Deloitte.

Getting cloud right

How can banks stay ahead of the curve?

Contents

Executive Summary

Cloud's benefits and value for banks

Cloud enables banks to improve their business agility, drive innovation by tapping into cutting-edge technology, leverage industry-specific solutions, and shift their spending paradigm from CapEx to OpEx.

Key success factors for cloud transformation

Cloud transformation projects must start with defining a 'cloud strategy' closely aligned with the organisation's broader business strategy, followed by complying with risk management and governance requirements, with a financial analysis justifying the investment. The subsequent actual migration to the cloud will call for a corporate culture change to drive innovation and fully leverage cloud capabilities.

Cloud cyber security

Cloud services extend the IT footprint of organisations, thereby increasing the risk of cyberattacks. This means that robust arrangements for cyber security should be implemented. These should cover seven cyber domains: network and infrastructure security; identity and access management (IAM); data protection; logging and monitoring; resilience; DevSecOps; and governance, risk and compliance.

Why have banks been reluctant to use cloud?

So far, regulations, combined with data security and the challenges of cloud transformation, including risks associated with outsourcing critical processes, have discouraged many banks from adopting cloud services. In comparison, major cloud service providers have increased their global physical presence, and in some cases resolved issues regarding the obligation to host data within the country where the data is collected. Transformation challenges can be overcome by adopting a structured approach to adopting the cloud.

A thorough risk assessment and an ongoing vendor management process (i.e. an ongoing process aiming at nurturing and developing the relationship with the vendor to get the most out of their products) should enable banks to mitigate data risks and third party risks.

Compliance with regulatory requirements

Using cloud services raises questions about regulatory compliance, because processing sensitive information or client identifying data (CID) is subject to national regulations. These have prevented many banks from embracing the cloud. Since regulations differ between countries, this report presents the EBA considerations (see sidebar for CSSF specific rules).

How to select the right cloud service provider

Finding the right cloud service provider depends on your cloud strategy and the current and future technology operating model you are planning. Deloitte recommends a framework for assessing your operating model and the service offerings of potential cloud service providers from a range of different perspectives: regulatory aspects, compliance, cyber security, and technology issues.

Introduction

Cloud is not the future or an emerging trend anymore. It is a mature business model that constitutes a critical tool for financial institutions to stay competitive in today's challenging business environment. Success with process re-engineering and efforts of digitalisation with emerging technologies such as artificial intelligence are dependent on the smart usage of cloud services.

Some banking regulators and supervisors recently published guidelines to enable banks to make more extensive use of cloud services, whilst at the same time stating that banks cannot relinquish their accountability for outsourced IT services.

This report provides an independent perspective on the major opportunities and risk management issues, but also – based on our practical experience – a high-level roadmap to cloud transformation and the common pitfalls that banks should consider. This report also provides tools to answer some important questions about IT:

- How can we seize opportunities while mitigating risks?
- How can we keep up with innovation while avoiding costly mistakes?
- How do we survive and thrive in the cloud?

- Leveraging cloud services represents a shift in management attitudes – organisations are moving away from a do-it-all-yourself mentality in favour of external providers with scalable, flexible, faster, and sometimes cheaper services. While some organisations are apprehensive about using the cloud, it should be an integral component of today's service-delivery model as it enables banks to tap into new market opportunities and access new delivery channels.

Some banks are therefore moving to a 'cloud-first' strategy. Cloud deployments with off-the-shelf offerings are becoming ubiquitous, while on-premises deployments are becoming the exception. Many RegTech companies [1] offer software as a service out of the cloud. Banking-focused boutiques offer managed services which are already compliant with banking regulations across all technology layers from infrastructure to software, enabling banks to accelerate their cloud adoption by providing out-of-the-box compliance with industry-specific regulations.

Cloud success stories

Société Générale and Microsoft Azure [2]: "Société Générale partnered with Qarnot Computing and the Microsoft Azure team to build a new financial simulation platform. Market activities require complex financial simulations that run on large-scale grid computing infrastructures. The new platform is flexible, scalable, environmentally responsible, and designed to support the growth of Société Générale's business in a rapidly changing economy."

Cloud specifications and meaning

Banks and major cloud service providers are on a collision course. For example, Amazon offers cash services, credit cards, and other basic financial products including Amazon Pay. Another example is Alibaba with its spin-off AliPay, which has over 900 million customers, far more than the largest US bank. Both Alibaba and Amazon have improved their ability to offer business banking services on their platforms. More broadly, there are predictions that devices such as Alexa, Siri, and Google Home will be the future of banking, since these smart AI bots will act as a financial assistant in everyday life. Imagine asking Siri: "Can I afford this car now or should I wait until next year?" Embracing the cloud is a matter of survival in a business environment where innovation, disruption, and competition are pushing banks to improve efficiency and become more agile, while providing added value to their customers. Successful leaders should think 'customer first' if they want to survive in today's fast-evolving and competitive marketplace, and the enabler for this is 'cloud-first'.

What is the cloud? The cloud consists of a broad range of offerings where services are provided internally or externally through a third party, and is always purchased "as-a-service". Offerings vary from basic computing resources to platforms and fully functional software ready to deliver business value. In order to be considered a cloud service, it should live up to a set of characteristics. The generally accepted definitions are outlined below:

Cloud characteristics

- **On-demand self-service:** customers can deploy the required resources on their own without going through the cloud service provider.
- **Broad network access:** the services are available through a network (or over the internet) using standard connection mechanisms.
- **Resource pooling**: through a multi-tenant model, all computing resources are pooled to deliver services on-demand.
- **Rapid elasticity:** computing resources are provisioned and Vreleased immediately, and often automatically, according to customer demand.
- **Measured service:** cloud resources and services are automatically controlled, optimised and measured for reporting and invoicing.

Cloud specifications and meaning

Cloud deployment models

- **Public cloud** (off-premise or external): cloud computing services provided by suppliers to multiple customers via a cloud computing architecture that allows customers to share computing resources. Swisscom Cloud or DigitalOcean are examples of public clouds.
  A hyperscale public cloud is a category of public cloud providing a larger pool of resources, serving millions of users and combining hundred thousands of individual computers into a low cost resource pool with maximum availability. Amazon Web Services, Microsoft Azure and Google Cloud are prominent providers of hyperscale public clouds.
- **Private cloud** (on-premise or internal): cloud computing services owned and operated on-site by a single organisation. For Virtual Private Cloud services the infrastructure is located at a Cloud provider and fully supported by them, but the environment remains 100% dedicated to a single organisation.
- **Hybrid cloud** (integrated public and private service): a mixed environment combining public and private cloud. A modern development focuses on the aspect of management from a single point as opposed to managing each cloud instance from discrete consoles.
- **Community cloud**: a public or private cloud shared by an industry group, government agency, or other association with similar demands or interests.

Cloud delivery models

- **Infrastructure as a Service (IaaS)**
  This provides low-level resources such as computing, storage and networking for customers to build scalable applications. AWS EC2 is an example of IaaS providing 'virtual machines'.
- **Platform as a Service (PaaS)**
  One level above IaaS, PaaS provides a managed environment to develop applications such as a Java runtime or a NoSQL database. Google Cloud's App Engine is an example of PaaS providing a managed Java, Python, Go or node.JS environment for developing applications without the need to manage the underlying infrastructure.
- **Software as a Service (SaaS)**
  This provides user-ready, out-of-the-box software providing a specific built-for-purpose business service to the customer. Microsoft's Office 365 is an example of a SaaS, where customer can use the service without managing any aspects of the underlying software and infrastructure.
- **Managed Services (MS)**
  MS are an additional layer of services delivered on top of cloud services, to manage processes such as 24/7 SLA monitoring, operational management, liability frameworks, ecosystem integration, audit, security, fail-over management, compliance and other processes. In the banking industry, Avaloq's managed services ensures that banks are in compliance with regulations and manage all the operational and regulatory aspects of the underlying systems.
- **Business Process as a Service (BPaaS)**
  BPaaS is a form of Business Process Outsourcing (BPO) that employs a cloud computing service model to deliver automated services sourced from the cloud and operated within a shared multi-tenant infrastructure. Whereas the aim of traditional BPO is to reduce labour costs, BPaaS reduces labour costs through increased automation and economies of scale. As an example, Deloitte's BPaaS offerings provide managed logs analytics and managed cyber risk with specific industry skills, especially for customers in highly-regulated industries.
- **Cloud stack**
  A cloud stack is a software layer that can be deployed on computing infrastructure to provide a cloud environment. As an example, Microsoft installs an Azure layer or stack on top of dedicated hardware (e.g. HPE, Dell or Lenovo) which creates the Azure environment. An Azure stack can also be deployed in a private data centre to simulate some features of Azure cloud in a private environment.

"Many large corporations, especially those for which 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." [3]

Benefits of the cloud for banks

Running a business in the cloud offers numerous advantages depending on the industry, business size, and location. Deloitte has grouped the potential benefits for banks into the following four categories:

- Improved business agility
- Innovate through consumption of external services
- Leveraging industry-specific solutions
- Shift in IT spending pattern

Each of these attributes brings valuable benefits when implementing a cloud strategy. For example, a shift in spending can enable companies to reduce working capital and free up cash to invest in exploring new technologies; while an improvement in agility can facilitate innovation and also accelerate the shift towards IT service consumption instead of IT ownership, which impacts the spending pattern. A successful cloud transformation should capture the benefits from all four areas.

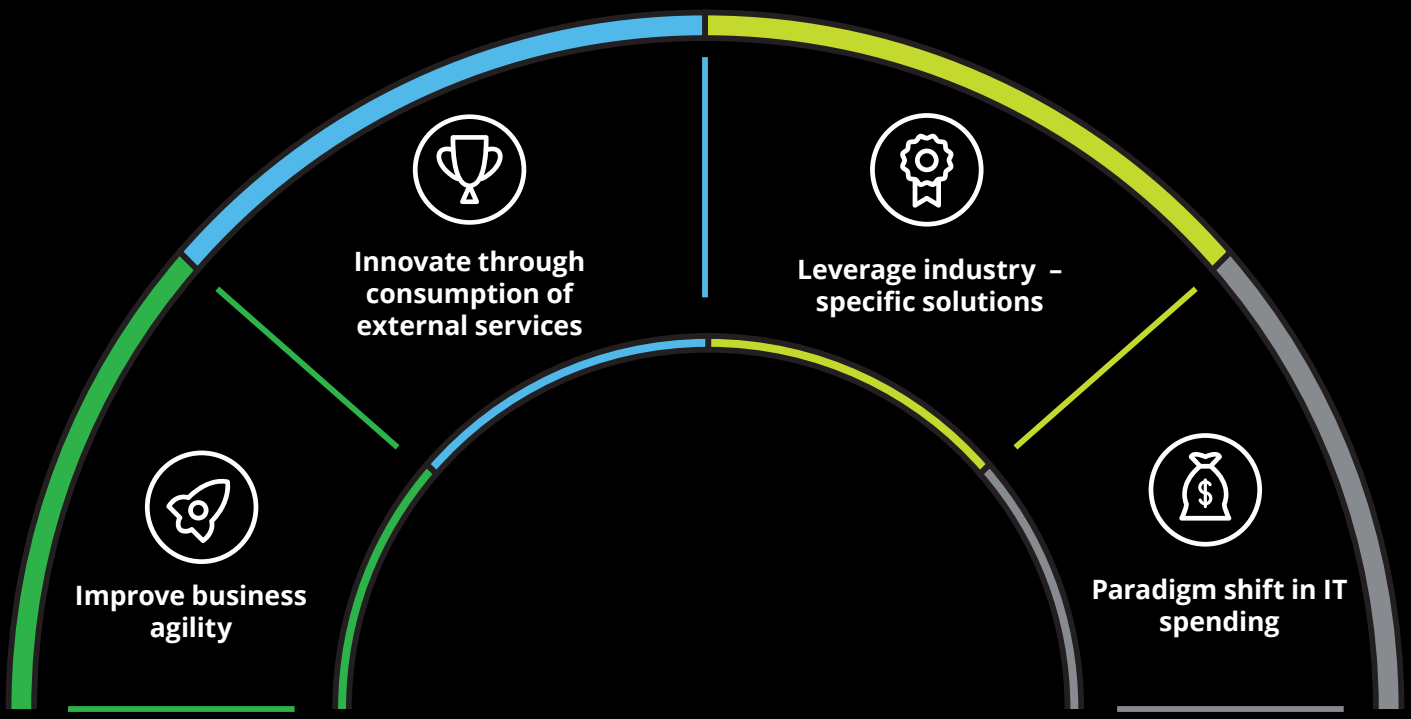


Figure 1 - source: Deloitte Cloud benefits for banks

Innovate through consumption of external services

Many banks still today rely heavily on legacy systems such as mainframes and old programming languages such as COBOL, which restricts business agility. This is sometimes called technology debt. The rise of the digital economy has put pressure on financial players and triggered the need to pursue digital transformation and integration of new digital technologies quickly in order to respond to changes in the market and consumer behaviour. Legacy systems often do not provide the appropriate level of agility that is needed to keep up with the pace of change.

FinTech companies were created 'digital and cloud-native'. Disruptors such as N26 and Revolut are not only able to deliver solutions at much faster pace, they also attract customers and gain market share due to their user-friendly and innovative solutions, fuelled by an agile, cloud-based infrastructure.

"Many banks around the world are aggressively pursuing a mobile-first strategy. Some have launched mobile-only bank brands to fend off FinTech challengers, while a vast majority are enhancing their mobile apps with new features such as person-to-person payments, personal financial management tools, and virtual assistants." [4]

Deloitte recommends a multi-stage approach for traditional banks to move away from legacy systems towards the cloud. This begins with an evaluation of the suitability of the cloud for key applications and processes and a gradual shift from legacy systems towards the public cloud (if compatible with regulations), since this type of cloud model yields the most benefits in terms of elasticity, functionality, and cost efficiency. A hybrid cloud architecture is the industry standard today, but there will be an increasing shift towards the public cloud due to the benefits from hyperscale cloud services.

Cloud success stories

Capital One and AWS [5]: "Capital One moved its mobile servicing platform to the public cloud using AWS. Leveraging public cloud enabled them to find and fix previous performance issues in their applications. AWS enabled them to develop their ideal application by removing the constraints that were preventing them to reaching their objectives."

Innovate through consumption of external services

Banks need to fully embrace the cloud and re-imagine their processes. The only way for a bank to be competitive in the future will be to embrace big data across all its product offerings and leverage AI to change the customer experience.

This cannot happen without at-scale computing and storage. It is impossible to re-imagine mobile banking, payments or efficient lending without an underlying cloud platform. In the future, Robo-investors (AI bots that replace portfolio managers and outperform them) will need systems that can process huge volumes of data, something that banks cannot do neither easily nor cost-efficiently with on-premises solutions.

Cloud success stories

Citigroup and IBM [6]: "Citigroup was seeking to reduce time to market for the company's more than 20,000 internal applications. Developers who were usually forced to wait up to 45 days for infrastructure resources to be provisioned could access servers in less than 20 minutes using IBM Cloud, streamlining development cycles and drastically reducing the time to value for the company to deliver applications to their customers."

Disruptive technologies are strategic assets in the financial industry, but adopting and extracting value from them within a reasonable timeframe can be a challenge. What if you could use them as an outsourced service instead of hosting and owning them? By giving access to a range of specialised tools and services, cloud services provide an ecosystem of Centres of Excellence that can be accessed rapidly through the internet, making organisations more competitive.

State-of-the-art cloud platforms offer key capabilities in strategic domains such as analytics (Google Cloud's Dataproc), blockchain (AWS Blockchain), and distributed mobile applications (Azure Mobile Apps) enabling software development teams in banks to stay ahead of the innovation curve. Developing or owning new technologies becomes an obsolete burden when they can be used in applications as a service in a seamless manner.

Leverage industry-specific solutions

Using IaaS or PaaS to build applications offers enormous flexibility in terms of design and functionality; however, flexibility also comes with challenges. Highly regulated industries such as banking have a complex burden of regulations and compliance, which makes a do-it-yourself option for applications development both costly and risky.

Banking-focused solutions delivered as higher-level services such as SaaS or BPaaS can provide an out-of-the-box solution and help banks cope with the regulatory burden by ensuring regulatory compliance, auditability, transparency, and security along the whole value chain, from the provision of infrastructure to the delivery of the service to the end-user. A Managed Services provider can guarantee end-to-end responsibility and act as a single point of contact for banks, greatly simplifying operations and management. This shift to service consumption replaces the in-house software development processes, delivery and operations model that banks have, and this inevitably has implications for the organisation and its employees.

Cloud success stories

Deutsche Bank and Avaloq [7]: "The introduction of the Avaloq Banking Suite enabled Deutsche Bank Luxembourg to migrate its various business areas into a new, unified cash ledger, enabling it to offer its customers the full range of services while reducing complexity, risks and costs, and paving the way for future growth. The relevant banking areas migrated in one move from the existing core banking system to the Avaloq IT platform."

Cloud service providers can deliver banking-specific solutions such as core banking, risk analytics with comprehensive portfolio management, securities management, online banking platforms, payments or back office services such as settlement services, corporate actions services, and reconciliations.

Providers benefit from economies of scale by re-using their solutions across multiple customers, and so in many cases are able to offer their service to banks at a lower cost than an in-house process. Standardisation can also be achieved when using mid- to high-level services such as PaaS or SaaS; however little standardisation is available from IaaS due to the wide variety of design choices that remain available to the developer.

Add-on services and functions are not automatically provided when using IaaS or PaaS, such as disaster recovery, integration, supportability, and operability assurance; these aspects can also be handled by SaaS providers that specialise in banking.

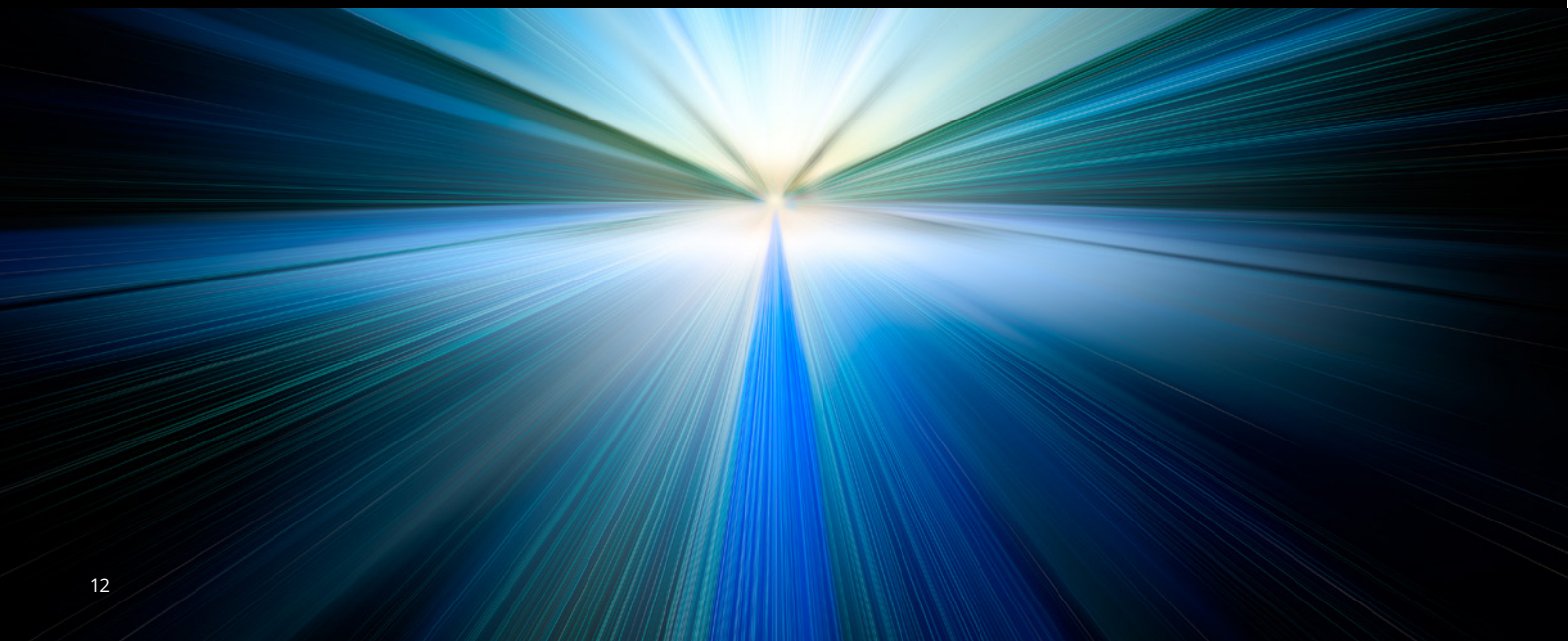
Shift in IT spending pattern

Cloud provides a shift from CapEx (Capital Expenditure) to OpEx (Operational Expenditure), as a result of switching from asset ownership to service consumption. The following advantages emerge from this change:

- **Flexible pricing** (only pay for what you use). Only consumed services are charged for. This may lead to cost savings, especially for punctual and intensive workloads such as daily, monthly and year-end processing. However, there may or may not be cost savings, depending on how the cloud services are consumed.
- **No upfront infrastructure investment.** Being released from large upfront costs enables organisations to reduce their working capital, and the cash this releases can be used to pursue other growth or innovation ventures. It is important to keep in mind that some upfront costs such as costs of integration, connectivity and migration can still be incurred when moving to the cloud.
- **No depreciation, renewal costs or obsolescence of infrastructure.** With the purchase of infrastructure there is always the risk of aging and obsolescence; this can be avoided by consuming resources as a cloud service.

Cloud success stories

Credit Suisse and Cloudera [8]: "[Credit Suisse] developed an enterprise-wide Big Data platform on the Cloudera Enterprise solution. This decision enabled the bank to leverage cutting-edge, on-demand and highly scalable data analytics capabilities, while being released from infrastructure-related decisions and maintenance."



Why have banks been reluctant to use the cloud?

The cloud has been widely adopted across various industries and has become a pillar of the IT systems of modern companies. Yet challenges remain for banks, mostly because of strict data regulations, doubts around data security, third party risks and transformation challenges.

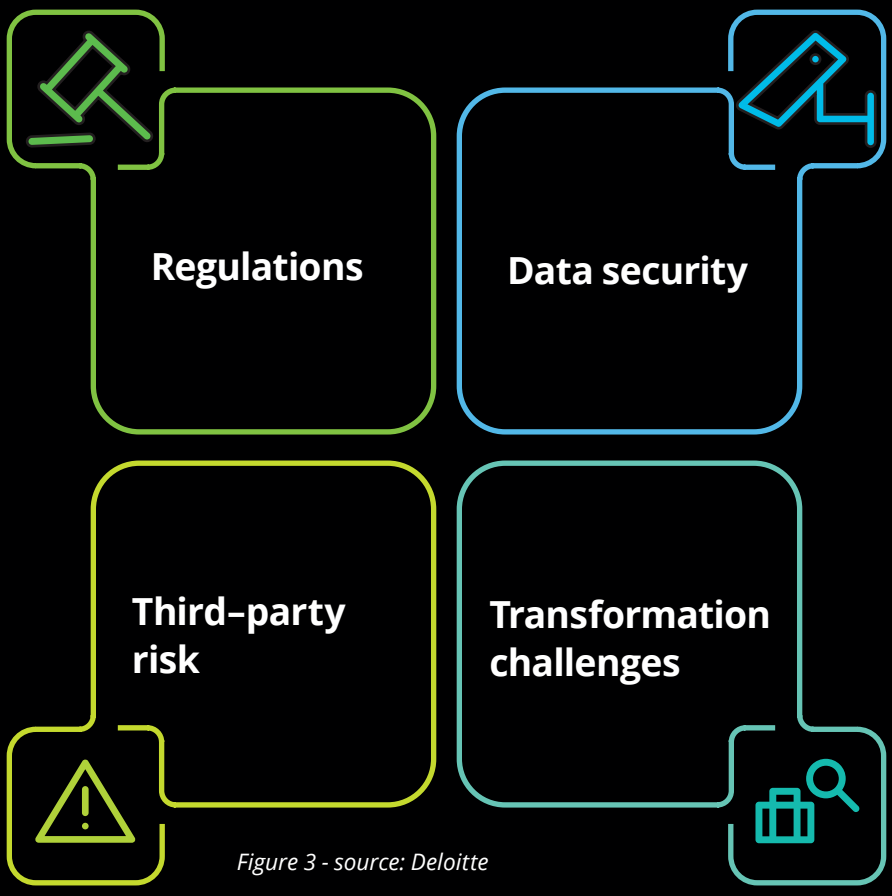


Figure 3 - source: Deloitte

Regulations

National regulatory authorities often insist that data held by domestic companies should be kept only on servers in that country and access to data should only be possible from within the country, and that they may impose legal obligations relating to investigations, data recovery or the location of employees. This means that a cloud service provider has to use local servers, which creates a major challenge for the operating model of global cloud service providers.

Major cloud service providers have tried to increase their global footprint by building more data centres in new locations close to their customers. This helps banks meet some of the regulatory requirements by having data physically located in the same country. Some cloud service providers already operate in compliance with the requirements of local financial authorities.

Banks need to understand the legal structure and framework within which the cloud company operates, and that it may need to comply with the regulations in multiple jurisdictions—including the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of the US—as shown by the efforts of a US law enforcement through US courts to gain access to data on a cloud service providers server in the Republic of Ireland.

Data security

Keeping data safe from unauthorised external access, damage or corruption is a challenge for the financial services industry. Client-side encryption guarantees that an external party or even the CSP cannot access data, since the bank and not the cloud service provider holds the encryption and decryption keys, making it impossible for the cloud service provider to access readable data. However, client-side encryption may affect performance and significantly limit the benefits of the cloud, such as search capabilities, artificial intelligence and analytics—thus a trade-off between functionality and security must be found.

Integration with on-premises solutions for data-management, identity and access-management policies and other security systems should also be considered. In the case of SaaS or BPaaS, data cannot be accessed by the CSP unless it is agreed or needed to provide the service, for example to restore data or ensure business continuity. In order for banks to pursue the optimal strategy and processes to protect information, Data Protection & Privacy should be a pillar in their cyber security strategy.

Third-party risks

Running central systems in the cloud, such as core banking systems, creates a dependency on the cloud service provider. This calls for a risk assessment and vendor management process to ensure alignment between the business objectives and service delivery from the CSP.

From a technological point of view, relying on a cloud service provider to run critical systems in the cloud should not be considered riskier than running the same systems on-premises, provided that the cloud service provider is compliant with financial regulations (e.g. for data retention, data access, and auditability) and the appropriate design and best practices are implemented. To mitigate supplier risks, organisations should implement a process to manage the life cycle of the supplier relationship and clearly align business goals with the services from the cloud service provider, while also managing risks and maintaining an exit plan.

Transformation challenges

Most major banks rely heavily on systems that run legacy applications. In order to move these applications to the cloud and fully reap the benefits of such a transformation, applications need to go through re-design and refactoring, which can be a costly and risky step. Simply switching virtual machines from a data centre to a cloud infrastructure will not deliver the full capability of cloud services: applications should bebroken down into API-connected microservices and use 'cloud-native' components to optimise costs, resilience, and availability. Since mainframes do not integrate well with cloud applications, banks face a situation that must be addressed in most cases with a 'big bang' approach, raising the transformation risks even higher.

IT is not the only part of a company impacted by cloud—the transformation causes a broad rethinking of the company's processes, operating model, and resources. For example, a lack of cloud talent is another major roadblock for banks. Given the broad range of impacts that moving to the cloud may cause for organisations, transformation constitutes an upfront investment that makes many banks hesitate.

Cloud success stories

Barclays and Salesforce [9]: "Barclays Bank streamlined the mortgage application process facing thousands of brokers and customers in the UK with cloud-based pioneering community platform Salesforce, which reduced frictions and delivery time across their mortgage business."

The regulatory context for cloud use in Luxembourg

Luxembourg's financial sector regulator (the CSSF) has been one of the first regulators in Europe to provide guidelines on outsourcing to the cloud. The cloud outsourcing circular 17/654 was published in April 2017 after a series of roundtables with the European Banking Authority and other EU regulators, as well as major Cloud Service Providers. The European Banking Authority published recommendations 11 months later in March 2018, which were then integrated into more general EBA Guidelines on outsourcing a couple of months later.

The cloud outsourcing circular is structured into 4 elements:

- Clarifying what cloud outsourcing is and when the circular applies
- The 4 key roles (i.e. the consumer, the cloud service provider, the resource operator and the signatory) and possible configurations (i.e. who can do what)
- Regulatory requirements in terms of governance, risk management, continuity, system security, contractual terms, activity monitoring, outsourcing oversight, right to audit and termination
- In which case the authority has to be notified or has to provide its approval prior to implementation.

After almost 2 years of experience and 60 cloud application files received, the CSSF published a revised version of the cloud outsourcing circular 17/654 in March 2019. The updated circular (i) introduces proportionality in the requirement for non-material/non-critical outsourcing, (ii) introduces a register of cloud outsourcing to be maintained by supervised entities (material & non-material), (iii) removes the requirement for a notification for non-material activities outsourced and (iv) includes investment fund managers in the scope of application.

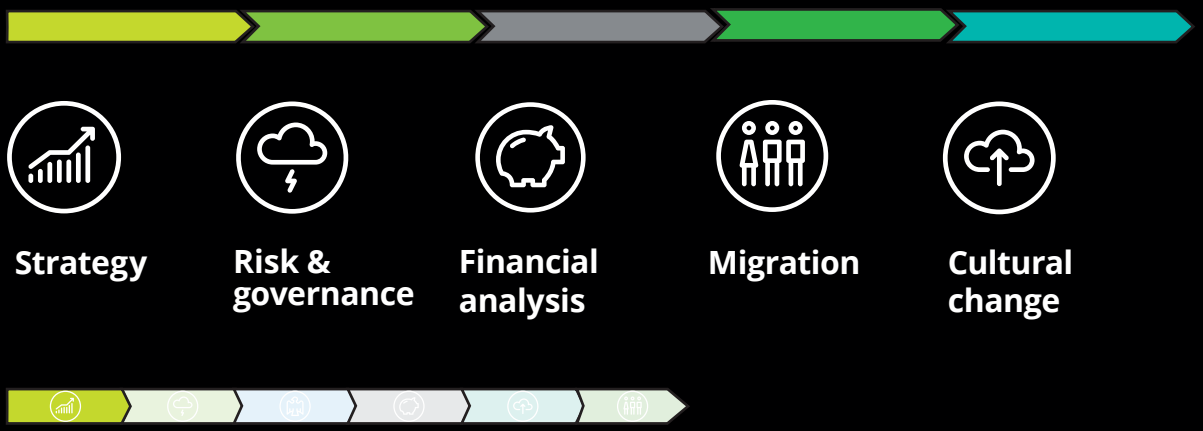
Where regulatory requirements are perceived as the major barrier – most institutions that use the cloud realize that these requirements address the key risks of using it. Capital One was a cloud success story that turned into major data breach with over 100 Million individuals impacted. The data breach was due to a misconfigured firewall and caused a 6.5% share price fall for Capital One following its announcement. Furthermore, these requirements were a strong incentive for the major Cloud Service Providers to adapt their contractual terms for the Financial Sector and particularly extending audit rights.

Here are the top 6 questions one should be able to answer before considering regulatory requirements and approaching the authority: Is it really cloud-based? Is it material/critical? What data will be sent/stored/processed? Who is doing what? Are there other providers behind? What are my risks?

The data question is particularly important to assess applicability of Professional Secrecy obligation and of the General Data Protection Regulation. Complying with the cloud outsourcing circular is not a waiver to these important legal requirements.

Key success factors for cloud transformation

Using cloud is not just a project: it is a fundamental change in the DNA of a company. To benefit fully from the advantages of the cloud, organisations need a digital transformation that goes well beyond a simple project. Deloitte recommends an approach to cloud transformation that consists of five phases, from strategy to cultural change.



Strategy

Define your objectives for the cloud. The benefits must be clearly articulated – greater operational efficiency, flexibility, agility, increased revenue generation, reduced costs, enhanced security, better risk management, return on investment, and so on. Cloud strategy should follow IT strategy, which should align with the business strategy. Cloud initiatives should always be linked to business value and fit with the overall corporate strategy. Deloitte has developed a framework of six building blocks on which to construct a sound cloud strategy.

Many large organisations already have a 'cloudfirst' strategy in place, meaning that with any project they look to the cloud before considering the in-house or traditional outsourcing alternatives. A cloud strategy should take into consideration not only the present but also the future; embracing cloud enables banks to adopt tomorrow's technology more easily, Blockchain being just one example.

Many large organisations already have a 'cloudfirst' strategy in place, meaning that with any project they look to the cloud before considering the in-house or traditional outsourcing alternatives. A cloud strategy should take into consideration not only the present but also the future; embracing cloud enables banks to adopt tomorrow's technology more easily, Blockchain being just one example.

Deloitte's cloud strategy framework

Architecture & Engineering

- Integration architecture
- Tooling
- Technical architecture

Security, Risk & Compliance

- Regulatory impact
- Security controls
- Data privacy implications

Figure 4 - source: Deloitte

"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. 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." [10]

Risk management

Moving services to the cloud transfers some of the responsibilities for risk management to the third-party cloud service provider. However, it is only the management of the risks that is transferred; accountability for the risks still resides with the bank, and not the cloud service provider. The company's operational risk management framework must therefore take account of the special circumstances arising from cloud service adoption. An important element of the framework should be to classify the information assets—such as intellectual property, customer databases and financial information—so that the inherent risks can be managed. The service contract should include terms that define the right to audit the cloud environment, and organisations must also prepare 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.

Cloud success stories

BNP Paribas Fortis and Google Cloud [11]
"The international bank needed to unify its marketing platform into a single tool to enable its marketers to synchronise efforts and align campaigns. The bank chose Fourcast to develop a new planning system to support marketing communications. Fourcast uses Google Cloud Platform to improve agility by deploying applications quickly without the need to own physical infrastructure; and by using Google BigQuery, their marketing data is automatically linked to their reporting tools." [14]:

Deloitte's holistic Third–Party Risk Management Framework

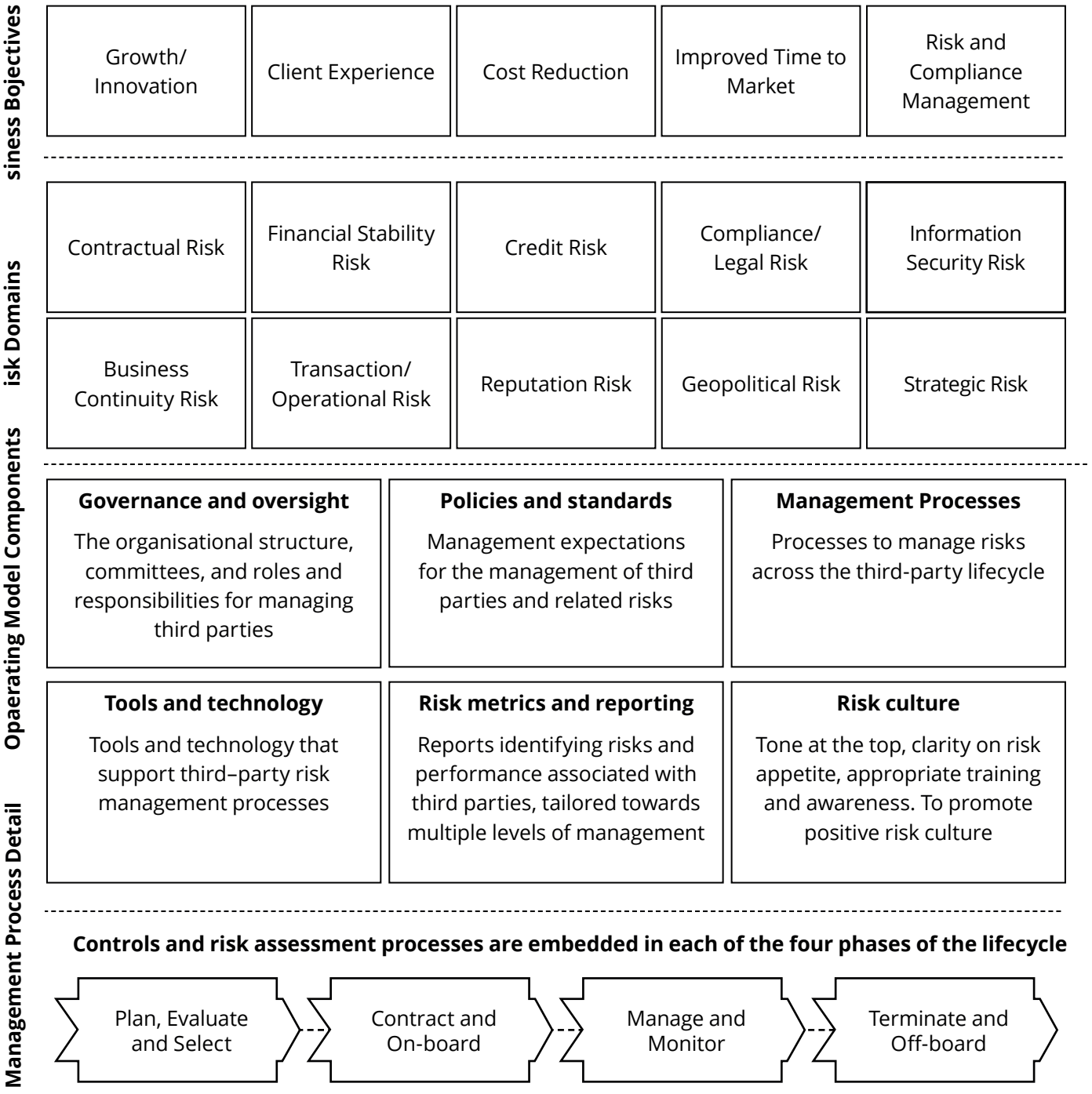


Figure 5 - source: Deloitte

It is particularly important for banks to consider legal and regulatory compliance during their risk assessment, which should involve the risk management functions and other stakeholders, and should be based on the 'three lines of defence' model. Compliance with national laws and regulations on data is a problem that must be addressed.

The European Union's rules also 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 citizens whose data is collected, stored and processed by organisations, but the scope of the Regulation extends to companies using servers outside the EU, if those servers hold data on EU citizens. The full implications of GDPR and other data privacy laws must be understood.

In order to mitigate third party risks stemming from a cloud service provider, organisations should follow a holistic approach, analysing risks into categories or 'risk domains' and mapping them to operating model components in order to ensure monitoring and controls are effective on an ongoing basis.

Governance

Banks must define how decisions specific to cloud solutions will be made. Governance processes relating to the use of cloud services should be developed: who is able to request them, how many resources can be provided, and what approvals are required. In addition to setting quotas, providing visibility and reporting usage will help to hold users accountable. Organisations should establish a robust cloud governance structure with three pillars of governance and ranking of elements within each pillar from strategic to functional.

How can governance be made sufficiently flexible to manage risk while supporting innovation and cost reduction? Establishing governance and controls provides direction for an organisation's adoption of the cloud. These should consider controls for business processes, applications, data, infrastructure, and organisational management.

Structured governance is required to monitor performance continually, improve service effectiveness, and align investments with business objectives.

To avoid new or additional risk, governance should ensure proper due diligence and security, and should specify standards for which services are permissible and which are not. In practice that could mean that business services can get integrated and used—as long the service is built on Microsoft or Google cloud components—if these vendors have already been approved for use by the company.

Deloitte's IT governance framework

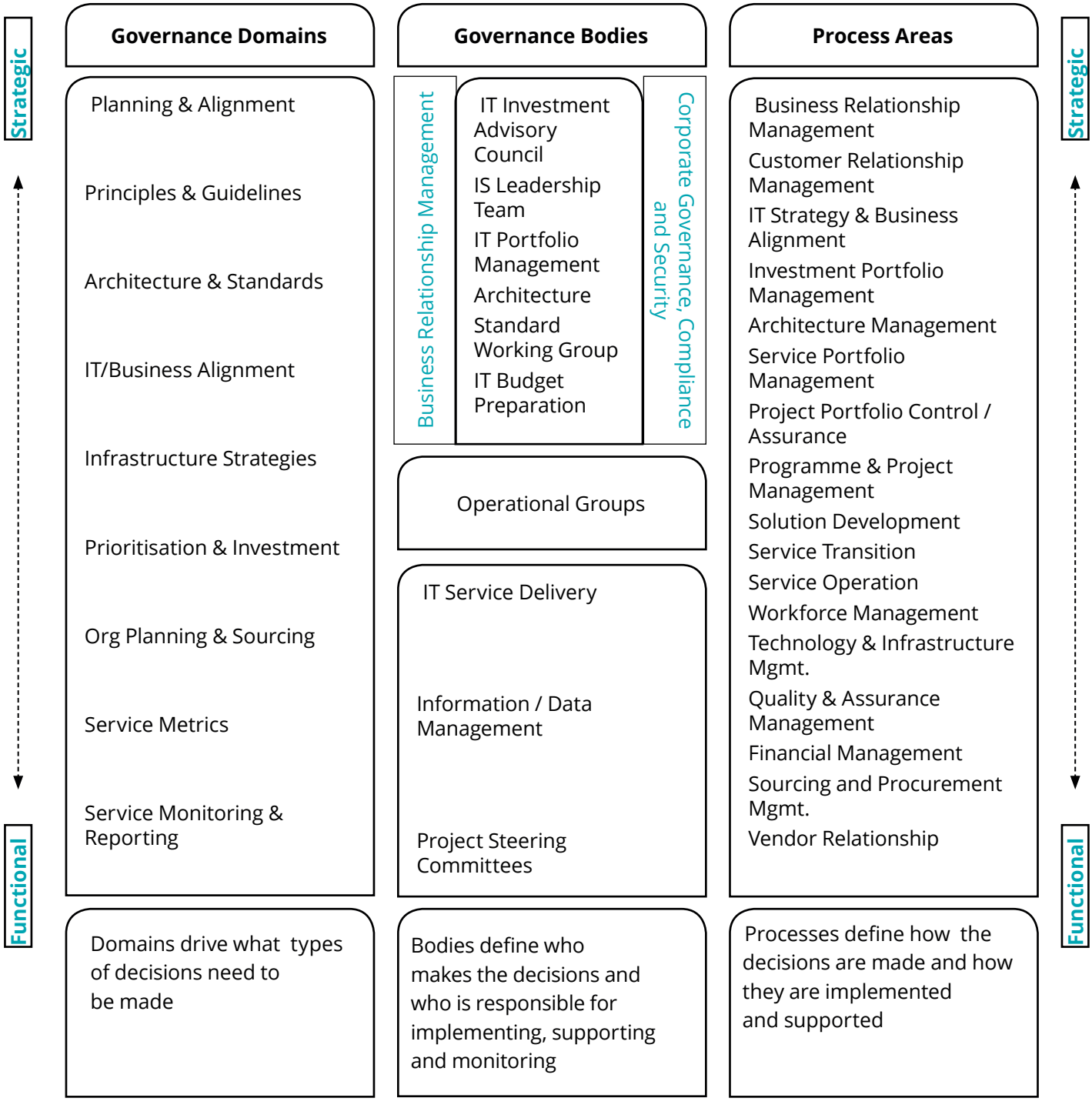


Figure 6 - source: Deloitte

Financial analysis

A business case should be developed to justify the migration of workloads to a cloud environment in order to mitigate risks relating to cost management. Organisations should analyse the quantitative financial benefits of transition to the cloud. C-Suite executives want to know: what are the cost drivers for cloud transformation? What are the high-level benefits of embarking on a cloud transformation? How may these benefits be realised? Financial benefits from cloud will not be limited to IT, since they will impact time-to-market, innovation and competitiveness (as outlined earlier in this report). While these business benefits must be considered in each case, they may be difficult to evaluate quantitatively and are heavily dependent on the organisation's structure and strategy. We therefore propose three areas for analysis in building a financial case for the cloud from an IT perspective.

Organisations are looking for clear directional impact by analysing the quantitative benefits of cloud. C-Suite IT executives want to know: what are the net costs and benefits of embarking on a cloud transformation? How can we capture the cloud value to offset transformational costs?

Cloud success stories

HSBC and Oracle ERP [12]: "Global banking giant HSBC used Oracle ERP Cloud to re-engineer the financial management processes across its global Operations, Services and Technology division. The bank transformed procure-to-pay, expenses and project accounting across its global operations and functions, not just in the organisation of its global service companies. Ultimately, all third party costs and a significant portion of the global cost base are managed by Oracle ERP Cloud."

Migration

Applications may follow different migration paths, ranging from a simple 'lift-and-shift' where applications are re-hosted in a cloud environment without further amendments, to a complete refactoring of the application using 'cloud native' components. Each approach has pros and cons: for instance a complete refactoring is costly and creates vendor lock-in, but it also allows applications to leverage fully the capabilities of the cloud such as elasticity, high availability and high resilience. Re-platforming applications on PaaS is a trade-off chosen by many organisations, since in many cases it provides most benefits from the cloud without the lock-in.

Organisations should proceed with a phased approach to conduct migration in an efficient manner.

Transporting legacy applications to the cloud is a thorny challenge for many banks—for this reason Deloitte acquired Innowake® [15], which can translate Cobol/PL1 code into Java code, helping to refactor legacy software into cloud-ready applications.

In case of mass migration, an Application Migration Centre of Excellence should be created to benefit from efficiencies and economies of scale. After migrating, ensure shutdown of legacy on-premises systems to avoid parallel operations and costs.

Corporate culture

Cloud is not just about technological transformation, but also about adapting the corporate culture to use of the cloud, and adopting a new mind-set for working and collaborating in order to leverage the technology. People need to start thinking 'cloud', for example by adopting DevOps practices. 'DevOps' is a contraction of 'Development and Operations', and is a paradigm for software production which consists of streamlining the lifecycle from development to production. DevOps enables companies to increase their agility and innovative abilities whilst reducing risks and delivery cycles. Corporate culture needs to change, from a mind-set focused on static, policy driven operations towards small entrepreneurial units that have a much greater freedom of choice. Business leaders should embrace the entrepreneurial spirit and empower business units to take advantage of the flexibility offered by the cloud in line with the defined governance structure.

" 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." [13]

Organisations should follow a culture change roadmap to bring people along and make a cloud transformation not only a technical implementation but an end-to-end transformation across all dimensions of the company.

Business buy-in is crucial, because cloud means business transformation. It is essential to have the active support and involvement of senior executive management and board. Whether the migration towards cloud is initiated by IT, a banking business line, or another part of the company, the benefits and the costs must be demonstrated to, and signed off by, the company's leaders. In turn they must incorporate the cloud strategy within the company's overall business plan. Impacts on human resources must also be considered, since a cloud transformation can lead to a shift in the headcount and skills required within the company, because IT services are now run by a cloud service provider, and not by the company itself.

Cloud cyber security

Cloud is not only redefining the IT landscape but also how security measures are designed and implemented. In particular, the migration to a virtual data centre forces organisations to rethink security and privacy from the ground up. At one time, the security of cloud service providers was a significant concern for many companies, worried that cyber attackers would find it easier to penetrate the cloud than on-premises systems. Even today this issue – together with privacy concerns – is one of the biggest barriers to cloud adoption. However, cloud security (at least at the hyperscale cloud service providers) can in fact be a positive argument for adoption of the cloud, since cloud service providers invest more in security than most multinational companies will ever be able to. Security is in effect part of the main business process of cloud service providers, and not just a support process.

What is new from cyber security perspective in the cloud?

As businesses move to cloud computing, employees in principle are able to access their work applications and corporate resources through almost any internet-connected device. As a result, they want and expect 'anywhere-access' on a device of their choosing. Since data is transmitted through unsecure public internet networks, the 'old' security solutions for in-house systems do not offer the protection required. In fact, perimeter-based security has not been effective for some time against modern cyber threats; and with cloud computing it is even less effective. There is also a shift from segregated IT systems to a cloud environment where virtual machines and networks share the same physical resources, posing different security challenges for cyber professionals.

Through 2022, at least 95% of cloud security failures will be the customer's fault." [14]

Security of the cloud

The cloud service provider is responsible for the reliability, security and compliance of the services that make up the cloud. These include responsibilities for the integrity of the hardware, software, networking and facilities that run the cloud services.

Security in the cloud

Organisations should implement controls for elements which they are responsible for. This will depend on the cloud services they use.

For example, if an organisation transfers an application to an IaaS environment, it is responsible for some of the infrastructure security. On the other hand, organisations using SaaS solutions are only responsible for data, governance and security compliance.

It is important to understand that the division of responsibilities for securing cloud workloads differs between the types of service. However, the liability for data stored and processed in the cloud, as well as overall security of a cloud based solution, always remains with the organisation using the cloud services.

Cyber security perspective in the cloud

User/Shadow IT

The accessibility and ease of subscription to cloud services created a situation in which employees were able to use cloud applications for work-related data exchange that were not approved by the company IT. Similarly business units could buy the cloud services they wanted without following procurement procedures or giving consideration to security or privacy issues.

There were various reasons for this, but the consequences were often the same—breached accounts, leaked data, malware spread across the company. Organisations need to have an answer to this problem in order to protect their digital assets. A key element is to be able to identify and manage the cloud services that are used or could be used from the organisation's managed devices and networks.

Concentrated Risk

An accumulation of valuable items will attract the attention of people with malicious intent. This is true for valuable physical items as well as information. The risk of a successful attack is greater for a cloud service provider because it would probably involve the information of many different customers. Companies have to rely on their cloud service provider to address and mitigate many of the risks since they cannot manage the risks themselves within the shared responsibilities model. Cloud service providers in turn are highly motivated to invest significantly in defence measures to maintain their ability to withstand threats and make attacks on them cost-prohibitive. In order to select the right cloud service provider, organisations should examine closely how cloud service providers are managing such risks and what kind of contractual liability they have for a breach of data security. In addition they should examine additional risk mitigating functions.

Modern Attack Surface

New technology and digital solutions bring new methods of cyber attack and make old ones obsolete. The cloud is no exception. Employees of cloud-enabled organisations often work from any devices anywhere on the planet, making it more difficult than ever to protect the organisation's data. Not only must the intranet and cloud workloads be secured, but every user device should also have technical measures in place to protect data. To add to the problem all the cloud-enabled devices in the organisation must be monitored 24/7 and in real time, since once a security breach occurs it won't take long for the hacker to target the 'crown jewels' of the organisation's information and data.

Controls Gap

Using cloud services requires a re-think of the controls an organisation should use. Monitoring and securing a cloud-only or (more often) hybrid environment requires new methods, processes, and technology, because even the most mature and safe cloud service provider technology still depends on customers using it in a secure way. Risks of failure are high—attacks can go undetected, data can be lost, and reputations can be damaged.

Third–party Risk

When a company uses cloud services it connects its infrastructure to a cloud service provider's. Security for the overall system depends not only on the organisation using the cloud services, but also on the cloud service provider's security controls. The cyber risks are the same as with the on-premises infrastructure. This means that physical security of the cloud service provider equipment, software and hardware updates, internal governance processes,and technical controls have to be assessed by a potential user in accordance with its own security and privacy requirements. Organisations considering a cloud solution should insist on seeing the cloud service provider's controls and certifications, and check whether there is a single place where such documents are stored (e.g. a trust portal or similar). If gaps in controls are identified, the organisation should either switch to a different cloud service provider or close the gaps with its own security controls.

Addressing cyber risks in the cloud

Cyber risks need to be addressed as organisations embrace cloud, mobile, social and analytics technologies. Organisations should develop a cyber risk framework that focuses on delivering end-to-end cloud cyber risk capabilities, incorporating considerations about privacy, security, monitoring, incident response, and governance for integrating cloud services across the organisation. In Deloitte's Cyber Risk Management framework there are three pillars ("Secure. Vigilant. Resilient") and seven cyber risk domains.

Secure

The Secure pillar of a cyber risk management framework provides protective elements. It contains three domains. The first domain, Network and Infrastructure security, covers the virtual infrastructure with a focus on protecting network traffic, hardening endpoints like API gateways, and protecting services. Identity and access management, the second domain, is designed to help address different cloud requirements for authentication, authorisation, access governance and accountability. Specific elements include multi-factor authentication, privileged access management and access certification. The third domain, Data Protection, covers controls recommended for protecting data at rest, in transit, and in use: core elements are encryption, key, and certificate management.

Vigilant

The Vigilant pillar involves the provision and integration of information, from both on-premises and cloud sources, to enable security teams to identify, detect, and respond more effectively to security threats. The domain Logging and Monitoring involves techniques for detecting security events, collating a multitude of log sources, and integrating with a Security Information and Event Monitoring (SIEM) system to monitor the cloud, to enable the organisation to identify where critical data assets reside, who accesses them, and how they are used.

Resilient

The Resilience domain covers designs for 'always-on' capabilities, and new models for contingency planning, recovery, and resilience. As cloud computing becomes a more integral part of core business operations, it becomes necessary to reduce downtime due to disruptions from minutes to seconds. A mature cloud service provider provides accessible features such as scalable, on-demand APIs that allow companies in a cost-effective way to create redundant infrastructure and back-ups with low latency to reduce disruption. Other design concepts and tools are cross-region replication of virtual instances, multi-availability zone deployments, and data archiving services. The domain **DevSecOps**, encompasses secure configuration, vigilant security monitoring, and resilient deployment designs. It is worth mentioning that while IaaS provides the building blocks for resilient systems, their effective implementation still relies on the development teams and no availability is guaranteed by the cloud service provider at the application level, since their SLAs stop at the infrastructure level in the case of IaaS. On the other hand, SaaS solutions and managed cloud services can provide SLAs at the software level, giving contractual guarantees of higher level services resilience compared to IaaS or PaaS providers.

The aforementioned security concepts are brought together to achieve business goals with secure software. To define and manage the cyber risk requirements specific to the organisation, the **Governance, Risk, and Compliance (GRC)** domain provides guidance for establishing governance, policy, standards, processes, technology, and reporting, in order to achieve the goals of the organisation.

In conclusion, through the use of a cloud security framework, an organisation is able to design, implement and operate cloud services securely and benefit from the inherent security features that cloud service providers provide as part of their service.

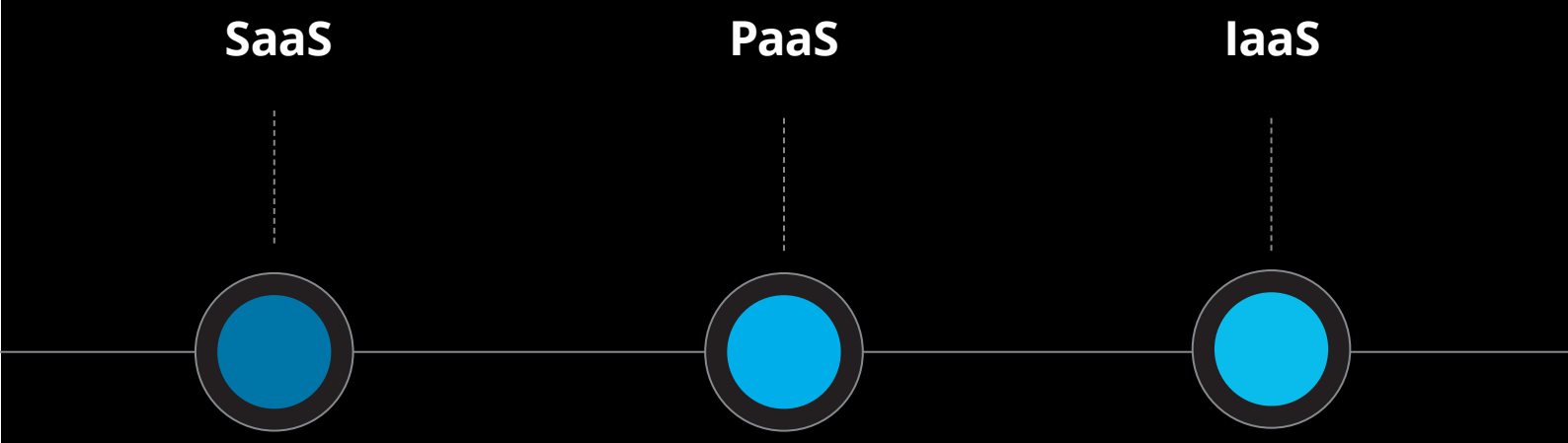
"It is no longer acceptable for security teams to hold back cloud initiatives with unsubstantiated cloud security worries. Security and risk management leaders should be tasked to develop new approaches to securely and reliably leverage the benefits of SaaS, PaaS and IaaS." [15]

Selecting the right cloud service provider: A two-step approach

The large number of cloud offerings on the market makes it difficult for organisations to find the right supplier. To this end, Deloitte proposes a two-step approach to shortlisting and assessing a service providers.

Step 1: Evaluate your IaaS and PaaS provider based on your SaaS needs

The market for cloud services contains different delivery models (IaaS, PaaS, SaaS) available to banks, ranging from local players to global hyperscaling cloud service providers with local data storage.



A bank should begin by choosing its cloud service provider(s) that have the best SaaS spectrum coverage for the essential services the bank wants to use, since in the future, most off-the-shelf solutions will be delivered as SaaS. This spectrum should define the requirements for IaaS and PaaS services that the cloud service provider must be able to deliver.

SaaS providers build their services on top of PaaS or IaaS services. As an example, SAP's ERP solutions can be used as a SaaS hosted in Amazon Web Services, Google Cloud or Azure Cloud infrastructure. Based on an inventory of all relevant applications and services an organisation would need to use from the cloud, a decision can be made about which provider should be selected to carry out the risk assessment and due diligence in order to minimise the number of providers to be assessed.

Deloitte proposes an evaluation of cloud service providers according to two key dimensions:

1. Scaling capabilities
2. Banking specialisation

Deloitte cloud appetite framework

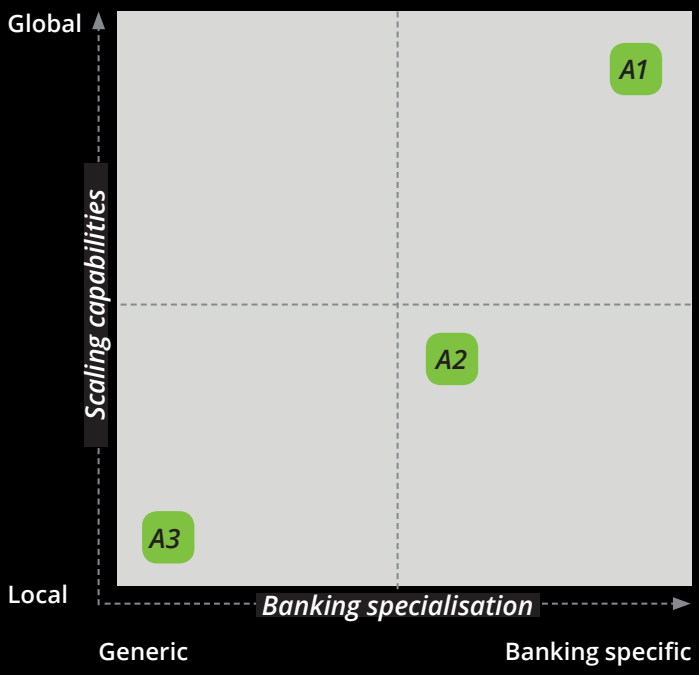


Figure 7 - source: Deloitte : SaaS spectrum of three applications (A1, A2, A3) in this example, can help organisations define their PaaS and IaaS requirements.

Scaling capabilities

A bank needs to decide from which locations it would like to receive cloud services. For example, regulations in the bank's home country might prevent it from transferring customer or financial data abroad. It may therefore be essential for the cloud service provider to have a global footprint with data centres in multiple regions and with the ability to scale.

Banking specialisation

Some cloud service providers offer generic services such as IaaS or PaaS to various industries, while other cloud service providers provide tailor-made solutions specific to banking. In general, it is easier and less risky for banks to select providers with banking specialisation and knowledge of financial industry laws and regulations, that can for example offer transparency with their internal control system, provide access to audit reports, and have templates for service contracts that are compatible with local laws and regulations.

With the Deloitte framework for defining the required SaaS spectrum, a bank can narrow down the list of available cloud service providers to a shortlist of providers that are able to meet its needs. This shortlist of providers then needs to be assessed further in order to select the one that is most suitable for the organisation's requirements.

Step 2: Assess the shortlist of cloud service providers

Below we summarise the key aspects for evaluating cloud service providers by banks. For each of these dimensions, there are a number of key aspects to consider and important questions to answer.

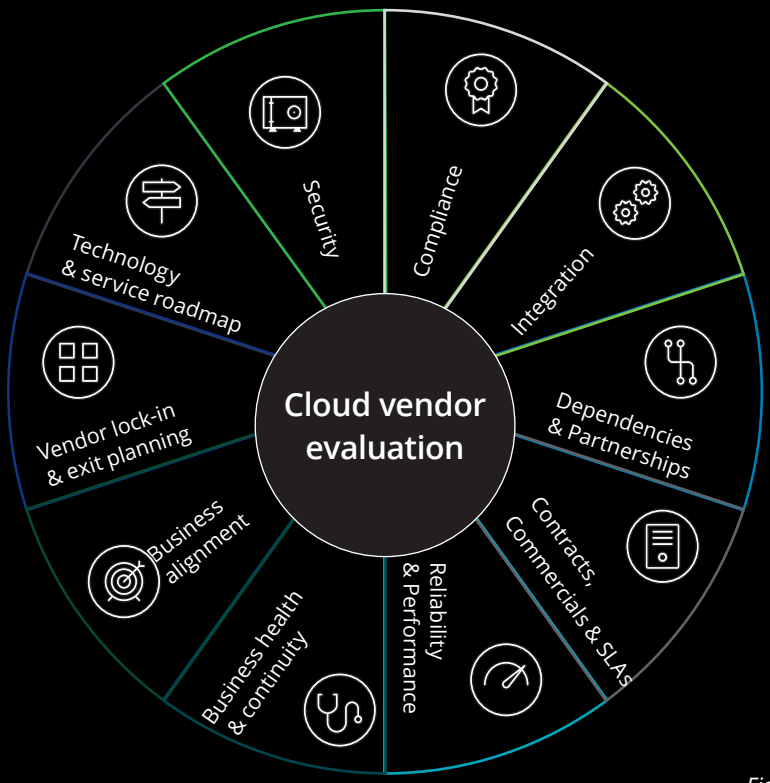


Figure 8 - source: Deloitte

Data security, data governance and business policies

What is the cloud service provider's position regarding the CLOUD Act and the provision of client data to foreign governments? Where are its data centres located? Since security and compliance regulations vary from country to country, organisations operating worldwide need to be aware of the jurisdiction in which their cloud service provider hosts data, how the data is protected from unauthorised access, and what are its policies regarding local and foreign laws on matters such as data disclosure to foreign authorities (e.g. CLOUD Act).

Evaluate the cloud service provider's capabilities in terms of security operations, security governance and system security, and make sure that it has demonstrable risk-based controls aligned with your organisation's own security processes and policies. Verify that user access and actions are auditable and are in alignment with the security responsibilities as set out in the organisation's business policies or service contract.

Compliance with regulations, certifications and standards

Ensure that the cloud service provider follows compliance guidelines that apply to your industry and organisation. Whether you are committed to GDPR, SOC 2, PCI DSS, HIPAA, ISO 27000 series or some other standard, make sure you understand what it will take to accomplish compliance once your applications and information are in a cloud environment.

Ensure you understand where your duties lie regarding compliance, andwith which aspects of regulations the cloud service provider will enable you to comply. Verify that the provider's compliance certificates are valid and obtain guarantees of resource allocations such as headcount and budget to maintain these standards in the future.

Service dependencies and partnerships

Cloud service providers may have relationships with other providers to deliver their services. Evaluate these relationships and the levels of accreditation, technical capabilities, and staff certification of the underlying providers. Analyse dependencies involved in the provision of the cloud service and look for potential flaws or mismatches with the cloud service provider's claimed certifications. SaaS providers typically build their services on top of major IaaS providers, so it must be clear from where and how the service is being delivered, and if this fits with the organisation's own policies.

Reliability and performance

Analyse the performance of the service provider against their SLAs for the last 6-12 months and the cloud service provider's transparency with audit reports and control frameworks. Downtime is inevitable and every cloud service provider will experience it at some point; what matters is how the cloud service provider deals with any downtime. Ensure that the monitoring and reporting tools on offer are sufficient and can integrate into the organisation's overall management and reporting systems. Confirm that the selected cloud service provider has established, documented and proven processes for dealing with planned and unplanned downtime.

Evaluate the cloud service provider's remedies and liability limitations when service issues arise, as well as its disaster-recovery provisions and processes and its ability to support the organisation's data preservation expectations, including recovery time objectives (RTO). This should include at least criticality of data, data sources, scheduling, backup, restore, and integrity checks.

Integration with other systems, hybrid cloud capabilities

Consider how processes or data hosted in the cloud will integrate into your workflows now and in the future. For example, if your company has already invested heavily in a provider's ecosystem (e.g. Microsoft's Office 365), it may be a good idea to use cloud services from this same provider (in this case Microsoft Azure), since some of them grant licences and often free credits to their customers.

Integration between a private and public cloud enables banks to create efficient, coherent hybrid 0applications. This integration canbe facilitated by using the same stack in the public cloud as in the private data centre. OpenStack provides an open-source and open standards stack to build highly compatible applications with no lock-in and enables more customisation than branded stacks. Managed versions of OpenStack can be delivered by vendors such as Rackspace, RedHat, IBM or Suse. SaaS solutions should provide APIs to connect applications to other data sources and interact with the bank's systems.

Contracts, commercials and SLAs

Cloud agreements can appear complex, SLA definitions in particular. Cloud service providers often use complex terms and conditions that make it difficult to compare the service levels of different providers. It is important to understand the level of service promised by each cloud service provider and perform market research to compare offerings and get the best value for money.

Business alignment

Ensure that the chosen cloud service provider understands the business of the organisation and the precise objectives it is seeking to achieve with the cloud. The focus should be on high-level business value such as streamlining product delivery or reducing time to value, rather than low-level, technical indicators such as server up-time or database throughput.

Organisations within a vertical industry such as banking should make sure that the cloud service provider understands the industry; in certain cases, this can mean choosing a smaller specialised player like Rackspace over a hyperscale provider in order to leverage industry-specific tools.

Managed Service Providers (MSPs) deliver managed cloud services and act as a broker between the end-user and an IaaS or PaaS provider. MSPs provide an additional layer of management to handle contracting, financial management, security, and compliance, and can also deliver industry-specific capabilities.

Vendor lock-in and exit planning

Lock-in is a risk not just because of the costs, but also because a bank must be able to change and adapt to new regulations and requirements. Being able to move workload on-premises (Hybrid Cloud) or using open standards helps to ensure continuity of the service. Vendor lock-in usually stems from proprietary technologies that do not integrate with those of competitors, or from inefficient processes or contract constraints. The portability of applications may be impacted if they heavily rely on unique proprietary components. Ideally an organisation should choose value-added services that have competitive similar alternatives, monitor the availability of those services in the market to spot risks of lock-in early enough, and plan an exit strategy at the start of its relationship with a chosen cloud service provider.

Business health, continuity and company profile

While the assessment of the technical and operational capabilities of a potential supplier is obviously important, you must also take time to consider the financial health and profile of your shortlisted providers.

If a cloud service provider gets into trouble, it may not have enough financial resources to meet its obligations or refund losses; to this end, a business continuity plan in case of a default of the cloud service provider including notification period, data migration support and intellectual property must be carefully prepared.

Technologies and service roadmap

Understand where the cloud service provider is heading over the next four years and make sure it aligns with the organisation's cloud and business objectives. Does the provider plan changes that would involve re-coding applications? Will there be a change in its certifications or security standards? Assess the impacts on workloads and take them into consideration when building the case for cloud.

Conclusion

Cloud provides transformative opportunities for organisations and is a vital competitive component in today's challenging marketplace. Cloud is not an easy technology to adopt, but the potential benefits and opportunities outweigh the challenges and risks associated with cloud transformation.

To maximise cloud's added value, an organisation should follow a structured approach, starting with the definition of a clear strategy (and involving a wide range of stakeholders), clarity of vision and expectations, knowledge of options, understanding of business drivers (both opportunities and risks), proper planning, disciplined execution and ongoing governance and management.

This report has set out the steps an organisation should consider in order to get things right and become a best-in-class cloud-first company that thrives in today's competitive market.

Contacts

Stéphane Hurtaud
Partner, Information & Technology Risk
+352 45145 4434
shurtaud@deloitte.lu

Patrick Laurent
Partner, Technology & Innovation Leader
+352 45145 4170
palaurent@deloitte.lu

Authors

Beat Burtscher
Director, Digital Solutions
Tel: +41 58 279 64 65
Email: bburtscher@deloitte.ch

Alexander Norring
Senior Consultant, Risk Analytics
Tel: +41 78 740 35 36
Email: anorring@deloitte.ch

Pavlo Riabchuk
Manager, Cyber Risk Services
Tel: +41 79 521 85 90
Email: priabchuk@deloitte.ch

Guillaume Beaud
Consultant, Cloud Engineering
Tel: +41 77 435 47 26
Email: gbeaud@deloitte.ch

References

1. Deloitte, "RegTech Universe," Deloitte, [Online]. Available: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html. [Accessed April 2019].
2. Microsoft, "Societe Generale's complex financial simulation platform expands on Azure Service Fabric architecture," Microsoft, [Online]. Available: https://customers.microsoft.com/en-us/story/societe-generale-complex-financial-simulation-platform-expands-on-azure-service-fabric-architecture. [Accessed April 2019].
3. Deloitte, "Maintain control in the cloud," 2018.
4. Deloitte, "The value of online banking channels in a mobile-centric world," Deloitte Insights, 2018.
5. Amazon Web Services, "Capital One on AWS", Amazon Web Services, 2019. [Online]. Available: [https://aws.amazon.com/solutions/case-studies/innovators/capital-one/. [Accessed February 2019].
6. IBM, "Citigroup transforms application development with an IBM cloud solution," IBM, 2011.
7. Avaloq, "Avaloq onboards Deutsche Bank Luxembourg," Avaloq, May 2018. [Online]. Available: https://www.avaloq.com/en/news/-/asset_publisher/vCbePfJNFpkG/content/avaloq-onboards-deutsche-bank-luxembourg. [Accessed February 2019].
8. Cloudera, "From the early planning stage to final deployment and beyond," Cloudera, [Online]. Available: https://www.cloudera.com/about/customers.html#. [Accessed February 2019].
9. Salesforce.com, "See how Barclays simplifies mortgage applications for thousands of brokers and customers.," [Online]. Available: https://www.salesforce.com/customer-success-stories/barclays/. [Accessed February 2019].
10. Deloitte, "Maintain control in the cloud," 2018.
11. Google, "BNP Paribas Fortis: Aligning marketing teams and resources to improve productivity," Google, [Online]. Available: https://cloud.google.com/customers/bnp-paribas-fortis/. [Accessed February 2019].
12. Oracle, "Top Oracle partners are building successful ERP cloud businesses. Here's how.," Oracle, 2016. [Online]. Available: https://blogs.oracle.com/profit/cloud-confident. [Accessed February 2019].
13. Deloitte, "Secure and Private Computing for Banks on a Cloud Platform," 2015.
14. Gartner, "Is the Cloud Secure?," 2018.
15. Gartner, "Security of the Cloud Primer for 2019," Gartner, 2019.

Deloitte.