Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing'

W. Kuan Hon [a,*], Christopher Millard [b,c,**]

[a] Privacy, Security and Information Group at Fieldfisher, London, UK
[b] Centre for Commercial Law Studies, Queen Mary University of London, London, UK
[c] Bristows LLP, London, UK

Keywords:
Cloud computing
Cloud contracts
Banks
Financial institutions
Financial services regulation
Banking regulation
Outsourcing
Audit rights
IT risks
European Union

ABSTRACT

This paper looks at EU banks' use of public cloud computing services. It is based primarily on anonymised interviews with banks, cloud providers, advisers, and financial services regulators. The findings are presented in three parts. Part 1 explored the extent to which banks operating in the EU, including global banks, use public cloud computing services.

Part 2 of this paper covers the main legal and regulatory issues that may affect banks' use of cloud services. It sets out how EU banking regulators have approached banks' use of cloud services and considers regulators' lack of cloud computing knowledge. The paper further considers how the regulation of outsourcing applies to banks' use of cloud services, including whether cloud computing constitutes "outsourcing". It analyses the contentious issue of contractual audit rights for regulators as well as legal and practical issues around risk assessments, security, business continuity, concentration risk, bank resolution, and banking secrecy laws.

Part 3 looks at the key contractual issues that arise between banks and cloud service providers, including data protection requirements, termination, service changes, and liability.

All three parts of the paper can be accessed via Computer Law and Security Review's page on ScienceDirect at: http://www.sciencedirect.com/science/journal/02673649?sdc=2. The full list of sources is available via the same link and will be printed alongside the third part of the article.

1. Introduction

This paper considers legal and regulatory issues that may affect banks' use of cloud computing. It first sets out how EU banking regulators have approached banks' use of cloud services, including issues posed by regulators' limited knowledge of cloud computing and regulatory fragmentation.

Second, the paper considers how rules developed by financial services regulators in relation to outsourcing apply to banks' use of cloud services. In this respect, it considers the extent to which use of cloud computing constitutes "outsourcing" by the bank, and if it does, whether it involves outsourcing of "critical or important" operational functions, or "material outsourcing". The article then analyses the contentious issue of contractual audit rights for regulators as well as legal and

* *Corresponding author.* Fieldfisher, Riverbank House, 2 Swan Lane, London EC4R 3TT, UK.
E-mail address: kuan.hon@fieldfisher.com (W.K. Hon).
** *Corresponding author.* Centre for Commercial Law Studies, Queen Mary University of London, Northgate House, 67-69 Lincoln's Inn Fields, London WC2A 3JB, UK.
E-mail address: c.millard@qmul.ac.uk (C. Millard).

https://doi.org/10.1016/j.clsr.2017.11.006
0267-3649/

practical issues raised by regulatory requirements such as risk assessments, security, business continuity including exit plans, concentration risk and bank resolution, continuing regulatory oversight and banking secrecy laws.

2. EU FS regulators' approach to cloud

The EU seems relatively "late to the party" in providing specific rules or guidance on cloud use by FS institutions. Other jurisdictions' FS regulators have previously issued such rulings or guidance, e.g. the US (FFIEC 2012). They are even updating them, e.g. Australia's APRA (APRA 2015 replacing APRA 2010), although APRA has tightened its approach, having observed "weaknesses" in Australian banks' approach to cloud risk management, and now it questions "the appropriateness of transitioning systems of record" (critical systems) to public cloud.

There are various problems regarding FS regulation and cloud, which are set out in detail below:

- some FS regulators' relative ignorance regarding cloud, which feeds into many regulators' "anti-cloud" perspective;
- interpretations of FS regulatory rules by regulators that impose requirements which are hard or impossible and/or cost-prohibitive to meet in cloud;
- also related, continuing lack of clarity as to what is or is not permitted, leading to regulatory uncertainty for banks, e.g. (BBA 2016); and,
- lack of regulatory harmonisation.

2.1. *Cloud knowledge*

EU FS regulators' own self-reports indicate that regulators lack cloud knowledge. Almost half of such regulators responding to the ENISA Study said their knowledge of cloud computing was medium (27%) or poor (18%).

This accords with the findings from our interviews. For example, a provider commented on some regulators' "ignorance": "Lots of rules or guidelines, even if written recently, don't understand how cloud works. This is very frustrating". Similarly, a bank felt the FCA was "making lovely soft noises" about cloud which have lacked understanding. Even a regulator (with technical expertise) felt, "many [regulators] don't have the right knowledge to progress well with cloud; they don't know what to ask for from the bank or provider".

Illustrating regulators' lack of knowledge about cloud, a recent discussion paper on innovative uses of consumer data by FIs stated that data security risks were "especially relevant when, for instance, the database is not stored locally within the financial institution, but outsourced to cloud services that only operate online and are, thus, subject to cyber-attacks" (EBA 2016a, para.84). This fails to recognise that banks' *internal* systems are constantly subject to massive cyber-attacks, including phishing attacks on bank employees and attacks on ATMs (Kaspersky 2016), (PWC 2014), (Symantec 2012). In the US, banking regulators' examiners are trained on cloud and virtualisation, (e.g. (FDIC 2015, four-and-a-half day course), (Board of Governors of the Federal Reserve System 2016, one-week course)). A similar approach could be taken in the EU.

Table 1 – Cloud guidance of the Monetary Authority of Singapore (MAS).

The MAS' approach to cloud
An example of an FS regulator with a sophisticated approach to cloud is Singapore's MAS, whose technology risk management guidelines (with associated checklist) has had sections on cloud and shadow cloud since 2013 (MAS 2013b). MAS' latest outsourcing guidance (MAS 2016b replacing MAS 2011) contains a specific section on cloud, which together with its associated FAQs (MAS 2016a) addresses cloud in a technically-sophisticated, cloud-aware manner, perhaps motivated by a desire to increase hitherto relatively low cloud up-take.[a] This indicates the evolution from a conservative, cautious, initial attitude into a more balanced, cloud-appropriate one. In this sense, it appears that MAS is leading the way, and EU regulators could take note. Specific examples of MAS' approach are included below.

[a] Interestingly, Singapore bank DBS announced in June 2016 a pilot of Microsoft's Office 365 with all staff worldwide to be migrated by end 2016 (DBS 2016a), and on the same day as MAS' new guidelines were released announced a contract for DBS to use AWS to create a hybrid cloud environment; it will initially use AWS for pricing and valuing financial instruments for risk management (DBS 2016b).

FS regulators' knowledge of actual cloud usage by banks also seems limited: 64% thought cloud adoption in FS was low, 18% very low, whereas actual adoption levels as reported by both FS institutions and providers were higher (ENISA Study). Some regulators are reportedly bringing in cloud consultants, internal and external, which should be helpful.

In addition, providers should be willing to be more transparent: "That's what the regulator is looking for, if it's not getting it from the provider it will block [the cloud transaction]". Providers could do more to educate regulators on their systems and processes. Familiarity with how particular technologies operate may help get regulators more comfortable with cloud use by banks (Singapore's MAS provides an example of this, as set out in Table 1).

2.2. *FS regulators' cloud guidance*

2.2.1. *Overview*

In the EU, regulatory uncertainty remains a significant barrier. One bank noted, "We don't know if the regulator will allow it or not. It's difficult for management to deal with. [. . .] It's the key thing that makes banks scared of cloud". It also called for regulators to spell out clearly the reasons for their concerns, rather than just "we're unhappy with that".

EU regulators prefer private cloud; many are negative towards public cloud, with 23% of participating FS regulators believing it should "never" be used in FS (ENISA Study). But, as an adviser pointed out, if regulators force the use of only private cloud, that would restrict new entrants, reducing both competition and innovation. Furthermore, control may be better with private cloud, but security is not necessarily better. The preference for private cloud is "not necessarily based on fact but sentiment". A provider also noted that, while FS regulators' main purpose is protecting the public, the benefits of