4 JUNE 2020

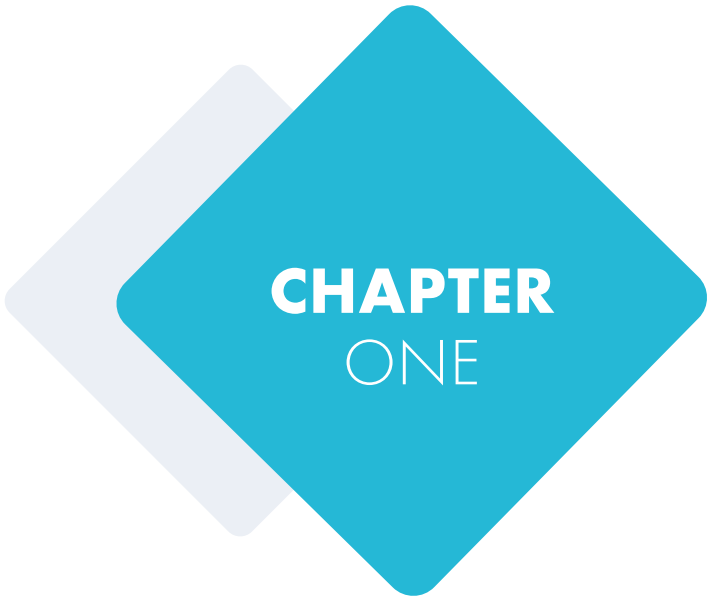
The use of Cloud Computing by Financial Institutions

TECHNICAL PAPER

CONTENTS

ABBREVIATIONS

AD	Active directory
ADFS	Active Directory Federation Services
AI	Artificial intelligence
BARE METAL	Base IT infrastructure enabling cloud computing
CAPEX	Capital Expenditure
COBIT	Control Objectives for Information and Related Technologies (by the Systems Audit and Control Association)
CSC	Cloud Service Customer
CSP	Cloud Service Provider
FI	Financial Institution
GDPR	General Data Protection Regulation
IoT	Internet of things
ITIL	Set of detailed practices for IT service management (formerly Information Technology Infrastructure Library)
ML	Machine learning
NCA	National Competent Authority
OPEX	Operational Expenditure
SDLC	Solution Delivery Lifecycle
SLA	Service Level Agreements
VSI	Virtual Server Infrastructure



1 Introduction

Over the recent years, cloud computing has become a significant technological enabler for innovative service development. Cloud allows industries to tap into new service models, utilising its technological advancement for new and better services to customers, improving productivity, cost-efficiency and flexibility of internal business processes. Ultimately, cloud computing can provide a foundation for the digital transformation of the industry in question.

The financial sector is in the process of adopting cloud computing to take advantage of the aforementioned benefits. New opportunities for service delivery to customers, serving their needs and expectations, are as relevant as improving security, reducing costs and improving flexibility in the conduct of business. Cloud can also open new markets and enable mature financial services institutions to find new ways of competing with FinTech market entrants.

The cloud security framework matured fast and heavily. Nowadays, cloud computing seems to be as well-placed as (if not better than) other traditional IT paradigms when it comes to safeguarding integrity and availability. Cloud services embody redundancy, high availability and resiliency thanks to their distributed nature. Public cloud gives the ability to scale at a more significant level than financial institutions would be able to achieve on their own. Resilience, speed and security are the building blocks of cloud offerings and the core business of any Cloud Service Provider (CSPs). In most cases, CSPs have stronger security than most individual companies can maintain and manage on-site. Moreover, the big cloud providers have large teams of security engineers and, given that cloud is (one of) their core businesses, they are continuously investing in meeting the strictest and newest security standards that constantly adapt to managing evolving threat vectors and threat actors.

However, cloud adoption by the financial industry has to consider the highly regulated nature of the sector and pay special attention to stability and safety. European banks operate within a framework of financial rules aimed at ensuring proper governance and control of risks (internal governance guidelines), especially in those situations where third parties are involved in the operation of ICT systems[1]. These rules set

[1] EBA Guidelines on ICT and security risk management (under development): https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

the framework for supervisory engagement with European banks throughout the entire life of the cloud relationship in the EU's financial sector. Mindful of possible risks triggered by cloud technology, thorough assessments are conducted on the potential impact of cloud on financial institutions' operational risk, to be assessed against the operational risk posture of the current IT environment. Hence, understanding of the technology and its implications for operational processes is critical.

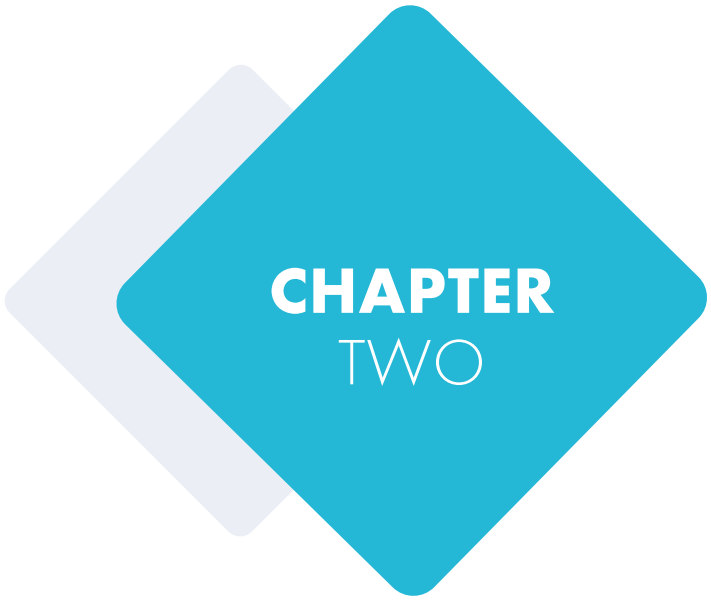
This paper aims to support financial institutions and competent authorities' understanding of the advantages and particularities of cloud computing in areas such as security, risk mitigation and regulatory compliance.

Significant features of cloud technology in financial services require special attention and consideration. Looking at the fast-evolving cloud service environment as well as the close interaction of European banks with their supervisors in different Member States, a harmonised approach to the considerations presented by national competent authorities (NCAs) will be essential. Cloud computing's potential for agility and flexibility goes beyond the framework of a single jurisdiction. A fragmented understanding of cloud by NCAs regarding key considerations can severely hamper the systematic approach of European banks to cloud, whether they rely on one or multiple providers in a multi-cloud environment. By contrast, a harmonious understanding of cloud across European borders will foster the adoption of public/hybrid cloud and multi- cloud use by European banks in a more unified way.

Ultimately, banks would be able to provide more innovative services to their customers across Europe, allowing FIs to focus on their core businesses, while leveraging the specialty of CSPs to provide secure, scalable, reliable, and fast networks and computing.

This paper aims to support the necessary understanding of cloud use by financial institutions. Mindful of the complexity of both the technology itself and banks careful implementation of it within their business processes, not all relevant aspects of cloud can be addressed comprehensively in this single document. Instead, additional technical papers of the EBF Cloud Banking Forum will target, at a later stage, specific issues of relevance. This is the reason why issues such as cybersecurity, though highly important for the adoption of cloud technology across all industry sectors, will not be developed in detail in the following chapters.

> "Cloud solutions offer banks the flexibility to tailor the scaling up of capacity to meet their activity levels"



2 Overview of cloud services

In order to gain a deeper understanding of the advantages and specifics of cloud computing, it is necessary first to take a look at existing cloud compositions and service models.

2.1 Cloud composition

Cloud computing deployment can be distinguished according to three categories:

Public Cloud is a cloud computing environment where cloud solutions are located outside the bank's perimeter. Therefore, within a public cloud setup, not all controls will be operated by the institution itself. This does not change accountability of Cloud Service Customers (CSCs) according to the applicable legal framework. Logical access control functions are provided to the company using publicly hosted cloud services (e.g. through authentication mechanisms), any other company can subscribe to the same services, available over the internet.

Private cloud solutions are located inside the banks' own perimeter and therefore leverage all the established controls of the respective bank. Computing resources are used solely by the one single organisation, either physically in the company's on-site data centre(s) ("on-premises") or externally with the third-party provider ("hosted private cloud").

A hybrid cloud solution is an integrated cloud service, using both private and public clouds to perform distinct functions within the same organisation. Hybrid cloud adoption reflects a macro trend common to all financial institutions and is viewed as a key enabler for next generation technologies, free movement of data and integration into the ecosystem.

Hybrid Cloud for the purpose of this paper is defined as a cloud computing environment that uses a combination of private cloud (where most financial institutions started their cloud journey) and public cloud services that may include third party service offerings such as Platform as a Service (Paas), Infrastructure as a Service (IaaS) and SaaS (Software as a Service). These platforms are connected through automation and orchestration tools.

2.2 Different cloud service models

Cloud services know multiple facets of service design, each with effects on the role of CSP and CSCs. It is important to recognise that cloud's potential is not limited to the simple external data storage, but rather consists of fast-developing service models which will further evolve in the future.

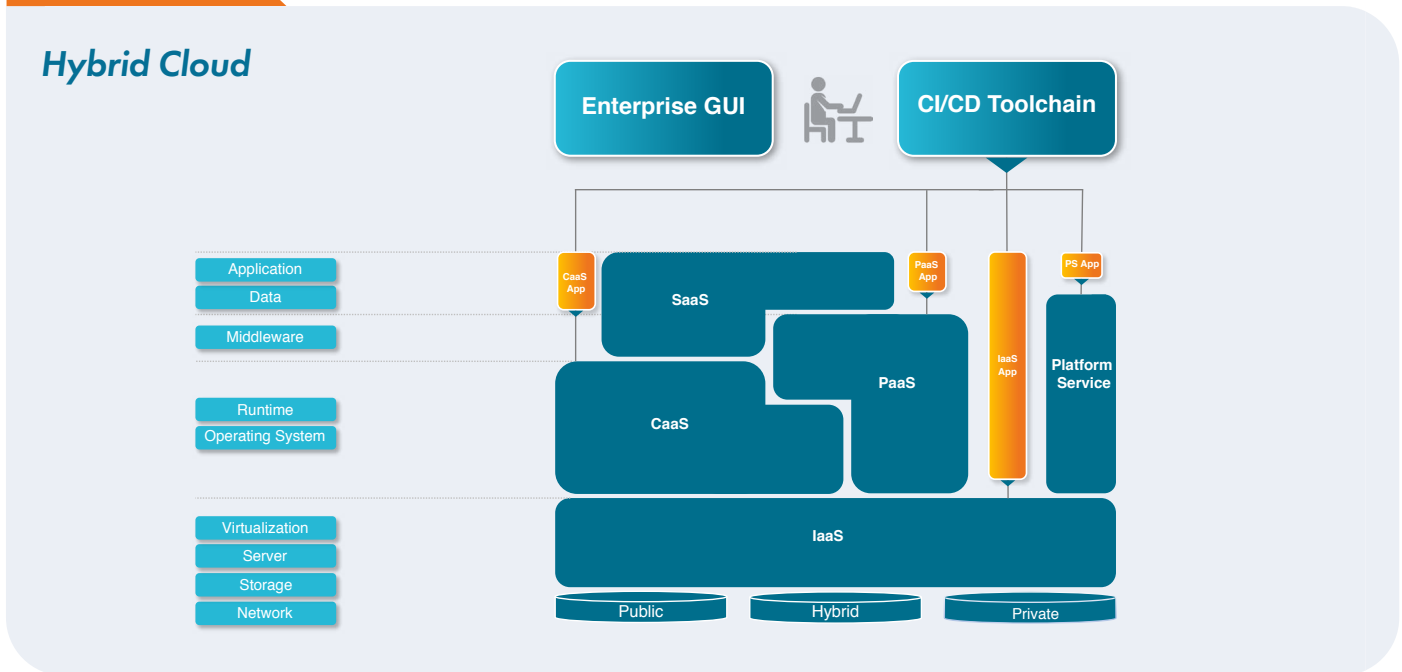
When looking at these cloud solutions – especially from a risk-based approach – distinctions must be made between different models, triggered by technological differences.

TABLE 1

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Container as a Service (CaaS)	Software as a Service (SaaS)
Supplies customers with IT infrastructure, provided and managed over the internet on a pay-as-you-use basis, e.g. servers and storage. The two common models of delivery for IaaS are 'bare metal' and Virtual Server Infrastructure (VSI). In the case of bare metal the financial institution or their designee manages the servers, storage, virtualisation, OS, middleware, runtime, data and applications. In the VSI model the financial institution manages the OS, middleware, runtime, data and applications.	*Supplies customers with an on-demand environment for developing, testing, delivering and managing software applications over the internet. The financial institution manages its data and applications.*	*Offering for container-based virtualisation in which CSPs offer a complete framework to customers for deploying and managing containers, applications and clusters. CaaS offers a completely enabled container deployment service with security and governance control for IT management.*	*Allows customers to connect to and use cloud-based application over the internet on a subscription basis e.g. an online collaboration tool. The entire stack is managed by the service provider.*

Within the CSP market, many engagement models deploy these services to market, for example captive models, fixed-term contracts, open models, pay per use. Considering these different cloud service models, please take note of the following overview for IT functions in a hybrid cloud environment (example).

FIGURE 2



2.3 Industry experience with cloud

Today, the use of cloud – though innovative and constantly evolving at a technological level – is generally known to European enterprises. SaaS models have been adopted over the recent years, familiarising enterprises with subscriptions to software hosted at CSP facilities.

According to Eurostat, cloud computing usage by EU enterprises grew rapidly over the last few years. While in 2014 it still stood at 19%, in 2016 the number increased to 21%[2]. In 2018, 26% of EU enterprises with at least 10 persons employed purchased cloud computing services[3].

FIGURE 3

Use of cloud computing services and high level dependence on the cloud, 2018 (% of enterprises)

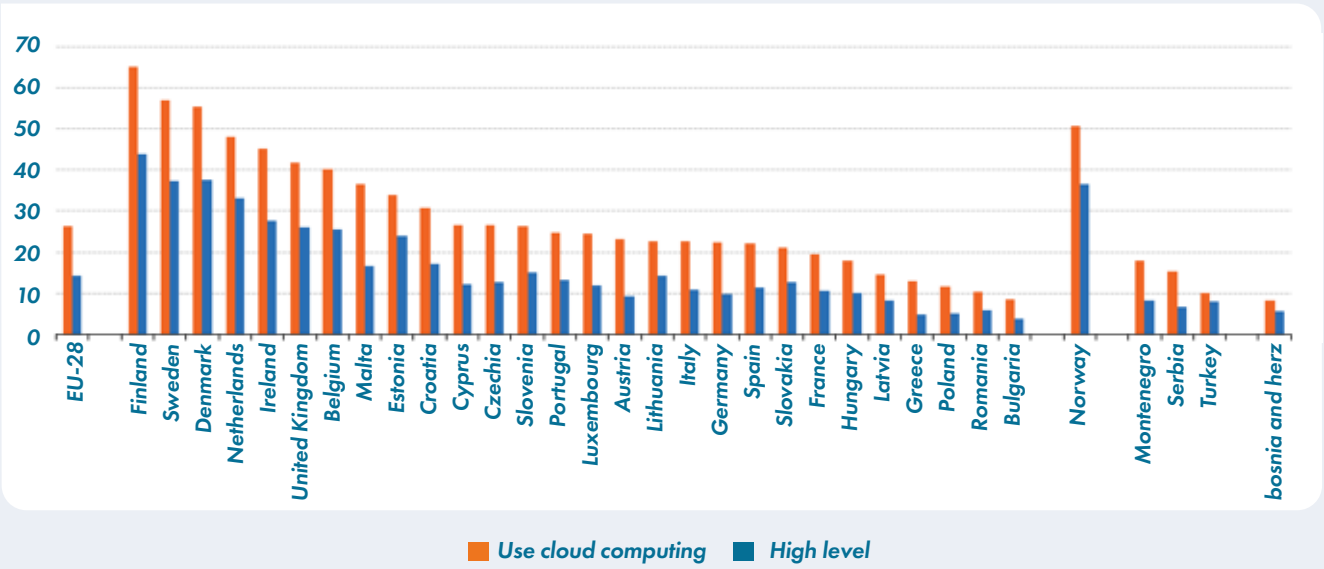
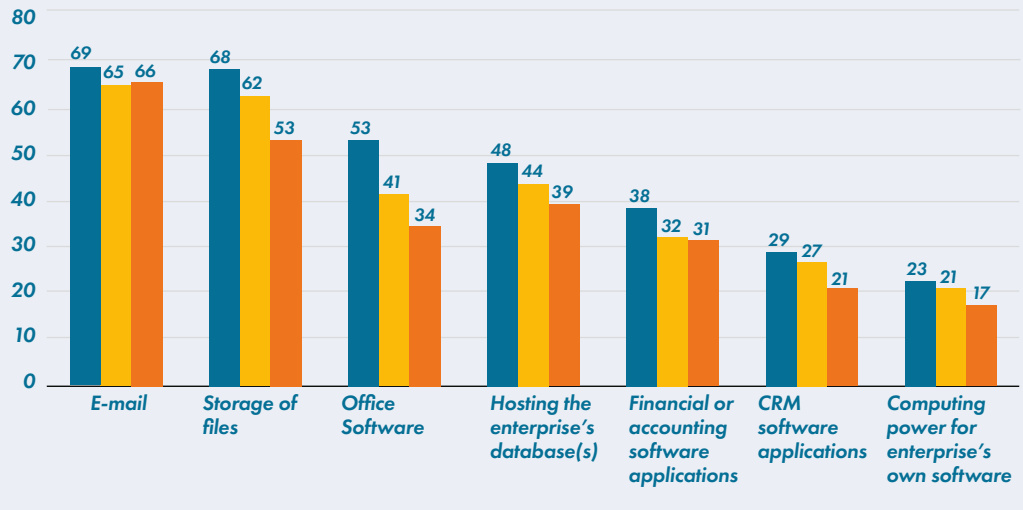


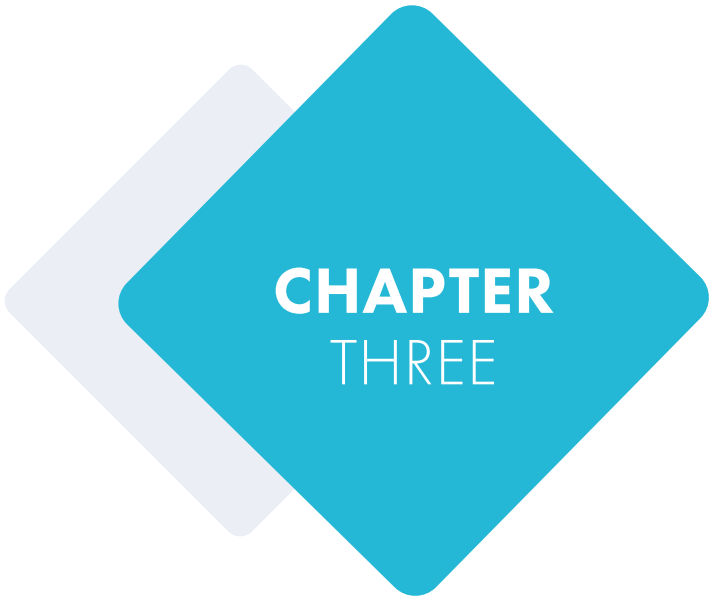
FIGURE 4

Use of cloud computing services in enterprises, by purpose, 2014, 2016 and 2018 (% of enterprises using the cloud)



Source: Eurostat (online data code: isoc_cicce_use)

[2]Eurostat, https://ec.europa.eu/eurostat/documents/2995521/9447642/9-13122018-BP-EN.pdf/731844ac-86ad-4095-b188-e03f9f713235.
[3] Ibid.



3 Why European banks use cloud services

Banks require intensive use of technology for operation. Traditionally this has been solved by on-premises systems, deployed locally on the company's own computer infrastructure. However, the progress of technology has accelerated dramatically, requiring banks to embrace this development in the financial market. They do so consciously and strategically.

Cloud has become a key technology to develop new financial services and to innovate, to collaborate with third parties and to compete in the digital context. The market dictates the speed of change. Flexibility and time to market are imperative for banks and cloud computing is the technology with the greatest potential to meet both needs. Banks need cloud technology to compete with other non-regulated players entering the marketplace on a level playing field. Innovative, fast-evolving cloud technologies allow banks to take advantage of the best-suited technology for customers and business processes at each moment. Nowadays customers demand immediacy and personalisation. This can require banks to rely on third parties that provide new – sometimes tailor-made – general-purpose services. Cloud also creates opportunities for increasing specialisation. Banks can dedicate their top talent to business problems while leveraging CSPs for non-core capabilities like management of infrastructure.

Recent mergers and acquisitions in the market reflect strategic considerations of market players in terms of promising IT tools for future business operation. Market developments show that the majority of IT tools needed to serve customers' needs will run 'cloud first strategies' in the future. Consequently, slowing down a financial institution's path to cloud adoption might limit the institution's competitiveness compared to FinTechs and Big Techs in particular. Today, banks face an overall trend in the IT industry, that can be expected to further increase over time.

A driver for this trend is the opportunity to use cloud for access to transformational technologies. This possibility complements the general benefit of cloud to access vast and increasing volumes of data in a cloud-ecosystem. Transformation technologies are fundamentally and rapidly changing the way we think about business today. They are driving a shift of investment from legacy technology and

business strategy to investment in more innovative business models, supported by the new innovative technologies, and they are essential to undertakings to remain competitive, viable and potentially more secure. For example, Distributed Ledger Technology promises to transform the speed, efficiency and trust of transaction processing. Analytics and "Big Data" technologies promise to provide many benefits, including advanced insights into complex data sets, driving new business opportunities, reducing fraud and significantly improving cyber security intelligence. Likewise, AI enables increasingly complex interactions between entities, e.g. helping end users with problem solving. These transformation technologies may be rapidly integrated into businesses as part of increasingly complex and dynamic ecosystems, which are often more transparent and resilient than their legacy counterparts. They support increased connectivity demands from clients and stakeholders who increasingly expect rapid access to data and services.

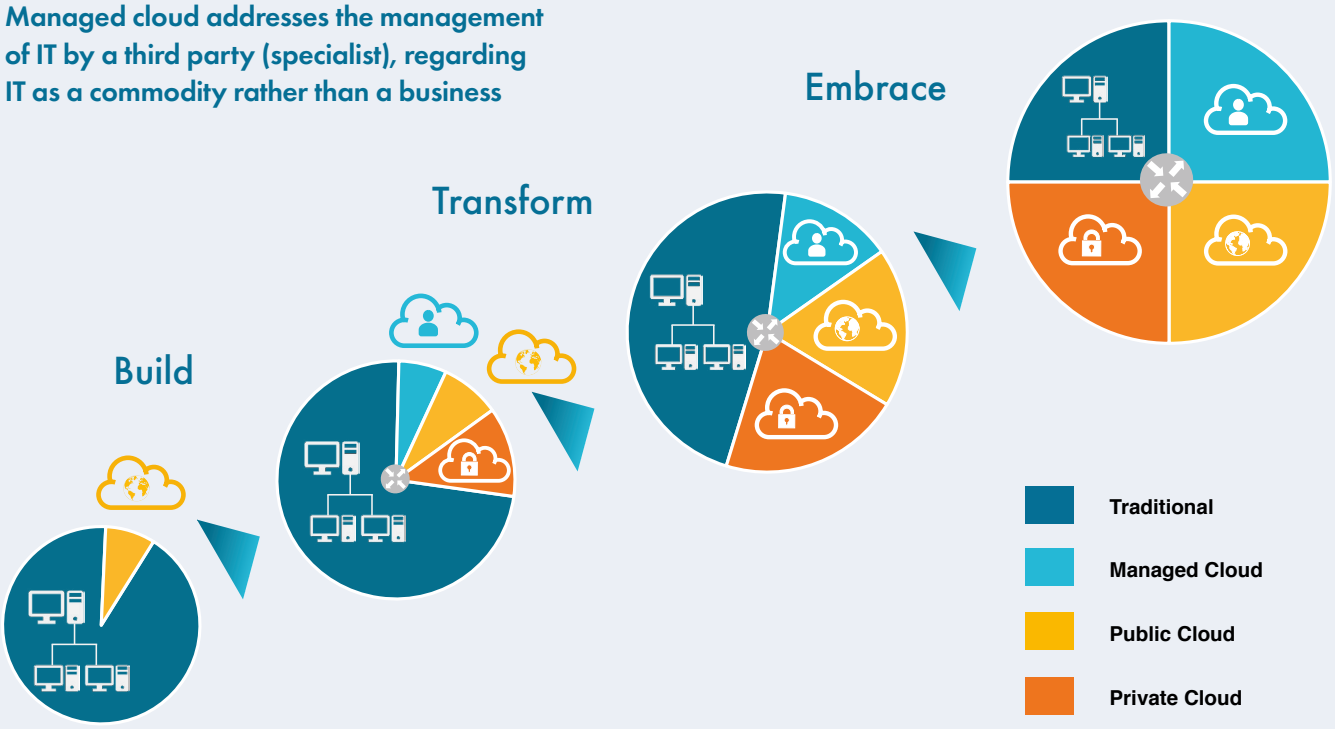
These cloud business relationships and operational cooperation with CSPs help to introduce innovative service solutions, providing hitherto unknown potential for banks' business processes.

One of the big challenges in banking IT is to deal with peaks in computing demand. They may be caused by the typical day cycle (day trading, night processing) or by extraordinary events (e.g. major financial market news, price changes, marketing events). Banks dedicate themselves to the provisions of stable, reliable and trusted services for their customers. Financial stability is a prerogative.

The migration from on-premises IT solutions to cloud is a conscious and careful journey for banks. It starts from and evolves the existing IT structures and services of banks. Gradually, private cloud solutions can be built, transformed into cloud model combinations and finally embraced in a diverse environment. This journey is not a disruption, but an evolution:

FIGURE 5

Managed cloud addresses the management of IT by a third party (specialist), regarding IT as a commodity rather than a business



Cloud adoption by European banks along this journey is being driven by several factors: the need for increased agility/flexibility, reduced infrastructure, more transparent cost and security improvements.

TABLE 6

	Traditional IT on-premises	Cloud-based IT
Flexibility	*Very limited – flexible to grow, but costly and slower*	*Very large*
Time to market	*Long*	*Almost instantaneous*
Cost management	*Not possible once the investment is done*	*Dynamic, allowing for forecasting*
Impact on Capital ratio	*High*	*Like any other profit & losses expense*
Security	*Solutions for existing services, based on inhouse-resources and external support*	*Dedicated CSP cloud security offerings as part of their core business. Allows for in-built service security solutions and dynamic large-scale inclusion of leading tech (e.g. artificial intelligence).*

Looking at IT capabilities, and guaranteeing stable operations of the financial system require spare capacity to be available in case of need. Having this capacity available in the banks' inherited model creates a significant cost footprint and necessity to maintain infrastructure that may (only) be needed on rare but significant occasions. Cloud computing provides for an excellent technical solution to computing demand peaks. It allows service providers to make resources available via an accessible network where multiple clients can share the same resources.

Clearly, this requires security considerations. A major concern from a risk and compliance perspective is the network perimeter. CSPs can offer advanced capabilities to individual financial institutions in this area, considering their focus of business and experience in the market.

An example of improved agility can be the move of selected front-end systems, such as broker-dealer systems, by some financial institutions into the cloud. This allows them to scale up a moment's notice, while interfacing, either to their own trusted in-house back-end system or to innovative cloud-based services, e.g. using distributed ledger technology such as trade settlement and accounting. In addition, non-core banking functions such as Human Resources and customer relationship management could leverage state of the art cloud service offerings.

In a rapidly changing environment, leaner operating models and a focus on business value are crucial for financial institutions to succeed. Cloud services are not only a technological trend which providing ICT solutions with a never-seen-before agility/flexibility. They can also have a

significant and positive impact on the financial institutions balance sheets. Traditional on-premises IT infrastructure and developments require an upfront Capital Expenditure (CAPEX), incurred by a business to create future benefits such as the acquisition of assets, which, necessarily, have to be designed according to the maximum workload. The system will not be available until the end of the project, and usually requires large payments in advance. In contrast, cloud-based technology allows financial institutions to add new resources or remove them instantly, as required.

This allows IT resources to scale up and down according to the business' needs and facilitates flexibility by a pay-per-use model. Therefore, IT operations can move from CAPEX to Operational Expenditure (OPEX), incurred for the day to day functioning of a business. CAPEX and OPEX are treated very differently for tax and accounting purposes. OPEX allows a formerly fixed cost to be transformed into a variable state. This helps to improve competitiveness, to increase reaction times of institutions to relevant developments and to focus on use case implementation more effectively. Ultimately, it creates business value.

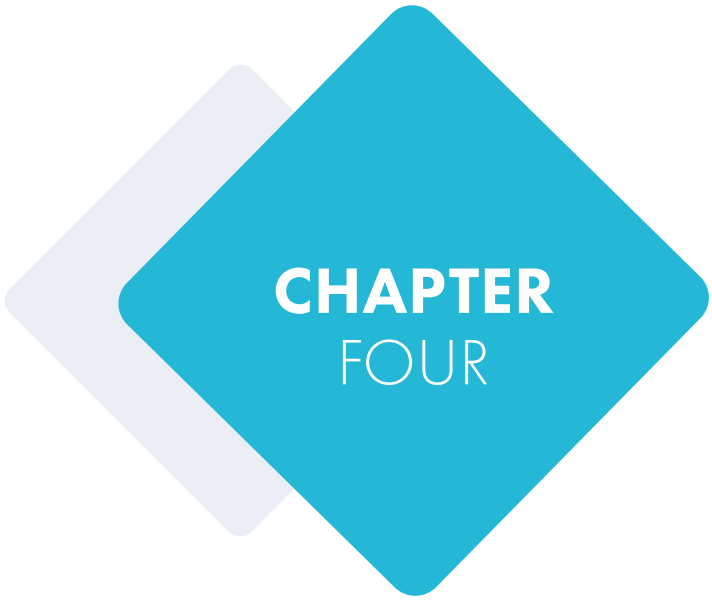
More specifically, this 'CAPEX to OPEX' transformation provides an added value to financial institutions in terms of capital ratio. Today, the current prudential treatment of software discourages the investment that financial institutions make in software assets due to the obligation to deduct them fully from Common Equity Tier 1 capital[4]. There is a need to raise additional CET1 funds to offset deductions. Using cloud services provided by CSPs can ease this tension, leading thereby to a reduction of required capital when deploying new services.

TABLE 7

Traditional approach to financial services	The target state for financial services
On-premises and community[5] ***Supports banks' need to:***	**Hybrid Cloud** ***Supports new generation of banking services:***
seamlessly connect with people, organisations, systems and processes across the globe. ***rapidly process, and reliably and safely store and retrieve large and variable volumes of data.*** ***adapt to the changing needs of clients through offering trusted, high quality and competitive services.*** ***share common innovative technologies with other financial services to customers and to create new markets.***	***emerging ecosystems for financial services.*** ***reduced time to market, increased agility and scalability by enabling more rapid adjustment of IT services to support business operations.*** ***conversion of fixed-asset product-based overheads to variable service-based assets (CAPEX to OPEX).*** ***"Immersion" of banking services into client systems becomes more feasible, clients can get the business services they need on demand triggered by the ability to simultaneously use common "services".***

[4] Amendments introduced in the final text of the CRD/ CRR Review (published 7 June) allows to exempt certain investments in software assets from this deduction. However, this exemption only applies to those software assets that meet certain conditions (as specified by the EBA in regulatory technical standards to be developed) and only applies two years after the entry into force of the Regulation, see Article 36 (1) (b), Article 36 (4).

[5] See "The NIST Definition of Cloud Computing", Special Publication 800-145, Sep 2011: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf



4 Understanding of cloud computing

The views of cloud computing by regulators, technologists and service users are different. Although not conflicting, they need to be balanced to enable the most effective use of cloud technology in financial services.

To attain a higher level of maturity, a mutual understanding and agreement needs to be fostered through coordination and communication between regulators, technologists and service users. The specifics of cloud technology and its control demand need to be understood and reflected upon carefully.

> “All cloud computing risks need to be evaluated prior to any planned cloud migration”

Four important basics regarding data ownership and management shall be postulated upfront, unaffected by raising cloud adaption:

ONE
Banks continue to own their data.

TWO
Banks will choose the geographic location(s) in which to manage their data.

THREE
Banks can download or delete their data whenever they need to.

FOUR
Banks should consider the sensitivity of their data and decide how to protect it or make it available, i.e. by using suitable cryptographic services for encryption and authentication.

Based on these statements, this paper aims to present different cloud service models, elaborate on the necessary risk-based approach, help the categorisation of the control demands in a cloud environment, show the banks’ respective awareness and highlight their careful migration to cloud.

4.1 Cloud-specific considerations under a risk-based approach

As required by the applicable regulation, both banks and NCAs assess the cloud computing adoption – regarding a specific use case – with a risk-based approach.

However, this makes a common understanding of cloud computing risks and available controls fundamental. As any transformation of complex services may suggest, the journey to a well-controlled cloud adoption requires careful assessment and mitigation of potential risks.

A common understanding enables:

- a common "language" or framework for understanding, assessing and communicating relevant and beneficial cloud computing principles and control objectives.
- a consistent means to prioritise the most significant risk management activities related to cloud adoption and use.
- a unified position between the EBA/NCAs and banks, to send clear signals to cloud service providers and technology innovators about specific financial services requirements.

Key risk areas for cloud computing must be understood in the context of cloud computing's technological features and service design. Operational risks relate both to the adoption of cloud computing and to the operation of cloud services. As in any other service relationship, all cloud computing risks need to be evaluated prior to any planned cloud migration, and managed, when performing operations in the cloud. Therefore, the already existing IT control processes of banks, based on standards such as COBIT or ITIL, need to be reviewed in light of cloud specifics.

Factors that must be taken into consideration are:

- the cloud service models (e.g. SaaS, PaaS and IaaS), aligned to traditional computing control areas, where the level of risk relates to the cloud service model selected. In these models, risk management and the operation of IT activities are shared between cloud service providers and cloud service customers. The "balance" of responsibility for IT control management shifts from cloud service provider to service user as we move from the top of the stack, e.g. SaaS, to the bottom of the stack, e.g. IaaS.
- The cloud deployment model (e.g. internal, public, and hybrid), where routine accountability remains primarily with CSCs who selected the model for their business, and where their data subject needs to be supportive and informed about data management, data location and network management.
- The specific characteristics of cloud computing (e.g. self-service, accessibility across networks, resource pooling, rapid elasticity, metered services), where governance controls are necessary to provide timely management information and escalation/response in case defined thresholds are breached.

4.2 Categorising the associated control demand of a cloud offering

The risk of the different cloud service models needs to be identified, assessed and managed by banks. This requires understanding of how risk in cloud services can be distinguished and rated, creating the respective control demand.

European banks are well aware of the attention that such control demand deserves. Operational and financial stability are core concerns prior and during the usage of cloud services. Consequently, the selection of services and their migration to cloud are conducted consciously.

Cloud operates on the shared 'responsibility' model. This means that depending on how the financial institution is consuming cloud both the CSP and financial institution must understand their areas of responsibility with regard to the control landscape.

This is not to be misunderstood for the concept of accountability. Accountability remains fixed with the financial institution regardless of what services are being obtained from the cloud. 'Responsibility' for the purpose of this paper should be understood as a term allowing for clear definitions of who is operating specific controls (the CSP or financial institution) and what level of visibility the financial institution has into how those controls work. There are several ways this can be accomplished by having a well-defined approach with the CSP.

Different from other IT paradigms, cloud computing inherits technological dimensions and features that can have a positive effect on the control demand.

In order to be fully aware of the evolving service characteristics, five major dimensions need to be considered regarding the control demand of a particular cloud offering.

The layer of abstraction sourced, e.g. the selected cloud service model and use case. In general, in IaaS the CSC is using an IT infrastructure deployed and managed by the CSP, but all processes and activities implemented on this infrastructure remain under the full control of the institution (e.g. workload distribution, Solution Delivery Lifecycle, application changes).

Going up the stack, the implication of the partner in the activity will increase. Using PaaS, workload distribution will be controlled by the partner. With SaaS, the application management, including changes (content and timing) will not be handled by the institution anymore. However, not all services are equal, and, for instance, there are IaaS services like Grid IaaS where some additional components will be managed by the CSP, while in other SaaS implementation processes, such as the identity and access control, these can remain under control of the CSC. Ultimately, a specific control assessment will be needed for each cloud service. It is important to note that IT general controls remain relevant regardless of where they are operated.

Ownership of the control framework
The framework includes relevant network perimeter control, access management and internal enforcement of rules. Using a visual: the network perimeter can be compared to a city wall. The wall itself and everything inside follows internal rules. Access is granted at the gate under control of the "city council". This means for cloud solutions, that in a bank's private cloud the network perimeter control and access management are still with the institution, whereas in a public cloud this control leverages the features implemented and offered by the bank's partner (the CSP) outside the "city wall".

The legal and regulatory context
Depending on the jurisdiction applying to the cloud service contract, the activity supported by the cloud usage or the location of the data/compute, different levels of data access and control may be needed. Laws and regulations may specify requirements for regulatory notification and approval for the use of cloud computing for regulated activities and reporting of material incidents.

Criticality of data

Different categories of data can be drawn, according to their sensibility and the data subject. Thus, customer's sensitive personal data requires higher protection than public data used for intra-day risk computing.

Criticality of function

This dimension outlines how dependent the day to day operation is on the function sourced through a cloud service. The criticality is effected by the impact of the function when not performed properly. For example, while an institution's business processes could run without an HR system for a short period of time, this is not true for the core banking system, which would bring the institution to halt when failing.

To provide for a better visualisation of the risk dimensions, please consider the following rating grid. Each dimension is assigned a numerical value according to the described features:

TABLE 8

Dimension/ rating	1	2	3	4	5
Layer	*IaaS Based on market standards*	*IaaS plus Vendor specific additions*	*PaaS Based on market standards*	*PaaS with vendor specific additions*	*SaaS*
Control framework	*Private setup*	*Hybrid, within network perimeter all accesses are controlled by institution*	*Hybrid, within network perimeter accesses are partially controlled*	*Hybrid, with partial public setup outside of network perimeter control*	*Public setup*
Legal and regulatory context	*Only an EU home country regulation applicable*	*Only EU country regulation applicable (but of more than one Member State)*	*Mainly EU regulation applicable but also "recognised" third countries regulation involved*	*Mainly non-EU regulation applicable but from "recognised" third countries*	*Regulation of "non-recognised" third countries applicable*
Criticality of data	*Public data*	*Internal "low-relevance" non-identifiable data*	*Internal relevant non-identifiable data*	*Internal relevant identifiable data*	*Internal relevant identifiable sensitive data*
Criticality of function	*Replaceable and not relevant part of core processes*	*Replaceable but necessary for internal processes*	*Necessary for external processing*	*Part of core process, necessary for full function, recovery target in disaster recovery up to 48h*	*Unavoidable part of core process*

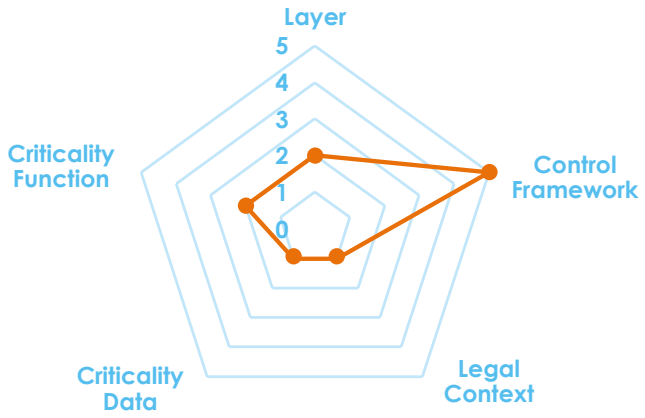
European banks consider these control dimensions carefully for the identification of cloud-related risks and their management. Weighing the dimensions' interactions and connecting its numerical value, the following spider chart shall give an indication on how to support awareness visually and how to guide attention within the risk assessment by banks for individual cloud service constellations.

The higher the assigned number for each risk dimension, the more attention to control is likely to be required by the bank. Visualising the dimensions altogether, figure 9 allows for a graphical understanding of the need for attention to cloud-particularities (according to the growing size of the encircled area). It can be used to trigger respective risk management attention: the bigger the area, the more attention to control should be dedicated to the service from a risk management perspective.

To provide for an example, the spider chart below contains the intra-day risk computation for a trading operation[6]. This example case is:

- running on hardware which is hosted in the bank's home country (legal context),
- utilising vendor specific additions to an IaaS cloud service (layer).
- If the bank's workload exceeds certain thresholds beyond the on-site compute capacity, additional capacity in a public cloud will be leveraged (burst to public cloud). For the purpose of this example, the trading operation in question is considered low with regard to criticality of function, using non-critical data.
- However, the public cloud is not within the bank's network perimeter (control framework).

FIGURE 9



Layer	2
Control Framework	5
Legal Context	1
Criticality Data	1
Criticality Function	2

Once the control demand has been understood, a balanced approach can be applied. For example: In the given case in figure 9, data is considered non-sensitive and public (transaction execution on a regulated market). As a result, no advanced controls for data protection have to be added. The extent of necessary controls will be directly driven by the risk exposure. The ability of the institution to control the risk can be directly derived from the combination of the level control tool provided by the CSP and implemented by the bank – allowing a more accurate expression of the level of exposure due to cloud computing – and the exposure itself.

[6]For more examples, please consider the Annex.

4.3 Different roles of banks and Cloud Service Providers

The visual tools under 4.2 helps to understand and assess the potential impact of cloud adoption on the operational risk of institutions. Central to such assessment is an understanding of what controls are in place and what party is in charge of them. It is important to recognise that cloud computing offers a more nuanced controls landscape than traditional IT services. In turn, the responsibilities within this landscape require an understanding of how CSPs and financial institutions in their role as CSCs work together.

This in no way implies that financial institutions are not living up to the responsibilities placed upon them by financial regulation as the basis of continuous financial supervision. The accountability of banks remains unquestioned[7]. European banks take risk control and financial stability very seriously not only for reasons of regulatory compliance but to deliver the best service possible for their customers.

Nevertheless, cloud computing is shaping different roles for the parties involved. Traditionally, when third parties are involved in the provision of a service, customers specify to them their service demand, followed by the supplier building a solution to meet the customer's requirements. Afterwards, the supplier manages and operates the solution on behalf of the customer. In the case of cloud solutions, the CSC does not always fully delegate these functions to the CSP, but the business model is based on the CSP having product offerings that the customer can use on a consumption basis. The CSC itself is responsible for building and configuring his services in the cloud as he sees fit and the CSC remains responsible for the management and operation of the service.

Service hosting controls and service management controls are distinct from one another.

> "Cloud computing offers a more nuanced controls landscape than traditional IT services"

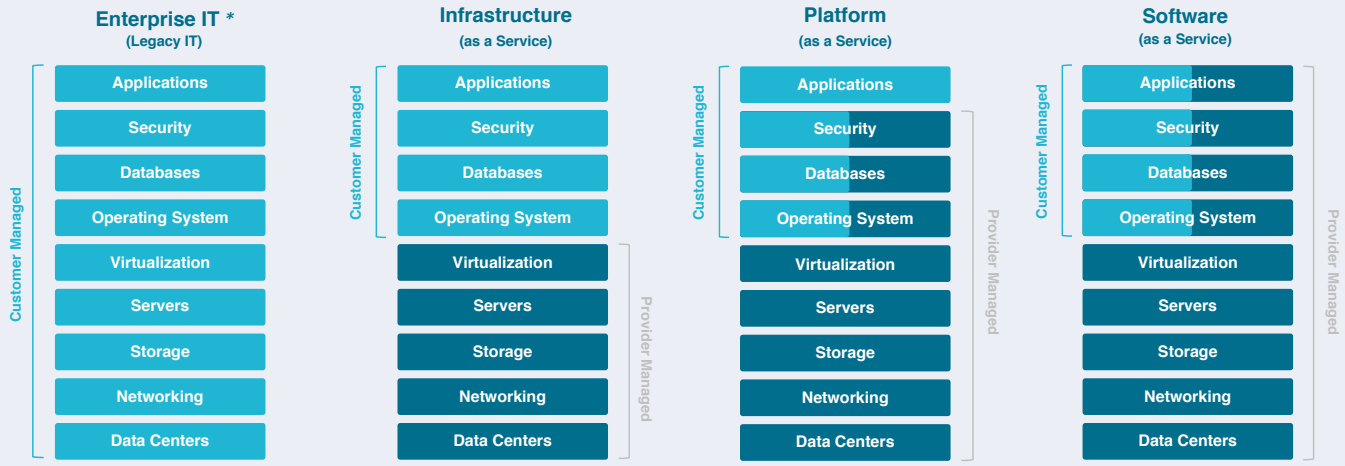
Where a CSP supports hosting, and a CSC supports the management of its computer controls, this needs to be viewed as a combined responsibility. Where both hosting and management are supported by the CSP alone, this is more akin to traditional outsourcing.

IaaS and PaaS cloud computing customers are building systems on top of cloud infrastructure. Although the CSC is always accountable and required to supervise and monitor any process affecting its activities, the "low level" security and compliance responsibilities are usually divided between the CSP and financial institutions as CSCs. The latter control how they create the architecture and secure their applications and data put on the infrastructure. The CSPs on the other hand are responsible for providing services in a highly secure and controlled environment as well as providing a wide array of additional security features. A generic compliance structure for CSPs facilitates the understanding of the control environment and risk mitigation implemented by the service, supporting a high level of transparency. The level of information provided by the CSP shall be sufficient to ensure the financial institution can make informed security decisions instead of decisions based on a notional perception of security.

[7] See above Chapter 4.2

Consequently, banks and CSPs operate with the help of a nuanced controls landscape, as indicated by this exemplary orientation:

FIGURE 10[8]

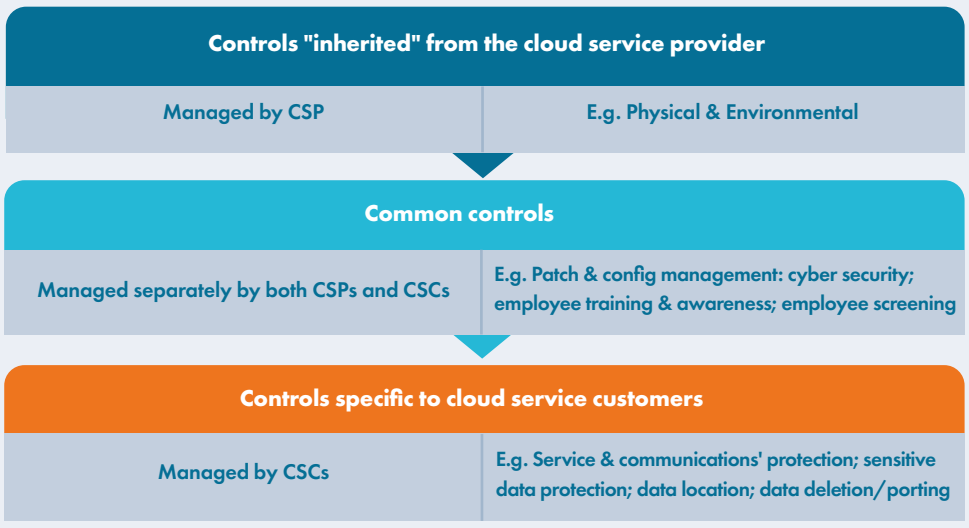


*If operated by the own entity

The technological nature of cloud, paired with distinct roles for both CSPs and CSCs, requires a close look at the division of controls for a cloud service in question. In order to reflect this evolving controls landscape in banking supervision, NCAs are invited to consider figure 10 carefully when assessing the management of relevant risks by banks according to applicable financial regulation. The cloud service models PaaS and SaaS show a visible difference to other IT paradigms.

To reflect the cooperative nature of the controls landscape, please consider the following controls origin:

FIGURE 11

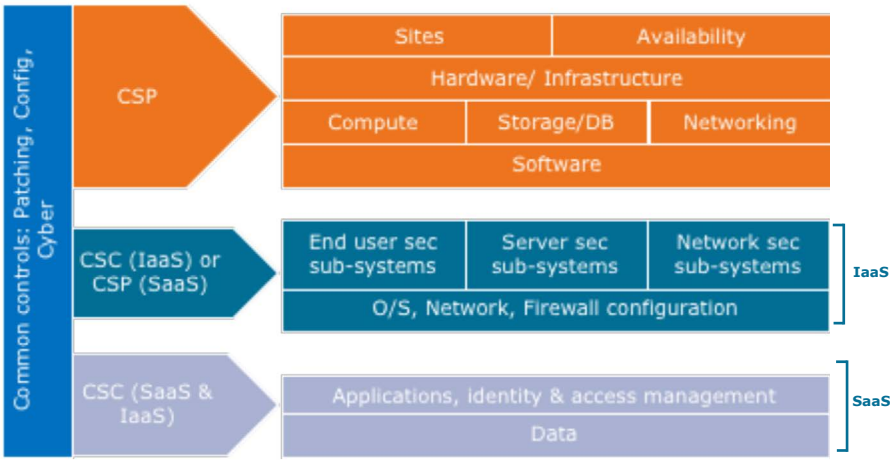


[8] Based on the figure at: https://mycloudblog7.wordpress.com/2013/06/19/who-manages-cloud-iaas-paas-and-saas-services . While innovative cloud services constantly evolve, thereby preventing an exhaustive and static overview, this simplified visual will help to understand the distinction between management features according to cloud services in question.

Projecting the understanding of the different roles in the controls landscape to the cloud service models available, please consider figure 12. CSCs remain accountable for computing, although with cloud computing they no longer operate all the IT controls in the cloud computing infrastructure themselves.

The responsibility over the management and operation of IT controls may be shared with CSPs. The degree of control allocation depends largely on the cloud service model, with more controls managed and operated by CSCs in IaaS than in SaaS.

FIGURE 12



The environment of cloud services provided to financial institutions is continuously developing. Based on the understanding of control demand, control origin and shared responsibility, the institutions can engage with CSPs on a new operational process that may be required to manage the relationship and the shared obligations for management effectively.

4.4 Careful consideration of cloud migration

Business users of cloud services need to consider various issues before moving their own activity into cloud service productivity tools. European banks choose a strategic and carefully planned approach to using cloud computing[9], which has a positive effect on the identification and management of risks[10].

Cloud solutions provide for technological opportunities to lift an application or landscape out of its current hosting environment and shift it to another. For example, lift-and-shift of on-premises hosting to the public cloud. This would include a migration of three top layers: application, database and OS layer. Besides the speed of such migration, advantages can include cost-effectiveness, reduced disruption and quick return on investment.

However, such technical solutions for rapid migration does not automatically imply financial institutions seeking out cloud solutions in a less secure – because rapid – way. Quite the opposite, "lift-and-shift" solutions are weighed by financial institutions in the light of responsibility and regulatory framework. While companies may choose to "lift and shift" in terms of moving applications in their current state, meaning no

[9] See Chapter 3 for the banks journey to cloud.
[10] See Chapter 4.2 for support tool regarding risk awareness.

modernisation or other changes, they still re-evaluate the control landscape. Careful planning and agreements are necessary not only regarding controls, but the operational processes that will be required to manage effectively the relationship between the CSP and CSC. This can include organisational steps such as monthly Service Level Agreements (SLA) and risk reporting meetings, periodic reporting to executive management and/or board as well as other actions – depending on workload and data criticality. Consequently, financial institutions consider a transformative development towards cloud on basis of a carefully established cloud migration strategy. This strategy clearly defines the business outcomes the financial institution is seeking and the timeframe to achieve predefined goals.

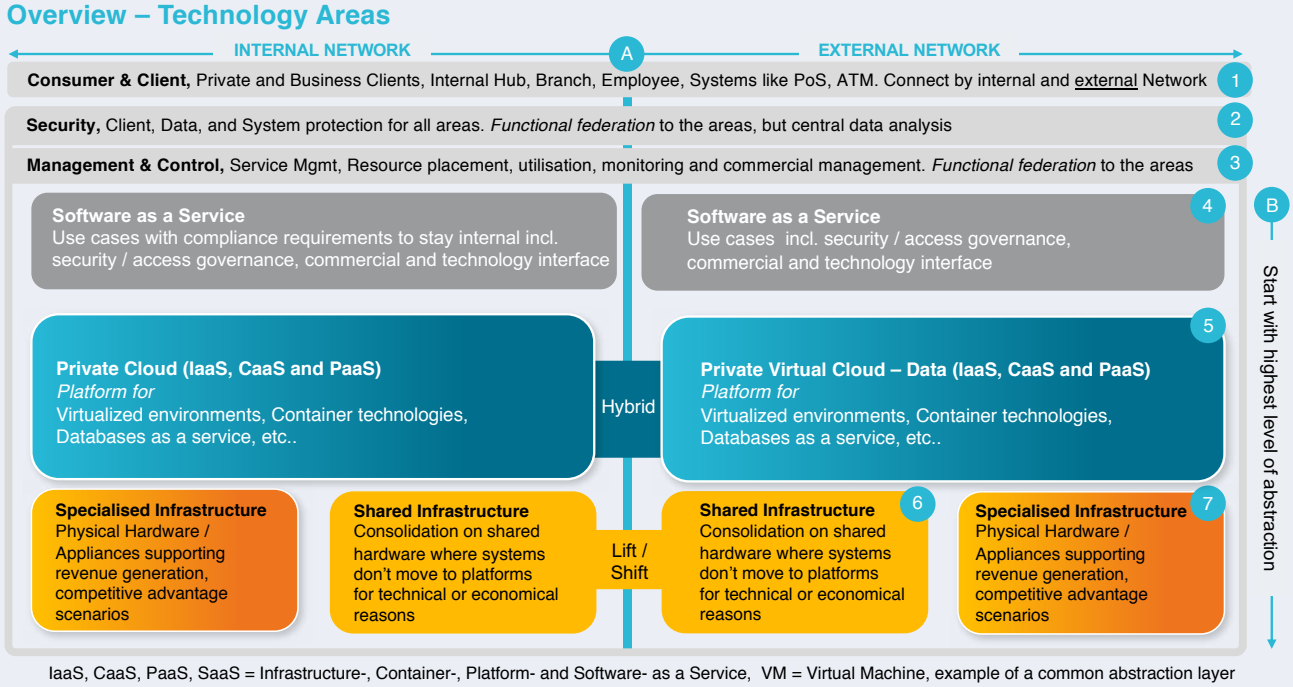
A careful adoption of cloud in the financial industry should consider general assumptions:

- Appropriate standardisation of technology components and services, interfaces and controls can enable universally understood, seamless and secure interconnectivity and appropriate isolation between cloud-ready networks.
- A gradual cloud adoption uses commonly understood service models and use-case scenarios, driving towards the highest possible level of abstraction from technology resources.

Figure 13 shows the typical landscape of a financial institution's services, ranging from highly

FIGURE 13

Target Technology Framework



IaaS, CaaS, PaaS, SaaS = Infrastructure-, Container-, Platform- and Software- as a Service, VM = Virtual Machine, example of a common abstraction layer

customised platforms (lower left corner) to highly generic software as a service offering (upper right corner, box labelled No. 4).

For the banks to leverage cloud technologies, an educated decision must be taken on whether cloud service and deployment models will best suit the banking service needs according to efficiency, efforts to migrate, security, complexity and interoperability and which models these are.

This can be achieved by mapping the status quo and the future needs for the cloud service layers as part of the above mentioned cloud migration strategy:

ONE - consistent interface layer for all consumers.

TWO - federated and requirements-based implementation of security.

THREE - orchestrated monitoring and control information.

FOUR - internal and external SaaS to be considered if the function is standardised across markets.

FIVE - compatible, interoperable Hybrid Cloud Compute Platform.

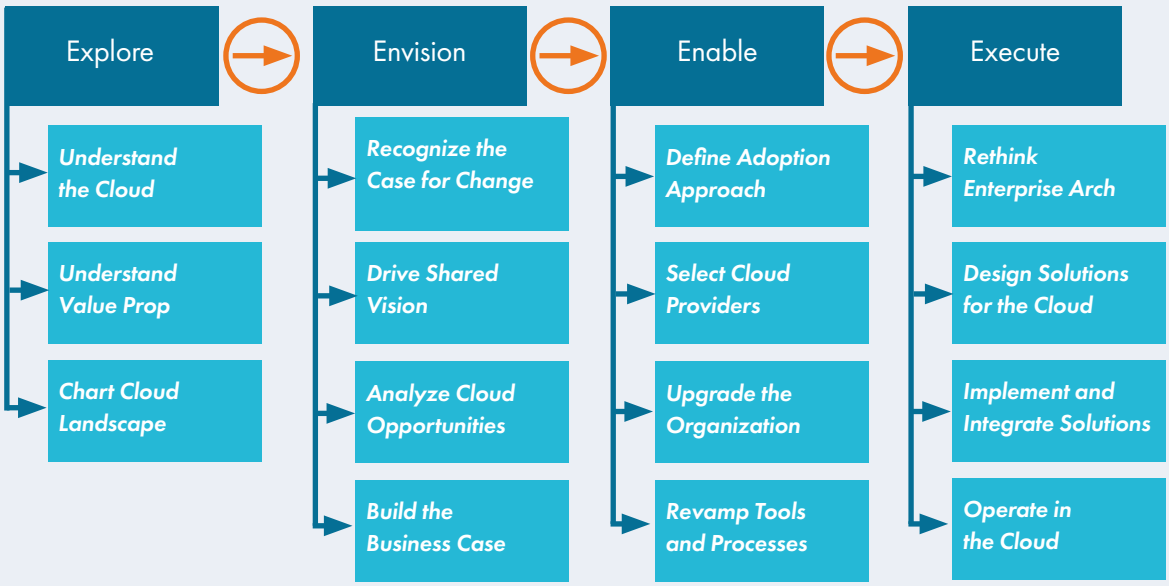
SIX - use available IaaS where it is not economically viable to transform to the Hybrid Cloud.

SEVEN - use specific infrastructure only if needed e.g. for latency aspects; keep overall footprint low.

Following these steps, banks can achieve a fit-for-purpose adoption of cloud services. Combined with the sound awareness for the controls demand[11], a well-controlled cloud environment for financial services can be established.

On their journey to the cloud, financial institutions can consider – within their individual cloud migration strategy – certain helpful elements for different steps of the way:

TABLE 14



Source: 'To the Cloud: Cloud Powering an Enterprise'[12]

[11] See Chapter 4.2

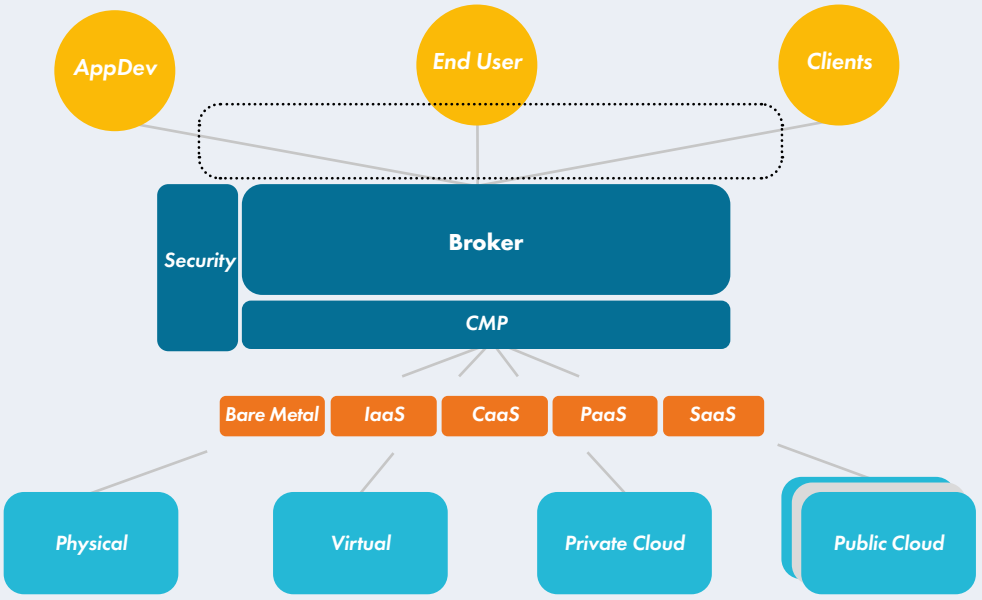
[12] Pankaj Arora, Raj Biyani, Salil Dave, 'To the Cloud: Cloud Powering an Enterprise', 2011, McGraw Hill.

Untouched from the technological development and the changes of IT architecture, European banks serve their customers with service solutions covering the full range of financial needs. However, cloud technology can assign a new dimension to the IT management that underpins financial services. Within the cloud environment, banks – utilising cloud computing for the benefit of customers and business processes – find themselves in the nexus of this modern service operation. Additional to the traditional infrastructure dimension, IT evolves into the role of 'Service Broker'. Management skills, e.g. regarding vendor relationships, become important.

European banks carefully design their journey to cloud in accordance with such an envisaged 'Service Broker' function. It allows business operation in a multi-cloud environment, utilising service solutions from a multitude of CPSs. While doing so, financial institutions stay alert to the consequences for operational risk and the control capacities. Ultimately, attention by institutions and NCAs – based on a risk-based approach – should focus on the successful management capabilities of banks for the indicated service brokerage. Applying the management function, European banks then use the changed IT capacities for the execution of traditional as well as innovative financial services.

FIGURE 15

IT as Service Broker



CHAPTER
FIVE

5 Conclusion

The gradual adoption of cloud computing is a macro trend common to all industries, progressing at a measured pace as the industries, including the financial sector, gain maturity in their understanding of cloud and their capabilities increase. Used wisely it can help to control cost in a more efficient way, improve the flexibility of the business model, allow operational specialisation and improve resilience. With cloud computing further evolving, more advantages are expected to become apparent in the future. As IT is the backbone for banking operations, associated efforts are a big contributor to healthy and competitive financial institutions.

Cloud computing is a key enabler for a successful data economy and service delivery, as it can seamlessly connect banks with other financial institutions, customers and FinTech innovators. The pervasive and secure use of cloud – benefitting customers and banks alike – supported and consistently governed through a risk-centric approach by banks is in alignment with the already existing risk management culture of banks.

As much as cloud computing supports financial innovation, the understanding and quantification of risks associated with new technology is often a challenge. That is why it is important that the risks perceived by banks are reconciled with those risks of greatest concern to regulators. Acknowledging the fast-developing cloud environment, European banks and CSPs aim to support this process. Based on a thorough awareness of risk dimensions, banks carefully migrate services to cloud with attention to consistency, security and corresponding risk management. The visualisation provided under Chapter 4.2, picked up further by examples in the annex, aims to support this awareness. CSPs on the other hand actively engage with their customers to provide services in a highly secure and controlled environment. Together, both parties operate in the face of cloud-specific control demand and an evolved controls landscape following the innovative technological nature of cloud.

NCAs are invited to consider the aspects presented in this paper when conducting their own assessment of institutions' risk identification and management with regard to cloud services. This should reflect the increasing 'service brokerage' role of institutions for their IT capacities, based on cloud solutions in a multi-cloud environment. Resting on the EBA GL and following their own risk-based approach, NCAs find themselves in a key position to contribute to a harmonised supervisory framework

for cloud adoption in Europe. Without a common understanding of cloud by regulators, European banks and CSPs, different national approaches could provide for regulatory fragmentation across Europe, ultimately hampering cloud adoption by financial institutions.

This paper aims to contribute positively to the discussion on cloud, sharing fundamental information as a basis for current and future supervisory engagement with European banks and CSPs. A harmonised regulatory approach to cloud will help to facilitate its innovative potential in finance, foster its adoption by the European banks and aid the financial sector in further endeavours of digital transformation.

> “Cloud computing is a key enabler for a successful data economy and service delivery, as it can connect banks with other financial institutions, customers and FinTech innovators seamlessly.”

Back-end systems	Systems which do backend processing of data which can be accessed e.g. by front end systems (e.g. ledgers, booking).
CaaS	Offering for container-based virtualisation in which CSPs offer a complete framework to customers for deploying and managing containers, applications and clusters. CaaS offers a completely enabled container deployment service with security and governance control for IT management.
CI/CD toolchain	Continuous integration and continuous deployment of code changes into existing instances at any time not being restricted by predefined release cycles or change windows. To enable this, highly standardised coding and testing principles are necessary as well as highly automated test and deployment procedures to control the risk of change.
Cloud computing	An innovation in computing that allows for the use of an online network ('cloud') of hosting processors so as to increase the scale and flexibility of computing capacity. Cloud allows industries to tap into new service models, utilising its technological advancement for new and better services to customers, improving productivity, cost-efficiency and flexibility of internal business processes.
Cloud deployment model	Defines rules and guidance on where workloads are deployed. For example, highly critical workloads to be deployed on a private cloud. Low criticality functions can be deployed on a public cloud.
Cloud service model	Outlining the usage of cloud services with definition of IaaS, PaaS, CaaS and SaaS.

Control framework	A process and governance framework defined by the institution to control and protect the environment. The control framework also ensures compliance to the regulatory framework.
Front-end systems	Systems offering user interfaces for direct interaction with the users.
Grid IaaS	IaaS model which is setup in a grid computing environment to offer.
GUI	Graphical User Interface.
Hybrid Cloud	For the purpose of this paper, hybrid cloud is defined as a cloud computing environment that uses a combination of private cloud (where most financial institutions started their cloud journey) and public cloud services that may include third party service offerings such as Platform as a Service (Paas), Infrastructure as a Service (IaaS) and SaaS (Software as a Service). These platforms are connected through automation and orchestration tools.
IaaS	Supplies customers with IT infrastructure, provided and managed on a per-use basis, e.g. servers and storage. The two common models of delivery for IaaS are 'bare metal' and Virtual Server Infrastructure (VSI). In the case of bare metal, the financial institution or their designee manages the servers, storage, virtualisation, OS, middleware, runtime, data and applications. In the VSI model the financial institution manages the OS, middleware, runtime, data and applications.
Intra-day risk computing	Online computation of the risk the institution is exposed to by trading activities.
Lift-and-shift	Moving an application from one technology platform to another without a functional change. May apply to physical moves also in the context of infrastructure.
Managed Cloud	Future-oriented perspective on cloud, envisaging a 'commoditized' cloud use in the mid- to long-term. Managed cloud allows each customer to choose which IT functions it wishes to manage in-house, while leaving all the rest to its service provider. Managed cloud services can include infrastructure and application level support.

Multi-cloud environment	Environment allowing the CSC to utilize cloud service solutions from a multitude of CSPs.
Network perimeter	Defines the border between internal network segments and the outside networks like the internet, customer's and counterpart's networks.
Orchestration tool	Orchestration is the automated configuration, management, and coordination of computer systems, applications, deployment and services. (https://www.redhat.com/en/topics/automation/what-is-orchestration)
PaaS	Supplies customers with an on-demand environment for developing, testing, delivering and managing software applications. The financial institution manages its data and applications.
Private Cloud	A cloud computing environment where solutions are located inside the banks' own perimeter and therefore leverage all established controls of the respective bank. Computing resources are used solely by the one single organisation, either physically in the company's on-site data centre(s) ("on-premises") or externally with the third-party provider ("hosted private cloud").
Public Cloud	A cloud computing environment where cloud solutions are located outside the bank's perimeter. Therefore, within a public cloud setup, not all controls will be operated by the institution itself. This does not change accountability of Cloud Service Customers (CSCs) according to the applicable legal framework. Logical access control functions are provided to the company using publicly hosted cloud services (e.g. through authentication mechanisms), any other company can subscribe to the same services, available over the internet.
SaaS	Allows customers to connect to and use cloud-based application over the internet on a subscription basis e.g. cloud-based email and collaboration systems.

Annex 1
Use Case: IoT

Meeting clients needs is crucial to succeed in today's business environment. Clients of financial services hardly ever want a financial service for its own sake. Rather, they want a product which they cannot afford without a loan or an easy payment service (instant buy). Being close to the data means being close to the customer, i.e. actively engaging banking services in a vertical economic integration. Most clients happen to be in the cloud already, either with their mobile phone or Internet of Things (IoT) enabled machines in the industry 4.0.

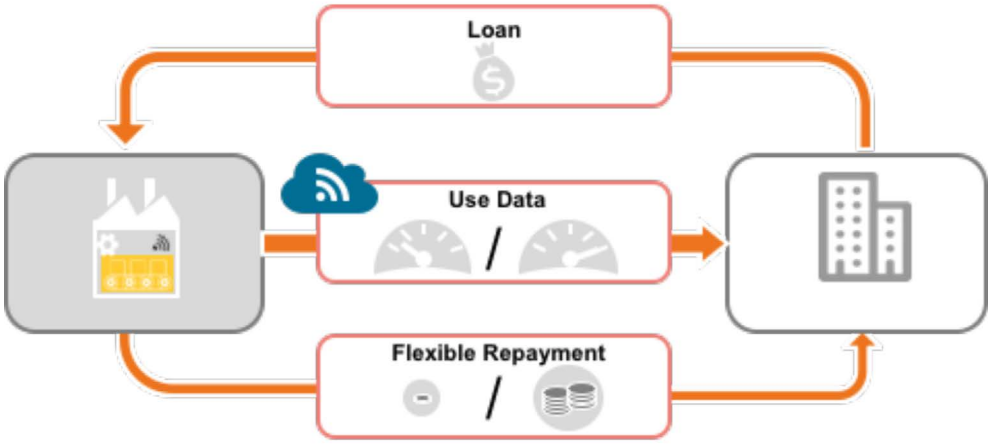
A credit-related data-driven product is a pay-per-use loan, i.e. an investment loan with variable debt services based on real machine usage. If the machine is used less than planned, the repayment of a loan cost less than that of a traditional loan with linear repayment. If the machine is used more than planned, the repayment of the loan costs more than the one of a traditional loan. Whether the machine is used less or more than planned is answered by the machine data provided to the bank. For this purpose, cloud enables timely and secure data transfer. In a hybrid cloud set-up, the link to the customers can be achieved by mapping rack numbers to a client's loan in the on-premise systems.

Layer: The Layer used can range from IaaS, based on market standards, to using SaaS. The first option would be to build up a tool based on IaaS and PaaS services allowing for storage, monitoring as well as data preparation and processing. Moreover, one can build alert functions that activate certain routines once new data comes in. Retention requirements can also be met in storage functionalities.

Alternatively, most cloud service providers offer IoT SaaS services.

Control framework: Access is controlled by the financial institution; however, as the machine and its data are outside the control framework, the framework is a hybrid one with partial public setup outside of network perimeter control.

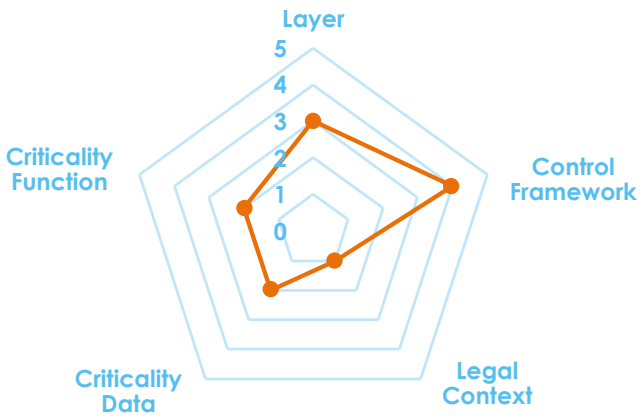
Legal context: Credit-related products are only offered in certain pre-defined regions, i.e. a contract and data location in a home country in the European Union.



Criticality of data: Machine data with low criticality, since it does not include personal identifiable information.

Criticality of the function: Function is replaceable but necessary for internal processes. Replicability can be achieved by implementing a multi-cloud strategy where the function can be shifted to another infrastructure in an exit plan scenario.

The result of the evaluation should be to tackle the highest risks first, i.e. in this case this would be the control framework.



Layer	3
Control Framework	4
Legal Context	1
Criticality Data	2
Criticality Function	2

The bottom-line for the security of cloud usage is to make the most out of the innovative product without increasing the risk profile. An ideal result is to achieve overall risk reduction using cloud security products leveraging the economies of scale. For example, a CSPs Cloud Platform offers default data encryption at rest and in transit at scale. Beyond this, it is also possible for financial institutions to generate, store and use encryption keys independently, i.e. bring-your- own-key. New CSP's Data Loss Prevention API can also help discover, analyse, classify and redact any unintended sensitive elements in datasets collected from machines in real-time, using over 70 predefined or customized detectors. The API is designed to be platform-independent, multi-cloud ready and can stream data from virtually anywhere.

Annex 2 Use Case: Online collaboration

The objective of this use case is to evaluate a mock-up scenario for cloud-based collaboration system deployment within a financial European institution 'Contoso Bank'.

Many banks, including Contoso Bank, choose to deploy cloud-based solutions as an enterprise platform for enterprise-wide messaging and collaboration. This platform delivers supporting email, chat, telephony & (unstructured) document management services for all business departments. While a vast majority of business processes have minimal interdependency upon messaging and collaboration systems, this is not true in every instance.

For example, email may be used in support of a critical business processes used within specific departments, i.e. the support of trade finance activities in Contoso Bank. The typical initial deployment is hybrid, with a strategy to maximise use of cloud gradually. The extent of hybrid among financial institutions varies greatly. At one end of the spectrum an institution only has its authentication service on premise (ADFS) with all collaboration functions such as email services, document storage, chat, online meetings and voice/video calling functions running in the public cloud; while at the other end, you will find banks that choose to deploy more cautiously starting off with a hybrid setup either keeping certain subservices on premise or moving only a subset of users onto the public cloud for online collaboration, or a combination of both. For the Contoso example, the hybrid setup involves using a federated on-premise authentication (ADFS) infrastructure, cloud-based email for 90% of its users (keeping other users on premise), storing personal documents in the cloud for the same users and generally encouraging the setup of online meetings and group/team collaboration tools across the enterprise. 10% of internal users that fall within the scope of MIFIDII have their mailbox and telephony services still on premise due to mandatory telephony recording requirements and other compliance challenges. All cloud-based users rely upon a public cloud solution with data at rest stored the region (EU). All classes of data can be safely used in the cloud solution as per updated data handling guidelines.

Looking at these assumptions for the Contoso use case, the evaluation of the control demand of this cloud offering would show:

Layer: Online collaboration is a SaaS solution.

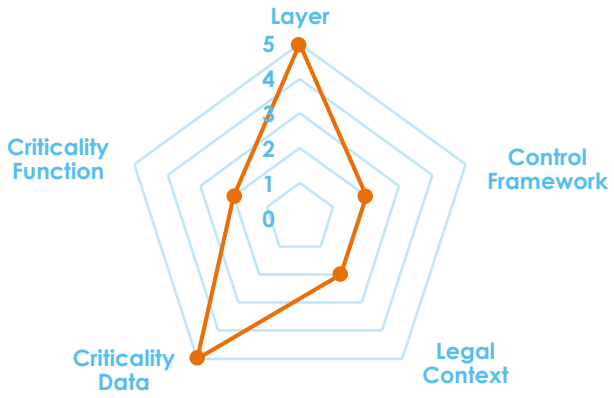
Control framework: Contoso Bank made a choice to keep identity management and authentication services on premise. Identities are provisioned from on premise HR systems to Active Directory (AD) on premise, and from there onwards to Azure Active Directory (AAD) using the AAD Sync tool. Authentication for the tenant is also done against the internal AD using Active Directory Federation Services (ADFS). Use of online accounts in the cloud is not allowed. Only corporate

approved devices can connect to the ADFS servers. This matches the category "Hybrid, within network perimeter all accesses are controlled by Institution".

Legal and regulatory context: The bank is a European multinational institution, so the context would match "Only EU regulation applicable (but of more than one Member State)". If, as with many institutions, they have a reduced presence in the USA, Singapore or Hong Kong this would change to "Mainly EU regulation applicable but also "recognised" third countries regulation involved". This mock-up addresses the former.

Criticality data: Since all data can be stored in the solution this is "Internal relevant identifiable sensitive data".

Criticality of function: The criticality has already been addressed in the paragraphs above and is rated as "Replaceable but necessary for internal processes" although in some cases this could be argued as "Necessary for external processing" (for the trade finance example above). The former rating was kept because the trade finance function that generates less than 2% of global revenue has its mailboxes kept on premise in the hybrid environment for now. As these move into the public cloud, upgrading to the next level can be considered.



Layer	5
Control Framework	2
Legal Context	2
Criticality Data	5
Criticality Function	2

Following the surface area of the figure, focus should be placed on Layer and Criticality Data. The control demand graph provides some insight into the potential inherent risk an institution may be concerned with when deploying this cloud solution. We will focus on the two higher numbers to translate the control demand further into a risk context.

The Layer is SaaS, but the collaboration tools involve also a leading product that is widely used across the entire industry both on premise and more recently in the context of cloud. In some ways it can be seen as moving and hosting the otherwise on-premise collaboration systems to a cloud context, like a platform cloud solution, with the difference that now the provider manages elements like upgrading, patching etc. on behalf of the bank. The provider demonstrated high transparency on how they manage and secure the service and is certified against industry standards that map to the internal control framework of Contoso Bank. A thorough risk assessment has been performed to assess the service, and several elements were identified which have a positive (risk reducing) impact on risk. The provider does not manage any

data access but instead offers Contoso granular controls over each part of the service. All data is encrypted and protected throughout the entire lifecycle, and the service applies verified security and operational processes meeting industry standards. The hybrid setup allows dynamic moving of data back on-premises, and contracts meet all regulatory requirements.

The Criticality Data rating implies a high inherent risk, since any type of data is now managed by the cloud solution. However, the risk assessment clearly indicated a significant reduction of the residual risk to the data by moving this to a cloud provider. The reason for this is a combination of the data being encrypted by a sophisticated encryption technology where the root keys remain controlled by Contoso bank, with a very granular data protection access list being applied to the most sensitive categories of data. It was not possible to protect data in this way on-premises, and thus the residual data protection risk was moved from medium on premise to low in the cloud according to the risk assessment, even though the control demand is high (and so is the inherent risk for this dimension).

Annexes 3-5 Use cases: Data Use cases preliminary remarks

For banks, data is an asset with ever increasing value. Operationally, the bank needs to guarantee data quality, standardisation, consistency and availability. For innovation, the bank's data scientists will need to have access to an evolving set of data visualisation tools on anonymised data. At the same time, data privacy regulation requires banks to be very conservative when it comes to storage and usage of data.

The need to gather ever increasing amounts of raw data and turn them into actionable metrics is generally known under the umbrella name of "Big Data". Also, upcoming technologies such as machine learning (ML) and artificial intelligence (AI) depend heavily on the availability and control of data assets. For this paper, three distinct areas in data use cases shall be presented. Each of these areas has different needs.

The necessity to be, at the same time, innovative and conservative, makes the area of data use cases an excellent field to demonstrate the need for hybrid cloud adoption, represented by the following examples of different control framework charts for different data functions. An example of a secure hybrid cloud implementation specialised in data use cases is an AI-powered CSP's Autonomous Database, running in the public cloud as well as on "Exadata Cloud at Customer" machines.

Data lake processing

The term "data lake" is commonly used to indicate a repository of data stored in its natural, unprocessed, raw format. It contains structured data from corporate databases, unstructured data such as recorded phone messages or data copied from public social websites, and anything in between. The business activity of "Data Lake Processing" picks up all available data in a timely manner and drops it in the data lake. The data lake of financial firms will contain personally identifiable data, or "PII" data, information that can be used, uniquely, to identify, contact, or locate a single person. Business practices and legislation call for conservative use of that PII data.

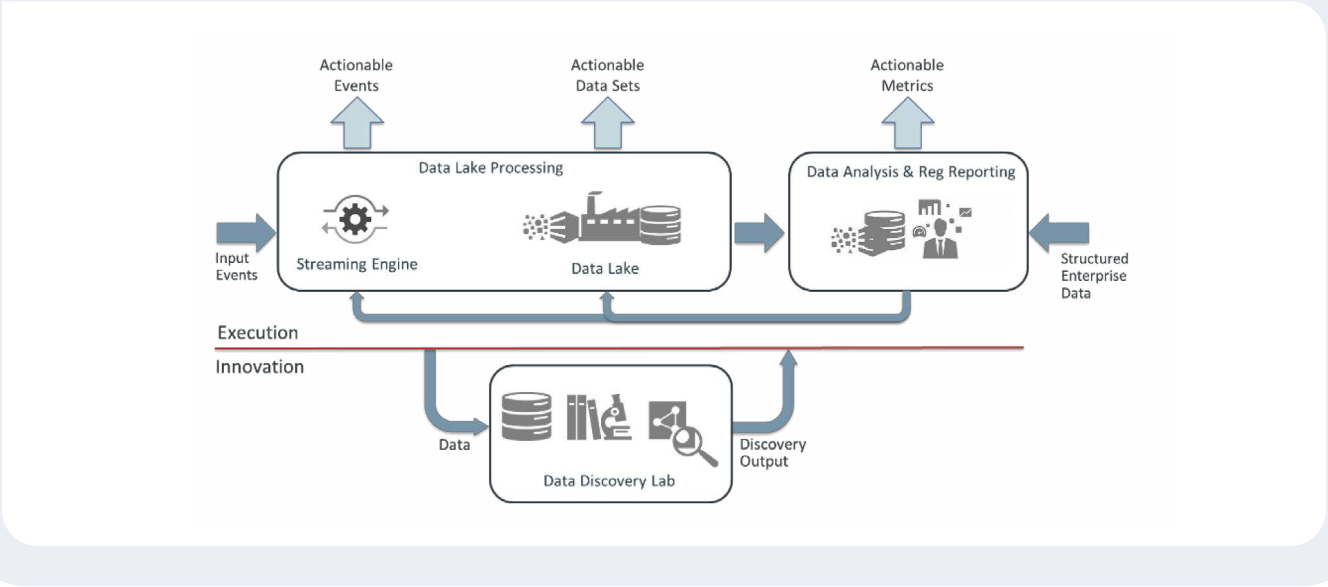
Data Analysis and Regulatory Reporting

In the business activity "Data Analysis and Regulatory Reporting", the raw data from the data lake is organised, categorised, combined, abstracted and turned into metrics that are actionable by systems and business users. This is where the raw data is mined into insights using Big Data techniques. The data from the

data lake is used to train Machine Learning and Artificial Intelligence algorithms, which will start making predictions. Better, faster and more innovative data analysis creates better metrics for decisions, improving business performance and competitiveness.

Data Discovery Lab

Since data analysis has a direct impact on business performance, financial services firms organise data discovery labs staffed with data scientists. These labs continuously improve the methods to turn raw data from the data lake into metrics, constantly innovating, thereby staying ahead of the competition. They scientifically study and improve Machine Learning and Artificial Intelligence algorithms.



Annex 3 Use Case: Data Lake Processing

When defining cloud requirements for the data lake, which will contain PII information, a lot of attention will go to data privacy and the legal context. Banks could opt to store the data in a private cloud solution, maintaining a lot of control. Since standardisation is important, banks might want to maintain the data in an IaaS Layer based on market standards.

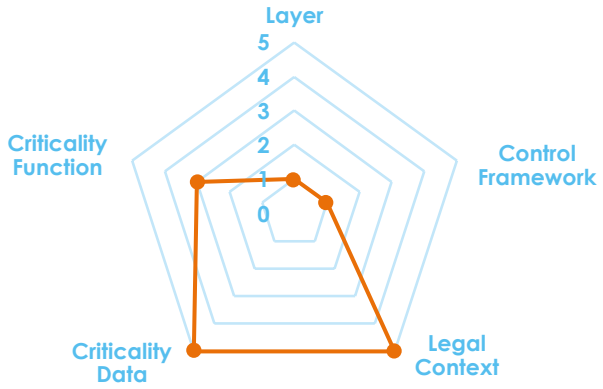
Layer: The data lake is the foundation of data monetisation, irrespective of mining tools. Therefore, the lowest common denominator of standardisation is important.

Control framework: The data in the data lake will contain private customer information. Keeping the data in a private setup will inspire trust in how privacy is treated.

Legal Context: The more centralised the data lake is, the more valuable global metrics will be. Therefore, compliance targets the broadest set of regulations.

Criticality Data: The data in the data lake will not only contain private customer information, but also data that is of critical importance to the financial institution.

Criticality Function: The data lake is important. Temporary unavailability will not stop core business processes, but external financial reporting will depend on it.



Layer	1
Control Framework	1
Legal Context	5
Criticality Data	5
Criticality Function	3

Annex 4
Use Case: Data Discovery Lab

Data scientists will consistently be on the lookout for new methods and tools to find value, insights and AI predictions in the raw data. For the purpose of rolling out new tools, public cloud solutions can be very appropriate. If their work is done on the basis of anonymised data, then data privacy and control become less of an issue.

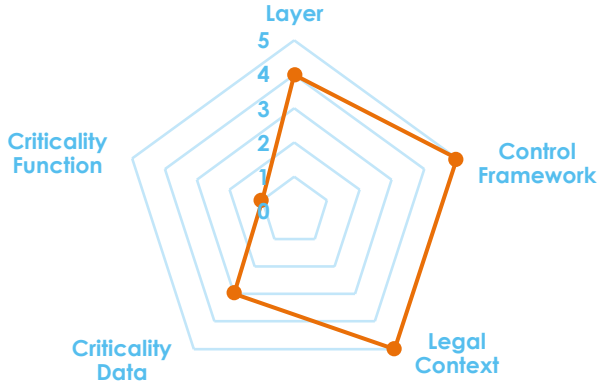
Layer: The task of a data discovery lab is to innovate faster and provide better metrics. Data discovery, artificial intelligence and machine learning tools will change often and are usually located in the PaaS layer.

Control framework: Using tooling based on transformational technologies in a public cloud setup can allow faster innovation. The risk of data leakage should be handled by anonymising the data for the discovery lab.

Legal Context: Metrics from data discovery and machine learning will be based on global data. Consequently, compliance must target the broadest set of regulations.

Criticality Data: For data discovery, personally identifiable data is not important and should be anonymised.

Criticality Function: Non-availability of the data discovery lab will be detrimental to the value of the financial institution in the long run but will not stop any business process immediately.



Layer	4
Control Framework	5
Legal Context	5
Criticality Data	3
Criticality Function	1

Annex 5
Use Case: Data analysis and regulatory reporting

Data analysis and artificial intelligence can be very powerful, because data is turned into actionable metrics and predictions that drive business decisions, in turn control and legal context become extremely important. In contrast, the permanent availability of the metrics is less important. Where standardisation is important for the data lake, this appears less so for the data analysis and machine learning activity. Data analysis benefits from more innovative and powerful capabilities. Better analysis provides competitive differentiation. Therefore, the Layer will likely be PaaS with vendor-specific features.

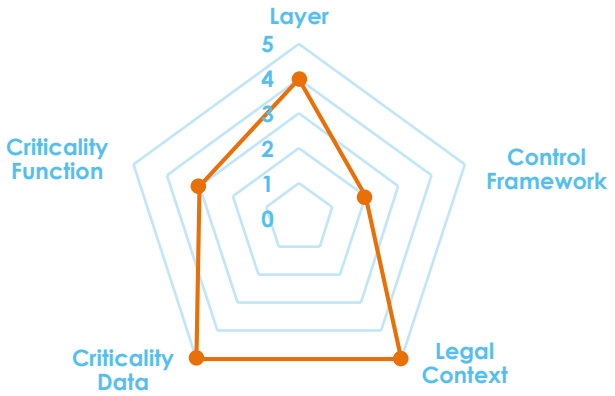
Layer: Data analysis uses tools that reside in the PaaS framework. Depending on the tooling used, regulatory reporting will reside in PaaS or SaaS solutions.

Control framework: Since the cloud provider offers secure access and privacy control means, tooling for analysis and reporting can reside in public PaaS or SaaS. However, because of the sensitivity of personally identifiable data, at least parts of the data should continue to reside in- house. A hybrid cloud is a good choice here.

Legal Context: Regulatory reporting can be regional, but metrics from daily data analysis are more valuable if they are global. Therefore, compliance targets the broadest set of regulations.

Criticality Data: Since data analysis runs on the actual data lake, the criticality of data needs to account for the processing of private customer information.

Criticality Function: Unless data analysis is also used for processes like real-time AML, temporary unavailability will not stop the core processes, but external financial reporting will depend on it.



Layer	4
Control Framework	2
Legal Context	5
Criticality Data	5
Criticality Function	3

Annex 6
Use Case: Transformational Technologies

Inspired by the Fintech movement, banks are looking into the field of new technologies to create new customer experiences and open new revenue streams. Cloud technology provides the necessary enabling infrastructure and computing power to put transformational technology into testing and – following careful processes to ensure safety for clients and business processes – to work.

To provide some examples from a vastly expanding field of technological innovation: Blockchain is regarded as a technology with the potential to transform distributed ledger technology (DLT), cross-border payments, identity management and trade finance, amongst others. Artificial intelligence has quickly become a technology that is complementing algorithms in – for example – security and risk management systems, financial planning and fraud detection. Digital assistants use artificial intelligence to improve customer service. 'Internet of things' is becoming relevant in financial services in trade finance and supply chain financing, as well as wearable devices providing data for life insurance, personalised policy management and pricing. Robotic process automation (RPA) is starting to add more intelligent automation in banking processes, resulting in cost reduction and better customer service and reporting.

Experimenting with transformational technologies often happens in technology labs based on cloud technology, benefitting from a thorough risk awareness by banks.

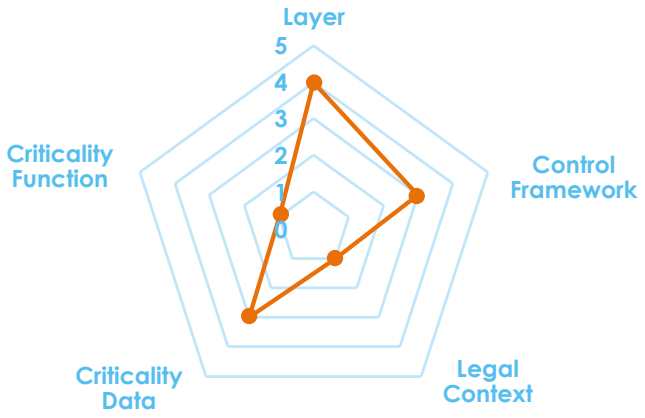
Layer: Technology labs need to cater for easy addition of the latest technologies. Tools will change often and are usually located in the PaaS layer. Vendor-specific additions are welcome, as innovation and differentiation are key. For example, a bank ran a blockchain proof of concept that delivered nearly instant cross-border payments with increased data privacy and security by leveraging the built-in identity management and data encryption features of an CSP's Blockchain Cloud Service, running in the PaaS layer.

Control framework: Although a full public setup creates more flexibility, banks that experiment with transformational technologies will want more control. Some outcomes need to be confidential as they're targeted to differentiate the bank in the market.

Legal Context: Experiments with transformational technologies usually start in one location. Therefore, the legal context should be only the EU home country. However, as experiments grow and move to production, that legal context will become broader.

Criticality Data: Technology labs often work with anonymised data. PII-data should be avoided.

Criticality Function: Non-availability of the technology lab will be detrimental to the value of the financial institution in the long run but will not stop any business process immediately.



Dimension	Rating
Layer	4
Control Framework	3
Legal Context	1
Criticality Data	3
Criticality Function	1

Annex 7 Use Case: Early Warning System (EWS)

The EWS is an AI-powered application that collects and analyses large amounts of data to identify whether clients are exposed to potential risks, a task currently performed manually by credit risk analysts.

The EWS application is 'fed' real-time market data from external data and information providers (specialised on the financial community) and news from public sources. The system is capable fo processing up to 80,000 articles, every day, from all over the world, in different languages, in local media outlets. All 'harvested' relevant external data then being captured on a CSP's cloud storage as data backend. Subsequently, the application uses the CSP's Natural Language Processing and translation services to scan the news articles and uses multiple Machine Learning algorithms to determine sentiment, trends and specified warning signals.

Credit risk analysts can set their own warning criteria. For example, if a client's share price falls by more than a pre-set percentage, or a client's media coverage is negative based on sentiment analysis.

The system learns from experience, so in time it will become better at identifying the sentiment of news and developments in the market.

Layer: Through machine learning, the SaaS application of EWS scans financial and non-financial information, such as published news items from all over the world.

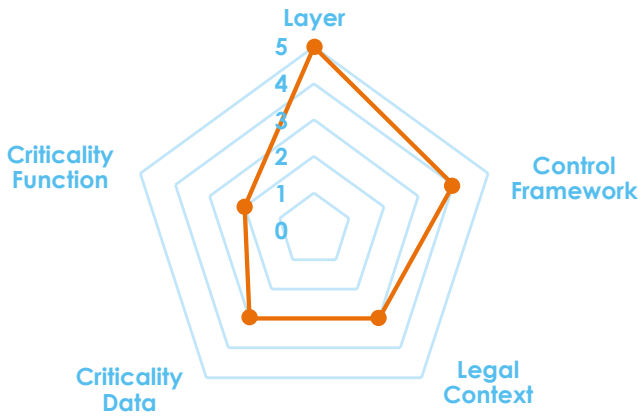
Control framework: EWS uses the CSP's natural language processing and translation services for articles published in different languages in local media outlets.

Legal Context: The bank is a global financial institution, so the context would match "Mainly EU regulation applicable but also "recognised" third countries regulation involved".

Criticality Data: EWS application collects and analyses large amounts of data from public and subscribed sources and correlates with corresponded clients to identify whether clients

are exposed to potential risks (data relevance for internal purposes).

Criticality Function: The function is replaceable, but necessary for internal processes. Credit risk analysts set their own warning criteria. For example, a client's share price falls by more than a pre-set percentage, or a client's media coverage on specific subjects which possibly resulted in negative sentiment. With provided faster and better insights, the credit analysts can take appropriate actions.



Layer	5
Control Framework	4
Legal Context	3
Criticality Data	3
Criticality Function	2

THE EBF CLOUD BANKING FORUM

European banks want to adopt innovative cloud technology, to allow them to operate in a fast-developing digital environment, to serve customers and to adapt their business in order to strive for the EU's digital leadership role. In December 2017, the European Banking Federation launched the EBF Cloud Banking Forum, a policy hub on cloud computing for European banks and Cloud Service Providers to support a harmonised supervisory approach towards cloud computing. This will facilitate the adoption of public/hybrid cloud computing by European banks on a larger scale.

The EBF Cloud Banking Forum focuses on specific regulatory developments related to cloud technology. The forum fosters the important exchange of IT architects, legal experts and cloud specialists from among EBF members (national banking associations and over 15 banks), Cloud Service Providers, and observers. The latter consist of Cloud Service Providers' trade associations and EU authorities (ECB, EBA, European Commission).

FOR MORE INFORMATION CONTACT

European Banking Federation AISBL

Brussels
Avenue des Arts 56, 1000 Brussels,
Belgium,
Julian Schmücker
Policy Adviser - Digital Innovation
+32 2 508 3744
j.schmucker@ebf.eu

Frankfurt
Weißfrauenstraße 12-16,
60311 Frankfurt,
Germany

EU Transparency Register ID number:
4722660838-23

EBF Cloud Banking Forum