Legal high Committee for
Financial markets of Paris

EXCERPTS FROM THE REPORT ON CLOUD BANKING: STATE OF PLAY AND PROPOSALS

Legal High Committee for
Financial markets of Paris

May 2021

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

REPORT ON CLOUD BANKING: STATE OF PLAY AND PROPOSALS OF THE LEGAL HIGH COMMITTEE FOR FINANCIAL MARKETS OF PARIS

Given the popularity of cloud computing technology[1] and the challenges that its use entails for the financial industry, including the banking sector, the *Haut Comité Juridique de la Place financière* de Paris (HCJP) took up this topic and, in February 2020, created a working group[2] to analyse such phenomenon in the light of the current architecture of the rules applicable to the banking sector in terms of prudential and supervisory matters. Initially focusing on issues relating to the contractual power relationship between users (banks) and providers of this technology (IT providers), the working group considered the forthcoming changes to the European legislation in the context of the European Commission's new digital finance strategy for the EU financial sector[3], and the package of measures implementing such strategy. Amongst those measures, the working group identified the draft European regulation on digital operational resilience of the financial sector (DORA), which is currently being discussed within the Council,[4] as partly addressing the main issues raised by the use of the cloud technology by banks and therefore allocating its efforts on the analysis of this draft regulation.

The working group is well aware of the limited nature of the exercise it has undertaken so far.

Firstly, the analysis was carried out from the sole perspective of the banking sector and therefore does not take into account the views of other participants in the financial sector in a broader sense (such as investment firms, asset managers, insurance companies, etc.), who are also subject to, as «financial entities»,[5] DORA, it being specified, moreover, that such draft regulation is not confined to cloud services, but covers wider information and communication technology (ICT) services.

Secondly, this report does not address the provisions of the regulation related to the operational resilience of financial entities, which are one of its pillars.

---

[1] *See the definition of Cloud in Annex 2.*

[2] *The composition of the working group is set out in Annex 1 to the French version of the report.*

[3] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a digital finance strategy for the EU of 23 September 2020, COM(2020) 591.*

[4] *At the time this report was drafted, under the Portuguese presidency (https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0595).*

[5] *See in this respect the contributions of stakeholders from the different financial services industries received by the European Commission with regards to the draft DORA regulation.*

Finally, as relevant as it may be, the draft regulation DORA does not address all the issues raised by the use of Cloud (and more generally, of ICT) by financial sector participants, as those are described in this report (see Section 1 (*Issues related to Cloud banking*)).[6] Other legal instruments in force and draft legislations currently pending examination aim, more specifically, to address those issues (such as the NIS directive[7], which is currently being reviewed[8], the legislations GDPR, as well as the draft regulations «Digital Services Act»[9] and «Digital Market Act»[10]).[11] The working group wished to focus its efforts on the draft regulation DORA considering the relevance of the issues it contemplates in the light of the analysis carried out by the working group and described at the beginning of this introduction. Consequently, the working group has not, for the time being, undertaken out a detailed analysis of these legislations or legislative proposals.[12]

After discussing the concerns raised by the use of the Cloud in banking sector (Section 1 (concerns raised by the use of the Cloud in the banking sector)) and describing the existing regulatory framework (Section 2 (The apprehension of the Cloud by the banking regulation: between fragmentation and heterogeneity)), this report details the challenges that institutions are facing today in their

---

[6] *In particular, issues related to the oligopolistic structure of the market for the provision of cloud services, the extraterritoriality of US procedural and repressive legislation and the EU's data protection sovereignty, and finally, IT security.*

[7] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Directive on Network and Information Security, or «**NIS Directive**»). This Directive sets out a series of requirements relating to network and information security (including cyber security) which apply to «Digital Service Providers» (DSPs) and «Operators of Essential Services» (OES). This directive notably concerns companies in the energy, transport, banking, financial markets, health, drinking water distribution and digital infrastructure sectors. It was implemented in France by law no. 2018-133 of 26 February 2018 related to various provisions for adapting to European Union law in the field of security, the implementing decree no. 2018-384 of 23 May 2018 relating to the security of networks and information systems of operators of essential services and digital service providers, the ministerial order of 13 June 2018 setting out the procedures for reporting incidents and, finally, the ministerial order of 14 September 2018 setting out the security rules and deadlines referred to in article 10 of decree no. 2018-384 of 23 May 2018 on the security of networks and information systems of operators of essential services and digital service providers.*

[8] *https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union; proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS II).*

[9] *Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020 (COM(2020) 825 final et 2020/0361 (COD)).*

[10] *Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020 (COM(2020) 842 final et 2020/0374 (COD)).*

[11] *Many other legislatives instruments are in preparation. See for example: E. Jouffin, La convergence des préoccupations dans la divergence des moyens, Banque & Droit n° 196 mars-avril 2021, p. 4, which refers to a «regulatory hubbub».*

[12] *Furthermore, it should be noted that the European Commission has completed its work on IT resilience specifically in the financial sector with the publication, on 24 September 2020, of a new draft directive: proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 (COM(2020) 596 final), which aims, in particular, to ensure consistency between the above-mentioned directives and the DORA Regulation.*

relationships with ICT Providers. As such, this report provides a synthetic critical analysis of certain the provisions of the draft regulation DORA and makes amendment proposals (Section 3 (Towards a new regulatory paradigm for IT outsourcing in the financial sector: the DORA Regulation)).

SUMMARY OF THE CONCLUSIONS OF THE WORKING GROUP

Section 1: concerns raised by the use of the Cloud by the banking sector

The Cloud is an IT organisation and management tool for companies that allow them to remotely access and use standardised digital services provided by information communication technology service providers. The Cloud technology enables these services providers to provide to their customers infrastructure, IT platform, application and software services. It has gradually been deployed in the global banking and financial sector, initially for back office and support functions, then marginally in core banking business services and operations, in conjunction with the emergence of neo-banks and open banking market participants, where such technology has a growing role in the customer experience. The result is an irreversible trend towards the digital transformation of banks using cloud solutions and the resulting benefits for both banks, in terms of managing their technical resources, and customers.

However, their large-scale deployment at the very heart of banking and financial businesses, which involves transmitting sensitive customer information and data to unsupervised third parties, comes up against a number of difficulties that highlight the growing dependence of banks on a small number of Cloud Providers, mainly American and Asian, to whom regulations of the banking sector do not apply, by definition. Thus, the oligopolistic structure of the Cloud market, coupled with the technological dependence of banks on the expertise of Cloud Providers, leads to a deep interconnection with the entire financial system and is likely to reverse the traditional bargaining power between the customer and the service provider. This concentration of phenomenon in the Cloud market also highlights the existence of risks of anti-competitive behaviour in digital markets. Several reforms on competition law in this respect have been initiated or are being discussed in the various territories concerned: the European Commission recently published the Digital Services Act and the Digital Market Act which aim to ensure a fair competitive environment in the digital services sector.

As mentioned above, the main Cloud Providers are not European. Though, the fact that they are subject to third country legislations raises questions on the application of foreign legal or regulatory provisions, this is particularly the case of American ones such as the CLOUD Act, which conflicts with EU law or that of its Member States, such as notably the General Data Protection Regulation (GDPR) or, in France, the blocking law of 1968 or the banking secrecy. This observation raises several strategic concerns, particularly in terms of controlling access to, and the use of, data and preserving their confidentiality, security and integrity, but also, more generally, in terms of IT

security. In practice, there is traditionally a risk of data capture for the purposes of «intelligence» activities legitimised by the application of extraterritorial regulations.

Finally, another inevitable consequence of the high concentration of Cloud Providers is the introduction of an uneven contractual bargaining power, not only because of commercial issues, but mostly because of the outsourcing of critical or important functions to these providers. Whereas the absence or failure to comply with certain contractual provisions set out in outsourcing contracts for essential or material operational services or other tasks exposes banks to the risks of administrative sanctions risk, or liability, in particular regarding their clients. Conversely, Cloud Providers, generally as most bank subcontractors, are not subject to the rules imposed on the banking sector.

These observations point to the deficiencies of the contractual relationships framework between banks and their Cloud Providers and, more generally, the limits reached by the banking regulations currently in force.

Section 2: how the banking regulation is taking Cloud into account?

Concerns around Cloud outsourcing services related to banking activities – though not only banking activities – has prompted reactions from supervisors, such as the ACPR since the early 2010s, so as to create a specific regime. However, the regulatory approach to this phenomenon, both at a national and a European level, has proved to be incomplete and heterogeneous.

At the European level, the banking supervisor paid attention to the development of outsourcing, which led in Europe to guidelines issued by the Committee of European Banking Supervisors (CEBS), an advisory committee with no regulatory or supervisory powers, and then to recommendations issued by the European Banking Authority (EBA), the European supervisory authority that succeeded the CEBS, which supplemented CEBS guidelines. Such recommendations concerned in particular to the assessment of the critical nature of outsourced activities, the notification to the competent national supervisor of the relevant outsourced activities and the provision of a register of outsourcing arrangements, the location and compliance of data processing, the security of information systems, the consideration of risk management and contractual framework for the outsourcing chain, the contractual implementation of an effective audit right for the supervised institution and the competent authorities with respect to cloud services providers, and finally, the application of business continuity plans and reversibility plans. The specific treatment reserved for the Cloud was however short-lived. Indeed, the EBA finally decided to include Cloud into the general outsourcing regime when developing guidelines on outsourcing, which came into force on 30 September 2019 (the Outsourcing Guidelines).

At the level of the Member States, the regulatory framework remains heterogeneous. In France, there is a legally binding regime for outsourcing banking activities.[13] As of 2013, the ACPR officially addressed the issue of the Cloud through a market consultation, which concluded that the use of certain external IT services should be considered as the outsourcing of essential or important operational services or other tasks falling under the outsourcing regime. In the other Member States, various legal instruments, generally non-binding, have been adopted. More recently, most Member States' supervisors reported to the EBA that they comply with its Outsourcing Guidelines, to the exception of Spain and Poland. However, the regulatory framework of the various Member States governing the use of Cloud by banks remains quite heterogeneous, some being seen more restrictive than others, as noted by the European Commission in its impact assessment ahead of the draft regulation DORA.

As a result, regulating Cloud banking through of critical or important functions outsourcing regulations, while not specific to the European model, has reached its limits particularly in the context of European legal environment. The Outsourcing Guidelines do not indeed give sufficient consideration to the growing role of information and communication technology providers in general (and cloud services providers in particular) and do not reflect the reversal of the balance of power between the bank and its subcontractors.

Therefore, a paradigm shift had to take place: this is at stake with the draft regulation DORA introduced by the European Commission in September 2020, which combines, on the one hand, the existing regulatory framework, in particular the Outsourcing Guidelines, and, on the other hand, the change of approach which aims to subject these providers to the surveillance of a financial supervisor.

Section 3: towards a new regulatory paradigm for digital outsourcing in the financial sector: the draft regulation DORA

The draft regulation DORA (standing for Digital Operational Resilience Regulation) provides harmonised requirements aiming at to upgrading and safeguarding the operational resilience of regulated institutions and professionals operating in the banking, financial markets and insurance sectors. In particular, it seeks to address concerns relating to the growing exposure and dependence of regulated professionals towards ICT Providers (including Cloud Providers), the lack of an

[13] *Initially, regulation 97-02, replaced by the Ministerial order on internal control of 3 November 2014.*

harmonised framework for managing ICT-related risks and the inadequacy of the current regulatory framework on outsourcing in view of the imbalance observed in the relationship between these providers and financial entities.

The draft European regulation, which will be directly applicable in the Member States, is based on two pillars:

• the obligations applicable to financial entities dealing with ICT Providers, to be implemented on the basis of a proportionality principle and with a view to managing ICT-related risks; and

• the supervision of ICT Providers established within the EU that are considered as «critical» by the European supervisory authorities, based on specified criteria.

In this respect, the working group sought to highlight the contributions of the draft regulation DORA that are relevant for the purposes of this report and to make recommendations to address the difficulties one comes across in the following areas:

• supervision of critical ICT Providers: conditions relating to the geographical links with the territory of the Union of critical ICT Providers, the determination of their critical nature, and sanctions for breaches by critical ICT Providers;

• adjusting the prohibition for financial entities to use critical ICT Providers that are not established within the EU, notably with respect to the time at which such prohibition becomes effective and the evolution of the critical nature of the ICT Provider;

• exclusion of Intra-group ICT Providers from the scope *ratione personae* of the ESAs oversight and under certain conditions, from the scope of the prohibition from using critical Third Country ICT Providers; and

• strengthening the contractual obligations of ICT Providers.

INTRODUCTION

What is the Cloud?

Plurality of definitions – Cloud computing, which translates into French as «*informatique en nuage*»[14], is defined in various ways by a fairly high number of official bodies, including the following definition «*a method of processing customer data, operated over the Internet, in the form of services provided by a service provider*».[15] This definition further specifies that «*cloud computing is a particular form of IT management, in which the location and operation of the cloud is not made known to customers*».[16] Further definitions are given in Annex 2 to this report.

In other words, the Cloud is a mode of IT organisation and management that allows remote access to, and use of, standardised, automated, virtualised and industrialised/mutualised IT services (software, applications, platforms, infrastructure, storage, *etc.*), which are provided by a Cloud services provider (the «**Cloud Provider**») to several customers, as on-demand services and generally billed on a per-use basis.[17]

As a matter of principle, the Cloud Provider thus provides its customer by means of a subscription, with a range of IT resources/services including, generally:

• the provision of an IT infrastructure (a fleet of machines, servers for data storage, *etc.*);

• the provision of a platform for the development and use of digital tools (computer applications, *etc.*) belonging to the client but whose production and operating resources are hosted by the Cloud Provider;

• according to an extended approach, the provision by the Cloud Provider of a tool (software, application, etc.) and associated ready-to-use services (corrective and evolutionary maintenance of the tool, hosting of the tool, *etc.*).

---

[14] *For ease of reference, the term «**Cloud**» will be used in this report and not «cloud computing».*

[15] *Opinion of the Commission générale de terminologie et de néologie published in the Journal Officiel de la République Française (JORF) of 6 June 2010, Vocabulaire de l'informatique et de l'internet, NOR: CTNX1012892X.*

[16] *Same reference as above. Definition taken from the US National Institute of standards and technology (NIST) (https://csrc.nist.gov/publications/detail/sp/800-145/final).*

[17] *In other words, the Cloud is an «advanced form of outsourcing, in which the client or user has an online service which administration and operational management are carried out by a subcontractor. Cloud Computing is also characterised by on-demand billing and almost immediate availability of resources» (Revue Communication Commerce Électronique, La définition des contours juridiques du Cloud Computing, Granrut law firm, November 2012).*

The customer accesses these services,[18] both on demand, and remotely, through an extended digital network, such as the Internet.

Standardisation in the absence of a normative framework – The Cloud is currently not subject to any specific legislative and/or regulatory framework, whether at an international, regional and/or national level.[19]

However, the international standards committees which are the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) have designed three Cloud specific standards including, in particular, ISO/IEC 17788:2014 «Information technology – Cloud computing», which provides an overview of and defines the vocabulary applicable to, Cloud services. In particular, such standard conceptualises the various services layers, namely: software (or application) as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS). It also specifies the terminology for cloud deployment models, including a distinction between public and private Clouds.[20]

The national standardisation body, AFNOR, issued several standards in this respect in 2014 and the National Agency for Information Systems Security (ANSSI) published a set of requirements applicable to Cloud Providers in 2016.[21]

These standards are not legally binding, notably with regard to Cloud Providers, and compliance with such standards is therefore voluntary for the market participants. However, in practice, they seem to be gaining ground in terms of concepts and descriptions of service layers[22] and Cloud models.[23]

The main Cloud models – The adoption of the Cloud as a new technology can occur under three basic models: the private Cloud (which itself can be divided into an internal or external private Cloud), the public Cloud, and finally the hybrid Cloud.

---

[18] We usually speak of «services layers», each layer corresponding to a Cloud service (IaaS, PaaS, SaaS). These different categories of services are detailed below.

[19] See, however, in the area of banking and finance, the opinions expressed by the regulators, which are mentioned below.

[20] The two other standards are: (i) ISO/IEC 17789:2014 «Information technology – Cloud computing – Reference architecture». More technical in nature, it contains diagrams and descriptions that show how the different aspects of the Cloud fit together; and (ii) ISO/IEC 27018:2014 «Information technology – Security techniques – Code of practice for the protection of personally identifiable information (PII) in the public cloud acting as a PII processor».

[21] ANSSI, Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences – Version 3.1 of 11 June 2018 (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf).

[22] See the above footnote 18.

[23] See for example: https://aws.amazon.com/fr/types-of-cloud-computing/ ; https://docs.microsoft.com/fr-fr/learn/modules/intro-to-azure-fundamentals/what-is-cloud-computing.

Briefly, the main features of those three models are as follows:

• the private Cloud corresponds to the implementation of Cloud services by means of an infrastructure dedicated to a user; such infrastructure is assigned for the exclusive use of such user and is located either within such user's premises, with or without the assistance of an external service provider (internal private Cloud), or within the Cloud Provider's premises (external private Cloud).

• Conversely, the public Cloud corresponds to the implementation of Cloud services through an infrastructure shared with several users, customers of the Cloud Provider. Such infrastructure is located in the provider's premises.

• Finally, between those two models, the hybrid Cloud is a combination of the two previous ones. Thus, an infrastructure dedicated to a user that is a customer of the Cloud Provider (private Cloud) and an infrastructure shared between several users that are also customers of the Cloud Provider (public Cloud) coexist.

It should be noted that there are further variations of the Cloud:

• the community Cloud, which is an external private cloud dedicated to several users (customers of a Cloud Provider) operating in the same sector of activity; and

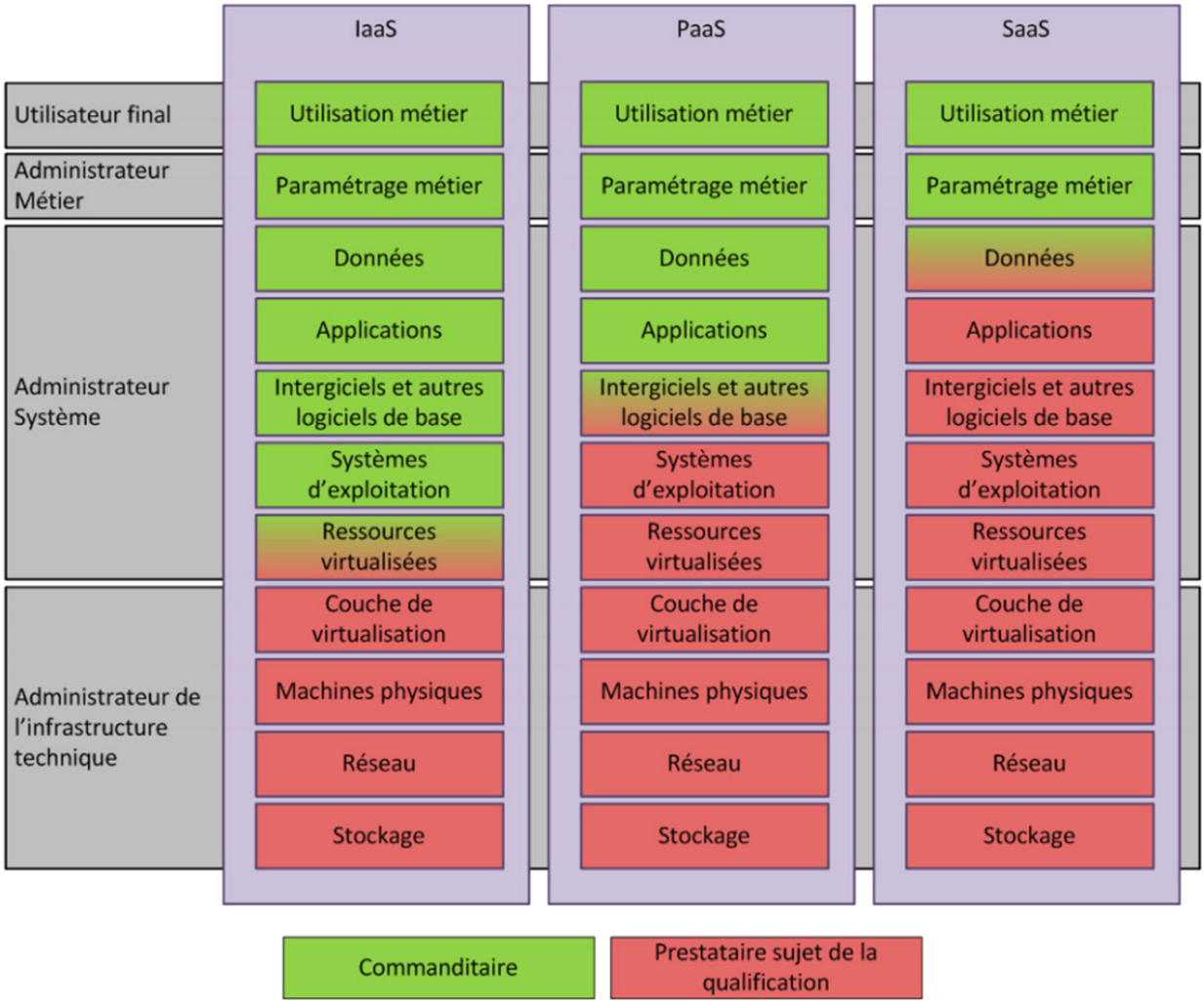
• the sovereign Cloud, which corresponds to a Cloud model «whose data is entirely stored and processed on national territory by an entity under French law and pursuant to French laws and standards».[24] It may be a public cloud, but only if it is provided by a company governed by French law, subject to national law and respecting the conditions of data localisation.[25]

The various «services layers» of Cloud – As earlier mentioned, users standard ISO/IEC 17788:2014 identifies three layers of cloud services tailored to different customer needs, namely IaaS, PaaS and SaaS.

[24] *Information note of 5 April 2016 on Cloud Computing by the Director General of local authorities and the Director of the Archives de France: https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf.*

[25] *It can be noted that the concept of a sovereign Cloud is quite elastic and is not necessarily limited to a national territory. Indeed, it is common to speak of a European Union-wide sovereign cloud, as opposed to cloud services provided by companies in third countries (see for example, J. Henno, Demain, un cloud souverain européen ? Les Echos, 25 January 2021.*

What services/activities exactly do they include? The following diagram[26] is commonly used to illustrate the layers of services that Cloud Providers generally offer.



[26] *Included in the ANSSI document: Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences – Version 3.1 of 11 January 2018 (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf).*

In its study, taken over by the EBF, the Basel Committee applies the above classification to the financial sector:[27]

• Infrastructure as a Service (or IaaS)[28] is the service whereby the Cloud Provider provides its customer with an IT infrastructure (server, storage, backup, and computing capacity, networks, *etc.*), which the customer can use or configure remotely to create its environment. The customer does not need to invest in the acquisition of equipments and resources, which are virtualised and outsourced to the Cloud Provider (and/or the latter's subcontractor(s)) and which the customer rents. However, the customer remains in control of (and responsible for), in particular, its applications, data and their storage, certain network components and the operating system, for which it shall, among other things, provide maintenance.[29]

• Platform as a Service or PaaS[30] includes the services of IaaS but goes further: besides the infrastructure (servers, storage, networks, *etc.*), the Cloud Provider also provides, directly and/or through its subcontractor(s), so-called «middleware» tools (operating system, database, web server, *etc.*). In the context of PaaS, the Cloud Provider makes available to the customer, generally through a lease, an IT environment (platform), within which the customer can develop, create, configure, test and run its own tools (applications, software, *etc.*). The operating system, infrastructure, etc. are the responsibility of the Cloud Provider, while the customer retains full control over the tools

---

[27] *Basel Committee on Banking Supervision, Good practice - Implications of developments in financial technology for banks and banking supervisors, February 2018 and European Banking Federation (EBF), The use of Cloud Computing by Financial Institutions, 4 June 2020, Technical paper. See also, ACP-Banque de France, Les risques associés au Cloud computing, Analyses et synthèses, n° 16, July 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013).*

[28] *For instance: Microsoft Azure.*

[29] *The ANSSI defines IaaS as a «service [which] concerns the provision of abstract computing resources (CPU power, memory, storage, etc.). The IaaS model allows the client to have virtualised outsourced resources. The latter retains control over the operating system (OS), storage, deployed applications and certain network components (e.g. firewall)». (ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – référentiel d'exigences, Version 3.1 of 11 June 2018).*

For the Banque de France, «(the) IaaS (...) offers an IT infrastructure such as computing power, virtual machines including an operating system, storage, backup services» (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, July 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

Sometimes reference is also made (as in the above-mentioned FBE study) to CaaS or Containers-as-a-Service. This is a variant of IaaS. According to Orange Business Services, «CaaS uses the principle of the IT container, which is a unit that brings together the code and configurations of an application. This system allows the portability of applications across networks, storage and servers. Containers allow the pooling of computing resources at the level of code libraries in order to deploy applications more quickly. When applied to the cloud, the use of containers optimises the multi-site scaling and orchestration of applications hosted on a cloud infrastructure.»

[30] *Example: IBM Blockchain Platform (IBM).*

(applications, software, etc.) that it installs, configures and operates on the platform.[31]

• Finally, Software as a Service or SaaS is the service best known to the general public.[32] The Cloud Provider provides the customer, generally through a lease, with: (i) tools (software, applications, *etc.*) that it hosts directly in its information system on a platform (that includes all hardware, servers, networks, set up and operated directly by the Cloud Provider, to ensure hosting), or indirectly through its subcontractor(s) and which are accessible and usable remotely (via the Internet, *etc.*) by the customer; and (ii) related ready-to-use services, such as maintenance (corrective and evolutionary) of tools, hosting of tools, *etc.* and which are provided by the Cloud Provider and/or its subcontractor(s).[33]

It should be noted that there are other services included in the Cloud, such as the service of providing a virtual desktop or hosted virtual desktop (Desktop as a Service or DaaS)[34], whereby the Cloud Provider allows the customer, usually by means of a subscription, to access a virtual office remotely (via the Internet, *etc.*). «*(T)he DaaS consists of offloading the management and delivery of working environments (but sometimes also applications) to the (c)loud*».[35]

---

[31] *The ANSSI defines «PaaS» as a «service [which] concerns the provision by the provider of application hosting platforms. The client does not have control over the underlying technical infrastructure, which is managed and controlled by the service provider (network, servers, OS, storage, etc.). However, the client has control over the applications deployed on this platform. He may also have control over certain services that make up this platform or certain configuration elements depending on the distribution of roles defined in the service. Example: applications in containers managed by an orchestration tool» (ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – référentiel d'exigences, Version 3.1 of 11 June 2018).*

The Banque de France states that «(t)he PaaS (...) provides an integrated development and/or execution platform, based on a catalogue of components softwares and standardised techniques whose underlying infrastructure is transparent to the user» (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, July 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

[32] *Example: Office 365 (Microsoft).*

[33] *The ANSSI defines «SaaS» as a «service [which] concerns the provision by the provider of applications hosted on a shared platform. The client does not have control over the underlying technical infrastructure. The service provider manages all technical aspects requiring IT skills in a transparent manner for the client. The client retains the possibility of making a few business settings in the application. Examples: CRM, collaborative tools, messaging, business intelligence, ERP, etc.» (ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – référentiel d'exigences, Version 3.1 of 11 june 2018).*

For the Banque de France, «(t)he SaaS (...) is an application solution responding to a precise field of use supporting a business function (customer relationship management, financial management, etc.) or a cross-functional service (messaging, collaborative tools, etc.).» (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, July 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

[34] *Dominique Filipopone, DaaS ou la virtualisation du poste de travail dans le cloud, Journal du Net, 1st September 2001 (https://www.journaldunet.com/solutions/cloud-computing/1091879-daas-ou-la-virtualisation-du-poste-de-travail-dans-le-cloud/).*

[35] *Dominique Filipopone, DaaS ou la virtualisation …, op. cit.*

«Banking» Cloud

Over the last ten years or so, the Cloud gradually became established in the global financial sector, thanks to the advantages offered by this new form of IT management which favours access to technological innovation, performance and security (speed, flexibility, volume, energy capacity, *etc.*[36]), while rationalising resources, expertise and costs for users. The assessment of these advantages is a matter for the strategy of each category of actor, it being specified that the deployment models for the Cloud allow this technology to be adapted to the needs of users.[37]

The Cloud emerged as a key technology to enable the digitalisation of the financial sector, especially in the banking one. This technology has proven to be an accelerator, and even an emulation factor, for small/medium-sized incumbent firm as well as for new intrants in the banking sector, such as fintechs and neo-banks, which find in it a means of deploying a range of digital banking and financial services in a very limited time to market. This agility is made possible for these types of companies mainly by using Cloud Providers (private, external and/or public), whereas large incumbent banking groups approached this new technology in a cautious way by making it cohabit with legacy IT infrastructures.[38]

The progressive movement of major banking groups towards the Cloud, particularly hybrid, has been confirmed over the years but concerns mainly so-called «support» functions (such as human resources management, communication, *etc.*) and only marginally «core business» functions (such as account management services and the issuing and management of associated means of payment, granting of credit, *etc.*).[39] Nevertheless, new strategies are emerging, such as those initiated in July 2020 by two major European banking groups, which decided to house their banking activities in a public cloud.[40]

In view of the growing use of the Cloud by the banking sector and the challenges related to such use, particularly regarding control over the storage, access and use of data relating to the bank's «core

[36] *Lamy Droit du Numérique, Lamy Pratique, Éditions Wolters Kluwer, May 2015 : «Cloud Computing was born from the observation that many servers in the world are not used to their full capacity and that the company's needs in terms of power and storage capacity can vary over time. Cloud Computing therefore consists of pooling these servers and considering the computing and storage power of the servers as electricity».*

[37] *La Tribune, Pourquoi les banques cèdent aux sirènes du «cloud», 1st July 2019. See in 2011, l'Agefi, L'informatique dématérialisée à l'essai dans les banques françaises, 3 March 2011.*

[38] *Le Cahier Techno, Cloud computing: de l'expectative à la mise en pratique, Revue banque n°748, May 2012.*

[39] *Le Cahier Techno, L'heure du Cloud public a-t-elle sonné pour les banques françaises ?, Revue Banque n° 835, September 2019.*

[40] *Les Echos, Après Deutsche Bank, HSBC s'allie avec un GAFA pour se déployer sur le Cloud, 18 July 2020 ; Les Echos, Cloud bancaire : les banques européennes avancent leurs pions, 22 July 2020.*

business», along with risks associated with cybercrime[41] and technological sovereignty concerns, the *Haut Comité Juridique de la Place financière de Paris* (HCJP) decided to carry out this study.

It focused solely on credit institutions within the meaning of article L. 511-1 of the French monetary and financial code (for the sake of convenience, the term «bank» will be used indistinctly). Consequently, this study does not touch on other types of regulated institutions in the banking sector (in particular, financing companies, payment institutions and electronic money institutions), nor does it look at firms that are subject to other sector-specific regulations in the broader financial sector[42] (such as investment firms, asset managers, insurance and reinsurance companies, *etc.*), although issues concerns raised by the use of the Cloud are relevant to them[43], notably in the context of financial sector groups that include companies subject to those regulations.

For the purposes of the analysis, we will therefore use the term «Banking Cloud» in a generic way in this report to refer to the use of the Cloud (without distinguishing between its different forms)[44] by banks.

No one disputes the irreversible trend of digital transformation of banks by means of Cloud computing solutions and the resulting benefits, both for banks in terms of managing their technical resources, and for customers. However, their large-scale deployment at the very heart of banking and financial businesses,[45] which involves transmitting customer sensitive information and data to unsupervised third parties,[46] comes up against several difficulties that highlight the growing dependence of banks on Cloud Providers, to whom banking sector regulations does not apply.

The topic of outsourcing services related to banking activities to the Cloud – though not only banking activities – has prompted reactions from supervisors such as the ACPR since the early

[41] According to IBM, the financial services industry is the one most affected by cybercrime in 2019, accounting for 17% of attacks, among the 10 most affected industry sectors (consumer, transportation, media, professional services, etc.) in the year. IBM Security, «X-Force Threat Intelligence Index 2020», p. 29 (https://www.ibm.com/downloads/cas/DEDOLR3W).

[42] Such as Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MIFID), Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking up and pursuit of the business of insurance (Solvency II), Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services (PSD) or Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up and pursuit of the business of electronic money institutions (EMD).

[43] As such, see EIOPA's guidelines dated 6 February 2020 on outsourcing to Cloud Providers, as well as ESMA's guidelines dated 3 June 2020 on the same topic.

[44] However, the focus will be on public and hybrid forms of the cloud, as these are the forms that are most likely to generate risks for banks.

[45] Such as the collection of deposits from the public, granting credits, advice and asset management, etc.

[46] Such as their asset situation, their indebtedness, their bank details, etc.

2010s, so as to create a specific regime. More recently, the period of intensified partnerships between banks and Cloud Providers has highlighted the difficulties in the practical implementation of the European regulatory framework, which is now evolving to better address the IT, operational and legal security issues of the banking Cloud.

TOWARDS A NEW REGULATORY PARADIGM FOR IT OUTSOURCING IN THE FINANCIAL SECTOR: REGULATION DORA

HCJP proposals to improve DORA

I- Surveillance of critical ICT providers

1.1 - Description of the issue

1.1.1 - Obligation of establishment within the Union

Article 28(9) of DORA provides a principle of prohibition for financial entities to «*use an IT service provider established in a third country*» which would qualify as critical within the meaning of article 28(2) of the DORA Regulation.[47]

Such providers are those who «*has not set up business/presence in the Union*» according to the definition of «third country IT service provider» set out in article 3(19) of DORA (the «**Third Country ICT Providers**»).[48]

These notions are particularly vague and are not formulated in a legal way. What does the notion of activity mean?

1.1.2 - Contractualisation with the European subsidiaries of critical ICT Providers and submission of the service agreement to EU law

While DORA provides for the obligation to insert those provisions which are referred to in article 27(2) of DORA (see below the proposals set out in paragraph 3.2.4 (Contractual obligations of

[47] *«Financial entities shall not make use of an ICT third-party service provider established in a third country that would be designated as critical under point (a) of paragraph 1 if it were established in the Union.»*

[48] *Article 3(19). See the terms used in the French version, which are not more precise: «un tiers prestataire de services informatiques qui est une personne morale établie dans un pays tiers, et qui n'a pas établi d'activité ou de présence dans l'Union».*

ICT Providers) in this respect), it does not require the service agreement to be entered into through the European establishment of the critical ICT Provider.

1.1.3 - Sanctioning critical ICT Providers obligations

Finally, although DORA provides for a supervisory regime for critical ICT Providers, it is not specific in terms of obligations and sanctions. Indeed, the draft regulation only directly imposes on these providers to communicate information, to allow such ESA acting as lead supervisor to carry out investigations and inspections, to respond to recommendations issued by the lead supervisor following its assessments and, finally, to cooperate in good faith with the lead supervisor[49] if necessary under penalty.[50] However, pursuant to article 37, where recommendations issued by lead supervisors are not implemented by critical ICT Providers, financial entities are responsible for suspending the use of services provided by the providers, or even for terminating the service agreements, at the request of their own supervisors.[51]

1.2 - Proposed changes

1.2.1 - Creation of a European subsidiary

In order to ensure a more effective supervision of critical ICT Providers, it is necessary to impose the creation of an establishment within the Union. There are two possibilities:[52] either a branch or a subsidiary, *i.e.* a company with legal personality. In terms of supervision, the branch has many disadvantages related to the lack of legal personality, starting with its submission to the law of the registered office of the legal person to which it relates, *i.e.*, in the case of main cloud services providers the law of a third country, as well as the absence of its own governance structure.

By way of comparison, a parallel can be drawn with regulation (EC) No. 1060/2009 on credit rating agencies (the «**CRA Regulation**»). This is indeed the choice made by this regulation, according to which only ratings issued by legal persons established in the Union and registered with ESMA can be used for regulatory purposes by regulated entities (such as credit institutions, investment firms, etc.) (articles 4 and 14 of the CRA Regulation).

---

[49] *Articles 30(1) and (3), 32, 33 et 34.*

[50] *Article 30(4).*

[51] *Article 37(3).*

[52] *For example, the NIS Directive refers to the notion of a fixed establishment. See Recital (21): «For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through* ***stable arrangements****. The legal form of such arrangements,* ***whether through a branch or a subsidiary possessing legal personality****, is not the determining factor in this respect». See also Recital (64).*

Therefore, such an establishment should be in the form of a company with legal personality, thus having full legal capacity to bind itself towards third parties and to be accountable for possible breaches vis-à-vis the European supervisor.

1.2.2 - Contractualisation with the European subsidiary and submission of the service agreement to EU law

From the supervisor's point of view, in order to give full effect to the supervision of critical ICT Providers, the provision of their services to financial entities should be governed by agreements that are entered into with the subsidiary established in the Union. Such subsidiary would be fully responsible for the provision of these services, both vis-à-vis its customers, as well as its supervisor and, where appropriate, third parties.

In the same vein, and consistently with GDPR, the agreement for the provision of IT services entered into between the financial entity and the subsidiary of the critical ICT Provider in the Union should be subject to the laws of a Member State of the Union and the jurisdictional clause provided for in this agreement should designate the competent courts of a Member State of the Union.

1.2.3 - Sanctions

A specific sanction regime should be introduced, giving the ESAs competence to impose them (similarly to what the CRA Regulation provides, in terms of competence of the European authorities). These sanctions should be effective, proportionate and dissuasive (similarly to what GDPR (or the IA Regulation) provides).

Furthermore, article 37(3) of DORA should specify that where financial entities terminate contractual arrangements with critical ICT Providers at the request of the competent authorities, such termination shall not give rise to any right to compensation or indemnity of any kind for the financial entity's counterparties.

II- Modification of the prohibition for financial entities to use critical ICT providers established outside the European Union

2.1 - Responsibility for determining the «criticality» of Third Country ICT Providers

2.1.1 - Description of the issue

The combination of articles 28(1), 28(6) and 28(9) of DORA creates some uncertainty as to who will be responsible for determining whether a Third Country ICT Provider is critical or not. Whilst

article 28(1) clearly states that, in the case of an ICT Provider providing services within the EU, this responsibility lies with the ESAs, article 28(9) appears to be much more ambiguous, as it appears to place the burden of assessing the criticality of the provider if it were established in the EU, prior to any provision of services within the EU, on the financial entities.

2.1.2 - Proposed changes

It is proposed to amend the articles 28(1),[53] 28(6)[54] and 28(9)[55] of DORA to include an express reference to Third Country ICT Providers.

2.2 - Status of the contracts concluded with Third Country ICT Providers after the entry into force of the prohibition

2.2.1 - Description of the issue

As the Third Party ICT Service Provider may be considered as critical at any time during the life of the agreement for the provision of IT services that it would have concluded with a financial entity,[56] the relevant financial entity will be obliged to terminate such agreement in order to comply with the prohibition set out in article 28(9) of DORA.

2.2.2 - Proposed changes

It is therefore proposed to amend article 25(8) of DORA, which provides for the situations in which the agreement for the provision of IT services shall be terminated, by adding a new case in which

---

[53] A drafting proposal could be as follows: «1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall:

(a) designate the ICT third-party service providers that are critical for financial entities ***and the ICT third-party service providers established in a third country that would be designated as critical if they were established in the Union****, taking into account the criteria specified in paragraph 2;*

(b) [the remaining provision unchanged].»

[54] A drafting proposal could be as follows: «6. The ESAs, through the Joint Committee, shall establish, publish and yearly update the list of critical ICT third-party service providers at Union level, and ***ICT third-party service providers established in a third country designated as critical.****»*

[55] A drafting proposal could be as follows: «9. Financial entities shall not make use of an ICT third-party service provider established in a third country ~~that would be~~ designated as critical pursuant to point (a) of paragraph 1 ~~if it were established in the Union.~~»

[56] As these contracts are generally concluded for an indefinite period, they are intended to last over time.

the termination takes effect within a year after the financial entity notifies the Third Country ICT Provider of the termination following its classification as a critical provider by the ESAs.[57]

III- Exclusion of intra-group ICT Providers from the scope of the ESAs' surveillance and from the prohibition to use Third Country ICT Providers

3.1 - Description of the issue

Pursuant to the current drafting of DORA, Intra-group ICT Providers («**Intra-group ICT Providers**») that meet the criteria set out in article 28(1) could be qualified as critical and therefore fall under the supervision of ESAs (article 30). Furthermore, the current drafting of the definitions of Critical ICT Providers (article 3(18)) and Third Country ICT Providers (article 3(19)), combined with the prohibition principle discussed above, leads to the conclusion that Third Country ICT Providers that may qualify as critical, and that belong to European financial groups, may also fall within the scope of the prohibition set out in article 28(9).

Subjecting critical Intra-group ICT Providers to such supervision and, where they established in a third country, to this prohibition, does not seem to achieve the objectives of DORA. Furthermore, the prohibition would have harmful consequences for European financial groups that have created infrastructures outside the EU in order to meet specific technological needs that are not necessarily offered in the EU (e.g. access to certain innovations) and security needs (these infrastructures are hosted in entities controlled by these financial groups).

3.2 - Proposed changes

The amendment would therefore exclude any IT services provider, which is a subsidiary wholly owned by a financial group, and which provides its services exclusively within that group, from the scope of the supervisory regime for ESAs set out in article 30 and the prohibition set out in article 28(9).

[57] «***(e) when the ICT third-party service provider is an ICT third-party service provider established in a third country and It has been designated as critical pursuant to point (a) of paragraph 1 of Article 28 and is included in the list referred to in paragraph 6 of the same Article. In such case, the termination takes effect within a year from notice thereof served by the financial entity to the ICT third-party service provider.***»

IV- Contractual obligations of ICT Service Providers

4.1 - Description of the issue

The obligation to include in outsourcing agreements the clauses required by the relevant EBA guidelines exclusively applies to credit institutions. This is also the case in DORA.[58] In order to reduce the difficulties experienced by banks in their negotiations with Cloud Providers as described in this report and to improve the effectiveness of DORA in this regard, it is recommended that ICT Providers should also be required to comply with this obligation.

Moreover, the use of standard contractual clauses should be more strongly encouraged[59], or even required, in the light of what is provided in the GDPR.[60] The provisions of article 27(3) of DORA is very limited in scope in this respect (the parties «*shall consider the use of standard contractual clauses*»), as it implies that the parties are free not to use such standard clauses, as long as they have previously discussed this between themselves.

4.2 - Proposed changes

First, it is therefore proposed to:

Amend article 27(2) of the DORA. This can be done in two ways.

• First approach: to impose a positive obligation notably on ICT Providers (and not only on those deemed critical) to **ensure**[61] that the agreement includes the clauses provided in this article.[62] In this case, it may be noted that the parties should not be able to avoid the application of such obligation by submitting their service agreements to the law of a third country.

---

[58] *Article 25(1): «**Financial entities** that have in place contractual arrangements for the use of ICT services to run their business operations **shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation** and applicable financial services legislation.» To be read in conjunction with Article 27(2) which imposes a list of contractual clauses that must be included in service-level agreements concluded by financial entities.*

[59] *See Recital (55) of the preamble of the DORA Regulation which refers to the European Commission's initiative to develop a set of standard clauses applicable to cloud services.*

[60] *The GDPR provides that the controller or processor may only transfer personal data to a third country or to an international organisation if it has provided appropriate safeguards. These appropriate safeguards may consist in the use of standard clauses adopted or approved by the European Commission (see article 46(5), §(c) and (d)). While the use of such clauses is not imposed (nor is it the only way to provide appropriate guarantees (e.g. an approved code of conduct, a certification, etc.), the text is nevertheless quite encouraging. See for more details: https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne.*

[61] *In light of the Order of Internal Control, article 239: «Regulated entities **shall ensure**, in their relationships with their external service providers, that the latter: […]».*

[62] *«2. **Financial entities and ICT third-party service providers each ensure that the** ~~The~~ contractual arrangements on the use of ICT services shall include at least the following: [remaining provision unchanged]».*

• Second approach: to assert the public policy nature of article 27(2), without imposing any obligation on the parties. Without referring to the characterisation as a mandatory law within the meaning of article 9(1) of Rome I Regulation,[63] article 27(2) could simply specify that it applies «***irrespective of the law applicable to the contract***».[64]

Then:

Express reference could be made to the compliance of agreements for the provision of services with the requirements set out in article 27:

• in article 30(2), as part of the assessment carried out by the lead supervisors; and

• in article 31(1)(d), among the areas in which lead supervisors can make recommendations.

Finally, it is also proposed to:

Amend article 27(3) of DORA to strengthen the obligation to «consider» the inclusion of standard terms, by providing that, if such standard terms exist, the parties shall be obliged to use them, unless they can justify, by mutual agreement, their inadequacy in the relevant contract.[65]

[63] *Which falls under the application of the national law of the Member States, and therefore does not seem relevant to a provision of a European regulation.*

[64] *This being said, it should be noted that if the competent court is that of a third country, then it will probably not be required to apply the DORA Regulation to the services agreement (see paragraph 3.2.2(b) (Status of contracts concluded with Third Country ICT Providers after the entry into force of the ban) above). Therefore, in order to give full effect to this regulation, it is necessary, in any event, to require the parties to submit disputes relating to their contractual agreements to the jurisdiction of the court of a Member State.*

[65] *«3. ~~When negotiating~~ **In their** contractual arrangements, financial entities and ICT third-party service providers shall ~~consider the use of~~ **contractual clauses substantially compliant** with standard contractual clauses developed for specific services, **unless all the parties mutually agree that they can justify their inadequacy having regard to the particular circumstances of the contractual arrangement concerned.**»*