Meanwhile, recent research from Forrester reveals that nearly a third of enterprises are sceptical about IaaS clouds, largely because they believe existing internal infrastructure to be less expensive than what the cloud can offer.[2] Other studies show how the majority of CFOs/CIOs do not fully trust the cloud and have not started major initiatives, apart from pilots. For instance the "Cloud Monitor 2012" revealed only a third of German companies to be open to cloud computing.

So, why is cloud computing so slow to gain customer confidence and demonstrate its value? And what can cloud service providers do to build confidence in their prospective markets? To answer these questions, we first need to understand the role of trust.

Why the distrust around cloud computing?

Trust is a precondition for good business. When relationships are based on trust, costs are lower, communications between parties are easier and interactions are simpler. As a social construct, trust is defined as the mutual readiness between people and organisations to assume that fair-play rules will be met, even if opportunistic behaviour might be possible. In a business context, an additional assumption is that every effort will be made to ensure the quality of services provided.

The paradox for cloud computing is that companies with prior experience report largely positive results[3]. In other words, the cloud can be trusted. Yet as already demonstrated, inexperienced organisations remain reluctant. To answer why, we need to consider one of the biggest obstacles cited by decision makers – loss of control. "Better the devil you know than the devil you don't" goes the expression: While many providers offer better technologies, capabilities, and processes than internal IT ever could, IT and Business leaders are more comfortable knowing that the systems and data running their business are operated by people who work for their company.

Further distrust comes from IT staff at all levels, as staffing levels and quality of service are key metrics for their departments. IT departments clearly need to deliver services at the same level as external service providers; otherwise their roles will be called into question. However, the people with the technical knowledge required to understand requirements and define how cloud services could be used are also the ones who feel their jobs might be at risk. Decision makers concerned about their own job security are hardly likely to give cloud providers the benefit of the doubt.

We see a power struggle between the business, the IT department and service providers, each competing for the primary role: who is in charge of delivering the technology foundation for the enterprise? As many providers have found, once established, distrust is hard to shake off.

Cloud computing models are not going to be suitable for every scenario, and challenges will always exist, from architecture to operational management. However, questions about where to use cloud services are being clouded by whether to use them at all. In the coming sections, we look at the qualities cloud computing needs to exhibit at all levels, from foundation technology delivery through to governance and business alignment, to ensure that organisations can positively and confidently benefit from what it offers.

Note that for simplicity we shall refer to cloud computing in this paper, and only qualify it with terms like 'private' and 'hybrid' when we want to distinguish from the 'public' cloud.

THE BUSINESS BENEFITS OF CLOUD COMPUTING

Cloud computing involves the on-demand provision of standardised IT Services – infrastructure (e.g. computing capacity, data storage) or software applications. Various types of cloud computing exist, e.g. based on whether services are delivered privately in-house or by a third party provider. The latter case, known as public cloud computing, uses the Internet as a communications backbone.

Cloud services can be divided into four service layers. The IT-related services are confined to the offering of infrastructure resources, referred to as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). In comparison, the business oriented services are focused on the provision of applications and business processes, referred to as SaaS (Software as a Service) and BPaaS (Business Process as a Service).

Consumers and start-ups were among the first to move into the public cloud, benefiting from innovative (and often free) applications and cloud storage mechanisms, which could be accessed from virtually anywhere and from any device. More recently we have seen companies starting to leverage the numerous advantages of Cloud, such as:

- Economies of scale – cost sharing and multi-tenancy reduce the overall deployment and operational overheads for individual users.
- Resource sharing on standardised and virtualised platforms maximises utilisation of computing power or storage and balances shifts in demand.
- Standardised, web-based applications are delivered as a full service including hosting and maintenance – Buy instead of Make reduces both CapEx and OpEx.
- Scalability of IT resources that can flex on demand and are only paid for as they are used, reducing investment risks.
- Speed and flexibility to integrate business changes and respond to new opportunities e.g. merger & acquisitions, access to new markets.
- Services and data centres can be designed with high availability and maximum security in mind.
- SMEs can also benefit from state-of-the-art-technology and innovative solutions with increased usability and functionality with access at any time, on any device.
- Focus on core activities of the business rather than on infrastructure, freeing time to enhance existing business models or generate new ones.

Thus cloud computing can be a driver of business growth and value creation. But only if it can be trusted to deliver.

Building trust into cloud computing

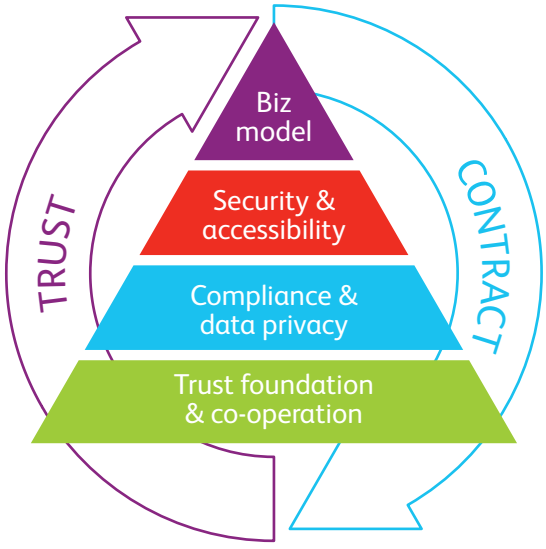
For us, the question is not whether cloud services are a good idea. We see cloud computing as a mega-trend towards delivering commoditised IT services as a utility, which has been taking place for many years. From a legal perspective cloud, and in particular 'public' cloud computing, is simply a flavour of outsourcing: cloud services are outsourced IT services with flexible contract durations. When thinking about delivery of IT capabilities to the business, a services-based approach offers a better place to start than one based on technical components. This principle remains true whether IT is being delivered in-house or as an outsourced service.

The 'Cloud Trust Pyramid' allows businesses to evaluate and manage the implications of transferring services to the cloud.

While the primary question remains how to leverage the benefits of cloud computing, current concerns are real and need to be addressed. BearingPoint has developed the "Cloud Trust Pyramid" (Figure 1) as a framework to analyse the criteria required to build and manage trust as a prerequisite for transferring services to the cloud. Each layer captures norms like laws and standards, as well as soft factors like attitudes to trust based on cultural values. Failure to fulfil Trust Pyramid criteria can lead to absence of trust, and therefore less probability of cloud services being adopted as well as reduced efficiency due to the overheads required to scrutinise service delivery.

Figure 1

The Cloud Trust Pyramid



As shown in the figure, trust and contracts work as a virtuous circle. With higher levels of trust, organisations can work according to the spirit of an agreement without needing to resort to contractual terms at every turn. When a distrustful relationship exists however, hard clauses of a contract play a larger role.

The BearingPoint Cloud Trust Pyramid comprises four layers:

- Layer 1 – Trust Foundation & Co-operation

Customers trust providers for two reasons. First, they trust the services provided: through individual experience, or that of others, people and organisations believe that services will act as expected. Second, they trust the people delivering the services – personal interactions engender and strengthen feelings of trust. Both will be based on experience but also psychological and intercultural factors.

- Layer 2 – Compliance and Privacy

Given that public cloud computing requires data to be stored off-premise, both service providers and their customers need to be aware of the data types and confidentiality levels involved, as well as the valid and applicable legal and regulatory frameworks that apply, including internal, regional and international legal, compliance and data privacy regulations.

- Layer 3 – Security & Accessibility

While data and service security is paramount, it should be balanced with ensuring accessibility to authorised users, wherever they are, otherwise the service becomes unusable. The IT department is responsible for defining of security requirements and mitigating risks, incorporating external standards and regulations. Requirements then need to be met by providers, without exception.

- Layer 4 – Business Model & Governance

For cloud computing to deliver, the services provided need to align not only with the organisation's operational and governance models, but also with its core business model in terms of functionality and scalability. Premeditated trust is essential: an organisation does not want to discover that services are not available or cannot scale at the moment when scaling becomes essential.

Having analysed the role of trust at each level, the Cloud Trust Pyramid offers a framework for organisations to assess both their own positions and their relationships with prospective service providers. We explore the layers in more detail in the following sections.

Trust foundation and co-operation

Trust is the foundation of every business relationship. For example, what gives people confidence to hand over their money to a bank? Or indeed, why should any organisation transfer sensitive and valuable information into the cloud? Given that providers achieve cost savings through automation, cloud computing fundamentally means doing business with someone you do not know. In this section, we first consider the role of trust, and then look at how this applies to the provision of cloud services.

The role of trust in business

For trust to exist, both provider and service need to earn the confidence of the customer. Even in business relationships with minimal touch-points, trust remains important at all levels – interpersonal, interdepartmental and inter-organisational. While trust implies preconceived risk, its presence enables a longer-term perspective, enabling people and businesses to get on with their jobs without concern about whether suppliers will deliver. So control is good, trust is "better" in business terms: increased trust lowers transaction costs.

Building trust means understanding the following:

- Trust creates Trust
  Trust cannot be assumed a priori but is developed step by step, so-called proof of trust. Generally speaking, trustful behaviours are sanctioned with greater trust, according to the principle of reciprocity. In a nutshell: trust creates trust, distrust reinforces distrust.

- Co-operation is built on trust
  Successful collaboration can only be acheived with trust, e.g. through readiness to exchange information relevant for a solution between provider and customer. At higher levels of trust, exchanges of ideas and open discussions become crucial for the development of new and innovative solutions.

- Maintaining trust
  Trust is maintained by fulfilling the stipulated expectations set by the other party. Building and losing trust is an asymmetric process, a virtuous circle or vicious cycle. It might take quite a long time to build up trust, but it is possible to jeopardise or to destroy trust within a few seconds.

Trust is strongly influenced by culture. For example, start-up companies or those with innovative technology leadership might have more positive attitudes to management and mitigation of risks. However an organisation whose values, culture, productions or services are based on security might demonstrate a risk avoidance approach. Such attitudes also depend on the organisation's business model – enterprises handling large amounts of confidential data have more risks than smaller companies handling non-confidential information, and attitudes will vary as a result.

Of course, simply having trust is insufficient for business relationships in itself. Conditions of service, together with contractual terms, define this understanding in formal terms to ensure both sides are clear on what is being provided and how much it costs, and to ensure a legal basis for the relationship should things go wrong. Contracts with an incomplete definition of obligations run the risk of future disputes.

Trust and cloud providers

Cloud computing is clearly an area where trust is of paramount importance. If the cloud is to add significant business value (as opposed to offloading the occasional processing task), an organisation will look to hand over potentially critical data as well as the ability to execute core business operations and processes. In other words, significant control is being handed over to a potentially unknown third party.

Cloud computing providers are starting from a position of distrust and therefore have their work cut out to assure prospective customers that they can deliver. Providers are not perfect – e.g., the International Working Group on cloud computing Resiliency (IWGCR) reported that 13 well-known cloud services achieved an average availability of 99.9% excluding network downtime.
While this is not that much different to the downtimes of many enterprise IT systems, it is far from the expected reliability of mission critical system (99.999%)[4] and paints a different picture to past marketing from cloud service providers.

We are seeing service providers presenting more realistic illustrations, helping organisations understand the benefits without ignoring the challenges. Our experience suggests providers still face a number of difficulties, including:

Fearful of losing control and mindful that services do not always meet expectations, organisations are looking for more than aspirational statements about cloud computing.

- Keeping up with changing security, data protection and international compliance requirements.

- Balancing efficiencies of automation whilst still being able to offer good customer service. Personal relationships play a crucial role in developing trust – a factor that many cloud providers are now taking into account through improved account management.

- Responding to country-specific variances in technical and customer service requirements. Cultural factors play a role in responses to queries, service requests and other provider-customer dialogues, e.g. in France (relationship first) and in Germany (information first).

Approaches

So, how can such a fundamental layer of trust be built between cloud providers and their customers? First and foremost, organisations owe it to themselves to undertake appropriate due diligence of both providers and service types.

To enable this to happen as smoothly as possible, the following best practices apply:

- Individual and institutional trust need to be based on evidence
  Transparency about strategic intentions, examples of adherence to the strategy and an organisation's reputation in the marketplace are starting points for a trust relationship. In addition the certification by independent parties (e.g. ISO 27000 compliance) and externally audited figures (e.g. financials as well as uptime, response time etc.) may add to the level of confidence. Research into providers can also be supported by general reputation or recommendations from others.

- Understand the trade-off between cost-benefits and adoption patterns
  While service adoption will be based on an expected return on investment (benefits minus costs), adoption patterns are tightly linked to «trustworthiness» aspects such as scalability, security, reliability etc. If these are not guaranteed during negotiation and fulfilled in production, trust will be undermined so decision makers need to do their 'homework', ensure they clearly state expectations and understand the real cost impact of their requirements.

- Prospective customers should seek transparency from providers
  To help buyers overcome loss of control concerns, all cloud providers need to be transparent regarding their solutions, availability, and issues. For example Amazon and Salesforce are leaders in transparency for their cloud services running a detailed, publicly available Service Health Dashboard. When Amazon encountered a major service disruption in April 2011, they published detailed information regarding the outage, its cause and resolution.[5]

- Providers should recognise cultural differences and market realities
  Due to different economic, political and development levels, cloud service providers cannot assume that what works in one country will work, or be trusted across the board. Market conditions and past trends make some countries more accepting of cloud computing than others, e.g., outsourcing quotas are higher in Anglo-Saxon countries, partially due to telecommunications deregulation prior to other European countries and differing attitudes to risk.

- All sides should consider pilot projects
  As with any major change, it makes sense for organisations to pilot cloud services before full scale adoption. Providers can also benefit, as pilots can strengthen trust and increase acceptance levels.
  At a national level, the more cloud initiatives there are in a country, and the more public authorities and private enterprises practice cloud sourcing, the greater the potential for trust.

Discussion: trust driving outcomes

To develop a relationship based on trust, organisations need to undertake two types of initial fact-finding. The first is whether a service is suitable, stable and capable of meeting the organisation's needs, and the second is whether the service provider is capable of being a trusted partner, or simply the supplier of a commoditised resource. While the former is clearly a gating factor to using a service, being able to grow relationships with partners is of significant value in the longer term. For all trust and co-operation levels there is the rule: the more directly that partners communicate and cooperate, the greater the potential to build and maintain trust.

At an organisational level, trust exists between teams – such as the customer's IT management and the delivery unit at the vendor. The closer the relationship between provider and customer, the better the exchange of requirements, expectations and ideas. This understanding can lead to more strategic partnerships that deliver value to all stakeholders.

SUMMARY

- Trust is hard to gain and easy to lose – expectation management is key
- Trust requirements increase with service criticality and contract duration
- Sustainable business relationships are founded on trust
- Providers need to demonstrate clear value in service delivery and operations
- Classify all data and services and find a pragmatic way to balance risks
- Trust between provider and customer enables closer collaboration, which creates greater trust

Compliance & data privacy

Much uncertainty around the cloud comes not so much from promises and capabilities but legal issues. When personal or person-related data is collected, processed or used in the cloud, protection must be ensured under data protection acts and other regulations: the burning question is whether any laws are violated using cloud services in a specific country, or indeed cross-border. Even lawyers and experts have diverging answers on this topic, due to the sheer complexity of current national and international law.

Organisations need to ensure that not only personal data but also trade secrets and research data are kept confidential. While mechanisms (such as restricting access or encrypting data) exist to ensure privacy requirements are met, the business models of some providers depend heavily on consumer data to achieve their own goals, e.g. new analysis services in the medical sector. Such models are as yet unproven, and even their discussion as potential options raises concerns in some quarters.

This leads to a fundamental paradox of the cloud. The level of compliance that needs to be fulfilled is much higher than with conventional on-premise IT; however underlying fears persist, notably loss of control and data risk. As some services are abstract and intangible, together with the risk of espionage, it is hard for cloud providers to fully counter all of these concerns.

Both transparency and trust are necessary to gain general acceptance for cloud services. Fundamentally, this needs to be both enshrined in regulation and reflected in the contract between supplier and customer.

Context setting – it's about the data

While no specific compliance and information privacy regulations exist for cloud computing, each country has relevant regulations in the context of data processing, IT outsourcing or service provision. The most critical of these are country-specific data protection laws. Pan-European regulations also exist, e.g. the EU Data Protection Directive (95/46/EU). But also compliance regulations need to be considered as Basel II, as well as ISO standards and international regulations such as the US Sarbanes-Oxley Act or Payment Card Industry Data Security Standard (PCI). While it is already difficult to comply with in-country requirements, the challenge becomes greater when IT services need to be delivered across multiple countries.

Overall, this area must be considered as a work in progress. In summary the most important regulations and challenges per region or per selected countries concerning the protection of personal data:

- EU member states are supposed to have an adequate level of data protection, and compliance with the specific laws in each state is mandatory. The European Commission designates countries outside the EU which have an appropriate level of protection, e.g. Switzerland, Canada, Argentina, Israel and the Isle of Man. European states that are not members of the EU or the European Economic Area (includes EU countries plus Iceland, Liechtenstein and Norway) depend on their own privacy regulations.

- The EU and Switzerland also grant an adequate level of data protection to US companies, as long as they have committed to the principles of the Safe Harbor program. Large providers like Microsoft, Amazon, Google and Facebook have already signed the agreement, which ensures the legal transfer of personal data to the USA. However some countries (e.g. Germany) have more restrictive data export laws which conflict with Safe Harbor[6]. Furthermore, only a low number of providers listed for Safe Harbor satisfy its formal prerequisites, as enterprises predominantly certify themselves without independent checks [7].

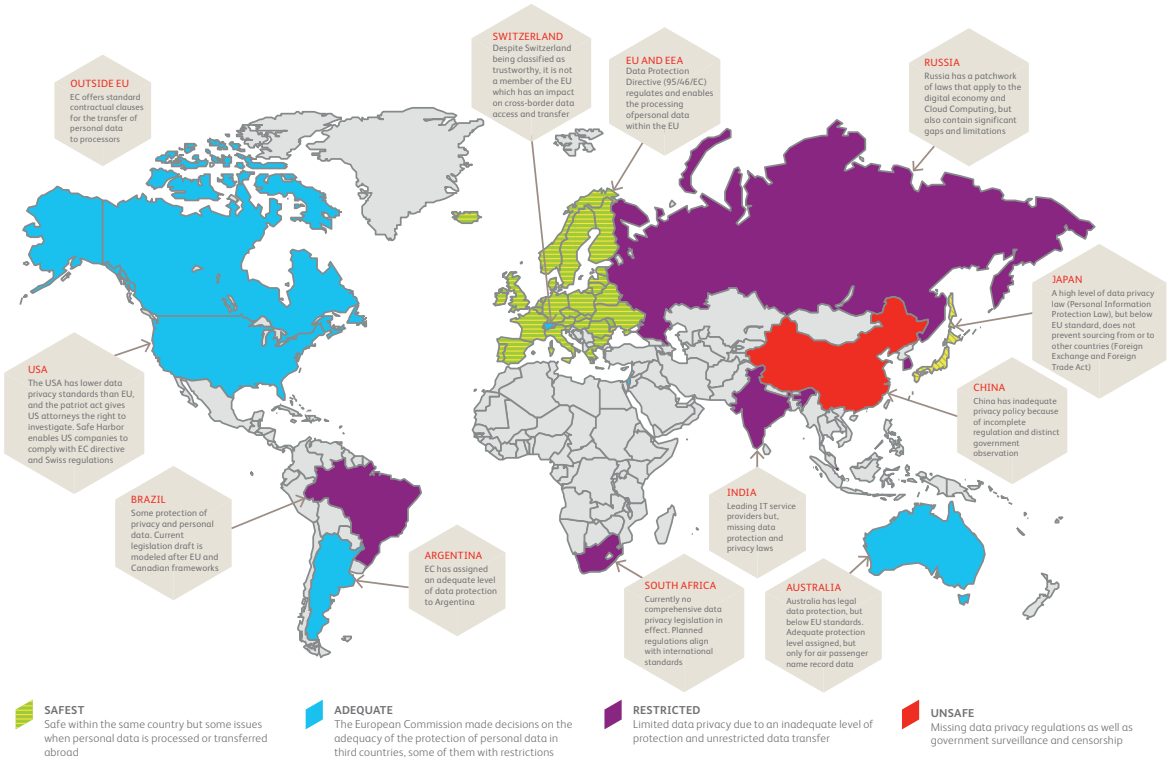
- Even where US providers have signed the Safe Harbor principles, European companies cannot transfer their data without risk to a US-based cloud. The 2002 US "Patriot Act" and the 2010 amendment of the Cybersecurity Act enables law enforcement agencies (LEA) access to such data in the course of an investigation. This results in an uncertain legal position due to overlaps between EU regulatory concepts and national rules, as well as uncertainty about the transfer of personal data outside Europe for criminal investigation purposes. LEAs must be careful not to exceed such powers, either in terms of application or territorially[8]. This risk should not be rated too high due to comparable laws regarding international law enforcement.

- The data processing of a cloud provider is subject to the law or the authority of the EEA state inwhich the provider is headquartered, no matter where customers are located. So commissioned data processing is only practicable if the provider is headquartered in an EU/EEA country and if the data is processed there. So US providers offering cloud services in the EEA have to guarantee that personal data does not leave this area, even if requested otherwise in US courts by US authorities[9].

- There are several countries which offer some privacy regulation as e.g. Russia or Brazil, but data protection laws do not fulfil EU standards. Outside of Western economies, China promotes itself as a source of cloud computing services. However, the country still regulates telecommunications and internet services heavily, providers are subject to clear government surveillance and censorship, and data privacy regulations are missing. Meanwhile India has a generally strong economy, but cloud computing has to be seen as a risk due to missing data protection regulations.

Figure 2

Mapping data protection levels from a European perspective



In order to reform the European data protection law the EU Commission has published a new European 'General Data Protection Regulation' on 25th January, 2012. If it gets approved as legal regulation and directly applicable law throughout the EU, both the current EU Data Protection Directive and country-specific laws will be replaced in most instances. An important innovation is the harmonisation of data protection laws across agencies in each country, enabling a kind of «European passport» of data protection law. While this proposal is mainly received positive, some aspects are still being criticised. Note that this new regulation will most likely not be effective before beginning of 2015 – so existing laws still apply.
Prof. Dr. Georg Borges / Kirstin Brennscheidt

Given such legal complexities, it becomes extremely hard for organisations using cloud computing for data which needs to be kept confidential to be fully compliant with national and international law, or to enable adequate information privacy. This results in a number of specific challenges:

- The focus of current legal debate is on contract and data protection rights, rather than issues like liability and intellectual property, data retention or tax regulation.[10] It is particularly problematic for cloud computing models to fulfil the compliance requirements of companies and authorities for data processing, including not only data protection and information security, but also controllability, transparency and influence, for both storage and transmission of data via public networks.[11]
- At the negotiating table, adequate legal regulation is often missing from cloud computing contracts. Standard contracts run contrary to individual customer requirements, e.g. in specifying data centre locations or data security stipulations. Well-known providers such as Amazon, Google or Microsoft use standardised terms and conditions excluding necessary regulations like auditing rights for the cloud user, which must be considered in customer specific negotiations.
- In the worst case scenario, a cloud customer will not be able to take legal action against an internationally operating provider and may have no access to the stored data that is their legal responsibility to protect. This possibility becomes even greater when looking at the still-insufficient results of legal challenges for cross-border outsourcing of data.

Against this background, it seems a wonder that any organisation has adopted cloud services at all. So, what can be done to improve trust?

Meeting regulation with contractual frameworks

The control of data residency is key – clients need do stipulate, within the range of countries the provider offers, which particular country a system and its data resides in.

Comprehensive cloud due diligence should look to provide clarity to stakeholders by indicating laws and regulations relevant to the services concerned, from a business perspective. Our view is that improved legal and regulatory frameworks, coupled with strengthening instruction and control duties through self-regulation and certification, will lead to a more trusting attitude towards cloud computing. However this will not happen overnight – in the meantime, organisations can consider the following:

- Confirm where the rights fall
  Cloud computing services are generally provided on the basis of a contract between cloud supplier and cloud user. Because there is no specific legal framework for cloud computing contracts, we recommend to include service content, the location of data centers, guarantee rights and liabilities in the contract.[12]

- Enforce privacy in the contract
  Providers must guarantee the confidentiality and integrity of entrusted personal data, if stipulated in a contract. As far as legally possible, data processing has to meet its contractual purpose, acting in the interests of the responsible data owner. The cloud service provider must also ensure that it observes other regulations required of its customers – assuming these are clearly articulated.

To achieve this goal, standard contractual clauses, such as those issued by the European Commission in 2010, can be an important tool especially for transfers of personal data to providers established in third countries. However it still remains unclear whether such clauses can be used for contractual relationships. Furthermore the EC still needs to update those clauses for European cloud providers wanting to deal with subcontractors outside the EU.

- Consider mixed contract types
  A complete set of contractual terms is not usually possible under one single type of agreement, since different service types can be provided in the context of a cloud service. Cloud contracts can be considered as mixed contract types with predominantly rental-based contractual elements corresponding to the nature of the cloud computing, that is providing hard and software temporarily and as needed.[13]

- Confirm guarantees and spread the risk
  Clear guarantees in the contract are important. According to European law e.g. a cloud provider must guarantee that personal data does not leave the EEA. Providers from countries with less secure regulations regarding information privacy, such as the US, have greater difficulty providing such guarantees. By way of contract negotiations around individual regulations, risks should be spread across all involved parties.

- Strengthen understanding of duties
  Given that cloud infrastructure is not restricted to certain locations, it becomes harder for cloud customers to carry out their statutory instruction and control duties.[14] Conformity with regulations and the requirements of the organisation must still be guaranteed however – e.g. through the anonymisation and masking of personal or consumer data. cloud providers can support their customers in these activities by being more transparent, so customers can choose the appropriate solution according to their own needs.

- Customers should review existing contracts
  Existing cloud computing related contracts have to be examined in detail and in doubt they have to be re-negotiated. In case of contractual deficiencies the responsible data protection authority can command a fine and prohibition of use.

Discussion: developing guidance and certification

The greatest leverage for a trustworthy cloud computing would be an internationally coordinated, reliable and optimised legal and regulatory framework. While international regulation is quite clearly a work in progress, cloud providers can do more to help customers conform with their own legal and regulatory obligations. For example, providers should improve their own auditing processes, certifications, branch-specific codes of conduct and self-commitments. While the cloud providers may submit themselves to third party audits (at their expense), more sophisticated organisations will expect to be able to audit cloud providers and receive full reports, rather than the summaries typically provided by cloud providers. These audits will prove to be cumbersome for the provider as they will be repetitive in nature and disruptive to key staff.

Cloud providers need to accept these audits as a "cost of doing business", but it is in the best interests for providers and their customers to work collaboratively. A consortium of customers from a particular industry could engage, at their expense, an audit firm to perform a detailed audit of the cloud providers compliance, privacy, and security controls and provide a detailed report. By having a pooled audit, customers can save money while still having the audit firm responsible to the customer rather than the provider. Providers can save time and effort in complying with these audits while embracing transparency for their largest customers. It is important to look for leading industry associations to begin driving these efforts.

We shall look at standards in the next section – however it is worth noting that most of the already established certifications, like ISO 27001, still refer to conventional data centres and services. As with legal audits, one approach we are seeing is voluntary certification.[15] For example, the German EuroCloud Association has developed the 'EuroCloud Certificate'. This seal of quality for SaaS applications is based on an audit of the cloud provider, to include areas such as contract, compliance, security, operation, processes and implementation. Other examples are the TÜV Austria Group's 'Trusted Cloud Certification' and the Security, Trust & Assurance Registry (STAR) from the US-based Cloud Security Alliance (CSA). STAR also includes a listing of cloud providers who have incorporated CSA measures in their service offerings. Meanwhile work is underway on defining a comprehensive "European Gold Standard" for cloud computing, which aims to provide a Europe-wide audit and certification process for cloud service providers.

A major step would be for international bodies to update existing standards and norms and match them with the requirements of global cloud service provision.

While more onerous controls (and therefore expense) can be avoided through use of self-regulation, it should be seen as supplementary to the legally binding protection of data privacy. Therefore, self-declarations need also to contain statements concerning compliance with national systems of laws, interoperability, data portability and quality of service.[16] The promotion of self-regulation and codes of conduct, and their acceptance (by cloud customers) as proof of compliance with obligations of care and control, are central to improving perceptions of the trusted cloud.

SUMMARY

- Use regular audits and certification processes to monitor and build trust
- Incorporate legal and compliance requirements into the contract
- Be aware of country-specific compliance & data privacy regulations
- Involve corporate risk management and IT security early in cloud projects
- Classify all data and services and find a pragmatic way to balance risks
- Governments are harmonising regulations to ease cross-border data flows

Security & accessibility

Security continues to be an issue for Internet-based services. Data theft and hacking are well-known problems, and the fear of industrial espionage prevents cloud services from being used for sensitive functions such as research and development, or those involving critical business data. The topic of security is therefore a high priority – even for cloud computing. At same time e-mails are exchanged without any encryption between companies exposing significant security vulnerabilities. However, if organisations make things too secure, users are prevented from accessing services. This leads to a separate challenge, that of accessibility and interoperability of cloud offerings.

Both security and accessibility can be addressed through the adoption of appropriate standards. However these are still immature in the domain of cloud. Against this background, what can both providers and customers do to raise the level of trust?

Balancing security needs with day to day access

Cloud computing requires confidence in the reliability, availability and safety of technologies and processes based on standards. In 2011 the US National Institute of Standards and Technology (NIST) surveyed the existing cloud standards landscape and collated standards into three groups:

- Standards for security focus on mechanisms (e.g. for network, physical or host security) and processes. Cloud security is about more than simply keeping the bad guys out, as it goes to the very heart of maintaining confidentiality during the use of publicly available services. Currently, difficulties in controlling confidential processing of person-related data mean that public or hybrid clouds can only be used restrictedly. However if data is anonymised or encrypted, and the cloud user keeps the key, the data will lose its personal nature and can therefore be 'uploaded' to the cloud without risk.[17]
- Portability standards concentrate on the challenge of transferring data and services between cloud computing providers, ensuring that data and workloads are managed within the cloud and made accessible to the customer in a form that other providers can handle and process. Service portability is important when moving to a new provider.
- Interoperability standards focus on migrating data into or out of the cloud as well as integration with on-premise IT. The US National Institute of Standards and Technology (NIST) divided standards for interoperability into two groups – self-service management and functional interfaces.[18]

German associations BITKOM and VOICE pointed out the main advantages of appropriate cloud standards as follows (particularly for medium-sized enterprises):

- Reduction of security, continuity, safety and business risks
- Reduction of implementation and integration costs of cloud computing
- Guarantee of service provider independence and minimisation of vendor lock-in
- More transparent and efficient processes of audit and governance
- Greater overall trust in cloud computing.[19]

Standards for cloud computing enable customer transparency i.e. regarding reference architectures, terms and conditions, management models and processes and legal specifications. While standards do need to be appropriate to each business, without cloud computing standards, service promises cannot be verified in advance.

Immature standards and the lock-in effect

An evaluation of existing international cloud standards by the German Federal Ministry of Economics and Technology (BMWi) from 2012 revealed that of 160 standards, only three can be regarded as mature and comprehensive.[20] Although many standards cover specific aspects of cloud computing, and while a large number of standardisation initiatives are underway across the world, these efforts have not led to a framework of easily manageable, cross-coordinated and generally accepted standards.

This leads to the following challenges:

- Security risks for cloud computing initiatives include the following vulnerabilities: registration without security authentication, insecure interfaces, criminal associates, insecure network infrastructure, theft of access data, lack of encryption and a non-transparent security situation of the provider. To avoid the loss of integrity, confidentiality or availability these risks have to be met with appropriate protection measures.
- As already discussed, it is complex to clarify which standards already exist or need to be established to ensure the exchange of information between cloud users and providers as well as between different countries and regions.
- In parallel with security, vendor lock-in is where customer dependencies on a given cloud provider or technology become restrictive, making it overly time consuming and expensive to migrate to another provider. Technical standards like data formats, protocols, APIs and other elements often differ between cloud providers, making change difficult or impossible.

Approaches

To respond to these challenges, organisations need a clear strategy that encompasses both security and accessibility aspects. Cloud service providers need to provide assurances on how they support a company's business security and privacy priorities. Potential risks have to be mitigated, not least the confidentiality, integrity and availability of computing resources and data has to be protected.[21]

To this end, the following strategic, management and operational aspects can be considered:

- Adopt a security strategy for cloud computing.
  Outsourcing to the cloud must fit with the security and risk strategy of a company. Cloud customers are responsible for ensuring they have an overall enterprise security and risk management process in place, which considers all relevant security threats and issues regarding cloud computing. Security management for cloud services includes some changes to the strategy of outsourcing, business continuity management strategies, as well as processes for security management, incident management, change management and process improvement. General fall-back and exit strategies must be worked out and supported by the cloud provider.
- Match cloud providers with the security strategy
  Before outsourcing functions to the cloud the existing security and risk strategy of the company has to be matched. In our experience it is crucial to ask tough questions early and involve risk management from the outset to ensure appropriate measures are in place. The optimal solution is to link the corporate IT security management components with the components of the cloud service provider and implement new processes if necessary, e.g. by implementing a recognised information security management system (ISO/IEC 2700x). The Cloud Security Alliance (CSA) also provides best practices for security assurance within cloud computing.
- Classify security of both data and services
  The security of data centres, data, platforms and of cloud services administration must all be assured. The legally compliant processing of person-related data is very important, but this is not sufficient by itself. It is essential to classify all data regarding the levels of risk, security and data protection (e.g. blacklist, greylist and whitelist). IT solutions such as encryption, anonymisation and data masking can also be incorporated to protect confidentiality of data effectively and often more efficiently than through legal compliance approaches.
- Address security architecture operations
  Defining an appropriate security architecture is of particular importance for the comprehensive protection of both resources and cloud users. Possible areas are cryptography, redundancy, access control, intrusion

prevention, intrusion detection, identity management, and logging & auditing. Operationally, a clear separation and documentation of the responsibilities and tasks is required. Measures to support operational activities include real-time health monitoring and alerting, which speeds investigation and mitigation; also audits and SLAs enable better risk management of cloud services.

- Plan for data migration
  As standards for data transfer between systems are either undefined or poorly adopted, customers can find themselves locked into a cloud provider because there is no manageable way to migrate data. Known examples show customers confronted with restrictive conditions and inflexibility of providers when trying to do so.

Companies need also to plan on how they could exit the relationship while retaining access to their data

- Think about the end-game
  To avoid problems when sourcing strategies change, the incorporation of an exit strategy is recommended before contract negotiations are concluded. The opposite of lock-in can also be true: instead of developing and maintaining individual applications, cloud services force companies to think about standardising their IT capabilities, making it easier to evolve and migrate them in the future.

BearingPoint advises companies to start with understanding the protection need, following by the definition of cloud specific safety requirements, through a security and trust check of cloud providers at all stages right up to safe deployment and data migration.

Discussion: towards safe, open international standards and contracts

All sides stand to benefit from the introduction of comprehensive standards around cloud computing. Whoever creates standards for cloud computing must work on a national and international level in co-operation with partners so that fair competition regarding price and solution can arise. Thus, organisations like the American NIST, the German BSI or the international CSA have an important role when developing standards and their objectives.[22]

Existing guidelines provide proven assistance to cloud initiatives regarding the security issues and tasks mentioned. For example, the EU authority for cyber safety, 'ENISA' provides such guidelines as a detailed checklist with assessment criteria for the cloud suppliers. Another example on national level is the measure catalogue developed by the German Federal Office for Information Security (BSI) which offers minimum safety requirements for providers.[23]

Open standards are predominantly international, based on use-cases. To counter lock-in and guarantee simpler movement between suppliers, open technical and organisational standards need to be defined with respect to service level agreements, general terms and conditions, to cover:

- Portability of data between the different cloud types (private, hybrid and public clouds).
- Provision of data in open formats for data migration.
- Technical, organisational and functional interoperability.

The specification of such standards is also needed to help adjust business processes more efficiently to cloud service requirements and to ensure legal confidence. Meanwhile, contracts can also be written to minimise lock-in. Fundamental considerations include ensuring the right of access to data, having transparent access to systems at all times, and having appropriate measures available should criminal proceedings be taking place against the vendor.

Ultimately, the old adage of "hope for the best and plan for the worst" should be considered going into any relationship with a cloud provider. Companies need also to plan on how they could exit the relationship while retaining access to their data.

SUMMARY

- Take charge of contractual terms for providers e.g. access to data and virtual machines
- Deliver a level of security, availability and business continuity that fits with the business need
- Use cloud ability to provide secure access to services anywhere, anytime and from any device
- Know the risks to prevent breaches and ensure customer data is kept confidential
- Use standards to ensure accessibility and interoperability for both data and servicess
- Avoid vendor lock-in by incorporating exit strategy in both contract and architectures

Business model & governance

The growth of cloud computing is driving a fundamental shift in how the business, IT department and providers collaborate, impacting trust relationships across all stakeholders. cloud services can have a direct business impact: e.g., if a provider's service becomes unavailable, this will have knock-on effects for the company's customers; equally, a lack of responsiveness from a provider when a service needs to be ramped up or slowed down can cause costly inefficiencies for the customer.

Aligning cloud services with the business requires higher levels of trust than simple questions of interoperability or security. Challenges range from identifying and adopting the right business models and governance structures, to ensuring effective IT support for business users. We cover these below, together with approaches to deal with them.

Context setting: Business model and cloud value-added

Business Models for cloud computing need to be both functionally compelling and capable of supporting customer processes and products. Providers and their customers will have different business strategies and goals, but the closer these are aligned, the greater the benefits. Alignment can be considered along the following dimensions:

- Product: What is the value proposition of cloud services delivered, and what are the dependencies to the service portfolio of the client?
- Customer: How are services delivered and how can the user experience be improved?
- Infrastructure: What resources, configurations and activities are required to produce and deliver the service?
- Financials: Which cost structures and revenue models are needed to generate sustainable value?[24]

Cloud computing grants the business direct access to commodity IT services, proven applications and in some cases, entire business processes. The resulting opportunity is to build upon these capabilities, changing business models in a way that generates added value for both customer and provider.

To support this, customers will need to adjust governance and organisational structures, decision roles and responsibilities of the IT organisation, both to respond to new business requirements and models, and to support the resulting multi-provider environment. The IT department has to generate value for the business more than ever, transforming from a supplier of individual IT services, into an intermediary consultant between business and cloud providers. In the past IT departments have tried to consolidate the number of IT providers, but with cloud computing the number of providers will grow – and so will the challenges.

Approaching the impact of cloud on the business

To enable cloud delivery models to align with customer business requirements, trustworthy relationships between the cloud provider, the IT department and the business have to be established. IT department decision processes and organisational structures have to be (re)designed and changed actively to leverage cloud computing and related business benefits, according to the following:

- Give authority to the IT department
  Companies need to deal with a multiple provider and service environment in a secure and efficient way. This can be achieved either by establishing the IT department as a central (Cloud) provider manager or by granting the IT department authority to define guiding principles across the organisation e.g. provider selection as well as security, data and reporting standards. In a federated governance model this would be balanced between corporate IT and the CIOs of the single divisions.
- Deliver business value through a managed IT service portfolio
  It is fundamental that the IT department generates business value by managing an optimal portfolio of IT services. The IT department has therefore to acquire a new skillset as a consulting service with a deep understanding of the business, in managing projects to objectively and efficiently assess the best fitting IT solutions that balance flexibility and standardisation, i.e. by combining specific in-house services with cloud solutions.
- Proactively decide when to build, buy or rent
  The core question "make or buy" has to become more essential for IT than ever. During the transformation process individual IT solutions - developed and operated by the IT department - will be increasingly replaced by externally provided, standardised software. Together, business and IT need to understand the real costs of bespoke software to decide when to rent a service, use a standard package, or build/maintain custom software.

- But the IT department needs to be pragmatic
  The IT department must not abuse these rights and responsibilities by trying to preserve the role as central provider with deep vertical integration. Security management also must not use this shift to establish higher security levels and in consequence make innovative projects unprofitable. To maintain the IT department's influence in the longer term, it needs to be perceived as adding value – otherwise, users and business departments may order cloud services directly from providers and bypass guidelines and standards. Too much enforcement and bureaucracy increases overall complexity and reduces the potential for cost effectiveness due to fragmented user volumes.

- Deliver operational management and reporting across multiple providers
  The business and IT department have to build confidence that IT services will be delivered from a variety of external providers in a secure, reliable and efficient way. This needs a bundled provider management incorporating standardised and coordinated reporting, processes and SLAs/contracts that match the requirements of the business, integrating best practices such as ITIL for service management, or CObIT for governance and control. Cloud services may be provided and used in different countries, so communication and escalation procedures need to be established across different service desks, availability times and providers.

Identifying the right path to adopt these models, assess potential cloud services and transform the organisation accordingly, will be discussed in the next chapter.

Discussion: cloud providers need to trust their customers too

Throughout this paper, the role of trust is considered against the need for formalising a relationship using contractual frameworks. To further demonstrate trust, cloud providers need to change their approach to contracts. Mark Jeftovic, CEO of SaaS provider EasyDNS, hits the nail on the head: "Software-As-A-Service is the cyber-equivalent of being the coffee-shop where your customers buy their bagel at every morning. Do you need to lock them into an auto-renewing 1-year commit in order to sell them breakfast and a cup-o-joe every day?"[25]

Cloud services should not require long-term contracts – they should have confidence in their ability to keep their customers happy enough to auto-renew on a monthly basis.

SUMMARY

- Identify cloud services and providers whose business models are compatible with your own
- Understand the real costs of in-house IT and bespoke software to decide whether to make, rent or buy
- Use cloud computing to generate new business value, not simply to cut costs
- Be agile - know your business imperatives and respond proactively
- Grasp the opportunity to restructure and develop new skills
- Governance is the key to aligning supply with business demand

Navigating through the cloud

So far we have established a sense of the potential and barriers of cloud computing. So what has to be done to start a successful cloud project or programme? How to select and assess matching cloud services and trusted providers? And how to migrate applications safely to the cloud? For adoption of cloud services to take place in any significant manner, it needs to be seen as a process starting with the development of a cloud strategy and ending with the organisational changes required to ensure it can deliver a return on its investment.

Identify business potential

Cloud computing provides undoubtedly huge benefits for the business, especially in dynamic changing environments, e.g. when setting up a new production plant or in the context of mergers and acquisitions, where IT services need to be consolidated and scaled with high speed. So requirements regarding the support of business processes or new distribution channels need to be defined based on the business strategy.

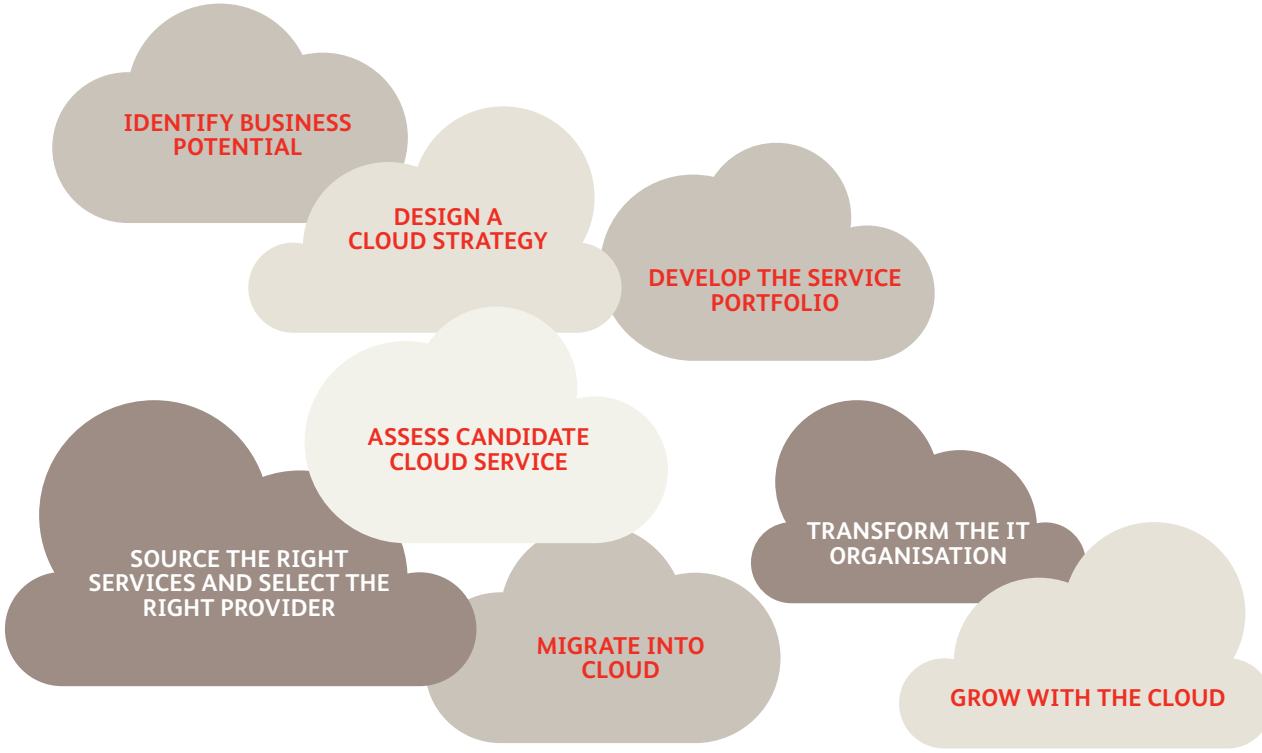
Design a cloud strategy

The most crucial decision for the cloud strategy is to choose the applicable delivery model: Public or private Cloud? Or the best of both?

This decision depends on the strategic business direction and on individual risk assessment. The private cloud scenario is either an evolution of proven IT outsourcing or a redesign of in-house IT. Both have in common that best practices of IT service delivery are applied based on a high level of standardisation, virtualisation and automation. The public cloud scenario is most likely supplementary to the in-house IT or to already outsourced IT services. Matching cloud services are opportunistically selected and enrich the IT service portfolio, replacing already existing solutions or integrating new services without much invest and effort. Further optional scenarios are so called hybrid or community clouds combining elements of private and public cloud for specific solutions.

Figure 3

Navigating through the cloud



Develop the service portfolio

Cloud services are provided in various types – as technology focused services (IaaS and PaaS) and business focused services (SaaS or BPaaS). Every service layer includes different types of provider and product so the specific benefits and risks are not simple to compare at first sight. Whatever the strategic decision might be, it is essential to map the existing IT portfolio of applications and services with potential cloud solutions in a structured and transparent manner.

Throughout this process it is important to ensure also a close interaction with the existing strategic IT planning and management processes. As markets and cloud models are currently changing fast and new benefits arise, the cloud strategy and service portfolio should be reviewed on a yearly basis.

Assess candidates for cloud services

Platforms for software development and testing are often regarded as a good starting point before considering more business-critical applications and services. These can dramatically save time and money for testing and therefore help reduce the time to market for new business services. But also SaaS e.g. for collaboration and CRM have proven to be effective first steps into the Cloud.

Initial focus has to be set on simple scenarios and low-risk pilots which include a rollback option.

Assessing the potential of a given service requires a detailed design that meets the business case and technical requirements. This design includes technical parameters like estimated number of users, usage in specific time frames and data volumes; financial aspects, business and organisational benefits as well as compliance and transformation risks also need to be considered. To meet security requirements in public cloud scenarios, certain architecture patterns may be considered, such as "Far Data" to keep critical data within the IT department or the exclusive use of full encryption.

Examples of trusted cloud computing

Following major initiatives by European governments focus on building trust in cloud services in order to use the potential of IT as driver for economic growth:

- The German Federal Ministry of Economics and Technology (BMWi) started the technology program "Trusted Cloud" to support 14 technology projects to develop cloud computing solutions for SMEs. BearingPoint leads the Competence Centre of this well-perceived technology program in media and industry.
- In the United Kingdom, the G-Cloud is an iterative program to boost the adoption of government use of cloud computing. The aim is to fundamentally change the way the public sector procures and operates ICT.
- The initiative "Andromède" in France (software in the Cloud), enables strategic software solutions on a national basis.
- As part of the Digital Agenda of the European Union the European Cloud Strategy addresses the need to act. One initiative is the "European Cloud Partnership" (ECP) which focuses on the bundling of the fragmented demand of cloud services in the public sector with the aim to set standards and reduce IT costs.

Identification and evaluation of appropriate service scenarios lead to a prioritised list of candidate cloud computing services. A comprehensive assessment of applicability and return on investment also facilitates the creation of specific guidelines for a possible request for proposal (RfP).

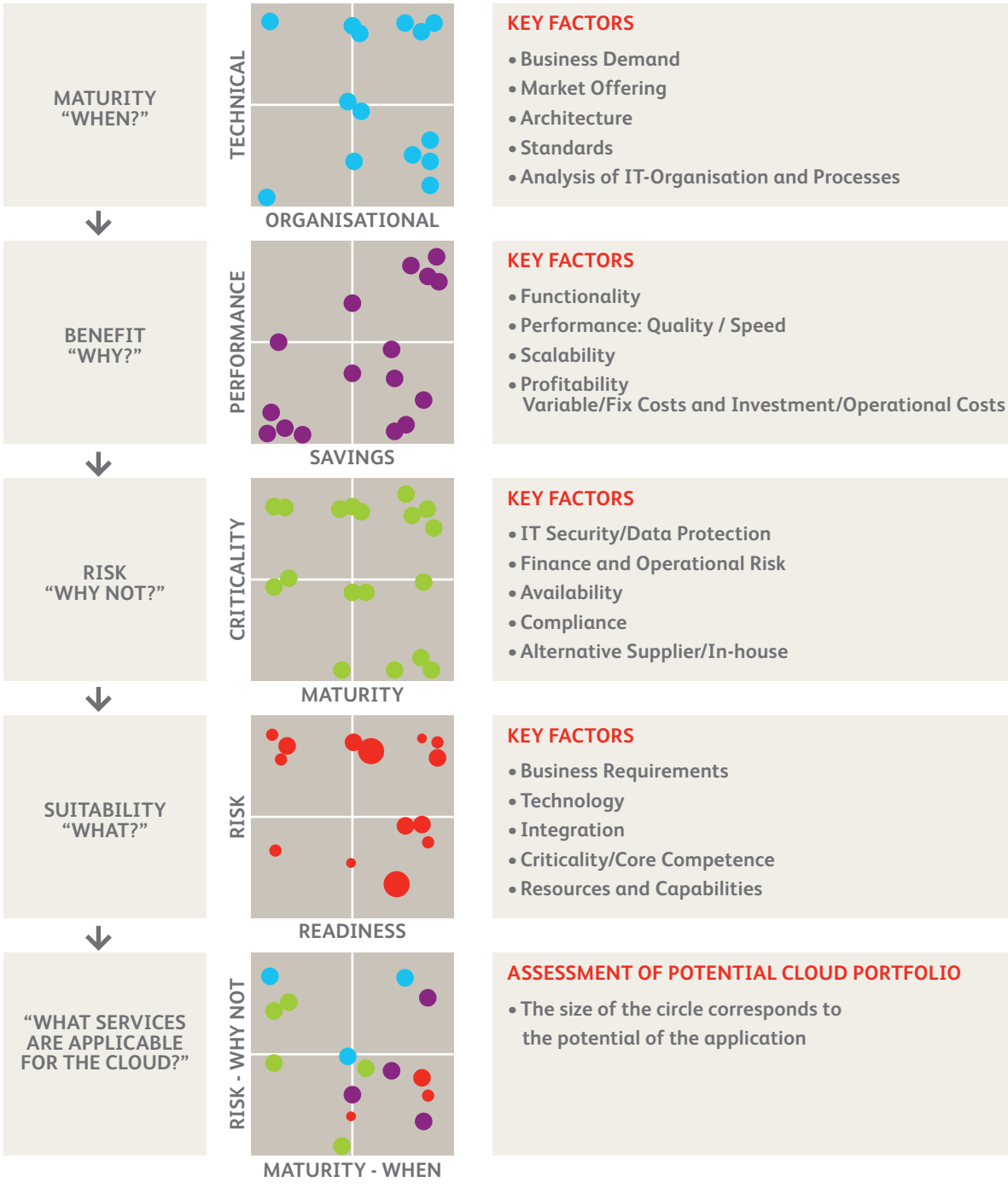
Figure 4 below shows an example of a cloud assessment.

Source the right services and select the right provider

If not performed by in-house IT, a shortlist of suppliers can then be identified and filtered on the basis of their capabilities and specific trust criteria. From a trust perspective, delivery of applicable cloud services needs to take into account the willingness of the organisation to adopt each service, based on past experience and market knowledge as well as the reputation of the provider.

Figure 4

Assessing candidates for cloud services



Cloud services and indeed providers need to be scrutinised in order to meet security, compliance and regulatory requirements. These aspects, terms and appropriate exit clauses need to be defined in the draft contract and then reviewed to ensure they offer the necessary safeguards. Service requirements should be reflected in an SLA and the pricing model should represent business needs. Where large public cloud computing providers offer standard agreements without any customisation options, these should be analysed in detail. If any criteria fail, either the vendor should adapt the agreement or the company should look for a more flexible cloud computing partner.

Migrate into cloud

Adequate project and change management methods and tools are required depending on the scale of the transformation of IT services into the Cloud. These include a migration roadmap and specific checklists for the technical changes, e.g. comprehensive testing as well as a Go-Live plan and data migration blueprint. The goal of organisational change management is to coordinate the necessary actions alongside gaining buy-in from stakeholders. A binding cloud roadmap defines improvement options which need to be closely monitored to ensure they can be achieved.

Transform the IT organisation

For sustainable integration of cloud services, the organisation and its relevant processes must be aligned with service delivery. IT application and service standardisation leads to standardisation of IT processes, which in turn – through inclusive self-service for end users – brings additional cost savings. Process automation needs to be an end-to-end solution. Even the termination of cloud services can be realised in a self-service way, secured by approvals, cancellation of user rights and automated backup & archiving.

Furthermore stringent IT governance needs to be established across regions and service lines to collate demand as well as supply and ensure adequate standards. The aim is to create a business demand-driven organisation, based on portfolio management techniques. Tool-based IT service management processes enable the management of a multi provider environment. Legal obligation can be secured by exercising audits e.g. in accordance with the prevailing data protection specifications.

Grow with the cloud

Once initial approaches to the cloud are successful it is important to get business people on board. Showing business benefits of cloud computing like agility, flexibility and cost savings makes funding and C-Level sponsorship much easier. The impetus of change can supersede structures that have evolved over time, but business value must not be forgotten. It is an on-going task to expand existing business solutions and generate new ideas for innovative business models, enabling the cloud portfolio to grow step by step.

Weather forecast: There's a silver lining in sight

To some, the term "Cloud" holds much promise, while to others it is too vague and unable to shake off its negative connotations. Providers and infrastructure vendors recognise that they can no longer simply label every new IT service "Cloud". Some have already dropped the use of the term in their offerings, focusing instead on value propositions which can be more easily perceived, understood and adopted by clients.

All the same, the potential for cloud-based services (whatever they are termed) continue to grow. In this section we consider a number of new trends that are having an impact on the ways cloud computing is perceived and used. We then revisit the role of trust, and how this also needs to evolve in the future.

Outlook on major trends within cloud computing

The initial effect of cloud computing has been in helping IT departments become more efficient through standardisation, commoditisation and outsourcing of key components. This is understandable: outsourcing of the IT infrastructure and applications is gaining in importance due to the continuing cost pressure on IT organisations and indeed, business as a whole.

A number of additional developments in IT are driving cloud computing beyond this efficiency-based position, and are likely to accelerate its adoption:

- Mobility
  Across a variety of mobile device types, consumer as well as business services are moving into the cloud. A future challenge for service providers is location-based services, e.g. use of a certain process and data presentation depending of the location of the customer. This can include elements like time zone, daylight, local hours of opening, weather conditions, traffic, laws, economic situation and culture.

With the growing importance of mobility services, IT will not only be in the cloud but in the ether, everywhere.

- Digital Society
  A broader perspective on mobility is how such devices and services are changing the way individuals and groups behave and interact. As one symptom, we use the term consumerisation to describe the increasing propensity for people to use their own devices and access services in the work place, rather than those dictated by IT – this includes cloud services.

We are moving towards a digital society in which our lives are acted out online, and the line between personal and work behaviour becomes increasingly blurred.

- Big Data
  The amount of data being created continues to grow, in terms of both volumes and rates of creation. This causes a challenge to organisations that are looking to use such information to support their decision making processes; it also represents an opportunity to achieve new levels of insight and understanding. The term 'big data' has been adopted to describe how organisations can use non-traditional data storage and analysis models, such as those adopted by massively scalable web sites used for search and social networking. Analysis at a massive scale can clearly benefit from the kinds of processing available to be delivered as a hosted service, i.e. from the Cloud.

- Sustainability and Green IT
  Faced with shrinking resources and changing demographics, organisations, companies and countries will only be successful in the long run when they act in a responsible and sustainable way. All actions therefore have to consider ecological and social impact. Because the usage of IT and the consumption of energy are closely linked, Green IT and Green-by-IT are two ways to integrate the aim of sustainability in the decisions of IT Management, e.g. through energy efficient data centres which use renewable energy, or the smart application of IT reducing or replacing energy-intensive physical/chemical processes.

The consequence of these developments is a profound change of the provided services and the provider landscape. Companies and organisations need to re-align and will have to focus far more on business and innovation instead rather than IT. Cloud service offerings reinforce trends towards to IT outsourcing and business orientation. Overall a slow but steady trend to Business Process Outsourcing and a focus on the core business areas will continue.

Towards the trusted cloud

Every day new, improved cloud services are launched and the pace of adoption is almost too quick to follow, driven by consumers – who now have the ability to migrate their personal data to Apple's iCloud, Google Drive or Dropbox with a single click. Perhaps this is no cause for concern. After all, more people have probably lost their data due to a hard drive crash than information privacy laws have been violated by major cloud players. But the underlying fear of loss of control remains, as well as concerns around economic espionage either by competitors or nation-states.

As long as companies are concerned about their customer data and their intellectual property as well as the ability to operate its business, only reliable and trustworthy providers and services will be successful in the long run. Critical questions, some solved for IT outsourcing projects long ago, must be raised and answered. Providers have to be serious about their obligations and offer their services with detailed service definitions and transparent contracts meeting all legal and ethical requirements, as well as providing a clear value proposition.

As cloud computing is a major driver for standardisation of IT services, providers should also collaborate in defining cross-service standards. As described by the term co-opetition[26]: the game must be defined so that the pie gets bigger for the parties involved. This means defining strategic cloud alliances to create cloud eco-systems. While providers need to invest resources to make the first move in the Tit-for-Tat game, they also have to be aware that trust is more rapidly lost than built. Governments play an important role in bringing different players and interest groups together to set the parameters for the cloud game.

In a globally interwoven world it is especially important to define transnational laws and regulations for data processing and data transfer. This is required as a means of delivering industry-wide policies that enable benefits to be leveraged on the broadest scale. Cloud computing can be a positive force to increase transparency and to raise data privacy regulations to the next level.

Clients also have to thoroughly and neutrally assess the offerings and the potential gaps to their requirements to make a sound decision. These goalposts are moving as well, given the still-increasing importance of responsible and sustainable business models.

Ultimately it is clear that the future of IT is in the cloud. As the symptom of industrialisation of IT services, cloud computing is the enabler of making IT cheaper and more convenient. The cloud drives the rise of the information economy and knowledge society. However, as long as not everybody has the same understanding what the cloud is, or indeed confidence in how it delivers, its benefits can be undermined. This makes it more important than ever to focus on business value which, ultimately, is what matters the most for trusted cloud computing, now and in the future.

The authors would like to thank Koji Nagai from ABeam Consulting; Nathan A. Ulery from West Monroe Partners; Wolfgang Correnz, Catalina Garces Gonzalez, Uwe Hasenhuendl, Caroline Neufert, Philipp Neuhaus, Jerome Martin, Elena Maasem, Maximilian Meermann, Dirk Melzig, Christian Meyer, Lutz Milke, Matthias Roeser, Stefan Schade, Marco Scharnetzke, Christian Wallat from BearingPoint; Jon Collins from Inter Orbis.

1 Gartner, Forecast: Public Cloud Services, Worldwide, 2010-2016, 2Q12 Update, 27/06/2012, http://bit.ly/P0nCj7
2 Forrester, Dave Bartoletti / Andrew Reichman, Understand The True Cost Of Cloud Services, 20/06/2012, http://bit.ly/PQ93RN
3 KPMG in cooperation with BITKOM, study performed by PAC, Cloud-Monitor 2012, 03/2012, http://bit.ly/PQ9886
4 Cloud failures cost $70M-plus since 2007, Loek Essers, Computerworld, 19/06/2012, http://bit.ly/N1b2R1
5 Amazon Web Services, Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region, 29/04/2011, http://aws.amazon.com/message/65648/
6 What Every CEO Needs to Know About the Cloud, Andrew McAfee, HBR, 11/2011, http://bit.ly/PQa4sY
7 Rena Tangens, Big Brother Award 2011 in der Kategorie „Kommunikation“, 04/2012, http://bit.ly/Mi4Uyd
8 Arnd Böken, Patriot Act und cloud computing: Zugriff auf Zuruf?, 01/2012
9 Prof. Ian Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, 11/2011,
10 Prof. Dr. Georg Borges / Kirstin Brennscheidt, Rechtsfragen des cloud computing – ein Zwischenbericht, 10/03/2012
11 Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – cloud computing - Version 1.0, 26/09/2011, http://bit.ly/S2Ulo0
12 BITKOM, Leitfaden cloud computing - Was Entscheider wissen müssen, 12/2010, http://bit.ly/NgbaIJ
13 Prof. Dr. Georg Borges / Kirstin Brennscheidt, Rechtsfragen des cloud computing – ein Zwischenbericht, 10/03/2012
14 BITKOM in cooperation with VOICE, Empfehlungen für den cloud computing-Standort Deutschland, 03/2012, http://bit.ly/S2V6gA
15 BITKOM in cooperation with VOICE, Empfehlungen für den cloud computing-Standort Deutschland, 03/2012, http://bit.ly/S2V6gA
16 BITKOM in cooperation with VOICE, Empfehlungen für den cloud computing-Standort Deutschland, 03/2012, http://bit.ly/S2V6gA
17 Patriot Act und cloud computing: Zugriff auf Zuruf?, Arnd Böken, Heise, 01/2012, http://bit.ly/Nqte4R
18 National Institute of Standards and Technology, NIST cloud computing Standards Roadmap - Version 1.0, 07/2011, http://bit.ly/PLIHiJ
19 BITKOM in cooperation with VOICE, Empfehlungen für den cloud computing-Standort Deutschland, 03/2012, http://bit.ly/S2V6gA
20 Federal Ministry of Economics and Technology (BMWi) , The Standardisation Environment for cloud computing, 02/2012, http://bit.ly/NK64VE
21 IBM, Security strategy roadmap for cloud computing, 2012, http://ibm.co/P0pb0p
22 Federal Ministry of Economics and Technology (BMWi) , The Standardisation Environment for cloud computing, 02/2012, http://bit.ly/NK64VE
23 Federal Office for Information and Security (BSI), White Paper: Security Recommendations for cloud computing Providers, 28/09/2010, http://bit.ly/Mi6whS
24 Alexander Osterwalder, Université de Lausanne, The business model ontology: a proposition in a design science approach, 2004, http://bit.ly/MgWEQ2
25 Mark Jeftovic, Contracts Suck 01/06/2011, http://bit.ly/P0pYyC
26 Adam M. Brandenburger / Barry J. Nalebuff, Co-opetition, 29/12/1997, http://amzn.to/L82EK1

BearingPoint® Institute

BearingPoint Institute Report Issue 002

institute@bearingpoint.com
www.bearingpointinstitute.com

BearingPoint® Institute

About BearingPoint

We deliver Business Consulting with Management and Technology capabilities. We are an independent firm with European roots and a global reach.

In today's world, we think that Expertise is not enough. Driven by a strong entrepreneurial mindset and desire to create long term partnerships, our 3,500 Consultants are committed to creating greater client value, from strategy through to implementation, delivering tangible results. As our clients' trusted advisor for many years (60% of Eurostoxx 50' and major public organisations), we define where to go and how to get there...

The BearingPoint Institute provides "thought leadership" across borders and industries by:

- Advising leaders to understand the evolution of the global economy at a deeper level
- Exploring new thinking and developing roadmaps
- Elaborating provocative points of view about strategy and organisational change.

www.bearingpoint.com

Argentina*
Australia
Austria
Belgium
Brazil*
Canada*
Chile*
China*
Denmark
Finland
France
Germany
Ireland
Italy*
Japan*
Korea*
Malaysia*
Morocco
Netherlands
New Zealand
Norway
Portugal*
Romania
Russia
Singapore*
Spain*
Sweden
Switzerland
Taiwan*
Thailand*
United Kingdom
United States*
Emerging Markets in Africa

*Markets served through our global network in Asia, North and South America: **ABeam Consulting, West Monroe Partners & Business Integration Partners**

Printer Le Réveil de la Marne *Printed on Satimat Green Paper: recycled 60%, FSC certified, mixed credit*

BearingPoint® Institute