Deloitte.

Maintaining control in the cloud

Developing and managing an effective cloud strategy

Contents

Introduction

The exponential rise in the popularity of cloud computing in the past decade proves beyond doubt that it has finally come of age. Cloud has many advantages over in-house IT infrastructure and traditional outsourcing services. Cloud is constantly available. Its applications are always up to date. It is flexible. It requires little capital investment. You only pay for what you use. It is tax efficient. It is the answer to so many problems. Cloud is the future...

...But it is not perfect. There have been some dramatic failures. For example, a glitch at a major cloud service provider (CSP) in February 2017 caused hundreds of thousands of websites using its services to function badly or not at all for a few hours.[1]

In another case, a CSP providing customer relationship management platforms to businesses suffered major disruptions in May 2016 when a power circuit breaker failed. As a result, the CSP's own customers were unable to use its services for a day and many lost newly inputted data.[2]

Lloyds, the specialist insurer, estimated in a report published in January 2018 that if an extreme cyber incident took a top cloud provider offline for three to six days it would cost US businesses around $15 billion[3] (R213 billion).

Despite these and other high-profile breakdowns at CSPs and the risk of even worse to come as pointed out by Lloyds, CSP customers – individuals, companies and other organisations – have generally remained undeterred. It is because the benefits of cloud are too important to ignore.

The US Department of Commerce's National Institute of Standards and Technology's (NIST's) famous definition is too long to reproduce here in full but the nub of it is that ***"cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources".***[4] The "network" is usually the public internet, but private networks are also used. One of the computer scientists who wrote that definition described the benefits as ***"cost savings, energy savings, rapid deployment and customer empowerment"***.

That is why cloud adoption continues on an upward trajectory. The worldwide public cloud services market for CSPs is projected to grow by 21 percent to $186 billion (R2.6 trillion) in total revenues in 2018, up from $154 billion (R2.1 trillion) in 2017, according to Gartner. The research firm expects revenues to grow another 63 percent over the next three years to reach $303 billion (R4.3 trillion) by 2021.[5]

So cloud is here to stay, and it is going to get much bigger. Yet potential pitfalls await unwary users, both during the adoption period and day-to-day running. I have already highlighted some of the problems affecting providers of cloud services, but corporate customers face a different set of self-inflicted risks. They need to know what they are. It is imperative they take steps to minimise those risks as well as maximise the opportunities, if they are to maintain control in the cloud.

Even though cloud services are now at a high level of maturity globally and maturing locally, companies using them still bear the eventual risks and responsibilities if things go amiss.

Maintaining control in the cloud therefore means creating a sound strategy for adoption and management. This includes selecting the right provider and getting the best contract terms.

It means ensuring that staff adjust to all the procedural and cultural changes that cloud entails. If staff do not adapt, many of the benefits of cloud will not be realised and errors are likely to be made.

It means integrating old and new technology to ensure that the cloud can work in the company's legacy environment. In the vast majority of cases, IT failures are more likely to happen at the cloud user end than at the cloud provider end.

And it means managing operational risk and compliance. Although a company can outsource its IT, it cannot outsource its risk management, legal and regulatory obligations.

I hope you find our insights, and our recommendations, useful.

Shahil Kanjee
Risk Advisory Africa Leader:
Cyber Technology Risk

Executive summary

Since it became widely available a decade ago, cloud computing has reached a level of maturity and usefulness that many company executives never imagined.

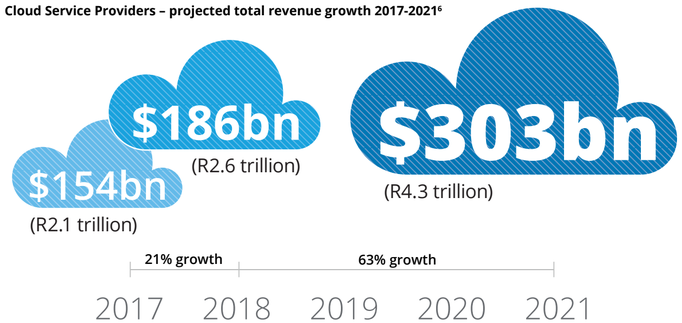
It has been widely adopted. Many large company now have a "cloud first" strategy, meaning that with any IT project they look to the cloud before considering the in-house or traditional outsourcing alternatives.

Whether public, private or hybrid, cloud offers many benefits. For example, it requires no capital investment, it is pay-as-you-go, it is tax efficient and its elasticity means it can quickly adjust to meet fluctuating demand.

It is technologically sophisticated. Additional features can be added to the customer's web browser, artificial intelligence (AI) is widely incorporated and growing security now inspires greater confidence.

Despite this level of maturity – in adoption, benefits and technology – using the cloud is not straightforward. Even though a large part of the IT function is now handed over to a cloud service provider, users still bear the ultimate risks and responsibilities if things go wrong, so they must stay in control.

Cloud Service Providers – projected total revenue growth 2017-2021[6]



Maintaining control means getting things right in four distinct areas, covered in four chapters.

Chapter 1

Is about ***creating a strategy for cloud adoption and management***.

Chapter 2

Looks at ***managing people and change***, ensuring that staff can adjust to the many procedural and ***cultural changes*** that cloud adoption entails.

Chapter 3

Deals with the ***integration of digital and legacy technology*** to ensure that the ***cloud technology*** can work in a company's legacy environment.

Chapter 4

Covers ***operational risk and compliance in the cloud*** – because although a company can outsource its IT to the cloud, it cannot outsource all of its risk management, legal and regulatory obligations.

What is cloud computing?

"Simply put, cloud computing is the delivery of computing services – servers, storage, databases, networking, software, analytics and more – over the Internet ("the cloud"). Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how you're billed for gas or electricity at home."[7]

"Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing."[8]

"In cloud computing, the capital investment in building and maintaining data centers is replaced by consuming IT resources as an elastic, utility-like service from a cloud "provider" (including storage, computing, networking, data processing and analytics, application development, machine learning, and even fully managed services). Whereas in the past cloud computing was considered the province of startups and aggressively visionary enterprise users, today, it is part of the enterprise computing mainstream across every industry, for organizations of any type and size."[9]

It is easy to be pointed in the right direction and given a list of recommendations to follow, but it may be not so easy to act on them. In conclusion, companies must plot a route through all the risks and complexities to ensure they have the **insight and focus** necessary to implement a cloud strategy.

Chapter One

Creating a cloud strategy

Cloud has most definitely arrived and is here to stay as a key element of corporate strategy – not just IT strategy, but overall business strategy. Whatever the reservations major corporations had about cloud computing when it first became widely available a decade ago, those reservations have been largely dispelled. Cloud services have reached a level of maturity and usefulness that many company leaders never imagined and cannot now ignore.

That maturity is demonstrated in three ways: level of adoption, range of benefits and technological sophistication.

Level of adoption

Many large companies now have a "cloud first" strategy, meaning that whenever they need new infrastructure, platforms or applications they look at the cloud first. Cloud first has been the norm for start-ups for a while and they have proved its benefits. Big companies have taken note and are following suit. Public cloud has proven more popular among small and medium-sized enterprises (SMEs) than private cloud because of the wider range of benefits it offers. On the other hand, many large companies, especially those for whom security is important, such as banks, have tended to prefer private cloud, or a public/private hybrid, because of the additional security, perceived or actual, it provides. This hesitancy on the part of large companies is disappearing. Where they can, they now tend to deploy public rather than private cloud.

The range of services has expanded, so much so that existing and potential customers are not always aware of exactly what is on offer. Supply is therefore exceeding demand, but as customers become more knowledgeable about what is available, demand will catch up.

Cloud adoption is widespread throughout Europe, the Americas and large parts of Asia. In the UK, for example, the majority of FTSE-100 companies now have some of their IT in the cloud. Data residency regulations can be obstacles to adoption, but they are surmountable. Many national authorities insist that companies holding data on their citizens and domestic organisations should be kept only on servers in that country, or in the case of the European Union, in an EU member state. The main CSPs can provide their clients with local servers but there are still doubts in some minds about how secure they are from authorities in foreign jurisdictions.

Of the 126 large global enterprises Deloitte counts among its clients, the vast majority are using the services of the big three cloud providers in some capacity. Despite this widespread adoption, the "depth" of adoption – how much each company actually uses the cloud – is not as significant. Many companies are still experimenting with how far they can go. Cloud allows them to "fail fast, fail often", and in doing so learn from their failures and take a more agile approach in future. Often the business departments push hardest to adopt cloud, rather than the IT department which may be reluctant to relinquish some of its control and status. The full potential of cloud is, therefore, still unknown.

The key benefits that distinguish cloud from in-house or outsourced IT

- ***Pay-as-you-go:*** You only pay for what you use, so upfront costs are low and running costs are transparent and controllable. By contrast, with IT outsourcing you agree a set amount in advance, which is cost inefficient if usage is below expected levels; and with in-house IT you have to make a large initial capital investment in servers, which again is cost inefficient if they are not used as much as anticipated.
- ***Tax advantageous:*** Cloud costs are operating expenses for accounting and tax purposes, and so fully tax deductible every year. This is in contrast to in-house IT costs, a large proportion of which are capital expenses, and so only partially tax deductible each year.
- ***Elastic:*** Customers can scale up and down very easily and quickly to meet demand.
- ***On-demand:*** Cloud can be used instantly. Pre-booking is not necessary.
- ***Up to date:*** If correctly specified, software updates, security and other features are automatically carried out by the CSP.
- ***Leaves the customer to concentrate on its core business:*** Instead of spending time, effort and money managing and maintaining IT infrastructure, platforms and software.
- ***Mostly delivered over the public internet, which is more flexible and cheaper than private networks:*** However, the internet is not the only communications medium; private cloud mainly uses private networks.

Range of benefits

Public, private and hybrid clouds offer flexible, scalable "as-a-service" functions – ***Software-as-a-Service (SaaS)***, ***Platform-as-a-Service (PaaS)*** or ***Infrastructure-as-a-Service (IaaS)*** – without the large start-up costs or technical expertise required for in-house IT architecture and code maintenance.

Cloud as an enabler for companies is radically different from traditional IT outsourcing. Long-established IT outsourced service providers (OSPs) have recognised this, adding cloud to their service range to become cloud service providers in competition with the biggest players.

Technological sophistication

The technology is now much more sophisticated than when it was first introduced. There is a vast array of features which can be added to the customer's web browser. For example, load balancing – distributing workloads and computing resources – can be set up in just a few minutes, and audit logs can be sent to a centralised logging platform.

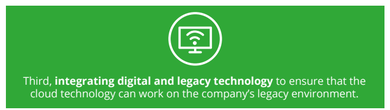
Artificial intelligence (AI) is widely incorporated. A cloud service can include automatic speech recognition (ASR) for converting a person's speech to text, and natural language interpretation (NLI) to allow the computer to understand sentences in human speech and text as opposed to commands given in a formalised computer language. The computer can then communicate back to the person in human language. This form of AI is known as a conversational interface, and has given rise to conversational robots, or "chatbots".

Cloud security now provides greater confidence. The security of CSPs used to be a concern for many large companies, worried that cyber attackers would find it easier to penetrate the cloud than on-premises systems. However, they now recognise that the big CSPs are as secure, or more secure, than most multinational companies. The CSP's security features can also be integrated with the customer's. Security is by no means perfect, but often the biggest breaches are caused by a lack of understanding by customers of how to work in the cloud. Different skills are required and customers need to be aware of this.

Maintaining control in the cloud

Despite this level of maturity – in adoption, benefits and technology – using the cloud is not straightforward. Even though a large part of the IT function is handed over to a cloud service provider – and with it, much of the operational hassle – users still bear the ultimate risks and responsibilities if things go wrong. So they must stay in control.

Maintaining control means four things



This report explores these four areas. The aim is to help senior executives in major companies across all industries develop and manage an effective cloud strategy – one that delivers the promised benefits while avoiding most, if not all, of the headaches. The remainder of this chapter deals with cloud strategy, while the three chapters that follow deal with the other topics.

Developing a strategy for cloud

Organisations often struggle to define a cloud strategy, or to link it to their broader business strategy. Consequently, they find it difficult to generate genuine business value from this type of digital transformation.

So who in the organisation typically initiates the move to the cloud? It can come from just one source, or several: it could be, for example, just IT, or risk management, or finance, or legal and compliance, or a business line, or the chief executive officer, or a combination of any of them.

Wherever the idea originates, **the protagonists must start by being clear in their minds about the desired benefits of a cloud strategy**. The benefits must be clearly articulated – greater operational efficiency, flexibility, agility, increased revenue generation, reduced IT costs, enhanced security, better risk management, return on investment, and so on. At the same time it must be recognised they are unlikely to be able to make a strong case for unwinding all the past investments made in on-premise technology and moving everything to the cloud in a two to three-year programme. A longer term, gradual approach is more pragmatic.

On the matter of cost reduction, costs may not necessarily be lower. Certainly there will be no up-front capital costs, but the pay-for-use model, if used extensively, is not likely to be cheap. Flexibility, agility and other attributes should be accorded more strategic importance than cost.

Next it is important to **enlist the support of the executive management and board**. Whether the move towards cloud is initiated by IT, a business line or another part of the company, the benefits and the costs must be demonstrated to, and signed off by, the corporate leaders. They in turn must incorporate the strategy within the company's overall business plan.

The type of deployment – public, private or a hybrid of both – has to be considered. Public cloud delivers the clearest benefits, but it comes with certain drawbacks such as less control and possibly higher security risks. In some cases, therefore, the company may wish to go down the private or hybrid route. Private cloud for use only by the company can be owned and run internally by the company itself, or owned and run externally by a CSP. If run by the company the chief drawback is that few of the advantages of cloud are realised because the company still has to invest capital in the infrastructure and manage everything. If run by the CSP, it will probably do this through a "virtual" private cloud that will still reside in the public cloud, so the client might still perceive that security is not as tight. A hybrid cloud contains elements of both public and private cloud. For instance, the database containing proprietary information might be kept on servers in the private cloud, while everything else is done on the public cloud.

The service model has to be decided upon. The most comprehensive service is Software-as-a-Service (SaaS). The next option is Platform-as-a-Service (PaaS), while the minimum offering is Infrastructure-as-a-Service (IaaS). Companies with a cloud first strategy will usually opt for SaaS, thus obviating the necessity for developing their own apps, managing their own platforms or building their own

infrastructure. If a company does want to develop its own apps, it could choose the PaaS model whereby the CSP provides just the platforms and infrastructure; or if it wants to develop apps and manage platforms, it will choose IaaS, whereby the CSP only provides the infrastructure.

A budget has to be worked out and the tax advantages considered. Much of the spending on internal IT is capital expenditure which can usually only be written off against corporation tax over a period of years. By contrast, all cloud spending counts as operational expenses which can be offset against corporation tax annually, making cloud very tax efficient. On the other hand, the variability in the operational costs of cloud – because it is a pay-as-you-go model – may make it harder for management to predict costs when they have become accustomed to in-house IT which is not based on usage.

Selecting the right CSP is important, Amazon Web Services, Google Cloud and Microsoft Azure being three of the most dominant. But there are many others such as IBM, Oracle Cloud, Ali Baba and Fujitsu as well as local in-country CSPs.

Some CSPs are more geared up to serving personal or small business customers than large companies – in contract terms and contract wording, for instance – so that has to be kept in mind. Competition or emotional reasons may also dictate the choice of supplier. Some retailers, for example, are reluctant to use Amazon's cloud services because of its dominance in online retailing.

Another consideration is vendor lock-in, where once a customer has committed to using one CSP it is difficult to move suppliers for technical reasons. Customers may therefore want to keep their options open by appointing two or three CSPs.

Culture in the cloud, dealt with in Chapter 2, has to be a priority, especially if the SaaS model is used because fewer application development staff will be needed. It may not be necessary to make them redundant, but re-allocating them to different positions or even departments comes with particular challenges of its own.

Integrating the CSP's cloud technology into the customer's legacy systems is an essential consideration but may not be easy, and is covered in Chapter 3.

Risk and compliance issues have to be considered, as Chapter 4 explains. Security in the cloud is generally strong, but companies with a low risk appetite in certain operational areas – financial services institutions, for example, concerned about fraud or distributed-denial-of-service (DDoS) cyber attacks – may feel safer keeping some operations on-premise. Similarly, national data protection and privacy regulations governing where customer data must be kept may convince companies to store data in-house.

The security provided by CSPs overall has noticeably matured and improved in recent years, and a range of options is available, tailored to the requirements of specific classes of customers. Several major cloud providers now offer security packages for highly regulated businesses like banks and law firms. The greater risk to security now tends to be how customers set and manage access rights, and the level of discipline applied to changes in configuration.

The security provided by CSPs overall has noticeably matured and improved in recent years, and a range of options is available, tailored to the requirements of specific classes of customers. Several major cloud providers now offer security packages for highly regulated companies like banks and law firms.

Creating a cloud strategy – recommendations

1. Understand who in the organisation typically initiates the move to the cloud.
2. Key decision makers must be clear about the desired benefits of a cloud strategy.
3. Enlist the support of the executive management and board.
4. Consideration must be given to the type of cloud deployment used- public, private or a hybrid of both.
5. The service model has to be decided upon. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS).
6. It's important to select the right cloud service providers (CSP) for the organisation.
7. Understanding and setting the culture in the cloud has to be a priority. w
8. Risk and compliance issues have to be considered. Security in the cloud is generally strong but companies with low risk appetite may feel safer keeping some operations on-premise.

Chapter Two

A new culture for the cloud

Companies often fail to take proper account of people in their digital transformation and change management programmes. The move to the cloud is no exception. Adopting the cloud can have a profound effect on the culture of the organisation. The impact on employees therefore needs to be assessed and managed if the transition is to be successful.

Some staff do not like the cloud. They can be sceptical about its benefits and its impact on their jobs. These reluctant adopters will not usually go so far as to sabotage its implementation and running, but their lack of commitment can make it a more difficult and lengthy process. Over time, though, people gradually adapt to technological change in a positive way. We have seen this countless times in the past, as mainframe computers have given way to personal computers, paper documents have been largely replaced by electronic documents and conventional marketing is being overtaken by social media campaigns. We are seeing similar levels of flexibility and acceptance among the workforce as companies move from on-premise to cloud computing.

Changing culture

Perhaps the most important thing to recognise is that moving to the cloud is not simply a question of moving IT off the premises to a third party provider, and then reverting to business-as-usual, using IT as it was before. With cloud, IT moves into a completely different field, offering much more than previously. Its scalability, flexibility and agility means it can be deployed by companies to expand their business in other directions. They can find new ways of working, create different products and services, engage with customers differently and generate alternative revenue streams.

Unfortunately, too many people – not just staff, but business leaders and IT executives as well – do not recognise these opportunities. Or if they do, they do not grasp them properly, taking a reactive approach and hoping the "cloud magic" will rub off on them.

That is why, in most cloud adoption cases, there has to be cultural change. Cloud is not just about technological transformation, it requires cultural transformation too. People have to adjust their thinking. They should not be using cloud like they used on-premise IT.

There will of course be upsets and casualties along the way. Some people will undoubtedly be reassigned to different roles, and possibly sent to other parts of the business. Others may be made redundant. It can be brutal.

Moving email systems to the cloud has had a dramatic impact on in-house email administrators in companies around the world. Redundancy has been one course of action, but in many cases employers have retrained them and deployed them elsewhere, so there can be positive outcomes even for the worst affected.

There has to be a comprehensive people change management programme, one that makes it clear to employees that cloud is not just a cost-reduction exercise or technological change but a re-thinking of the business; and one that shows them how to take advantage of the flexibility and agility that cloud offers, and build new things on top of that. Cloud has to be embraced. If people embrace it, then the rewards will follow.

Addressing people's concerns about their job security, and making them feel wanted, is key...

It is only natural for staff to be worried about losing their jobs if a new cloud service threatens to take over some or a large part of their role. Knowing that what they do today may not be required tomorrow can lead to low levels of commitment and poor productivity at one end of the spectrum, to sabotage at the other.

Employers need to counter this attitude by making people feel wanted. Even those whose jobs are most threatened might not need to leave if they can be found new roles in the same department or elsewhere in the organisation. Employers must make it clear to staff that the cloud does not have to mean the end of work as they know it, but more of a shift in roles and responsibilities. The message should be that the company is reorganising itself to achieve better business outcomes, and as part of that process will teach people new skills to match their changed job specification, or relocate them to a different part of the business.

For example, software developers working for a company that commits to SaaS could be told not to worry; they will be given new roles integrating cloud software with their company's legacy software. This will require new skills, as well as a greater understanding of the business and how it uses the technology, rather than understanding the technology itself, but it is still a great job.

The world of the cloud is highly automated, which means fewer people are needed to generate the same output – but in most cases the efficiencies of the cloud can lead to greater output, so the workforce headcount may remain the same or even increase. Cloud is quite likely to be a job creator, not a job destroyer. Both parties – employer and employee – have to recognise that moving to the cloud means a change in corporate culture, how things get done and how success is defined.

Managing insider risk

Insider risk can increase if the change process is not managed properly. The risk of employees committing fraud, stealing data, causing malicious damage or simply being negligent is a perennial problem, but one that companies have to be especially vigilant about in times of change when new policies and practices can disguise, or even encourage, untoward behaviour. More than half of high-impact data loss incidents are caused by people – staff or contractors – who have authorised access to a company's computer network. Using a cloud service provider creates an additional level of insider risk for companies which has to be managed. The company therefore needs to establish at the contract negotiation stage what recourse it has to the CSP for any risk-loss events. Responsibility for security has to be shared, with the company and the cloud provider understanding exactly what each is responsible for. Ultimately, however, the company – and individual senior risk owners within it – continues to be the bearer of these risks.

Insider risk in a cloud service provider is more difficult for the customer to manage than risk inside its own organisation because of various organisational, contractual and regulatory considerations. Any form of outsourcing necessitates some loss of control. For example, the customer may have no or little contractual right to monitor or request reports on insider risk from the provider; and the provider will apply its own privileged customer access controls, with the customer not being certain how adequate those controls are.

There are, therefore, several steps the customer should take before contracting with a CSP. ***A sound understanding of the customer's insider risk*** and how effectively it manages this is a pre-requisite for a meaningful dialogue. This normally involves carrying out an insider risk assessment of its own organisation. It should also discuss with the provider how the provider will manage its own insider risks – which could include conducting an insider risk assessment of the provider to identify consistencies and gaps with the customer's internal programme – and stipulate key elements of its own security measures that it believes ought to be adopted by the provider. Third Party Assurance reports, such as SOC 2, could assist companies in understanding the controls implemented by the CSP.

Major organisations generally manage their insider risk as well as any other corporate risk – applying role-based access controls, for example – but when it comes to the cloud their leaders often fail to carry through the necessary level of thinking to manage insider risk in the CSP. The gaps in the management of this risk can be glaring and become serious blind-spots.

Senior managers often have the wrong idea of what a malicious insider looks like. They may think it is someone who has recently joined the company. In fact, it is more likely to be a long-standing and previously loyal employee, contractor or business partner whose attitude shifts and feels justified in acting inappropriately or illegally. ***Knowing what a malicious insider looks like is crucial***. Not understanding this can lead to a lack of consensus among managers and disagreement on the measures and controls needed.

There are also some serious regulatory minefields to avoid, especially on the data privacy rights of their staff. ***Data privacy regulations must be adhered to***. It has been known for cloud customers to ask their cloud providers to monitor the customers' staff and report on their actions, without establishing the legal and ethical basis of such monitoring and reporting. This is a major error, with potential legal repercussions.

Formal governance is needed to ensure that staff monitoring meets a clear business purpose, is controlled, proportionate, reasonable, risk-based... and legal. In the absence of such a statement, both customer and CSP could be accused of disproportionate monitoring – of social media, for example – invading the privacy of staff and breaking data privacy laws.

For the customer to draw up such a policy statement and incorporate it into a cloud services contract may be an easy process, or it may be long and tortuous. Either way it is essential, and once in place it will strengthen the compliance of insider risk monitoring and should make it more effective.

A balancing act

Balancing a company's culture and public persona – as an employer of choice, the sort of organisation people want to belong to – with change management programmes and insider risk defences that are essential for the digital age, requires new thinking and steps that go beyond a traditional outsourcing mindset. Companies that get this balance right and manage their move to the cloud and the associated insider risks through a holistic, targeted strategy that closely involves their CSP will have a far better experience.

Balancing a company's culture and public persona requires new thinking and steps that go beyond a traditional outsourcing mindset.

A new culture for the cloud – recommendations

1. It's crucial to address people's concerns about their job security, making them feel needed, is key.

2. Before contracting a CSP, a sound understanding of the customer's insider risk and how effectively it manages this is a pre-requisite for a meaningful dialogue.

3. Knowing what a malicious insider looks like is vital. Not understanding this can lead to a lack of consensus among mangers and disagreements on the measure and controls needed.

4. Data privacy regulations must be adhered to. It has been known for cloud customers to ask their cloud providers to monitor the customers' staff and report on their actions, without establishing the legal and ethical basis of such monitoring and reporting. This is a major error, with potential legal repercussions.

Maintaining control in the cloud | Developing and managing an

Chapter Three

Integrating cloud technology

Integrating new cloud technology into a company's existing on-premise technology environments – some of which will be new, some very old – is a significant challenge and not without its risks. Legacy technology is heterogeneous, having grown organically over a long period, and not always well-understood as most or all of the original coders and developers will have left or retired.

The practical difficulties companies face when moving from their on-premise networks to new cloud technology, the basis of which is virtualisation, and how they surmount them is demonstrated by Vodafone Germany's experience, as written up in Deloitte's ***Tech Trends 2018***.[10] The company migrated from its own data centres to a cloud model, the objectives being to modernise IT operations, improve resilience, increase agility, reduce costs, scale up capacity and make disaster recovery easier.

However, some of Vodafone's legacy systems did not fit into the cloud's virtualised infrastructure. Those systems required significant development costs to prepare them for migration, which may not have been worthwhile for only this purpose. Vodafone therefore linked its cloud migration with a broader modernisation mission: the first part of that mission was to update some of its legacy core applications so they were not only fit for the cloud, but could also be used to develop new products, experiences and customer engagement; the second part was to decommission applications that had reached the end of their life.

Tools such as MuleSoft and Dell Boomi allows cloud services to connect with applications and data held elsewhere on legacy infrastructure so it can still be used. A company will sometimes announce it is going to move to the cloud and ditch its old technology. But when it prepares the detailed business plan and realises it is committed to contracts with data centres, and remembers it has made considerable investments in hardware which it will have to write off, it may find the sums do not add up. It may then delay the decision until another reason to change comes up – the expiry of a data centre contract, for instance, or the end of a hardware or software life cycle.

But the longer it holds on to its legacy systems, the harder it will be to move away from them in the future. Meanwhile, competitors that have already moved to the cloud may have become more agile and continue to accelerate away.

Automation should be a fundamental element of cloud services. Software automation tools, such as Terraform or Ansible, installed on the cloud platform and controlled by the customer remove a lot of the complexity of operating a fleet of virtual machines. Everything becomes faster and more efficient.

A big question for banks with huge legacy environments is how to adjust to compete with fintech firms and challenger banks, which are 100 percent in the cloud and have low capital costs because they have no, or little, high street presence. Clearly the incumbent banks must go down the cloud route. ***There are two options when integrating cloud with existing on-premise technology: add the cloud as another layer on top of legacy systems; or dispense with some or all of the legacy systems and start afresh in the cloud.***

Two of the main barriers to new entrants to the banking sector used to be that they needed a giant data centre and a big branch network to underpin their services. Remarkably the situation has reversed. Those barriers still exist, but they now act ***against*** the incumbents, making it harder for them to compete with their newer, more nimble competitors who are hoovering up profitable parts of their business.

The big banks have spun off digital teams and started anew. These units are not using the legacy technology but the cloud, and are rolling out new products and finding new ways of dealing with customers. But in most cases they are only bolt-ons. We will have to wait another five to ten years to see how all these scenarios play out, and whether the traditional banks can succeed in using the cloud and other strategies to retain a strong grip on their markets.

Decide whether to use generic or vendor-specific cloud services, and consider the upsides and downsides of both. Compared with five years ago, the maturity of the cloud is almost unrecognisable in certain areas. Perhaps the biggest area of change has been the increase in vendor-specific cloud services, where a CSP offers a service that is quite different, and not compatible, with the services provided by other CSPs. Google Cloud has done this with its BigQuery data warehouse and Amazon Web Services (AWS) with its Redshift data warehouse.

There are big benefits for customers of committing to one vendor in this way, such as only having to learn how to use a single technology, and provider tools that are specially designed to work together.

There is, though, a potential drawback. If the customer wants to change vendors at a later date, it may find it is locked in. The best way to avoid vendor lock-in is for the customer to architect its applications so they are portable. Another is to call on the services of a company that can transfer data between CSPs. There are a number of such companies that offer migration and mapping service across almost any infrastructure, from AWS to Google Cloud, from Oracle Cloud to VMware Cloud.

Data protection requirements

Cloud customers should know the geographic location of the CSP's servers and each country's data protection and other regulations. National authorities often insist that data held by domestic companies should be kept only on servers in that country. That means their CSP has to use local servers. However, that may not be enough to keep data safe from other countries' authorities, as shown by a US law enforcement agency's efforts through US courts to gain access to data on a cloud service provider's server in Ireland. Furthermore, a law passed by the US in March 2018 – the CLOUD (Clarifying Lawful Overseas Use of Data) Act – makes it clear that US authorities can demand that US companies provide them with data held on overseas servers.[11]

As a result, many cloud customers are encrypting their data to keep it safe from governments as much as from cyber criminals. The customer holds the encryption and decryption keys, not the CSP. If a CSP subsequently has to give its client's data to the authorities the data remains encrypted, so the authorities are denied access. The authorities therefore, have to approach and talk to the cloud customer to try gain access.

The location of servers is only one aspect of a broad range of data protection regulations that vary from country to country. The European Union's General Data Protection Regulation (GDPR), which came into effect in May 2018, is one of the strictest. It requires organisations to improve the privacy rights of EU residents and report data breaches within three days to the regulator and to the national data protection authority, rules that will be difficult and costly to comply with.[12] Penalties for non-compliance could be as high as 4 percent of global turnover.

Budgeting and cost/benefit analysis

The customer should carry out a cost/benefit analysis to calculate the initial costs of migrating to the cloud, and the long-term net savings. A cost-benefit analysis may reveal that it is more prudent to stick with some of the legacy systems for a little longer. In that case a hybrid cloud may be the solution, with some applications or components left in the old system and some moved to the cloud. Before any kind of move to the cloud is made it may be better to wait until a compelling event, such as the decommissioning of a data centre, or the natural end of a hardware lifecycle, happens.

Immediate cost reduction should not be the main reason for moving to the cloud. It should be the new capabilities it offers. In fact, the initial cost of cloud might well be higher, but the payback is that the business becomes more agile, products get to market quicker and revenues rise. Eventually, as the cloud infrastructure is optimised, the costs may fall. Services can be scheduled so they are not used at certain times, such as the weekends, for example, when workloads may be light.

Public versus private cloud

A decision should be made on whether to use the public or private cloud. Most corporations are opting for public over private cloud when they can because it provides more of the benefits. These days public cloud provides so many security features and controls that it can effectively operate as a private cloud. In fact, many CSPs have created "virtual private cloud" (VPC) segments on their public cloud platforms.

Public cloud and VPC may still be out of bounds for some firms – such as lawyers, banks and auditors – because they may be concerned about breaching data protection and other regulations, and so opt for private cloud, or keep everything on-premise. However, these fears are often misplaced. The UK's Law Society, for example, in its practice note on cloud computing, points out the risks to solicitors of using public cloud, but mentions no blanket prohibition on its use.[13] Indeed, it devotes much space to explaining the benefits of public over private cloud, although it stresses the customer should still conduct a full risk and compliance analysis before committing to either.

The UK's Financial Conduct Authority, in its ***Guidance for firms outsourcing to the 'cloud' and other third-party IT services***, says the cloud can "introduce risks that need to be identified, monitored and mitigated".[14] On the whole, though, it takes a positive attitude. "We see no fundamental reason why cloud services, including public cloud services, cannot be implemented, with appropriate consideration, in a manner that complies with our rules," it states.

Similarly, the South African Reserve Bank (SARB) has issued regulations (GN5/2018) relating to Cloud & Offshoring of Data which recognises the benefits of Cloud and stipulates the risk based principles that need to be adopted.

Integrating cloud technology – recommendations

1. A decision should be made on whether to use the public or private cloud and therefore automation should be a fundamental element of cloud services.
2. There are two options when integrating cloud with existing on-premise technology: add the cloud as another layer on top of legacy systems; or dispense with some or all of the legacy systems and start afresh in the cloud.
3. Decide whether to use generic or vendor-specific cloud services, and consider the upsides and downsides of both.
4. Cloud customers should know the geographic location of the CSP's servers and each country's data protection and other regulations. Be aware that national authorities often insist that data held by domestic companies should be kept only on servers in that country.
5. The customer should carry out a cost/benefit analysis to calculate the initial costs of migrating to the cloud, and the long-term net savings.

Chapter Four

Cloud risk and compliance

The operational risk and compliance requirements for companies using the cloud differ in several respects from those for legacy "on-premise" services. They can be difficult to understand and hard to manage, especially when operations span multiple countries, organisations and service providers. So what must senior managers do to meet, or even exceed, those requirements?

The risks

IT system failings, power cuts, insider fraud, cyber attacks from criminal gangs and hostile states... the list of risks facing companies is a long one. Failure to comply with legal and regulatory requirements is another major risk, the consequences of which, in terms of fines and other penalties imposed by the authorities, can be far worse than the harm caused other operational risk loss events.

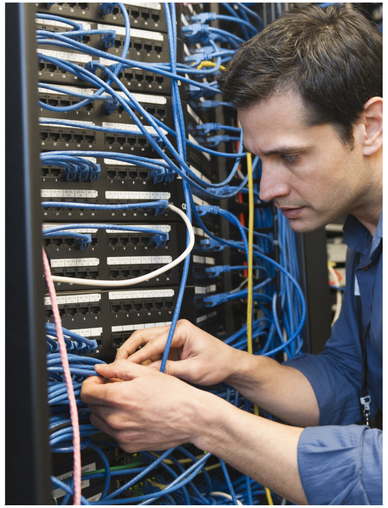
It is essential to understand the operational and compliance risks of outsourcing. Moving services to the cloud transfers some of the risk management duties to the third party CSP, but it is only the management of the risks that is transferred; ***accountability*** for the actual risks still resides with the company, not the CSP. Using the cloud also creates new types of risk. The company's operational risk management framework must therefore take account of the special situations arising from cloud service adoption. Companies should review the details of CSP compliance and assurance reports (SOC 1 and SOC 2 for example) to better understand the controls implemented at at CSP.

Organisations should create a risk management framework for the cloud. Many create a customised framework, but detailed customisation is not usually necessary. They can simply use their existing framework and modify it slightly to suit the cloud strategy. The framework should include the business case outlining the critical considerations for the outsourcing decision, outline the spectrum of risks created and categorise the importance of the functions moving to the cloud – "critical", "material" or "not material".

These categories have their origin in regulation, with different levels of regulation applying to each category, but they are increasingly used by companies for their own internal purposes.

Other important elements of the framework should be to classify the information assets – such as intellectual property, customer databases and financial information – so the risks to them can be managed; to include in the contract a right to audit the cloud environment; an exit strategy, with associated contractual conditions in place; a business continuity plan covering the full scope of the cloud service; IT service management procedures and controls; and a redesigned operating model to ensure the right team structure and capabilities are in place to manage the cloud services.

Proper due diligence should be standard for any outsourcing initiative to understand the key risks and embed controls into the contract. However, many companies do not spend enough time and effort checking the credentials, capabilities or contract terms of their CSPs. They believe that immensely successful global corporations do not need their tyres kicked before signing up. They are wrong.



The simplest way of managing supplier risk is to split cloud services across at least two CSPs, so if one of them encounters problems, data storage, communications, computing and other services can be quickly switched to the other.

Due diligence is needed for several reasons. First, a CSP's view of the risk landscape could be different from its client's, and there are differences in views between cloud service providers as well. Second, the client has to bear in mind it is negotiating with people who are not just corporate executives but individual human beings. In any particular contract negotiation with a CSP, its sales, legal and operational executives may have their own agendas as well as their employer's. Every contract negotiation, even with the same CSP, has to be conducted with that in mind. Third, cloud services are largely commoditised, and the client needs to know exactly what they entail.

Big CSPs, despite their sophistication, can still suffer from technical problems, cyber attacks, political intervention, litigation, power supply interruptions, financial difficulties and more. ***Supplier risk therefore has to be factored into the equation***. The customer must have a clear exit strategy if the supplier cannot deliver; in fact, being able to terminate a cloud service contract easily is often insisted upon by industry regulators. The simplest way of managing supplier risk is to split cloud services across at least two CSPs, so if one of them encounters problems, data storage, communications, computing and other services can be quickly switched to the other. A side benefit of dual supply is that it reduces cost risk; if both suppliers know a rival is already on the scene, they will find it harder to ratchet up their prices.

Cyber security

The risk of intruders gaining access to IT systems on the internet, and even to closed systems, has forced organisations to improve security. Yet attacks keep coming and corporate defences are breached with depressing regularity. ***Cyber risk deserves special attention***. Security must be tight.

The NotPetya ransomware that infected the systems of some of the world's largest companies in more than 60 countries in June 2017 sensationally illustrated the scale and seriousness of the threats. Denial-of-service attackers, financial fraudsters, disaffected insiders, organised criminal gangs, terrorists, unfriendly states – wherever the attacks come from, they are increasing in number and becoming more difficult to defend against.

Businesses are having to invest more money and effort to make cyber space safer for themselves and their customers. The big cloud service providers have better protection than most large corporations, but even they can be breached.

Governments have taken it upon themselves to help businesses large and small cope with the threat. At the European level, the European Commission recently introduced a "cyber security package".[16] The package includes a new EU Cyber Security Agency, based on the existing European Agency for Network and Information Security. The new agency will, among other things, run pan-European cyber security exercises, share threat intelligence by setting up Information Sharing and Analysis Centres (ISACs) and implement an EU-wide certification framework to confirm that internet-connected devices (the Internet-of-Things) are cyber secure. Two major pieces of EU legislation came into effect in May 2018 – the Directive on Security of Network and Information systems (NIS)[17] and the General Data Protection Regulation (GDPR). Both place huge compliance burdens on organisations, but they aim to greatly enhance information security and data privacy.

Member state governments are raising their game too, as exemplified by the UK which in 2016 extended its National Cyber Security Strategy for another five years with a budget of £1.9 billion[18] (R34 billion). The strategy includes two schemes in particular aimed at businesses. One is the 10 Steps to Cyber Security,[19] which explains what companies should be doing to protect themselves, starting with creating an Information Risk Management Regime and then taking other steps such as managing customer privileges, customer education, incident management and malware protection. The other is the Cyber Essentials certification regime,[20] which provides several ways for organisations, whatever their size, to gain a certificate showing they have taken action to protect against cyber attacks.

The National Cyber Security Centre, part of Britain's GCHQ intelligence agency, provides advice to organisations on cyber security in the cloud. It recommends following the centre's 14 Cloud Security Principles.[21] The first principle, for example, is about protecting data in transit between customer and service provider; the fifth is ensuring the cloud provider has a suitable governance framework; and the tenth is ensuring access to services is restricted to authorised and authenticated individuals.

Companies need to be aware of the overall cyber threats facing them, what specific threats could materialise when they move to the cloud and the additional security measures that should be taken. They also need to assess the cloud provider's cyber security procedures to make sure they meet the customer's needs.

Legal and regulatory compliance

Complying with national laws and regulations on data is a thorny problem that must be addressed. It raises difficult questions for businesses. Who owns the data? In which countries should the data be stored? Who is permitted access to data stored in another country? Data hosted on cloud services and other internet platforms is subject to the laws and regulations of the country where the data is stored.

The European Union also has rules that apply to data held outside its territory. The General Data Protection Regulation (GDPR), which came into effect in May 2018, is designed to improve data protection for EU residents whose data are collected, stored and processed by organisations; but the regulation's scope extends to companies using servers outside the EU, if those servers hold data on EU citizens. ***The full implications of GDPR must be understood***.

Russia too has taken steps that have adversely affected cloud service providers, albeit more dramatically. In April 2018, Roskomnadzor, Russia's communications watchdog, banned the use of Telegram, the encrypted messaging app used by the political opposition and journalists.[22] It started by telling internet service providers to block requests to Telegram's IP addresses. When Telegram customers found ways round that, including the use of cloud services, the government banned large numbers of IP addresses, including those of cloud service providers. This caused widespread collateral damage, causing havoc for cloud customers who were unable to access their services.

The cost of complying with data privacy and protection requirements is high. The cost of non-compliance can be even higher. Companies have several ways of complying. They can deploy sophisticated rules engines in their own servers, or in cloud servers, which can determine which organisations in which countries are allowed access to what data. Or data held in company or cloud servers can be segregated by country, with access to that data restricted to customers in that country.

Examples of "bad practice" include failing to keep up-to-date regulatory requirements for each country of operation, and failing to take into consideration the interconnected nature of data protection rules in a globalised digital environment.

It is therefore highly important to create a risk management and compliance framework for cloud. Otherwise there is a danger of getting bogged down in unfamiliar detail. A framework will help avoid pitfalls. It will help the company plot a route through all the risks and regulatory complexities, to ensure it gets the benefits it set out to get from the cloud.

Cloud risk and compliance – recommendations

1. It is essential to understand the operational and compliance risks of outsourcing.
2. A risk management framework within the organisation should be created for the cloud. Plotting a route through all the risks and regulatory complexities, will ensure the company gets the benefits it set out to get from the cloud.
3. Proper due diligence should be standard for any outsourcing initiative to understand the key risks and embed controls into the contract. Supplier risk has to be factored into the equation.
4. The risk of intruders gaining access to IT systems has forced organisations to improve security. Cyber risk deserves special attention. Security must be tight.
5. Complying with national laws and regulations on data is a thorny problem that must be addressed and the full implications of GDPR must be understood and adhered to.

Insight and focus

Deloitte understands the full range of opportunities and challenges that companies in all industries face when using the cloud. Through various practice areas we help companies adopt cloud technology and services, from advice, to delivery, to care and maintenance. We have teamed up with software vendors to bring the best cloud-based solutions to the market. We have also invested in our own cloud incubators, which have provided us with valuable insights. In fact, we are still experimenting and learning about the benefits that cloud can bring to companies, as well as the pitfalls they must navigate if they are to maintain control.

Deloitte's Risk Advisory Africa practice advises companies on how to mitigate risk and make informed and intelligent risk decisions in all areas of business, including the cloud. Cyber security is an especially serious risk; it is the domain of Deloitte's specialist Cyber and Technology Risk practice, which has a long track record of helping companies prevent cyber attacks and protect assets across all areas of operation, including those conducted in the cloud.

As we have shown in this report, successful use of the cloud depends on getting it right in four areas: creating a strategy for cloud adoption; managing people and change; integrating digital and legacy technology; and managing operational risk and compliance. For each area we make several key recommendations for companies to follow which we believe will be immensely useful.

If you would like to discuss any of these matters in detail, do get in touch with your Deloitte partner or our risk and cyber specialists.

Meet the team

Southern Africa

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Shahil Kanjee
Risk Advisory Africa Leader: Cyber Technology Risk
Mobile: +27 83 634 4445
Email: skanjee@deloitte.co.za

Gregory Rammego
Risk Advisory Africa Leader: Forensics
Mobile: +2 78 2417 5889
Email: grammego@deloitte.co.za

Wesley Govender
Risk Advisory Africa Leader: Data Analytics
Mobile: +27 83 611 2929
Email: wgovender@deloitte.co.za

Rushdi Solomons
Risk Advisory Africa Leader: Internal Audit
Mobile: +27 74 141 4444
Email: rsolomons@deloitte.co.za

Candice Holland
Risk Advisory Africa Leader: Regulatory
Mobile: +27 82 330 5091
Email: canholland@deloitte.co.za

Cathy Gibson
Risk Advisory Africa: Director
Mobile: +27 82 330 7711
Email: cgibson@deloitte.co.za

Derek Schraader
Risk Advisory Africa: Director
Mobile: +27 79 499 9046
Email: dschraader@deloitte.co.za

Michele Townsend
Risk Advisory Africa: Director
Mobile: +27 82 441 7164
Email: mntownsend@deloitte.co.za

West Africa

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

East Africa

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 720 111 888
Email: jnyangaya@deloitte.co.ke

Central Africa

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +260 973 224 715
Email: tsimon@deloitte.co.zm

Endnotes

1. Amazon WS official statement: https://aws.amazon.com/message/41926/
   FT.com story: https://www.ft.com/content/b809c752-fded-11e6-96f8-3700c5664d30
2. Salesforce statement: https://help.salesforce.com/articleView?id=Root-Cause-Message-for-Disruption-of-Service-on-NA14-May-2016&language=en_US&type=1
3. FT report: https://www.ft.com/content/c0b82d40-0061-11e8-9650-9c0ad2d7c5b5
   Lloyds press release: https://www.lloyds.com/news-and-risk-insight/press-releases/2018/01/failure-of-a-top-cloud-service-provider-could-cost-us-economy-$15-billion
4. https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published
5. https://www.gartner.com/newsroom/id/3871416
6. https://www.gartner.com/newsroom/id/3871416
7. https://www.microsoft.com/en-ph/smb/azureforSMB/thecloud101
8. https://aws.amazon.com/what-is-cloud-computing/
9. https://cloud.google.com/what-is-cloud-computing/
10. https://www2.deloitte.com/insights/us/en/focus/tech-trends.html
11. https://blogs.microsoft.com/datalaw/initiative/reforming-laws/clarifying-lawful-overseas-use-of-data-cloud-act/
12. https://ec.europa.eu/info/law/law-topic/data-protection_en
13. http://www.lawsociety.org.uk/support-services/advice/practice-notes/cloud-computing/
14. https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-'cloud'-and-other-third-party-it
15. https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
16. https://ec.europa.eu/digital-single-market/en/cyber-security
17. http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm
18. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
19. https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
20. https://www.cyberessentials.ncsc.gov.uk/
21. https://www.ncsc.gov.uk/guidance/cloud-security-principle-14-secure-use-service
22. https://www.ft.com/content/0ad32f0c-430f-11e8-803a-295c97e6fd0b

Notes

Acknowledgements

We are grateful to the Deloitte UK Cyber Risk Services team for their insight and guidance, without which this report would have not been possible.

Deloitte.