Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Banking in the cloud: Part 1 – banks' use of cloud services

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 providers
Cloud use
Cloud contracts
Banks
Financial institutions
Financial services regulation
Banking regulation
EU
European Union

A B S T R A C T

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 explores the extent to which banks operating in the EU, including global banks, use public cloud computing services. It describes how banks are using cloud computing and the key drivers for doing so (such as time to market), as well as real and perceived barriers (such as misconceptions about cloud and financial services regulation), including cultural and technical/commercial aspects. It summarises how banks have approached the cloud and how cloud providers have approached the banking sector.

Part 2 of this paper will cover the main legal and regulatory issues that may affect banks' use of cloud services, including how the regulation of outsourcing applies to banks' use of cloud services. Part 3 will look 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 paper.

1. Introduction

Public cloud services offer rapid provisioning, flexibility, simplification, agility and cost savings. Globally, 89% of banks used at least one cloud application in 2015 (57% in 2009), but only 1% were running "core" banking applications in-cloud, while most banks were hesitant to move customer or financial data to cloud (Temenos & Capgemini 2015). There is, however, great interest in banks' secure use of cloud, to which end the Cloud Security Alliance (CSA) established a Financial Services Working Group in 2015.[1] According to an adviser we interviewed, "They

* *Corresponding author.* Fieldfisher, Riverbank House, 2 Swan Lane, London EC4R 3TT, United Kingdom.
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.
E-mail address: c.millard@qmul.ac.uk (C. Millard).

https://doi.org/10.1016/j.clsr.2017.11.005

[1] https://cloudsecurityalliance.org/group/financial-services/

[banks] are going to have to do it [use cloud]", but the biggest problem is a "lack of understanding, inertia, and confusion about what the restrictions are".

Using banks operating in the EU (which we term "**EU banks**", even if headquartered elsewhere) as a case study, our research looks at "what's really happening out there", cutting through the rumours and hype to determine the opportunities and challenges banks face in practice when using or considering public cloud computing. Do problems arise from sector-specific legal or regulatory issues or from other factors – and how, if at all, have those problems been or could they be overcome?

This paper draws on two types of sources. First, we conducted desk research into public sources, including online reports and public conferences, regarding banks' use of cloud. Second, we engaged in qualitative research based on anonymised discussions with banks, cloud providers, regulators and advisers/experts regarding their practical experiences, with a particular focus on the UK and the approach of the UK's Financial Conduct Authority (FCA).[2] Some interviews involved legal professionals from the organisations involved, some commercial or business specialists or IT/security professionals, some a mixture. External advisers have helpfully provided a broad view of the position across their clients (bank or cloud provider). However, advisers are likely to be involved only in negotiated cloud contracts. As a result, banks may undertake more cloud transactions on providers' standard terms than those which were mentioned to us, because their value was below the relevant bank's threshold for such procurements and therefore "under the radar". EU laws are considered at Directive or Regulation level only; we have not separately researched national laws of other countries, reporting only what sources stated about such laws.

We cannot name participants who kindly agreed to be interviewed, or state which banks use which cloud providers where that is not public. Similarly, we are not identifying conferences/meetings conducted on the Chatham House Rule basis.[3] In some cases, we do not even know the names of banks or providers involved, as interviewees did not disclose such information. That certain banks or cloud providers were mentioned (or not mentioned) in this paper is no indication that they participated in our research.

2. What is cloud computing?

This section provides a brief introduction to cloud computing. It describes service models, deployment models, the layering of services, and common issues of cloud computing confusion.

2.1. *Service models*

"Cloud computing" essentially involves the use of computing resources over a network, typically the Internet, scalable with demand (Hon & Millard 2013a). Where the resources used are software applications, accessed through a web browser on the cloud customer's local device, but installed and running on remote cloud servers, the **service model** is called Software-as-a-Service (**SaaS**) (Mell & Grance 2011). Software applications available via SaaS vary, but may include website hosting, data storage (e.g. Box, Dropbox) as well as customer relationship management (CRM) whether B2C or B2B (e.g. Salesforce), HR and/or accounting/financial management (e.g. Workday), word processing, email and other office productivity applications (e.g. G-Suite [formerly Google Apps for Work] and Microsoft's Office 365), photo/file sharing (e.g. Flickr) and social networking (e.g. Facebook). Some SaaS software may even be licensed for installation within the datacentres of the customer or its third party vendor or host, such as Office 365.

Where the IT resources used over a network are computational power i.e. "compute" servers, storage capacity and/or networking, the service model is called Infrastructure-as-a-Service (**IaaS**). The cloud provider manages the hardware but the IaaS customer must self-manage its virtual machines (VMs),[4] including the operating systems and applications it installs within its own VMs. Thus, customers may use IaaS services (virtual servers, storage, networking) for anything they choose, subject to contractual restrictions imposed by the provider. IaaS services include AWS's EC2, S3, Route 53 etc., Google's Compute Engine (part of Google Cloud Platform, the umbrella term for Google's IaaS/PaaS offerings), IBM's Softlayer, and Microsoft's Azure.

Where the relevant IT resources comprise application hosting and deployment platforms that enable the use of software applications whose source code has been uploaded by the cloud customer, the service model is known as Platform-as-a-Service (**PaaS**). Examples include Google's App Engine (part of Google Cloud Platform), IBM's Bluemix (built on Softlayer) and Microsoft's Azure. As with IaaS, cloud customers have flexibility regarding how they wish to use PaaS. Some PaaS platforms may be installed in an organisation's own datacentres, such as the open source Pivotal Cloud Foundry, which can sit on Openstack (an open source IaaS platform).

Rather than using a particular SaaS service, a cloud customer could build equivalent software on IaaS/PaaS, given sufficient expertise and resources/time. However, it is usually more efficient, convenient, and cost-effective to subscribe to a SaaS service that already provides required functionality.

2.2. *Deployment models*

Cloud services also feature different possible **deployment models** (Mell & Grance 2011): public, private, hybrid and community cloud, each of which may involve IaaS, PaaS and/or SaaS. The two main deployment models are public cloud and private cloud. **Public cloud** involves the use of standardised, commoditised, physical hardware that is shared between

[2] We are very grateful to all who agreed to discuss their experiences with us.

[3] Where statements may be reported, but not who made them.

[4] The most common kind of "virtualisation" in computing involves server hardware virtualisation: many separate virtual computers, "virtual machines" or VMs, each with its own operating system and software applications but often serving different customers, run on the same physical server and other physical IT hardware (Hon & Millard 2013a). Virtualisation software includes VMWare's vSphere, and the open source Xen, a version of which AWS uses.