Singapore Journal of Legal Studies
[2017] 77–99

# FINANCIAL REGULATION AND DISRUPTIVE TECHNOLOGIES: THE CASE OF CLOUD COMPUTING IN SINGAPORE

MAZIAR **PEIHANI***

An important trend in the world of computing is the rise of cloud technology, whereby on-demand and self-service computing resources are delivered through the internet. The 'cloud' is a disruptive technology that challenges some of the entrenched business models of the IT industry, offering important benefits such as greater flexibility, scalability and utility-based pricing. This paper explores the use of cloud technology by financial institutions and the factors that impact further adoption of cloud technology in the financial sector. Furthermore, this paper investigates how the financial regulator in Singapore, one of the most important financial jurisdictions, is tackling the risks that outsourcing to the 'cloud' involves. It is argued that a number of novel features can be found in the regulator's approach, including a balanced use of principles and rules, a diverse and multi-layered structure of compliance strategies, and engaging cloud service contracts as a means to maintaining regulatory oversight.

## I. INTRODUCTION

Since their inception, digital computers have undergone significant changes. Those operating the first computers, some 70 years ago, dealt with enormous, metal-framed behemoths, occupying entire rooms and requiring specialised facilities to manage. Today's computers would be virtually unrecognisable to those early users; they are smaller, sleeker, and, as the ubiquitous use of smartphones shows, publicly available and mobile. There is, however, another important mutation that computing is facing; it is turning into what has come to be known as 'cloud' or a 'web of clouds'.[1] Cloud computing is a new model for delivering on-demand and self-service computing resources, thereby allowing computing power to be used where and when it is needed.[2] Cloud is a disruptive technology as it challenges entrenched business models of the Information Technology ("IT") industry such as rigid software and services licensing contracts. Cloud computing offers greater flexibility, scalability and utility-based pricing, opening new markets, products and services that gradually replace more traditional IT paradigms.[3]

---

* PhD, University of British Columbia.

1 "Let It Rise: A Special Report on Corporate IT", *The Economist* (25 October 2008) at 3, online: The Economist <http://www.economist.com/node/12411882> ["Let It Rise"].

2 Deloitte Center for the Edge, *Cloud Computing – Storms on the Horizon* at 2, online: Deloitte Center for the Edge <http://www.johnseelybrown.com/cloudcomputingdisruption.pdf>.

3 Alex Krikos, "Cloud Computing as a Disruptive Technology" (2011) 2:2 Cloudbook Journal, online: Cloudbook <http://media.cloudbook.net/pdf/cloud-computing-as-a-disruptive-technology.pdf>.

Driving this disruptive trend is the fact that both individuals and businesses have embraced cloud as the future of IT. In fact, as early as 2008, studies indicated that "69% of Americans [that] connected to the web us[ed] some type of 'cloud service"', such as email or online data storage services.[4] Companies too are also moving to cloud. Transitioning to cloud allows them to process massive amounts of data and tailor their services to the needs of consumers. For instance, AccuWeather which provides weather forecasting to 175,000 clients and has viewership of more than 1 billion, uses a cloud infrastructure that allows it to handle 10 billion data requests every day while reducing the IT costs by 40%.[5] Airbnb, which lets travellers book accommodation from guest hosts, uses cloud infrastructure too. The firm has managed to create a supply of accommodation that never existed before, "allow[ing] suppliers and renters to share feedback, [images], and reviews".[6] SunTrust Bank, with total assets of $178.2 billion, has transitioned from services such as loan origination and underwriting to cloud, thereby doing away with a myriad of complex back-end systems and difficulties in getting timely access to customer information.[7]

This swell in cloud computing has precipitated increasingly novel and complex legal and regulatory challenges, complex enough to warrant a specialised area of legal research. A growing body of literature explores issues posed by the cloud, including its effect on the confidentiality and privacy of data, and its relation to the law, such as in contract formation, and securing intellectual property.[8] An area, however, that has not yet received much attention is how cloud technology impacts the financial industry and how financial regulators are tackling the risks that outsourcing to cloud involves. The purpose of this paper is to help fill this gap by examining the regulation of cloud computing in Singapore, a major financial jurisdiction with regulatory arrangements and dynamics ripe for systemic attention.

The questions I investigate are twofold: How has the Monetary Authority of Singapore ("MAS"), Singapore's financial regulator, responded to the increasing use of cloud technology by financial institutions? How can the tools and requirements

---

4 "Let It Rise", *supra* note 1 at 4.

5 Charles Cooper, "The Cloud Drives a New Wave of Disruption" *CIO* (25 June 2015), online: CIO <http://www.cio.com/article/2940519/cloud-infrastructure/the-cloud-drives-a-new-wave-of-disruption.html>.

6 *Ibid*; Amazon Web Services, *Airbnb Case Study*, online: Amazon Web Services <https://aws.amazon.com/solutions/case-studies/airbnb/>.

7 "SunTrust Banks: Improving Productivity, Reducing Vulnerability Windows" *International Business Machines Corp* ("IBM") (25 February 2011), online: IBM <http://www-03.ibm.com/software/businesscasestudies/us/en/corp?synkey=Y818919P18846W63>; Emily McCormick, "Is Banking's Future in the Cloud?" *BankDirector.com* (12 September 2012), online: BankDirector.com <http://www.bankdirector.com/issues/technology/is-bankings-future-in-the-cloud/>.

8 See *eg,* James Ryan, "The Uncertain Future: Privacy and Security in Cloud Computing" (2014) 54:2 Santa Clara L Rev 497; Janet A Stiven, "Preparing and Advising Your Clients on Cloud Usage" (2014) 12:4 DePaul Bus & Comm LJ 421; Frank Pasquale & Tara Adams Ragone, "Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing" (2014) 17 Stan Tech L Rev 595; Chris Reed, *Information "Ownership" in the Cloud*, Queen Mary University of London, School of Law, Legal Studies Research Paper No 45/2010 (November 2009); W Kuan Hon, Christopher Millard & Ian Walden, "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now" (2012) 16:1 Stan Tech L Rev 79; T Noble Foster, "Navigating Through the Fog of Cloud Computing Contracts" (2013) 30:1 The John Marshall Journal of Information Technology & Privacy Law 13; Farisa Tasneem, "Electronic Contracts and Cloud Computing" (2014) 9:2 Journal of International Commercial Law and Technology 105.

being employed by MAS be explained from a regulatory governance perspective? In considering the latter question, I draw upon the regulation and governance scholarship. I argue that there are three novel features to MAS' approach: a balanced use of principles and rules in response to the cloud's risks and uncertainties; a diverse and multi-layered compliance strategy to achieve regulatory outcomes; and a strategy of engaging cloud service contracts as a means to maintaining regulatory oversight throughout the entire outsourcing process.

The paper proceeds as follows. First, I overview the typologies of cloud services and business models and the major trends in cloud technology used in the marketplace. I review (a) the adoption of cloud technology by financial institutions, (b) the factors pushing towards further adoption of cloud, and (c) those factors that have hindered the pace of adoption of cloud technologies. Second, I discuss both the regulation of cloud computing in Singapore's financial sector and the regulatory expectations that financial institutions need to meet when adopting cloud. The third part of this paper examines the regulatory requirements from the perspective of regulatory governance in order to identify the novel features and themes of cloud directed regulation. Isolating these novel features will help us better understand the regulator's approach and its effect on regulated actors' behaviours. I conclude by summarising the nature and importance of the relationships between the actors involved in cloud regulation. After highlighting these important relationships, I will emphasise several issues that need more consideration when considering legal strategies for governing cloud services.

## II. Overview of Cloud Typologies, Services, and Trends

Recently, a new concept—'cloud computing'—has emerged in the fields of computing and telecommunications: The notion of a 'cloud' symbolically represents the internet. "'Computing' refers to [the] functionalities offered by computers", including their "calculation [and] data storage capacities".[9] Although the cloud may appear to be a new solution, this technology can be traced back to the services offered by large technology firms, such as Amazon, Yahoo, and Facebook.[10] Among the most familiar cloud services are email services (such as Gmail), photo-hosting or music-sharing websites (such as Instagram or SoundCloud), and online financial management programs (such as Mint.com). What all these services have in common is that they allow customers to access their data from any Internet-enabled device without installing any files on their computer. "Emails, photos, and. . . records are stored on the cloud provider's servers, and the provider [grants] access to them anytime at the customer's request."[11]

---

9 Union Des Consommateurs, *Canadian Perspectives on Cloud Computing and Consumers*, *Final Report of the Research Project Presented to Industry Canada's Office of Consumer Affairs*, (Quebec: Union Des Consommateurs, June 2011) at 6, online: Union Des Consommateurs <http://uniondesconsommateurs.ca/docu/vieprivee/CloudComputingE.pdf>.

10 *Ibid*.

11 Renee Berry & Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing" (2012) Journal of International Commerce and Economics at 2, online: United States International Trade Commission <https://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf>.

While there is no consensus on the definition of the 'cloud', a widely used definition is the one developed by the National Institute for Standards and Technology ("NIST"):

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[12]

The above definition outlines some essential characteristics of cloud technology. The first is on-demand self-service. A cloud customer can unilaterally access and change its data as needed without the authorisation of the Cloud Service Provider ("CSP").[13] Second, because of wireless communication networks, a customer can find access to cloud services through any internet-enabled device such as mobile phones, tablets, and laptops.[14] The third feature concerns resource pooling.[15] The cloud allows services to be pooled and shared by multiple consumers. That is, although services can be customised to meet the client's preferences, a cloud's resources—such as storage, processing, and memory and network bandwidth—are shared among all customers. The fourth feature is a "rapid elasticity" of the services.[16] Essentially, this means that services can be released quickly so that the allocation of resources are commensurate with the customer's needs. This elasticity allows customers to customise their resource allotment depending on their demands at a given time.[17] Finally, cloud systems automatically monitor, control, and report resource usage. This characteristic not only brings transparency to usage but also allows the customer to pay only for the services that it has used.[18]

Cloud services are classified in various ways. One common classification describes cloud services as falling under three categories.[19] The first is Software as a Service ("SaaS") which refers to end-user applications or software used or accessed via the internet. SaaS requires little technical know-how on the part of users and is the most commonly used among consumers.[20] Common SaaS applications include "email, backup/disaster recovery, storage, and web hosting services".[21] The second category is Platform as a Service ("PaaS") which allows programmers to create and customise software applications. A PaaS customer does not need to actively manage processing or storage services and can just focus on programming applications.[22]

---

12 NIST, "The NIST Definition of Cloud Computing", by Peter Mell & Timothy Grance, NIST Special Publication 800-145 (Maryland: NIST, September 2011) at 2, online: NIST <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

13 *Ibid*.

14 Union Des Consommateurs, *supra* note 9 at 9, 10.

15 *Ibid.*

16 *Supra* note 9.

17 Berry & Reisman, *supra* note 11 at 4.

18 *Ibid*; Union Des Consommateurs, *supra* note 9 at 9, 10.

19 Mell & Grance, *supra* note 12 at 2, 3.

20 Berry & Reisman, *supra* note 11 at 3.

21 W Kuan Hon & Christopher Millard, "Cloud Technologies and Services" in Christopher Millard, eds, *Cloud Computing Law* (Oxford: Oxford University Press, 2013) at 5.

22 *Ibid* at 4, 5.

Finally, infrastructure as a Service ("IaaS") provides basic computing functions such as data storage and processing power. IaaS requires user sophistication and expertise but at the same time affords the user flexibility and control.[23]

Another common classification framework divides cloud technologies into four categories based on their deployment models:

- Private cloud: the relevant infrastructure is provided for the "exclusive use by a single organisation". The cloud "may exist on or off premises". "It may be owned, managed [or] operated by. . . the organisation [or] a third party, or some combination of them."
- Community cloud: where the cloud infrastructure serves a specific community of users (*eg* government bodies) that have shared interests or concerns.
- Public cloud: where the infrastructure exists on the premises of the service provider, and is open to the general public.
- Hybrid cloud: involving a mixture of the above models. For example, an organisation may use a private cloud for storing sensitive customer information and use a public cloud for certain tasks that require significant computational resources.[24]

Cloud computing appears to have a significant potential for growth. According to the International Data Corporation ("IDC"):

> . . . [T]otal cloud IT infrastructure spending (server, storage, and Ethernet switch) will grow by 26.4% in 2015 and will reach $33.4 billion, accounting for a third of all IT infrastructure spending. Private cloud IT infrastructure spending will grow by 16.8% year over year to $11.7 billion, while public cloud IT infrastructure spending will grow by 32.2% in 2015 to $21.7 billion. In comparison, spending on non-cloud IT infrastructure will remain flat at $67 billion.[25]

McKinsey forecasts the total economic impact of cloud technology to be somewhere between US$1.7 trillion and US$6.2 trillion annually in 2025.[26] The biggest driver of such growth is the rapid proliferation of applications and services that are available over the internet. Another significant factor is the world's population of internet users; it was estimated at 2.5 billion in 2013 but is expected to reach more than 5 billion by 2025. Given the increase in services offered by cloud technologies, these new users are likely to rely substantially on cloud-based processing, storage, and applications.

---

[23] *Ibid* at 4; Mell & Grance, *supra* note 12 at 2.

[24] Mell & Grance, *ibid* at 3; Hon & Millard, *supra* note 21 at 5.

[25] IDC, *Worldwide Quarterly Cloud IT Infrastructure Tracker*, online: IDC, <http://www.idc.com/tracker/showproductinfo.jsp?prod_id=961>, *cited in* "Worldwide Cloud IT Infrastructure Spending Forecast to Grow 26% Year Over Year in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC" *Business Wire* (6 July 2015), online: Business Wire <http://www.businesswire.com/news/home/20150706005147/en/Worldwide-Cloud-Infrastructure-Spending-Forecast-Grow-26>.

[26] James Manyika *et al.*, *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, McKinsey Global Institute (May 2013) at 61, 63, online: McKinsey & Company <https://www.sommetinter.coop/sites/default/files/etude/files/report_mckinsey_technology_0.pdf>.

Similarly, the demand for enterprise cloud is also expected to rise sharply. IT departments are facing increasing pressure to reduce costs and improve productivity. Cloud technology can facilitate achieving these objectives; it reduces costs and can help companies implement new applications and gain quicker and greater computational capacity.[27] Meanwhile, the cost of implementing cloud start-ups has fallen, while performance has improved. For example, renting a server in the cloud is now about one-third as expensive as buying and maintaining similar equipment. Falling prices can make cloud services particularly attractive to small and medium enterprises ("SMEs") as they often find it difficult to build and manage extensive IT infrastructure, given their more limited resources. Cloud technology is a cost effective choice because it allows SMEs to avoid tying up capital in IT, while avoiding the costs of the rapid obsolescence of technology—which is absorbed by the cloud provider. Yet, the computing power of cloud technology allows SMEs to compete with big firms, making it a very attractive option.[28]

### A. *The Cloud and the Financial Technology Industry*

The financial industry is currently undergoing important changes which will accelerate the adoption of cloud services. A new generation of laws and regulations have been ushered in since the global financial crisis. The increased regulation has substantially heightened the compliance burden on banks and strained their profit margins. For example, in 2006, the eight American banks labelled as being "globally systemically important", had their returns on equity of 30% on average.[29] In 2014, however, those same banks had returns on equity of less than 11%.[30] Moreover, banks are now facing encroachment from non-traditional financial firms that are at a competitive advantage due to their flexibility in embracing innovation and developing consumer-centric products and services.[31] A new generation of start-ups, commonly known as 'fintech firms' are working on alternative ways to traditional banking. They are expanding their market share by offering new and less costly solutions for payments, wealth management, and peer-to-peer lending and crowdfunding.[32] Several firms, including Lending Club and OnDeck (both focus on lending), have even gone public. Lending Club has arranged an impressive US$9 billion in loans through its marketplace. Users of Venmo, a payments app, transferred US$1.3 billion in the first quarter of 2015 alone.[33] In 2014, the 'fintech firms' attracted US$12 billion of

---

27 *Ibid* at 62, 63.

28 *Ibid* at 63.

29 "You're boring. Get used to it" *The Economist* (27 September 2014), online: The Economist <http://www.economist.com/news/leaders/21620201-big-banks-have-changed-lot-there-more-restructuring-come-youre-boring-get-used>.

30 *Ibid*.

31 Jamie Dimon, Chairman & CEO, JPMorgan Chase & Co, to Shareholders (8 April 2015), Annual Report 2014, *A Strong Corporate Culture*, online: <https://www.jpmorganchase.com/corporate/annual-report/2014/ar-strong-corporate-culture.htm>.

32 *Ibid*.

33 "The Fintech Revolution" *The Economist* (9 May 2015), online: The Economist <http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution>.

investment—a substantial increase from the US$4 billion that the firms had attracted the year before.[34] Given its growing influence, Goldman Sachs estimates the 'fintech' industry's revenue to be around US$4.7 trillion.[35]

In short, cloud computing offers a new way of adapting and responding to the new regulatory and market environments. Its scalability, agility and cost-effectiveness offer significant commercial benefits to financial institutions. Cloud computing does not require heavy investments in hardware and software.[36] A financial institution can forego a large upfront capital expenditure in exchange for a smaller, on-going operational cost. The rapid elasticity and the tailored services allow financial institutions to pick and choose the services required on a pay-as-you-go basis. Furthermore, banks not only save money based on tailored services, they also save money because of increased computing power.[37] Bank have to run millions of analytics calculations to assess the consequences of financial decisions and to determine what the impact on their businesses and outlooks will be. Such calculations require massive computing resources but can be done more quickly on cloud platforms.[38] This helps banks avoid inefficiencies. Studies also show that on average, 80-90% of computing resources in a company's IT department remain unused.[39] This happens because banks need to maintain massive Central Processing Unit and storage capacities to cover peaks in demand, but which remain under-utilised during low periods.[40] Cloud computing remedies this situation by diverting resources to and away from firms as needed, resulting in less idle time.[41] In addition, it lets financial institutions experience shorter development cycles for new products. As a result, the institutions can respond to consumer needs in a faster and more efficient way. Finally, cloud is "green IT." That is, it allows an organisation to transfer their services to a virtual environment and reduce energy consumption and resources allotted to excess capacities.[42]

While there is a trend towards cloud services, the financial industry is still in the early stages of cloud adoption. A recent survey by the Cloud Security Alliance indicates that the majority of financial institutions (61%) are only just developing a cloud

---

34 *Ibid*.

35 *Ibid*.

36 "Silver Lining" *The Economist* (4 October 2014), online: The Economist <http://www.economist.com/news/special-report/21621162-how-digital-revolution-can-help-some-workers-it-displaces-silver-lining>.

37 IBM Sales and Distribution, *Cloud Computing For Banking: Driving Business Model Transformation* (2013) IBM S&D Thought Leadership White Paper No IBW03005-USEN-00.

38 *Ibid*; Asia Cloud Computing Association ("ACCA"), *Asia's Financial Services: Ready for the Cloud: A Report on FSI Regulations Impacting Cloud in Asia Pacific Markets* (2015), online: ACCA <http://www.asiacloudcomputing.org/images/research/ACCA_Report_-_Web.pdf>.

39 Michael Wagner & Peter Henning Vages, "Cloud Computing for Financial Services Providers: Hype or Opportunity?" *Banking Hub* (February 2014) at 2, online: Banking Hub <https://www.bankinghub.eu/banking/technology/cloud-computing-financial-services-providers-hype-opportunity>. See also "Where the Cloud Meets the Ground" in "Let It Rise", *supra* note 1 at 6, 7, online: The Economist <http://www.economist.com/node/12411920>.

40 Wagner & Vages, *ibid* at 2.

41 Sahil Patani *et al.*, "Cloud Computing in the Banking sector: A survey" (2014) 3:2 International Journal of Advanced Research in Computer and Communication Engineering 5640 at 5641.

42 *Ibid*.

strategy within their organisation.[43] According to 86% of participants, security concerns were the top obstacle to adopting cloud technologies.[44] In particular, concerns over the confidentiality of data, the loss of control of data, and data breaches ranked as top security concerns.[45] Furthermore, 71% of financial institutions considered regulatory compliance as a reason to keep controls in-house and not to migrate to public cloud services.[46] Top compliance issues included malware detection, audit permissions, and the encryption/tokenisation of data.[47]

Other industry reports have similar findings. For example, a recent report by the ACCA indicates that financial institutions in the Asia Pacific region have been slow to adopt cloud services because of perceived regulatory challenges.[48] Such challenges are especially notable for wholesale operations involving customer data. The report highlights that in the surveyed jurisdictions regulation is inconsistent. Sometimes, no regulations on data use limitations or data segregation are present, and sometimes regulations are unclear or too restrictive (on cloud service contracts, data location, or auditing requirements, for example).[49] ACCA's report also presents other reasons for the slow adoption of cloud. These reasons include the reluctance of financial institutions to trust third parties with their customer data, their critical processes and the complex legacy systems of banks. However, these factors may have only slowed down the adoption of cloud, and it is unlikely that these challenges will stop the eventual uptake of cloud by most financial institutions.[50]

## III. Regulation of Cloud in Singapore's Financial Sector

### A. *Background*

Before discussing the cloud regulation in detail, a number of background points should be made. The first regards the financial landscape in Singapore. Singapore is one of the world's largest financial centres which is built around a core of domestic and international banks. As of February 2017, there were 126 commercial banks (121 foreign banks and 5 domestic) and 577 capital market service firms in Singapore.[51] Singapore attracts major international banks because of its "efficient market infrastructure and its. . . reputation for the rule of law and effective supervision".[52] These

---

43 Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector: Survey Report*, (March 2015) at 8, online: Cloud Security Alliance <https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf>.

44 *Ibid* at 8.

45 *Ibid* at 10.

46 *Ibid* at 11.

47 *Ibid*.

48 ACCA, *supra* note 38 at 8.

49 *Ibid*.

50 *Ibid* at 10.

51 MAS, Financial Directory, "Number of Financial Institutions and Relevant Organisations in Singapore (Last updated as at 8 February 2017)", online: MAS <https://masnetsvc.mas.gov.sg/FID.html>.

52 International Monetary Fund ("IMF"), *Singapore: Financial System Stability Assessment*, IMF Country Report No. 13/325 (November 2013) at 9, online: IMF <https://www.imf.org/external/pubs/ft/scr/2013/cr13325.pdf>.

factors contributed to making Singapore the third largest foreign exchange market in the world and one of the largest trading centres for OTC derivatives in Asia, as of 2012.[53] A cornerstone of Singapore's financial supervision is MAS. MAS is a self-funded agency that regulates and supervises all financial institutions, services and markets in Singapore. It licenses and oversees the banks, insurance firms and securities intermediaries, and also operates as the country's central bank.[54] MAS seeks to foster a sound and reputable financial centre, promote financial stability, and grow Singapore as an internationally competitive financial centre.[55]

The second point of note is that Singapore, like many jurisdictions, has not adopted any specific regulation relating to cloud computing in the financial industry.[56] Instead, relevant regulation, dealing more generally with outsourcing, is utilised. Broadly speaking, outsourcing can be defined as a financial institution's use of a third party to perform activities on a continued basis that would normally be undertaken by the financial institution itself. Thus, when a bank uses the services (*eg* data storage or processing) of a third party CSP, the bank can be said to have outsourced to that CSP.

The Joint Forum's guidelines on *Outsourcing in Financial Services* in 2005 represents the first international response to the increasing use of outsourcing by financial institutions around the world.[57] It sets out several principles that guide firms and regulators to mitigate the risks and concerns that arise from outsourcing. These concerns include operational risk, compliance risk and reputation risk, as well as the danger of over-reliance on outsourcing for activities that are critical to the viability of the firm or its obligation to customers.[58] To address these risks, the Joint Forum calls on financial institutions to take the following steps:

- Draw up comprehensive and clear frameworks for outsourcing.
- Establish effective risk management programmes.
- Perform appropriate due diligence on the financial and infrastructure resources of the service provider.
- Require contingency planning by the service provider.
- Negotiate appropriate outsourcing contracts.
- Protect the confidentiality of the firm as well as customer information.[59]

The Joint Forum also calls upon regulators to consider the outsourcing activities of financial institutions as an integral part of their supervision. Moreover, it emphasises

---

53 *Ibid*.

54 Christian Hofmann, "Bank Regulation in Singapore" (2015) 1:2 Journal of Financial Regulation 306 at 307.

55 *Ibid*; MAS, *Objectives and Principles of Financial Supervision in Singapore*, (Singapore: Monetary Authority of Singapore, April 2014), online: MAS <http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/Objectives%20and%20Principles%20of%20Financial%20Supervision%20in%20Singapore.pdf>.

56 In addition to Singapore, these jurisdictions have not adopted specific regulation regulations: Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Taiwan, Thailand, and Vietnam. See ACCA, *supra* note 38 at 14.

57 The Joint Forum, *Outsourcing in Financial Services*, CH-4002 Basel, Switzerland (February 2005) at 1, online: Bank for International Settlements <http://www.bis.org/publ/joint12.pdf>.

58 *Ibid* at 11, 12.

59 *Ibid* at 14-18.

that regulators should maintain their access to the books and records of financial institutions, that are in the possession of a service provider.[60] The principle emphasised by the Joint Forum is that outsourcing should not in any way hinder supervision by regulators. The Joint Forum's principles, as will be shown in the below Part, are also reflected in MAS' regulations on outsourcing.

The final point, is that when it comes to cloud computing in Singapore, financial institutions are subject to a variety of laws and regulations, some of which are not unique to the financial sector. For example, general data protection laws and regulations apply to financial institutions.[61] However, despite this overlap, the majority of the regulatory requirements in this area are still developed or administered by MAS. These include operational and technology risk management, business continuity management and outsourcing regulations. The following discussion will be predominantly concerned with outsourcing regulations as they represent the most direct and recent response to cloud computing.

## B. *The* Outsourcing Guidelines

MAS first issued the *Guidelines on Outsourcing* in 2004 with the aim of promoting sound risk management practices for outsourcing arrangements of financial institutions.[62] However, as technological outsourcing arrangements gained prevalence and sophistication, MAS proposed an updated version of the guidelines in September 2014 which were finalised following consultation with the industry in July 2016.[63]

The *Outsourcing Guidelines*[64] set out MAS' expectations for an institution involved in an outsourcing arrangement or one planning to outsource its activities to a service provider. The guidelines are based on the premise that outsourcing promises benefits but also poses risks to financial institutions.[65] For example, while the adoption of cloud services helps a financial institution to reduce costs, the services also expose the firm to reputational, compliance and operational risks. Such risks may arise from the failure of the service provider, breaches in security or the failure of the service provider to comply with the legal and regulatory requirements.[66] Regarding the scope of application, the *Outsourcing Guidelines* are particularly concerned with

---

60 *Ibid* at 18.

61 *Personal Data Protection Act 2012* (No 26 of 2012, Sing).

62 MAS, *Guidelines on Outsourcing*, (Singapore: MAS, October 2004), online: MAS <http://www.mas.gov.sg/~/media/resource/legislation_guidelines/securities_futures/sub_legislation/Outsourcing%20Guidelines.pdf> [MAS, *Guidelines on Outsourcing 2014*].

63 MAS, *Guidelines on Outsourcing*, *Consultation Paper P019-2014*, (Singapore: MAS, September 2014), online: MAS <http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/ConsultationPaper_Guidelines%20on%20Outsourcing.pdf> [MAS, *Proposed Guidelines on Outsourcing*]; MAS, *Guidelines on Outsourcing*, (Singapore: MAS, 27 July 2016), online: MAS <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial% 20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf> [MAS, *New Guidelines 2016*].

64 The *Guidelines on Outsourcing 2014*, *supra* note 62, and the *New Guidelines 2016*, *ibid*, are collectively, the "*Outsourcing Guidelines*".

65 MAS, *New Guidelines 2016*, *ibid* at 1.

66 *Ibid*.

material outsourcing; that is, an arrangement, which, in the event of service failure or security breach, has the potential to either:

- materially impact an institution's business operations, reputation or profitability; or
- adversely affect an institution's ability to manage risks and comply with applicable laws and regulations.

Moreover, an outsourcing arrangement is material if it involves customer information and, in the event of loss or unauthorised access to such information, can materially impact the institution's customers.[67] The following Part will take a closer look at the important provisions of the *Outsourcing Guidelines*.

### 1. *The Process of Cloud Adoption*

The board of directors and senior management of a financial institution have the responsibility to establish the appropriate governance and risk management framework for implementing cloud technologies within their firm.[68] The board should set the appropriate risk appetite regarding the cloud and it needs to weigh the issues regarding materiality and the risks associated with outsourcing, as outlined above.[69] The financial institution should perform due diligence in assessing the nature, scope, and complexity of outsourcing to ensure that the service provider has:

- the experience and competence to perform the contract;
- the financial strength and resources; and
- sound corporate governance, and internal controls and security measures in place.[70]

In the past, MAS expected financial institutions to notify and consult with it before entering into a material outsourcing arrangement.[71] Given the growing prevalence and complexity of the outsourcing arrangements, however, the *New Guidelines 2016* have removed such expectations.[72] As a result, financial institutions can now enter into a cloud arrangement without prior notification to MAS. Yet, it remains the responsibility of financial institutions to ensure the safety of their arrangements which continue to be supervised by MAS as well.[73]

---

67 *Ibid* at 1, 6.
68 *Ibid* at 9.
69 *Ibid* at 12.
70 *Ibid* at 13.
71 MAS, *Guidelines on Outsourcing 2014, supra* note 62 at 6.
72 MAS, *Public Consultation on Guidelines on Outsourcing, Response to Feedback Received*, (Singapore: Monetary Authority of Singapore, July 2016) at 9, online: MAS <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Response%20to%20Consult%20%20Outsourcing%20Guidelines%20Jul%202016.pdf> [MAS, *Response to Feedback Received on Outsourcing Consultation*].
73 *Ibid.*

2. *The Cloud Service Contract*

A financial institution is required to enter into a contract for using cloud services. MAS does not require any specific contract format but expects the agreement to define clearly the rights and obligations of both parties.[74] In particular, MAS requires the cloud contract to include certain principles and prescribed terms. For example, the contract should have provisions for the notification of adverse developments.[75] In other words, it should clearly specify the circumstances under which the service provider should notify the financial institution of an adverse incident. The financial institution should also have the right to terminate the contract and exit the outsourcing arrangement if the service provider breaches its obligations or undergoes a significant change such as a change of ownership or liquidation.[76] Finally, the contract should have clauses that set out the rules and limitations on subcontracting.[77]

3. *Confidentiality and Security*

As noted above, the service provider should have appropriate internal controls in place to safeguard the security and confidentiality of the financial institution's information.[78] Customer information should be disclosed to the service provider only on a 'need-to-know' basis. That is, the service provider and its staff should strictly use the customer information for the purpose of the contracted service only. Any unauthorised disclosure of customer information to any other party ought to be prohibited.[79] If a financial institution uses multi-tenancy arrangements, *ie* public cloud services, the service provider should be able to identify clearly and isolate the financial institution's customer information, documents, records, and assets to protect their confidentiality.[80]

4. *Business Continuity Management*

Under the principle of business continuity management ("BCM"), a financial institution should remain able to continue its business in the event of a service failure or disruption, or other unforeseen event that jeopardises the outsourcing arrangement.[81] The financial institution should determine that the service provider has business continuity plans ("BCP") in place that are commensurate with the nature, scope, and complexity of the arrangement.[82] BCPs of particular importance to cloud computing are setting recovery time objectives ("RTO") and recovery point objectives ("RPO").[83] A RTO is the target time duration needed to recover a specific function after a disruption. A RPO is "the acceptable amount of data loss for

---

74 MAS, *New Guidelines 2016*, *supra* note 63 at 14.
75 *Ibid* at 15.
76 *Ibid* at 15, 16.
77 *Ibid* at 16.
78 *Ibid* at 17.
79 *Ibid*.
80 *Ibid* at 17, 27.
81 *Ibid* at 18.
82 *Ibid*.
83 *Ibid.*

[a given] IT system should a disaster occur".[84] Furthermore, BCPs, including RTO and RPO, should be regularly updated and tested. The service provider should notify the financial institution "of any test finding that may affect the service provider's performance".[85]

### 5. *Audits and Inspection*

The cloud contract should give the financial institution the right to conduct audits on the service provider and its subcontractors and to obtain copies of audit reports.[86] In determining the frequency of audits, an institution should consider the materiality of the outsourcing arrangement as well as the nature and extent of risks that arise from it.[87] They should include "assessment[s] of the service providers' and its subcontractors' security and control environment, incident management process," and the institution's compliance with the *Outsourcing Guidelines*.[88] Significant issues and concerns in audit findings should be brought to the attention of the senior management (or the board) of the financial institution and the service provider. Senior management should ensure that appropriate and timely actions are taken to address the audit findings. Furthermore, copies of the audit reports must also be submitted to MAS.[89] Cloud contracts should also include clauses to allow MAS (or its agents) to exercise contractual rights on behalf of the financial institution, and access and inspect the service provider and its subcontractors to obtain the necessary records and documents.[90]

### 6. *Outsourcing outside Singapore*

An institution can engage a CSP in a foreign jurisdiction, provided that it performs due diligence in assessing that jurisdiction's risks; that is, that the institution assesses possible social, economic, and political conditions that may adversely affect it.[91] As a matter of principle, the financial institution should only outsource data to jurisdictions that uphold confidentiality clauses and agreements.[92] Institutions should not seek services from cloud services in jurisdictions that impede MAS' access to information because of legal or administrative restrictions.[93] Finally, the institution should notify MAS if an overseas authority seeks access to customer information or if MAS' rights have been restricted or denied.[94]

---

84 MAS, *Technology Risk Management Guidelines*, (Singapore: MAS, June 2013) at 23, online: MAS <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf>.

85 MAS, *New Guidelines 2016*, *supra* note 63 at 18.

86 *Ibid* at 21.

87 *Ibid* at 22.

88 *Ibid*.

89 *Ibid* at 23.

90 *Ibid* at 21, 22.

91 *Ibid* at 23.

92 *Ibid* at 24.

93 *Ibid*.

94 *Ibid*.

## IV. Cloud Regulation from a Regulatory Governance Perspective

In the following Parts, I will examine the regulations on cloud computing from a regulatory governance perspective. I draw upon concepts from established theories of regulation including principle-based regulation, management-based regulation, and responsive regulation. Due to the space constraint, I will not specifically discuss the similarities or differences between them. The reader can consult the rich body of literature on these issues that already exists for further discussion.[95] For the purposes of this paper, it is relevant to note that these theories stand in contrast with traditional 'command and control' regimes which seek to shape the behaviour of regulated actors through a top-down, adversarial, prescriptive approach.[96] They rely more on broad principles, which give significance to the judgments of the regulated actors with the purpose of achieving regulatory outcomes through shared understanding, dialogue, and collaboration.[97] They involve a shift in the centre of decision making from the regulator to the regulated actor; for, the latter is put in charge of planning and designing strategies to achieve regulatory outcomes.[98] Enforcement is responsive to, and commensurate with, the firm's behaviour. The regulator has a cooperative stance and focuses on achieving voluntary compliance. Undoubtedly, the background threat of the 'benign big gun' is present, and the regulator can impose severe sanctions to discipline intransigent actors.[99] In most cases, however, sanctions are not needed to achieve compliance, and enforcement resources are reserved for special cases of non-compliance.[100]

What follows should not be seen as an attempt to fit the cloud regulation with any particular theory. Instead, it seeks to leverage the insights of the regulatory governance scholarship to better understand how MAS regulates the use of cloud technology by banks. The focus will be on three key components of the regulatory

---

95 See *eg*, Julia Black, "Forms and paradoxes of principles-based regulation" (2008) 3:4 Capital Markets Law Journal 425; The Financial Services Authority ("FSA"), *Principles-Based Regulation: Focusing on the Outcomes that Matter*, (London: FSA, April 2007), online: FSA <http://www.fsa.gov.uk/pubs/other/principles.pdf>; Dan Awrey, "Regulating Financial Innovation: A More Principles-Based Proposal?" (2011) 5:2 Brooklyn Journal of Corporate, Financial & Commercial Law 273; Cristie Ford, "Principles-Based Securities Regulation in the Wake of the Global Financial Crisis" (2010) 55 McGill LJ 257 [Ford, "Global Financial Crisis"]; Ian Ayres & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University Press, 1992); Cary Coglianese & David Lazer, "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals" (2003) 37:4 Law & Soc'y Rev 691; Louis Kaplow, "Rules Versus Standards: An Economic Analysis" (1992) 42:3 Duke LJ 557; Lawrence A Cunningham, "A Prescription to Retire the Rhetoric of 'Principles-Based Systems in Corporate Law, Securities Regulation and Accounting" (2007) 60 Vand L Rev 1411.

96 Orly Lobel, *New Governance as Regulatory Governance*, University of San Diego School of Law, Legal Studies Research Paper Series, Research Paper No 12-101 (November 2012) at 7-10, 20; Cristie Ford, *Principles-Based Securities Regulation*, Research Study Prepared for the Expert Panel on Securities Regulation (2009) at 22, 30, online: Expert Panel on Securities Regulation <http://www.expertpanel.ca/documents/research-studies/Principles%20Based%20Securities%20Regulation%20-%20Ford.English.pdf> [Ford, *Principles-Based Securities Regulation*]; Awrey, *supra* note 95 at 283.

97 FSA, *Principles-Based Regulation*, *supra* note 95 at 6, 7; Awrey, *supra* note 95 at 283, 284.

98 Coglianese & Lazer, *supra* note 95 at 3, 4.

99 Ayres & Braithwaite, *supra* note 95 at 19-53; Robert Weber, "New Governance, Financial Regulation, and Challenges to Legitimacy: The Example of the Internal Models Approach to Capital Adequacy" (2010) 62:3 Admin L Rev 783 at 841.

100 Ford, "Global Financial Crisis", *supra* note 95 at 13.

process, namely: (1) the nature and characters of the regulation, (2) the modalities used to achieve compliance, and (3) the interaction between the regulator, the financial institutions, and the service providers.

### A. *Using Principles to Achieve Regulatory Outcomes*

Principles, for the purposes of this paper, are defined as directives cast at a high level of generality. This stipulation contrasts with a rule, which is more detailed, specifically tailored, and prescriptive.[101] Principles, thus, are more flexible and sensitive to the broader social and economic context. Looking at the *Outsourcing Guidelines*' provisions, one finds several directives that match the definition of a principle, including:

- Financial institutions should have appropriate governance and risk management frameworks for cloud.[102]
- Outsourcing to cloud should be based on a sound contractual basis.[103]
- The cloud arrangement should respect the integrity of financial transactions and records.[104]
- Financial services should remain available to consumers.[105]
- Customer information should be safeguarded from unauthorised access or exposure.[106]

These principles are outcome-oriented. That is, they focus on desirable regulatory outcomes, such as securing customer information or the availability of financial services. It is then the responsibility of the board and senior management of the financial institutions to devise and implement processes and strategies to achieve these outcomes. They are entrusted with governing, monitoring and managing the outsourcing arrangements, and can make judgment calls on how to meet the regulator's expectations.

While firms are expected to perform due diligence on the service provider and evaluate all the risks, MAS does not micro-manage this process. Firms have autonomy in negotiating the desirable cloud services and are not required to adopt any particular contract format. MAS does not unilaterally generate norms of behaviour; the regulated actors play a key role in determining the content of these principles. For example, to uphold the confidentiality principle, firms often need to encrypt and segregate customer information. MAS, however, does not prescribe any particular method for doing so. This is because prescriptive methods quickly become obsolete due to the fast-paced nature of the technological development. Firms are therefore free to choose risk mitigation strategies that they judge adequate given the current

---

[101] *Ibid* at 9.
[102] MAS, *New Guidelines 2016*, *supra* note 63 at 9-14.
[103] *Ibid* at 14-16.
[104] *Ibid* at 18.
[105] *Ibid* at 18, 19.
[106] *Ibid* at 17.

state of technology and their particular purpose. Hence, only the outcome—security of customer information—rather than the method, concerns MAS. In sum, the particular methods and rules used to uphold the principle—"customer information must be kept secure"—is not determined *ex ante*; rather, the regulator and the regulated flesh out these *ex post* in order to tailor them to the current marketplace and available technology.

### B. *A Hybrid Structure of Principles and Rules*

In some instances, MAS' approach to the cloud uses principles in conjunction with rules. For instance, the principle of appropriate governance and risk management for outsourcing is complemented by a specific rule that firms must keep a registry of all material outsourcing arrangements. Furthermore, this registry must be readily accessible by the board and senior management.[107] Another area where specific rules are especially conspicuous is in BCM. Under these rules, the maximum unscheduled downtime for each system should not exceed four hours per year. Moreover, in cases of a material system failure or security incident, the financial institution should notify MAS within an hour.[108] The following report on the root causes of the incident and impact analysis must then be submitted within 14 days. Finally, RTO should not be more than four hours from disruption.[109]

The BCM rules apply regardless of whether an institution uses in-house IT or has outsourced to a cloud provider. The rules clearly describe the regulatory outcome expected and reduce the need for judgment on the part of financial institutions, or their service providers, to a minimum. The rules clearly outline impermissible behaviour to preserve the integrity and availability of financial services. However, it is important to note that the highly technical and detailed nature of these rules requires constant adjustment to keep up with changing technology and developments in the market.[110]

### C. *Diverse and Multi-layered Compliance Strategies*

The regulatory strategies used by MAS to foster compliance with the *Outsourcing Guidelines* resemble a pyramid.[111] At the base of this pyramid are the regulated

---

[107] *Ibid* at 20.

[108] MAS, *Instructions on Incident Notification and Reporting to MAS*, (Singapore: MAS) at 1, online: MAS <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Instructions%20on%20Incident%20Notification%20and%20Reporting%20to%20MAS.pdf>.

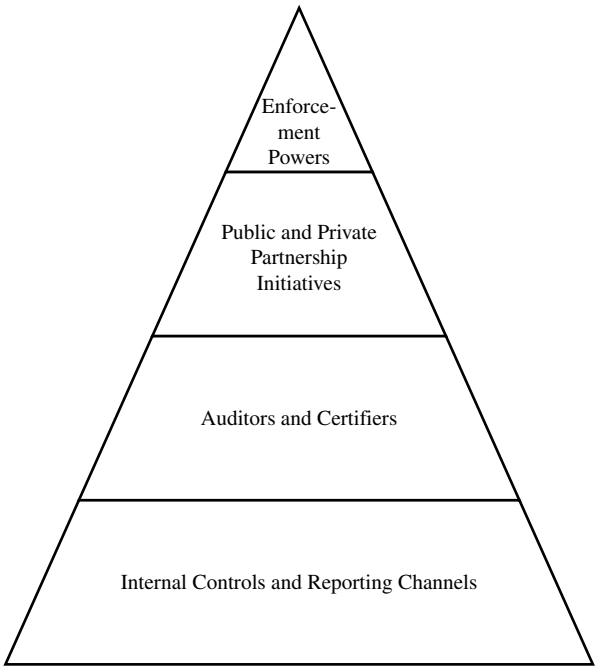
[109] MAS, *Notice on Technology Risk Management*, *CMG-N02*, (Singapore: MAS, March 2014) at para 6, online: MAS <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial% 20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/IID%20Notices/Notice%20CMGN02_2014.pdf>.

[110] Chris Reed, "Cloud Governance: The Way Forward" in Millard, *supra* note 21 at 371-374.

[111] On compliance and reporting pyramids, see Ayres & Braithwaite, *supra* note 95 at 19-53; Lobel, *supra* note 96 at 16, 17.

actor's internal controls. MAS relies significantly on financial firms' own due diligence in their assessment and monitoring so as to identify and address risks arising from their use of the cloud.[112] These internal checks and balances are buttressed by reporting requirements to the regulator. Next, compliance strategies utilise 'gatekeepers', such as auditors and cloud technology experts.[113] Gatekeepers help ensure that the firms' internal controls are suitably designed and effectively operated to meet the regulatory outcomes. Cloud certifiers play a particularly important role. They test the technical capacity of the service providers and examine their systems and controls against industry best practices. The certifiers can help provide an assurance that the service provider is trustworthy enough to handle corporate and confidential data. The audits of outsourcing arrangements are of particular significance given that they examine all key components of the service providers' systems and controls, including:

- Entry level controls: such as risk assessment, information security policy, and subcontracting contracts.
- General information technology controls: including physical security, incident management, and back-up and disaster recovery.
- Service controls: such as those relating to authorising and processing transactions, and to maintaining records.[114]




[112] MAS, *New Guidelines 2016*, *supra* note 63 at 18-20.
[113] *Ibid* at 16, 20-22.
[114] Association of Banks in Singapore ("ABS"), *Outsourced Service Provider's Audit Report (OSPAR) Template*, online: ABS < https://abs.org.sg/docs/library/abs-ospar-template.docx>.

At the third tier of the pyramid, one can also note the partnership programs between MAS and private and public actors. The best example of a public-private partnership is the industry-wide business continuity exercises that MAS and the ABS regularly conduct together. The last exercise was in November 2014, in which 141 organisations took part.[115] Participants included a wide range of financial institutions including, both commercial and investment banks, insurance/reinsurance firms, asset management firms, securities and broker houses, and the Singapore Exchange. The exercise provided an opportunity "for financial institutions to test and verify their crisis management plans" in the case of "cyber-attacks that could compromise data, [and] affect the availability of critical systems and services".[116] In addition to cooperative exercises, "MAS and the ABS Standing Committee on Cyber Security [have] jointly developed a set of industry guidelines on the planning and execution of penetration testing ("PT") of IT systems by financial institutions".[117] These initiatives are "intended to. . . raise the quality of PTs conducted by [the] financial institutions", and to strengthen the "cyber resilience of the financial sector". 11 major financial institutions subsequently participated in a PT exercise designed to test the suitability of these guidelines. The results were analysed and "shared with the industry to raise the awareness of common and high-risk vulnerabilities".[118]

MAS has also established partnerships with other regulators. Most notable, is MAS' partnership with the Cyber Security Authority ("CSA"), which oversees and strengthens cybersecurity in critical sectors such as energy, water and banking.[119] In partnership with MAS, CSA conducted the first cyber security table-top exercise, known as CyberArk IV, for the financial sector in May 2015. Similar to the business continuity exercise, this initiative was intended to test how the financial sector would respond to cyber threats.[120] All these exercises included financial institutions that have outsourced their IT operations to CSPs.

These partnership initiatives enable MAS to gain important insights. In fact, the interaction with other regulators and the financial community gives MAS access to a rich source of information which MAS leverages to assess risks more accurately and reliably. Moreover, developing guidance in collaboration with the industry and sharing the results and lessons helps establish best practices in the industry. Using the insights from the regulatory governance literature, one can argue that such initiatives can, over time, establish an "interpretive community," which constantly updates the content of regulations and promotes understanding of the regulatory expectations and outcomes.[121]

Finally, on the top tier of the pyramid, resides MAS' enforcement powers. If MAS is not satisfied with an institution's observance of the *Outsourcing Guidelines*, it can

---

[115] MAS, *Industry Tests*, *A Robust Financial Centre*, *Annual Report 2014/2015*, (Singapore: Monetary Authority of Singapore), online: MAS <http://www.mas.gov.sg/annual_reports/annual20142015/chapter_2/industry_tests.html>.

[116] *Ibid*.

[117] *Ibid*.

[118] *Ibid*.

[119] CSA, *About Us* (Singapore: CSA, 2 February 2017), online: CSA <https://www.csa.gov.sg/about-us/our-organisation>.

[120] CSA, News Articles, "CSA conducts first Cyber Security Table-top Exercise" (26 May 2015), online: CSA <https://www.csa.gov.sg/news/news-articles/cyber-security-table-top-exercise>.

[121] Ford, *Principles-Based Securities Regulation*, *supra* note 96 at 32; Awrey, *supra* note 95 at 310.

require the institution to take measures to address the deficiencies noted. MAS can also require an institution to modify or replace its cloud arrangements when adequate risk management is not in place or the overall security of customer data has been lowered.[122] Reference should also be made to the broad statutory powers of MAS. Under the *Monetary Authority of Singapore Act*, MAS can issue binding directions on financial institutions.[123] Any failure or refusal to comply with such directions is an offence and punishable by fines.[124] The *Banking Act* also allows MAS to give directions or impose requirements upon banks through issuing notices. In contrast to guidelines, such notices have a binding character and carry penalties for non-compliance.[125] In addition, MAS has the power to conduct on-site inspections and seek access to a firm's information and records.[126] Similarly, refusal to cooperate on the part of a financial institution is an offence and punishable by a fine.[127]

While MAS does not always disclose its enforcement actions to the public, an interesting example in which MAS did is the supervisory action it took against DBS Bank Ltd ("DBS") in 2010.[128] MAS took action against DBS for the service outage of its online and branch banking systems. Following the incident, which caused significant inconvenience to DBS' customers, DBS and its service provider, IBM, were directed by MAS to conduct an investigation into the causes of the breakdown. MAS concluded that DBS' system breakdown was partly due to the DBS' failure to "put in place a robust technology risk management framework".[129] DBS had not exercised sufficient oversight of the functional and operational controls employed by IBM. DBS was required to adopt a series of remedial measures and directed to set aside an additional S$230 million for operational risk.[130]

### D. *Governance through Contract*

Maintaining control over the regulatory process and the regulated actors is key to the success of any regulator. Cloud computing, however, poses an important challenge to financial supervision. As a matter of principle, a financial regulator does not have authority over the technology firm to which a financial institution has outsourced. Hence, the regulator cannot directly impose any requirements on the service provider or oversee the performance of the outsourced operations. MAS' novel solution is a form of 'governance through contract'. Once a financial institution decides to outsource to a cloud computing service, it should incorporate clauses into the outsourcing agreement that allow MAS to exercise the contractual rights of the

---

122 MAS, *New Guidelines 2016*, *supra* note 63 at 8.

123 *Monetary Authority of Singapore Act* (Cap 186, 1999 Rev Ed Sing), s 27A.

124 *Ibid.*

125 *Banking Act* (Cap 19, 2008 Rev Ed Sing), s 55.

126 *Supra* note 123, ss 27C, 27D.

127 *Ibid*.

128 MAS, Media Release, "MAS Takes Supervisory Action Against DBS Bank Ltd For Breakdown of the Bank's Mainframe-Storage Area Network" (4 August 2010), online: MAS <http://www.mas.gov.sg/news-and-publications/media-releases/2010/mas-takes-supervisory-action-against-dbs-bank-ltd-for-breakdown-of-the-bank-mainframe-storage-area-network.aspx>.

129 *Ibid*.

130 *Ibid*.

financial institutions against the service provider. Accordingly, MAS expects to have the contractual right to:

- Access and inspect the service provider and its subcontractors.
- Obtain records and documents of transactions and information of the financial institution given to, stored at, or processed by the service provider and its subcontractors.
- Access any report or finding made on the service provider or its subcontractors, such as audit reports.[131]

The outsourcing agreement should include clauses that require the service provider to comply with MAS' request for information as soon as possible.[132] A financial institution is responsible for ensuring that their service providers and subcontractors have met these requirements. For example, the financial institution is responsible for ensuring that subcontractors have provided adequate recovery and backup services.[133]

While it is a novel approach, governance through contract comes with limitations. Notably, MAS cannot take any direct enforcement action against the service provider or subcontractors. As a third-party beneficiary of the outsourcing agreement, MAS has to resort to judicial proceedings if the service provider or its subcontractor fails or refuses to comply with its directives. Such proceedings can prove costly, time-consuming and challenging, particularly if the service provider conducts business in another jurisdiction. As a result, rapid supervisory intervention to protect public interest may prove difficult when needed.

## V. Conclusion and Reflections

Cloud technology continues to evolve and so do the regulators' responses. As can be discerned from the above discussion, outsourcing to the cloud is a deeply complex process which engages a wide range of actors. Obviously, an important set of actors is the national governments that often try to establish a pro-technology image to attract businesses and investments to their jurisdictions. CSPs are also at the centre of the process. As cloud technology continues to advance and outsourcing costs drop, service providers will be better able to tailor their services to the demands of their corporate clients. At the same time, service providers have incentives to minimise their liability arising from controlling their clients' data. On the other side of the relationship, clients, such as banks, are facing increasing pressure from the post-crisis regulations and the new market entrants, such as 'fintech firms'. Banks see the cloud as a tool to reduce costs and increase efficiency and competitiveness. Finally, while consumers do not directly participate in the outsourcing process, they have the highest stakes in the migration process; it is their personal data which is transferred down the chain of service providers and subcontractors.

---

131 MAS, *New Guidelines 2016*, *supra* note 63 at 21, 22.
132 *Ibid* at 22.
133 *Ibid*.

Thus, the regulation of cloud technology does not take place in a vacuum but rather in an environment characterised by pressures and rival incentives and interests. Any regulatory regime faces an enormous challenge in balancing out these competing forces. Tradeoffs are inevitable; policy choices have to prioritise certain goals or objectives over others. Consider, for example, a national government that aims to improve the quality of life for citizens and business opportunities for enterprises by making fuller use of technology. As a government agency, the regulator needs to take into account this policy objective and cannot, therefore, oppose the use of cloud technologies by financial institutions. At the same time, however, the regulator is bound by law to safeguard the soundness of the financial system and to protect the privacy of consumer information, which might justify limiting the adoption of cloud technology. It is not an easy task to reconcile these two goals, particularly given that the regulator has to deal with actors, such as service providers, that reside outside of its regulatory purview. Further complications arise from the fact that financial institutions' service providers are often technology behemoths with substantial resources and power. A financial institution may, therefore, face hardship in negotiating an outsourcing contract that meets the regulatory expectations, particularly those regarding the regulator's rights to audit and inspect the service provider and its subcontractors.

The recent update of the *Outsourcing Guidelines* in Singapore highlights the rising significance of the cloud in the financial industry and the need for timely regulatory action. A gradual shift in MAS' stance on the cloud can be observed in that the Authority is becoming more receptive to outsourcing to cloud given that the technology is now mature, and regulatory concerns are more likely to be addressed. Projecting ahead, it is important to recognise that the adoption of MAS' *Outsourcing Guidelines* is just the starting point, and that the complex and multi-dimensional regulatory process goes far beyond this step. The most important factor, in fact, is the implementation process and the ensuing interactions between the regulator and the regulated firms that matter most; these cooperative ventures have the power to transform the entire regulatory regime. Throughout this process, as Julia Black notes, the regulator should observe, adapt and change its actions and strategies in light of what is learned.[134]

Given the great reliance of the *Outsourcing Guidelines* on internal controls and processes to achieve regulatory outcomes, the regulator should remain fully engaged and ready to challenge the assumptions and decisions of the board and senior management. An important lesson to be learnt from the recent financial crisis is that the systems and processes that firms put in place may be designed to achieve business outcomes that are at odds with regulatory goals.[135] The best example is the Internal Rating-Based models which were authorised by Basel II for risk weighing and collecting the regulatory capital buffers.[136] As it turned out, however, these models became tools to game the system and significantly underrepresented the risks that

---

[134] Julia Black, "Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis" (2012) 75:6 Mod L Rev 1037 at 1062.

[135] *Ibid* at 1047, 1048; Cristie Ford, "Innovation-Framing Regulation" (2013) 649:1 The ANNALS of the American Academy of Political and Social Sciences at 91, 92.

[136] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, (June 2006) at 52, online: Bank For International Settlements <http://www.bis.org/publ/bcbs128.pdf>.

banks were taking in the years preceding the crisis.[137] Thus, while internal systems and controls are an important component of the cloud regulatory regime, they should not give rise to the interpretation that the firm's assumptions and judgments can escape the critical assessment of regulators.

Remaining proactive and critical of the industry's assumptions is not yet an easy task. The unprecedented interconnectedness that cloud brings to the financial industry is an uncharted territory, raising a new host of issues such as data breaches, cyber security and IT glitches. These issues do not sit well with the current regulatory priorities and practices which focus mostly on traditional financial stability issues like bank capital and counterparty risk. A further challenge is the constant pressure that the regulators face to lower their expectations from the industry. One can take notice, for example, of the recent consultation on the proposed provisions for outsourcing. The participants, mostly financial institutions, managed to soften the original regulatory position in a number of areas. For example, the final *New Guidelines 2016* no longer provides that the period between audits on service providers should not exceed three years.[138] Encrypted information has been excluded from the definition of "customer information".[139] Consequently, obligations regarding the notification of adverse developments, limited disclosure and segregation do not anymore attach to encrypted customer information. In addition, financial institutions no longer need to incorporate indemnity clauses for MAS in their outsourcing agreements.[140] MAS' employees or agents will therefore bear any liability that may arise from accessing or inspecting the service provider or its subcontractors. There was not any non-business interest group or civil society actor to challenge the desirability of these concessions from a public policy perspective. Going forward, it is critical to further engage the broader public and non-business interests in the regulatory debates on the cloud so that the influence of the industry is kept in check and regulatory outcomes enjoy greater legitimacy.

One possible mechanism to ensure ongoing engagement with financial firms, and to adapt to their changing behaviour, is a routine of conducting regular industry-wide reviews on how firms manage and run their cloud businesses. The key question to investigate is how the firms' internal governance and management of the cloud works in practice, and to what extent their practices are aligned with regulatory expectations. These reviews can help convey the regulator's normative stance on the firms' cloud arrangements and identify challenges or weaknesses that exist in their risk management practices. As a result, the high-level principles embodied in the *Outsourcing Guidelines* will be translated into more practical and tangible

---

[137] See *eg*, FSA, *Results of the 2009 Hypothetical Portfolio Exercise for Sovereigns*, *Banks and Large Corporations*, (London: FSA, 1 March 2010), online: FSA <http://www.fsa.gov.uk/pubs/international/sbc_hpe.pdf>; Simon Samuels & Mike Harrison, "Two Hundred Million Inputs: Can You Trust Risk Weightings at European Banks?" *Barclays Capital* (6 April 2011); Vanessa Le Leslé & Sofiya Avramova, *Revisiting Risk-Weighted Assets: Why Do RWAs Differ Across Countries and What Can Be Done About It?*, International Monetary Fund Working Paper WP/12/19 (March 2012), online: IMF <https://www.imf.org/external/pubs/ft/wp/2012/wp1290.pdf>; Andrew G Haldane, "The Dog and the Frisbee" (Speech delivered at the Federal Reserve Bank of Kanas City's 336th economic policy symposium "The changing policy landscape", Jackson Hole, Wyoming, 31 August 2012) at 8, 9, online: Bank For International Settlements <http://www.bis.org/review/r120905a.pdf>.

[138] MAS, *Response to Feedback Received on Outsourcing Consultation*, *supra* note 72 at 5.

[139] *Ibid* at 21.

[140] *Ibid* at 25.

guiding norms which reflect how firms actually run their cloud systems in the real world.

One final note is that there is much more to the regulation of cloud computing than what I have discussed here, which focused on cloud technology in the context of the financial industry. In particular, data protection laws and regulations most directly address the privacy concerns of individuals. These laws and regulations set out the requirements that businesses, including financial institutions, need to comply with in the collection, use, and disclosure of personal data. In Singapore, the *Personal Data Protection Act 2012*[141] is the main statutory regime for privacy, and it is administered and enforced by the recently established Personal Data Protection Commission. The dynamics of this regime and the effectiveness of its safeguards and remedies are important inquiries. However, examining this regime falls outside the scope of this paper.[142]

[141] *Supra* note 61.

[142] See on this inquiry Simon Chesterman, ed, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Singapore: Academy Publishing, 2014).