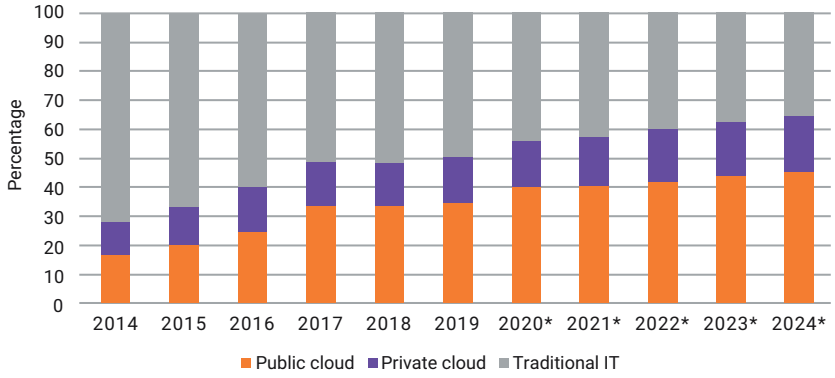
Cloud Computing Evolution and Regulation in the Financial Services Industry

亦有中文简体译本
www.isaca.org/currentissue

It has taken some time for cloud computing services to be accepted and adopted, but today, many enterprises, including those in the financial sector, are using the cloud on a daily basis.

The increase in digitization influences consumer habits and business interactions, leading many financial institutions to close their physical branches and to outsource processes, services or activities. One of the most frequently outsourced activities is IT; therefore, the management of outsourcing arrangements plays a crucial role in digitization strategies.

FIGURE 1
Worldwide Spending on IT Infrastructure by Deployment Type (*=forecasted)



KILIAN TRAUTMANN | CISA

Is an IT audit senior expert in the deposit insurance field as it relates to regulatory banking. He is a career author who has been published in various internationally renowned journals. His articles provide insights and solutions to issues at the intersection of IT, compliance and auditing. In the past, he worked in an audit firm belonging to a reputable tax-centered legal advice corporation in Germany. He also is a founding member and deputy director of the expert group Digital Trust, which is affiliated with the ISACA® Germany chapter.

This trend can be observed in worldwide spending on IT infrastructure by deployment type (**figure 1**).[1] In 2023, cloud services are forecast to account for more than 60 percent of worldwide spending on IT infrastructure, corresponding to annual expenditures on cloud IT infrastructure of US$100 billion (a 10 percent increase over the previous year) (**figure 2**).[2] The cloud application market will be valued at US$154 billion (a 5 percent increase over the previous year and a 400 percent over 2013) (**figure 3**).[3]

Although there are several cloud service providers (CSPs), the market is highly centralized, with a few major players (the so-called Big Techs) accounting for most of the market shares. In the third quarter (Q3) of 2022, the leading enterprises by worldwide cloud computing revenue were Amazon Web Services (AWS) (32 percent), Microsoft Azure (22 percent) and Google Cloud (9 percent) (**figure 4**).[4]

Given the nature, scope, complexity and risk of outsourcing essential processes, services or activities related to the performance of banking transactions and the provision of other financial services, it is crucial to implement adequate and effective controls.

The regulation of cloud computing demonstrates the evolving influence of digitization in the financial services and banking industry. This supervision is dynamic, as evidenced by the recent EU Digital Operational Resilience Act (DORA) through which cloud services will be subjected to further regulation.

The COVID-19 pandemic highlighted the value of swift IT capacity scaling and remote system accessibility and demonstrated that reliance on on-site technology is risky because it might become inaccessible in the event of exploited vulnerabilities or unforeseen external factors. In this regard, DORA addresses the risk of dependence on cloud service providers.

It is crucial for financial institutions to understand the role played by cloud computing in the increasingly digitized banking world, how to mitigate the risk of depending on cloud services, and the further development that may materialize through the rise of distributed ledger technology (DLT).

Digitization in Banking

The growth of digitization led to the creation of new banking[5] products. From a consumer's perspective, digital solutions offered by banks typically embody new interaction methods (e.g., robo-advisers, real-time credit scoring, digital budget tracking and video identification) and payment options (e.g., instant and mobile payments).[6] On the regulatory side, the Payment Services Directive (PSD2) notably opened the banking sector for tech-savvy organizations offering financial solutions. PSD2 introduced the requirements for payment account providers to permit third parties to exchange account information and begin payments. This regulation permits and fosters innovation and led to further transformation and innovations in the banking sector, such as open banking.

Open banking enables easy integration of all types of financial accounts and services from numerous previously unconnected institutions, resulting in the creation of new consumer financial services. Open banking is a type of Finance as a Service (FaaS) achieved when a group of financial institutions uses Software as a Service (SaaS) to supply and support various financial services. Hence, open banking is built on cloud computing. If application programming interfaces (APIs) are used to comply with open banking rules and receive customer approval, an open banking ecosystem gives third-party providers access to consumer banking, international and other financial data from various enterprises. One existing use case is buy now, pay later (BNPL).[7]

At present, additional banking product innovation is triggered by the rise of DLT.[8] DLT makes financing options more accessible (banking the unbanked) and streamlines payment processes (quicker settlement and clearing). Overall, DLT provides the option of decreasing the number of required intermediaries that were previously necessary.

DLT embodies technical precautions that make fraud and counterfeiting extremely difficult. This is also why this technology is likely to play a role in the digital trust literature and movement. For instance, DLT can enable new types of functionality by transforming digital securities into smart financial instruments with embedded business logic and self-executing life cycle functions, such as automated payment of dividends. This is in contrast to merely making securities digital in nature. Key potential advantages of using DLT in the financial securities area include instantaneous issuance, distribution and settlement of digital securities as well as quicker execution, reduced risk and lower cost per transaction.[9]

FIGURE 2

Worldwide Spending on Cloud IT Infrastructure in US$Billions (*=forecasted)

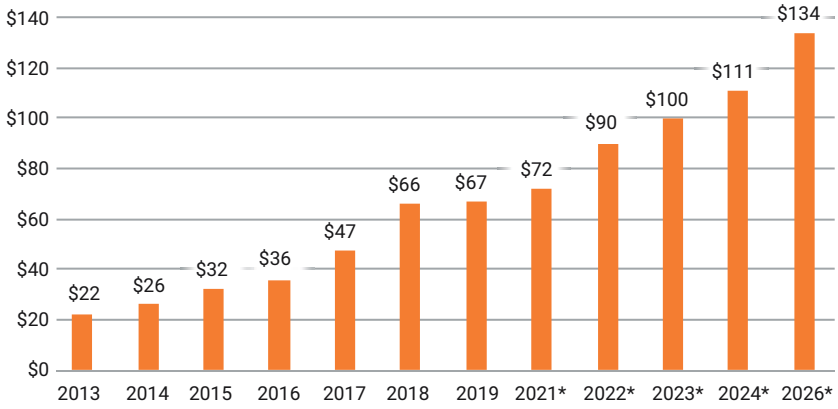
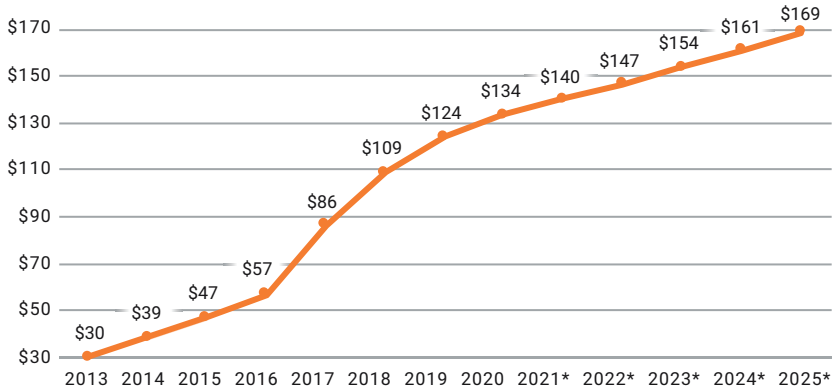


FIGURE 3

Worldwide Cloud Applications Market Size in US$Billions (*=forecasted)



Cloud Computing in Financial Services

Banking operations require extensive use of technology. On-premises systems installed locally on a bank's own computer infrastructure represent the traditional setup in the legacy financial industry. However, according to an industry report, 40 percent of servers suffer at least one unexpected outage per year. The average outage lasts 78 minutes and downtime costs are estimated at US$1,467

To compete with other unregulated enterprises entering the market, legacy financial institutions must take advantage of cloud computing services,

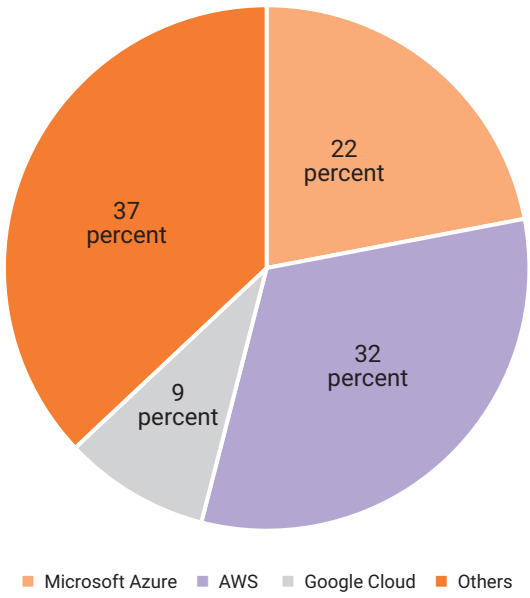
per minute (US$88,000 per hour).[10] As can be understood, implementing and administering servers on site comes with risk.

Whichever IT infrastructure is used, the fulfillment of business goals requires extensive information security including operational resilience. Any amount of downtime or data loss is unacceptable. Institutions may be able to mitigate these downtime costs by using cloud services from sophisticated tech service providers. These may provide a higher degree of security than running and administering systems on-premises.

Up until now, cloud computing has evolved into a crucial tool for the creation of new financial services, innovation, teamwork and competition in the digital sphere. Banks and financial institutions must embrace this change to remain competitive. For these institutions, flexibility and speed to market are essential. Cloud computing can enable both. To compete with other unregulated enterprises entering the market, legacy financial institutions must take advantage of cloud computing services, as expressed in an adequate IT strategy where IT is seen as a business enabler.

FIGURE 4

Worldwide Market Shares of the Leading Cloud Computing Providers in Q3 2022



Historically, it took European financial services institutions some time to adopt cloud computing. Main causalities come from legal concerns, information security and performance issues, reliability, the complexity of processing, operational control and governance. Compromised data are one high-profile example of the security concerns related to the cloud. The lock-in effect is another concern. Accessing cloud services using proprietary APIs and web interfaces means that a CSP-specific architecture must be implemented in the institution's IT environment. Overall, the lock-in effect imposes a certain level of risky dependence and high switching costs.

Of no less importance is the CSP's *de facto* status as a black box. Although audits can shine light into that box, the cloud market's high concentration and resulting market powers may impede access, information and audit capabilities.

In the beginning, financial services institutions adopted cloud services specifically for IT development and application infrastructure purposes. Today, core business functional systems (e.g., enterprise resource planning, data storage, investment management) are also conceptualized as involving cloud computing technology.

European Guidelines on Outsourcing and Cloud Services

As soon as financial services institutions became sufficiently aware of the benefits of cloud use and began adopting it, authorities pushed to strengthen the regulations around outsourcing. The goal is to address risk that may harm stable financial markets and consumer protection—such as data breaches—through the use of cloud computing resources. Outsourced business domains in the financial sector contain business processing services, including niche areas such as underwriting and collections, portions of technology platforms for corporate services functions, information and communication technology (ICT) infrastructure, application development and maintenance, administrative processes and, at times, complete business processes. The use of cloud computing technology is imminent in each of these domains.

In 2018, the European Banking Authority (EBA) published the first version of a general legal standard for outsourcing and beyond by financial services institutions.[11] National supervisory authorities and supranational regulators had to harmonize their policies and procedures to comply.

In response to the risk factors arising from the use of cloud services, in 2017 the EBA published recommendations and guidance for institutions using those services.[12] The guidelines specify requirements for outsourced cloud services. For example, the EBA requires institutions to guarantee unrestricted information, audit and control rights *vis-à-vis* the CSP.

In practice, these guidelines involve high costs. Because the outsourcing institution retains full legal responsibility for its outsourced processes, services or activities, it must implement adequate and effective control measures. The problem is that because the CSP market is so highly concentrated, there has been a shift in negotiating power from the financial services institutions to the CSPs. The result is a standardized contract with little leeway and institutions struggling to obtain contractually secured regulatory requirements.

Many outsourcing agreements do not provide sufficient safeguards that allow full-fledged monitoring of the subcontracting processes.

The EBA recommendation states that the right to audit is key to ensuring that important outsourced functions are provided as contractually agreed and in line with regulatory requirements.[13] Audit and access rights for competent authorities must be included in all outsourcing arrangements to ensure the effective supervision of financial services institutions. However, this contradicts the factual power of CSPs, which impose a risk to operations if their customers exercise audit rights (e.g., data centers might be overwhelmed if many audits are performed simultaneously). Therefore, CSPs prefer certifications such as audit reports by service organization controls (SOC) or International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards rather than granting full and unrestricted

audit rights.[14] Even if only a small portion of Microsoft Azure, AWS and Google Cloud clients were permitted to conduct costly on-site audits or inspections, CSPs would be unable to run their core business, resulting in service-level fulfillment threats. These interdependencies create a dilemma.

Even if contractual audits were granted to the demanding enterprise as EBA mandates, the national supervisory authority could not directly influence CSPs because audit rights were not directly granted to the authority itself. National authorities could supervise CSPs only indirectly via the institutions, which are reliant on cooperating CSPs. That is why EBA guidelines dictate that institutions should ensure that CSPs grant them as well as their competent authorities full access, information and audit rights. Still, many outsourcing agreements do not provide sufficient safeguards that allow full-fledged monitoring of the subcontracting processes. This compromises the institution's ability to assess associated risk factors.

Without prejudice to their final responsibility regarding outsourcing arrangements, financial services institutions may use pooled audits, organized jointly with other clients of the same service provider. Third-party certifications and third-party or internal audit reports made available by CSPs can be used as well.

Practical and Legislative Countermeasures

Deutsche Börse, a German international exchange organization and market infrastructure provider, initiated the Collaborative Cloud Audit Group in 2017. This industry wide initiative carries out audits of CSPs collectively, reducing the workload for all parties involved.[15]

ENJOYING THIS ARTICLE?

- Read *Cloud Fundamental Study Guide. www.isaca.org/emerging-tech-cloud*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

In 2021, the European Cloud User Coalition was founded by 12 European financial institutions. The coalition's goal is to promote the use of public cloud systems in the European financial services realm.[16] Financial institutions represented in the coalition have been developing common security standards and best practices for CSPs.

Institutions are using pooled audits by a group of auditors from different organizations and creating standard rules (self-regulation). Cloud customers must obtain regular evidence from the CSP that the agreed-on security requirements are being met. The proof should be based on a recognized set of rules such as ISO/IEC 27001:2022, which is commonly used in the financial services industry for information security management systems (ISMSs);[17] ISO/IEC 27002:2022, which is used for information security controls;[18] and ISO/IEC 27018:2019, which is used for the protection of personally identifiable information (PII) in public clouds acting as PII processors.[19] In Germany, one well-known and comprehensive set of security criteria for cloud services is the Cloud Computing Compliance Controls Catalog (C5).[20]

The cloud customer must check whether the scope and protection requirements cover the period the cloud services were used. If a CSP uses subcontractors, it must regularly demonstrate to the cloud customer that the subcontractors perform necessary audits.

Simultaneously, risk related to the concentration of the CSP market keeps growing. As **figure 4** illustrates, a few enterprises host an enormous amount of the world's data by market size. This raises concerns. In response, the European Commission proposed DORA, under which third-party service providers of critical information and communication technology (e.g., CSPs) will be supervised by an authority called the lead overseer.[21]

Outlook on Cloud Computing, Innovation and Regulation

In the early days of cloud computing, one of the main arguments against its use was the need for data security and protection. In compliance, there are still lively discussions regarding the use of virtualized computing resources. Outsourcing data streams requires caution regarding data security and protection. Looking at empirical public data to assess the comprehensive status quo, one might ask how the Ukrainian government was able to access and use computing resources containing sensible data during the Russian invasion in 2022. Ukrainian law mandated that certain government data and specific private-sector data be kept on servers physically situated in Ukraine. One week prior to the Russian invasion, the Ukrainian parliament introduced regulations allowing the transfer of public- and private-sector data to the cloud. Furthermore, the Ukrainian government issued a public plea for assistance to achieve that. One of the first entities to respond was AWS, the enterprise that accounted for 32 percent of the worldwide cloud services market in Q3 2022.[22]

The growing market shares of a few dominant CSPs go hand in hand with increasing risk.

Today, cloud computing happens mostly in individual data centers that provide access to servers. However, this trend may change. The growing market shares of a few dominant CSPs go hand in hand with increasing risk. A high degree of dependence on these providers exists. A CSP's unavailability, failure or some other event might endanger the soundness of a financial entity, and, ultimately, the entire financial system might be at risk of not delivering critical functions or at risk of other adverse effects including large losses and even bankruptcies.

Although it is possible to use multiple servers, traditional cloud services are centralized. The resources are hosted by one large entity that controls all the data and applications of its customers.

Numerous threats and vulnerabilities exist that can jeopardize the integrity of cloud-stored data.[23] Microsoft admitted that it unintentionally exposed information in business transactions with potential clients in October 2022 due to a misconfigured storage server (confidentiality threat). It attempted to minimize the seriousness of the leak, despite reports from a cybersecurity firm that 65,000 entities, many of them enterprises, had been affected by the exposure.[24] In the case of outages, the higher the dependence, the greater the loss. Numerous enterprises host their websites and store other data in data centers operated by one of the big three CSPs. In past years, multiple outages have occurred, during which data and services could not be accessed (availability threat).[25]

Therefore, CSPs must guarantee their confidentiality, integrity and availability. For example, a bank customer's

personal data can be leaked due to misconfigured servers (confidentiality threat) or know-your-customer (KYC) data can be altered or deleted due to weak identity and access management (integrity threat). A multilateral trading facility offering financial instruments via a web browser might suddenly realize no transaction fees due to the inaccessibility of its centralized hosted services (availability threat). Clearly, dependence on a CSP comes with risk.

To safeguard individuals' personal data against privacy violations, the European Union introduced the General Data Protection Regulation (GDPR). GDPR is comprised of three major components: data subject, data controller/joint controller and data processor. When a user has no direct control over the stages involved in data processing, GDPR assigns a shared duty to the processor instead of to the controller or joint controller. For instance, to comply with GDPR, an Infrastructure as a Service (IaaS) provider that offers a managed hosting service to users is responsible for processing the data generated by that infrastructure (e.g., recording and managing system and access logs). Before engaging in an activity involving personal data, actors are required to fulfill several requirements. The following conditions must be met before data can be stored: customer consent must be obtained, data must be encrypted, data must be erasable at any time and the retention term must be shorter than the total time required for all data activities.

It has become difficult to verify compliance with these GDPR requirements in a formal or automatic manner. Moreover, breaches occur in practice. In July 2021, the Luxembourg National Commission for Data Protection issued a decision against Amazon Europe Core. It found that Amazon's processing of personal data did not comply with GDPR. The commission imposed a fine of €746 million and corresponding practice revisions.[26]

Financial institutions are obliged to control their outsourced enterprises. A supplement to ISO/IEC 27001, the first global code of practice for cloud privacy, was adopted in 2014 (ISO/IEC 27018:2014), and the latest version was published in 2019.[27] Based on EU data protection rules, the standard provides CSPs operating as processors of personally identifiable information (PII) with detailed guidance on risk assessment and the implementation of adequate and effective safeguards to protect PII.

According to **figure 4**, the largest ecommerce platform (Amazon) accounts for roughly one-third of the cloud market worldwide. Therefore, conflicts of interest may exist with AWS's other market segments.

Oligopolistic markets, such as the cloud industry, could be complemented with decentralized services using DLT.

On the other hand, the evolution of decentralized services using DLT as a governance technology can be observed:

> *If blockchains are a new way to implement trusted transactions without trusted intermediaries, soon we'll end up with intermediary-free trust… Intermediary-controlled trust came with some friction, but now, with the blockchain, we can have frictionless trust.*[28]

This can give rise to a novel technology-driven organizational incentive model in which the benefits are shared equally between the data owners and the innovators—that is, the developers of applications and the operators of platforms. DLT aids deplatforming by partly redistributing power from centralized Big Tech to be more decentralized.[29] Oligopolistic markets, such as the cloud industry, could be complemented with decentralized services using DLT.

A decentralized system is a subset of a distributed system. The term decentralized means there is no single point in a decision-making process. Every network node decides its own behavior and the resulting system behavior is an aggregate response. The term distributed means the processing is shared across multiple nodes, but the decisions may still be centralized and use complete system knowledge.[30] This idea can be applied to decentralized cloud storage to gain an understanding of how the cloud market might further evolve. The cloud market can be distributed and decentralized by pooling (free) computing resources of individuals using DLT to create a storage network with no single network-based point of failure.[31] The network can host applications and websites with complete redundancy and provide numerous server resources for the demanding entity. This architecture has no single point of failure and is geographically distributed. When a network node is compromised by an attacker, a new node can be created automatically so that attacks are rather ineffective. Nodes span the network, like servers do in legacy centralized systems. In a decentralized

As technology has become a strategic consideration, financial institutions must monitor disruptive technologies and keep amending their product portfolios and internal processes.

model such as this, an incentive for these network nodes is required for them to provide computing capacity to the network. Just like in the traditional cloud sphere, operational costs (e.g., the costs of building and operating data centers and administering networks) are paid by customers. Therefore, node operators in a decentralized model receive monetary compensation.

Instead of hosting data within one central data center or even on site, DLT offers the possibility of a decentralized and thus lower-risk form of data storage based on thousands of geographically distributed nodes. Geolocating features can be used to select the geographic positions of network nodes, taking into consideration the regionally varying regulatory requirements. Individual nodes store only fragments of data, without read and write rights (data protection). Encryption techniques are used to ensure that data can be processed and read only by the intended recipients and to prevent any changes to or manipulation of the data.

As can be seen, DLT created an innovative ecosystem. The first commonly known use case of DLT is cryptoassets (e.g., bitcoin). The regulation around this new asset class has become dynamic, as can be illustrated by the EU Markets in Crypto-Assets (MiCA) regulation, which is based on the need to provide investors with necessary protection while maintaining financial market integrity and the stability of the financial system. As MiCA demonstrates, it is feasible to regulate DLT-based applications and services rather than try to regulate the technology itself.[32]

As soon as decentralized cloud infrastructure emerges to a sufficient degree, new approaches to regulating these service providers in the context of financial services will be needed. This is due to the industry's technology-based characteristics, especially decentralization and distribution.[33]

Until its bankruptcy filing and alleged fraudulent activities in November 2022, FTX was a cryptocurrency exchange. The downfall of FTX may stimulate financial supervisors to create further legal rules in the financial DLT sphere, especially regarding risk management and IT security.[34]

Any use of a third party implies counterparty risk. The alleged fraudulent activities by FTX and affiliated entities could have been technologically protected through the use of DLT, as it is possible to store and securely manage crypto assets.

Best Practices

The development of digital economies centered on the creation, gathering and safeguarding of information and data is ongoing. New markets and business opportunities are made possible by disruptive technologies such as cloud computing. This is notably true for the banking industry. However, as data become an indispensable asset and a key competitive differentiator, this process is also escalating competitive, regulatory and cybersecurity concerns. Therefore, the practical suggestions targeting the issues around cloud computing include:

- Management should evaluate a hybrid and multicloud approach to address dependency risk. Dependency assessments and exit scenarios must be regularly reviewed.
- In the financial realm, IT systems, IT processes and other components of the information network must ensure the integrity, availability and confidentiality of data. For these purposes, the IT system and process design must be based on common standards. Regarding outsourcing agreements, internal audits are required regularly to evaluate audit reports based on recognized standards (e.g., C5:2020, ISO/IEC 27018:2019). At all times, financial institutions must be in control of their outsourced service providers, including subcontractors. If concerns are identified, internal audit teams must perform further examinations.
- In any case, sole reliance on audit reports is insufficient. Corresponding institutional controls must be in place, and they must be adequate and effective. Some audit reports, such as the C5:2020, do describe corresponding controls. The client needs to check for these and they should likely be complemented by other controls.
- EU-based financial institutions and CSPs serving these institutions are advised to undergo a health check regarding their compliance status under DORA.
- As technology has become a strategic consideration, financial institutions must monitor disruptive

technologies and keep amending their product portfolios and internal processes as needed.

Conclusion

The emergence of new technology, new players and advantageous regulatory regimes has influenced Europe's financial industry. Financial technology firms (fintechs) have created new services and altered how enterprises interact with clients to meet their financial needs. One major disruptive force has been cloud computing technology, as its evolution has led to dynamic regulatory guidance.

Cloud computing offers many advantages. IT services can be used on demand, those services are scalable and flexible, and they can be billed according to the range of functions, duration of use and number of users, if required. The specialized knowledge and resources of the CSP can also be accessed, freeing internal resources for other tasks. In addition to processes, banking products can be innovated through cloud services.

However, in practice, the expected benefits of cloud use do not always materialize. One common reason is that critical success factors are not sufficiently considered in the run-up to procurement of the cloud technology.

It is evident that along with the benefits of cloud computing, there is risk. Specifically, dependence on the leading CSPs has grown significantly in recent years. In parallel, the regulation of cloud services in the financial sector is increasing, as DORA illustrates. Under the rule, CSPs are obligated to grant their customers in the financial sector—and their competent authorities—full access, information and audit rights. Soon, the so-called lead overseer will be the European Union's new watchdog, monitoring CSPs to ensure the stability of financial markets and maintain consumer protection.

Open banking and DLT provide complementary use cases built on cloud computing, and financial institutions are likely to advocate DLT due to possible efficiency and innovation gains. DLT-based cloud computing enables enterprises to minimize the risk of dependency. Because there is no single point of failure, single network nodes do not have read and write rights on the data stored in a Blockchain-as-a-Service (BaaS) database. With these new products for lower pricing, cloud computing may be complemented by actors from the DLT sphere.

It is arguable whether the technology itself—like the Internet—needs to be regulated from a financial oversight standpoint. Nevertheless, regulation that permits and fosters open and permissionless relationships is necessary for innovation to flourish in financial markets, and innovation is key to revenue.

Regulation that permits and fosters open and permissionless relationships is necessary for innovation to flourish in financial markets, and innovation is key to revenue.

Through open banking, the financial system is accessible to third-party providers, and its adoption is likely to increase. Therefore, the requirements for outsourcing management will continue to be the focus of supervisory authorities for ensuring stable financial markets while favoring consumer protection.

Endnotes

1 Statista, *Cloud Computing Dossier*, Germany, 2022, *https://www.statista.com/study/15293/cloud-computing-statista-dossier/*
2 *Ibid*.
3 *Ibid*.
4 Statista, *Marktanteile der führenden Unternehmen am Umsatz im Bereich Cloud Computing weltweit im 3*, Quartal 2022, Germany, 2022, *https://de.statista.com/statistik/daten/studie/150979/umfrage/marktanteile-der-fuehrenden-unternehmen-im-bereich-cloud-computing/*
5 Throughout this article, the term banking is used to represent a broad variety of financial services.
6 IDW Verlag, Kreditinstitute, *Finanzdienstleister und Investmentvermögen*, Germany, 2020
7 Kassab, M.; P. Laplante; "Trust Considerations in Open Banking," *IT Professional*, vol. 24, iss. 1, 2022, p. 70–72
8 Heckel, M.; F. Waldenberger (Eds); *The Future of Financial Systems in the Digital Age: Perspectives From Europe and Japan*, Springer, Singapore, 2022
9 Gramlich, V. et al.; "Decentralized Finance—The Rise of a New Paradigm?" REthinking Finance, vol. 6, 2022 p. 30–40
10 Veeam Software, *2022 Data Protection Trends Report*, Switzerland, 2022, *https://go.veeam.com/wp-data-protection-trends-2022*

11 European Banking Authority (EBA), *Consultation Paper: EBA Draft Guidelines on Outsourcing Arrangements*, France, 22 June 2018
12 European Banking Authority (EBA), "Recommendations on Outsourcing to Cloud Service Providers," 20 December 2017
13 *Ibid*.
14 Hashemi, J. B.; A. Yavuz; D. Akdeniz; J. Putters; "Pooled Audits on Cloud Service Providers, Part 1," *de IT-Auditor*, 11 May 2020, *https://www.deitauditor.nl/wp-content/uploads/2020/03/pooled-audits-on-cloud-service-providers.pdf*
15 Deutsche Börse Group, "Deutsche Börse and Microsoft Reach a Significant Milestone for Cloud Adoption in the Financial Services Industry," 6 May 2019, *https://deutsche-boerse.com/dbg-en/media/press-releases/Deutsche-B-rse-and-Microsoft-reach-a-significant-milestone-for-cloud-adoption-in-the-financial-services-industry-1540058*
16 European Cloud User Coalition (EUCU), "Why Did We Form a Coalition?" *https://ecuc.group/about-us/*
17 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*, Switzerland, October 2022, *https://www.iso.org/standard/82875.html*
18 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection—Information security controls*, Switzerland, February 2022, *https://www.iso.org/standard/75652.html*
19 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27018:2019 *Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, Switzerland, January 2019, *https://www.iso.org/standard/76559.html*
20 Amazon Web Services (AWS), "Cloud Computing Compliance Controls Catalog (C5)," *https://aws.amazon.com/compliance/bsi-c5/*
21 European Council of the European Union, "Digital Finance: Digital Operational Resilience Act (DORA)," 28 November 2022, *https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/*
22 Data Center Dynamics, "Ukraine Awards Microsoft and AWS Peace Prize for Cloud Services and Digital Support," 7 July 2022, *https://www.datacenterdynamics.com/en/news/ukraine-awards-microsoft-and-aws-peace-prize-for-cloud-services-digital-support/*
23 Kaya, D. et al.; "Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques," *International Journal of Research Publication and Reviews*, vol. 3, iss. 2, 2022
24 Kan, M.; "Microsoft Leaks Business Customer Data via Misconfigured Storage Server," *PC Mag*, 19 October 2022, *https://pcmag.com/news/microsoft-leaks-business-customer-data-via-misconfigured-storage-server*
25 Gunawi, H. *et al*.; "Why Does the Cloud Stop Computing? Lessons From Hundreds of Service Outages," Proceedings of the Seventh ACM Symposium on Cloud Computing, October 2016
26 DataGuidance, "International: CNPD Imposes €746M Fine on Amazon for Targeted Ad System," 30 July 2021, *https://www.dataguidance.com/news/international-cnpd-imposes-746m-fine-amazon-targeted-ad*
27 *Op cit* ISO/IEC 27018:2019
28 Mougayar, W.; *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley and Sons, USA, 2016
29 Flux, XDAO, *https://runonflux.io/xdao.html*
30 Eagar, M.; "What Is the Difference Between Decentralized and Distributed Systems?" *Medium*, 4 November 2017, *https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462*
31 Krishnaraj, N. *et al.*; "The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions—Challenges, Opportunities, and Standards," Blockchain Security in Cloud Computing, Springer, Switzerland, 2022
32 Beck, B.; J. C. Schmike; M. Hörauf; P. Scholl; "EU Markets in Crypto-Assets (MiCA) Regulation Expected to Enter Into Force in Early 2023," Mayer Brown, 14 December 2022, *https://www.mayerbrown.com/en/perspectives-events/publications/2022/12/eu-markets-in-crypto-assets-mica-regulation-expected-to-enter-into-force-in-early-2023*
33 De Filippi, P.; A. Wright; *Blockchain and the Law*, Harvard University Press, USA, 2018
34 Smith, T.; "What Is FTX?" Investopedia, 22 December 2022, *https://www.investopedia.com/ftx-exchange-5200842*