# Cloud concentration risk: A framework agent-based model for systemic risk analysis

*Received (in revised form) 30th July, 2020*

**Richard L. Harmon**
Global Head, Financial Services, Cloudera, UK

**Perukrishnen Vytelingum***
Head of Quantitative Modelling, Simudyne, UK

**Jiyan Babaie-Harmon****
Simulation Engineer and Operations Manager, Simudyne, UK

*Richard L. Harmon*

*Perukrishnen Vytelingum*

*Jiyan Babaie-Harmon*

***Richard L. Harmon**, PhD, is the Global Head of Cloudera's Financial Services Industry vertical and works closely with most of the top 100 global banks and leading regulators to help drive innovation on Cloudera's globally leading Big Data and Analytics platform. He joined Cloudera on May 2016, and has over 25 years of experience in Capital Markets with specialisations in Risk Management, Advance Analytics, Simulation Methods, Fixed Income Research and Customer Behavioural Analytics. Richard started his career at the Federal Reserve Bank of New York followed by leading fixed income and mortgage research teams at Citibank, Bankers Trust, JP Morgan and Bank of America/Countrywide Capital Markets. He is the cofounder of Risk Monitors, a General Motors Acceptance Corporation-funded Risk Management and Analytics startup, which was acquired by BlackRock, where he was a managing director and partner in the Risk Management Group. Richard left Blackrock to start and manage the North American business for Norkom Technologies, which was later sold to BAE systems. Starting in 2010, Richard was the Director of SAP's Europe, Middle East and Africa (EMEA) Capital Markets group, where he helped grow the business across the EMEA region. Richard has published extensively on a wide range of financial services topics and is frequently an invited speaker at many leading industry events. He holds a PhD in Economics with specialisation in Econometrics from Georgetown University, Washington, DC, USA.*

***Perukrishnen Vytelingum**, PhD, received a Master of Engineering degree in Information Systems Engineering (first-class honours) from Imperial College London, London, UK, and a PhD degree in Artificial Intelligence (AI) from the University of Southampton, Southampton, UK. He spent some time in academia as a Senior Research Fellow in the IAM Group, University of Southampton where he published over 30 peer-reviewed papers in the top AI journals and conferences. Thereon, he joined the industry as a Credit and Market Risk Quantitative Developer at Sungard/FIS and later as a Market Risk Quant at J.P. Morgan and is currently the Head of Quantitative Modelling at Simudyne. His main interests include agent-based modelling, market mechanism design, Evolutionary Game Theory and market simulations.*

***Jiyan Babaie-Harmon** is a Simulation Engineer as well as Operations Manager at Simudyne. He joined Simudyne in 2017, after receiving his degree in biomedical sciences at Auburn University, Auburn, Alabama, USA. He focuses on building agent-based simulations in the Simudyne SDK across a wide variety of applications and use cases that include finance, health and life sciences and defence. He graduated from the Barclays Techstars '17 accelerator programme and is a graduate of the University of Cambridge Judge Business School Executive Education Program. His main research interests include agent-based modelling and the study of Complex Adaptive Systems in Finance and the Biological Sciences.*

*30 Old Broad Street, 5th Floor,*
*London EC2N 1HT,*
*UK*
*Tel.: +44 7983 446740;*
*E-mail: rharmon@cloudera.com*

*St Michael's Alley, Langbourn,*
*London EC3V 9DS,*
*UK*
**Tel.: +44 7921 835030;*
*E-mail: krishnen@simudyne.com*

***Tel.: +44 7495 046338;*
*E-mail: jiyan@simudyne.com*

Journal of Financial Compliance
Vol. 4, No. 2 2020, pp. 1–25

2398-8053

**ABSTRACT**

*This paper provides a brief overview of key trends in cloud adoption and cloud deployment strategies, how global regulators are evaluating cloud-related operational risks and how might they deal with these potential risks in the future. Furthermore, the role of recent innovations in the Big Data and Analytics space has resulted in a next generation hybrid, multicloud architecture that addresses many of the near-term operational risks that regulators have identified with public cloud adoption. The last section of this paper outlines a framework agent-based model (ABM) that can be the foundation for regulators, market participants and cloud service providers (CSPs) to evaluate these types of risks. This approach can identify potential contagion trigger points that can lead to cloud-driven systemic risk events. The authors demonstrate how this framework ABM can be extended to evaluate regulatory policies under different criteria and market structures. Future research points to the integration of Evolutionary Game Theoretic configurations that could help determine the effectiveness of potential regulatory policies as well as identify circumstances where suboptimal regulatory and compliance outcomes arise.*

*Keywords: cloud outsourcing, operational resiliency, regulatory oversight, cloud concentration risks, agent-based simulation modelling*

## INTRODUCTION

> *'We are moving towards a world where there is a highly regulated industry that is running on non-regulated third-party infrastructure.'*
>
> *Anonymous CTO — G-SIB*

The earlier-mentioned statement summarises how profoundly the financial services industry will be transformed by cloud computing in the next five years. This seismic change will drive new innovations but concurrently introduce new types of risks that need to be addressed by regulators, the financial services industry and technology innovators.

Since the financial crisis, regulators have been consistently working to identifying emerging risks that can potentially result in financial stability events. One of these areas is around cloud concentration risks. In the past couple of years, more regulators have begun to explore this topic and are evaluating the potential operational and financial stability risks from the industry's accelerating movement to the cloud. Additionally, several global systemically important banks (G-SIBs) have also taken note and are beginning to consider this as a new factor within their operational risk frameworks. Their primary focus is on concerns related to vendor lock-in, consistent data governance and data security when adopting a multicloud strategy rather than the wider systemic risk exposures.

This paper provides a brief overview of key trends in cloud adoption and cloud deployment strategies, how global regulators are evaluating cloud-related operational risks and how might they deal with these potential risks in the future. Furthermore, the role of recent innovations in the Big Data and Analytics space has resulted in a next-generation hybrid, multi-cloud architecture that addresses many of the near-term operational risks that regulators have identified with public cloud adoption.

What is still outstanding, in the authors' opinion, is the need to analyse the financial stability risks associated with Cloud Concentration Risk. To do this properly requires understanding the linkage dependencies among cloud service providers (CSPs), financial institutions and their counterparties. This type of analysis can help regulators evaluate a wide range of regulatory paradigms that can be created to rein in cloud-related systemic risks while avoiding over regulation that can

stifle the innovation that cloud computing can provide to the financial services sector.

The last section of the paper outlines a framework agent-based model (ABM) that can be the foundation for regulators, market participants and CSPs to evaluate these types of risks. This approach can identify potential contagion trigger points that can lead to cloud-driven systemic risk events. The authors demonstrate how this framework ABM can be extended to evaluate regulatory policies under different criteria and market structures. Future research points to the integration of evolutionary game theoretic configurations that could help determine the effectiveness of potential regulatory policies as well as identify circumstances where suboptimal regulatory and compliance outcomes arise.

## CLOUD SERVICE PROVIDER OFFERINGS

The cloud environment can be simplified by segmenting this market into three types of services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).[1]

Infrastructure as a Service (IaaS): IaaS delivers cloud computing infrastructure, including servers, networks, operating systems and storage, through virtualisation technology. IaaS provides the same technologies and capabilities as a traditional data centre without having to physically maintain or manage all the physical components. IaaS clients access their servers and storage directly, but it is all outsourced through a 'virtual data centre' in the cloud. IaaS is the most flexible cloud computing service with the following benefits:

- Resources are available as a service
- Cost varies depending on consumption
- Services are highly scalable
- Multiple users on a single piece of hardware
- Institutions retain complete control of the infrastructure
- Dynamic and flexible

Platform as a Service (PaaS): PaaS delivers a framework for developers that they can build upon and use to create customised applications. All servers, storage and networking can be managed by the enterprise or a third-party provider while the developers manage the applications. This platform is delivered via the web, giving developers the freedom to concentrate on building the software without having to worry about operating systems, software updates, storage or infrastructure.

Software as a Service (SaaS): SaaS utilises the internet to deliver applications, which are managed by a third-party vendor, to its users. Most SaaS applications run directly through the web browser, which means they do not require any downloads or installations on the client-side.

Figure 1 provides a clear delineation between the three cloud service offerings.[2]

## INDUSTRY TRENDS IN CLOUD COMPUTING

Cloud adoption in financial services has been accelerating over the past few years. Enterprises are after the speed, agility, simplicity and lower costs that it provides.

The most recent analysis of the global cloud market by Gartner shows that IaaS market grew 31.3 per cent in 2018 to total US$32.4bn, up from US$24.7bn in 2017. As documented in Figure 2, Gartner estimates that Amazon continues to hold the largest market share in the IaaS market in 2018, with a 47.8 per cent market share. This is followed by Microsoft, Alibaba, Google and IBM. It should be noted that AWS and Microsoft have a combined global market share of 63.3 per cent in 2018, a slight increase from their 62.1 per cent combined global market share in 2017.

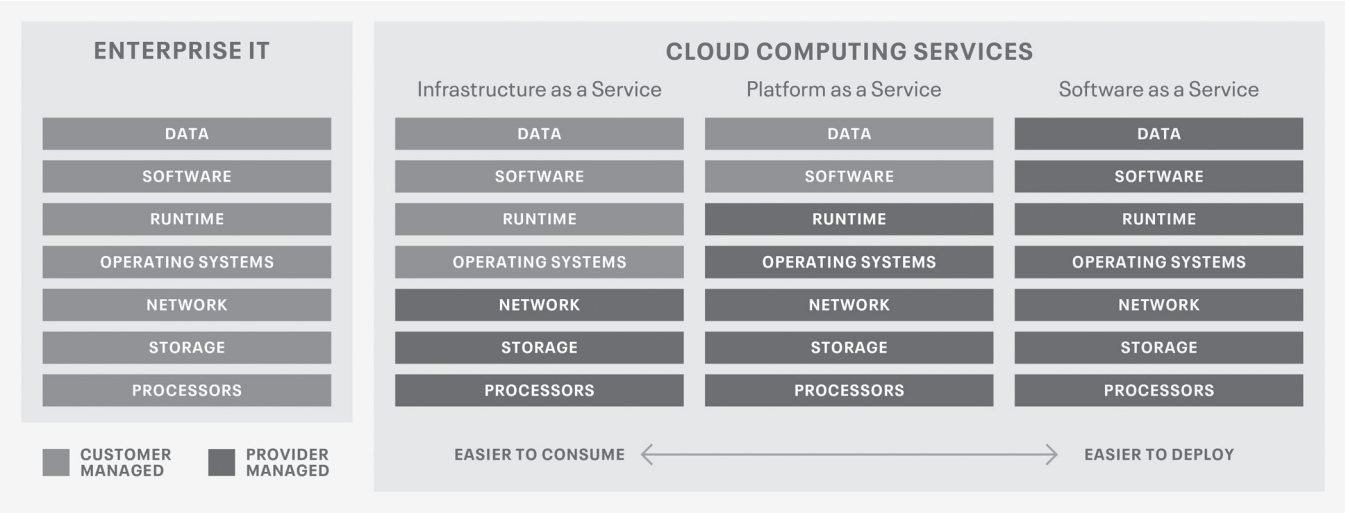


*Figure 1 Cloud service models*

| | 2018 | | 2017 | | 2018-2017 |
|---|---|---|---|---|---|
| Company | Revenue | Market Share (%) | Revenue | Market Share (%) | Growth (%) |
| Amazon | $15,495 | 47.8% | $12,221 | 49.4% | 26.8% |
| Microsoft | $5,038 | 15.5% | $3,130 | 12.7% | 60.9% |
| Alibaba | $2,499 | 7.7% | $1,298 | 5.3% | 92.6% |
| Google | $1,314 | 4.0% | $820 | 3.3% | 60.2% |
| IBM | $577 | 1.8% | $463 | 1.9% | 24.7% |
| Others | $7,519 | 23.2% | $6,768 | 27.4% | 11.1% |
| Total | $32,441 | 100.0% | $24,699 | 100.0% | 31.3% |

*Figure 2 Worldwide IAAS public cloud services market share, 2017–2018 (millions of US dollars)*
*Source: Gartner (2019) 'Forecast: Public Cloud Services, Worldwide, 2017–2023, 3Q19 Update'*

Gartner's research vice president, Sid Nag, highlights this trend in his analysis:[3]

> *Despite strong growth across the board, the cloud market's consolidation favours the large and dominant providers, with smaller and niche providers losing share . . . This is an indication that scalability matters when it comes to the public cloud IaaS business. Only those providers who invest capital expenditure in building out data centers at scale across multiple regions will succeed and continue to capture market share.*

*Offering rich feature functionality across the cloud technology stack will be the ticket to success, as well.*

## REGULATORY FOCUS ON THIRD-PARTY OUTSOURCING

The growth in cloud adoption across the financial services industry and the associated increase in reliance on third-party infrastructure providers have gained the attention of regulators at global, regional and national levels.

At a high level, a core regulatory concern is with the operational resiliency in the 'shared responsibility model' that exists between a cloud customer and the CSP. Within the context of the IaaS offering, while the CSPs retain responsibility over the lower level layers of infrastructure, the financial institution is responsible for the data stored and processed, the overall security of the solutions developed on the cloud and the ability to assess the CSP's compliance with mandatory resiliency requirements.[4]

### Global regulators

At the global level, the Financial Stability Board (FSB) and the Bank of International Settlements (BIS) have recently issued several publications focused on the operational and supervisory risks of third-party CSPs. A recent FSB study[5] identified a few notable market trends that highlight operational and financial stability concerns:

- From a survey of 294 global financial service institutions, the respondents exhibited a strong reliance on a narrow set of major CSPs.
- While currently very limited, the survey noted the accelerating use of cloud services for 'core' or critical systems.

Based on these trends, FSB identified several areas of concern related to financial stability:

- Operational incidents at third-party service providers may result in temporary outages affecting financial institutions, and misconfigurations of new tools could result in data breaches.
- Concerns about the ability to monitor and manage third-party CSP-related operational risks due to contractual limitations on institutions' and regulators' rights of access, audit and information.
- Bank resolution authorities may have difficulties when exercising step-in rights in resolution if critical bank data systems are held in third-party systems.
- There are a number of cross-border, cross-jurisdiction-related complexities in the oversight of providers and in the management of systemic risks.
- Potential concentration in third-party provision could result in systemic effects in the case of a large-scale operational failure or insolvency.

The authors emphasise the last two points as these are key factors that relate specifically to systemic risk exposures.

### European regulators

On the European side, there are several recent publications from the European Banking Authority (EBA), the European Central Bank (ECB), the European Systemic Risk Board (ESRB), the European Insurance and Occupational Pensions Authority (EIOPA), the European Securities and Markets Authority (ESMA) and the Bank of England that are focused on systemic risk-related concerns around third-partner outsourcing impacts.

ESMA[6] on 3rd June issued the latest European regulatory guidelines that intend to 'provide guidance on the outsourcing requirements applicable to firms where they outsource to cloud service providers'.

As with the EBA's earlier guidance, a key element of these future guidelines includes the requirement for a Cloud Outsourcing

Register to be in place by the end of 2021. This will be a critical element in providing regulators with greater transparency on what critical infrastructure and applications are running in the cloud.

> *A firm should maintain an updated register of information on all its cloud outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.*

The EBA published revised outsourcing guidelines for the banking sector in February 2019, that became effective on 30th September, 2019.[7] The key outsourcing requirements consisted of the following:[8]

- The revised guidelines are consistent with current outsourcing requirements within Payment Services Directive 2, Markets in Financial Instruments Directive 2 and the Central Registration Depository (CRD), but extend the scope of the previous Committee of European Banking Supervisors (CEBS) guidelines to cover all banking, payment and investment services.
- Each financial institution's management body remains responsible for its activities at all times and must ensure that sufficient resources are applied to the oversight and risk management of all outsourcing arrangements, with particular regard to those that support critical or important functions.
- Where the outsourced service provider is located in a third country, institutions must ensure that all EU legislation and regulations are complied with, including, but not limited to, the protection of personal data.
- To enable competent authorities to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring associated concentration risks, institutions must be able to provide comprehensive documentation on their outsourcing arrangements.

In principle, the combined ESMA and EBA guidelines appear to be one of the most extensive efforts by regulators to begin to manage perceived risks from CSPs.

Similarly, the ESRB's recently released study on systemic cybersecurity risk[9] noted that:

> *. . . the adoption of new technologies such as cloud computing creates new interdependencies with entities that may operate outside the boundaries of regulated financial systems.*

Furthermore, the UK House of Commons Treasury Committee[10] noted that the Bank of England, the Financial Conduct Authority and the Prudential Regulation Authority found:

> *At the system level, some third-party providers (including cloud service provides) may be a key point of concentration and present a single point of failure risk where an operational incident could have a widespread impact on the system.*

In their December 2019 consultation paper,[11] the Bank of England and the Prudential Regulatory Authority set out proposals for modernising the regulatory framework on outsourcing and third-party risk management. This consultation paper acknowledges the growing benefits of third-party cloud outsourcing arrangements 'to gain entry to new markets, lower operating costs, fuel innovation and adapt to the digital economy' but they layout their key cloud-related regulatory concerns:

- To ensure that confidential and sensitive data is secure at all times and accessible to firms and regulators, especially during or following an operational disruption.
- The technical complexities and constant evolution of the cloud complicate management oversight and risk evaluation.
- The heavily concentrated cloud market is dominated by a small group of

service providers which can result in vendor lock-in effects.
- Systemic concentration risk can arise if a major disruption, outage or failure at one CSP creates a single point-of-failure with potentially adverse consequences for financial stability.

Furthermore, the Bank of England and Prudential Regulatory Authority outline requirements for meeting EBA Outsourcing Guidelines mandating that an Outsourcing Register should be completed by 31st December, 2021. The Outsourcing Register should include:

- New outsourcing arrangements entered into from 30th September, 2019, onwards.
- Legacy Outsourcing Arrangements as they become due for review or renewal, intending to have a complete Outsourcing Register by 31st December, 2021.

### United States regulators

On the US side, regulatory entities coordinate their supervision of banks and their technology service providers through the Federal Financial Institutions Examination Council (FFIEC), whose members include the Federal Reserve Board of Governors, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau. The FFIEC sets policy regarding the responsibility of various agencies, which service providers get examined, the frequency of examination and the scope of supervision.[12,13]

The Federal Reserve, the US Congress and other policy leaders in the United States have started to explore whether the regulators are properly set up to ensure that they have the tools for addressing cloud concentration risk exposures. There has been much discussion on the use of the Financial Stability Oversight Council to designate Amazon Web Services, Microsoft Azure and Google Cloud as 'systemically important financial market utilities'.[14] This will continue to be a discussion topic with the US regulators looking internationally to address the global systemic risk issue around cloud concentration risk.

In testimony to Congress, Federal Reserve Governor, Lael Brainard, stated:

> *Certainly there's work internationally where we're thinking about precisely this question that you raise about the ability to failover . . . [regulators recognize that] migrating to the cloud mitigates some risks, adds other risks, and so we need to hold our institutions accountable for making that risk assessment in a very well-informed way and taking that migration very seriously.*[15]

### Asia region regulators

The APAC region is a global leader in many areas of mobile interaction and digital transformation. Regulators overall have been accommodating towards some use of cloud services, but some are still clarifying outsourcing rules and guidelines to help institutions achieve compliance. Generally, the APAC region has more regulatory restrictions on cloud adoption. Very few critical core banking systems currently reside in the cloud. More institutions will slowly begin to migrate to the cloud in the next few years although at a slower pace than in the United States or Europe.[16]

The Monetary Authority of Singapore has a consultation on new proposals to expand its regulatory oversight of bank outsourcing arrangements. The new regime will require banks to conduct due diligence checks on technology partners and demonstrate that they have satisfactory safeguards and response plans in place in the event of a disruption.

Similarly, the Hong Kong Monetary Authority is also enforcing third-party vendor risk management guidelines for financial services institutions.[17] The Australian Prudential Regulatory Authority outlined their oversight role for cloud computing services:

> *When the proposed use of cloud computing services involves heightened or extreme inherent risks, APRA encourages consultation prior to entering into any arrangement, regardless of whether offshoring is involved*[18]

## SYSTEMIC RISK AND CLOUD CONCENTRATION RISK EXPOSURES

The previous section highlights a few key examples of the breadth and variety of regulatory approaches being taken to address third-party CSPs. Regulators have, however, not yet addressed in sufficient detail specific concerns about potential systemic risk impacts. This is especially true of the risks associated with cloud concentration risk.

Detailed CSP IaaS cloud market share estimates for the financial services industry are not publicly released by the CSPs. Fortunately, in January 2020, the Bank of England published some high-level results of an annual survey of the 30 largest banks and 27 largest insurers that they supervise to understand how these institutions utilise the cloud. This includes a good selection of some of the largest global banks as many have significant operations in London.[19]

As revealed in Figure 3, the top two providers, AWS and Microsoft, probably have a slightly higher combined market share concentration in the financial services industry than Gartner measured across the overall market (see Figure 2).

It should be noted that in this publication the Bank of England stated:

> *Our survey indicates that for banks and insurers, the provision of IT infrastructure in the cloud is already highly concentrated.*

Furthermore, they mentioned that:

> *We will use the results of the survey to inform and adjust our supervisory approach to cloud oversight.*

While a diverse list of operational resiliency concerns has been identified across many regulator publications, outside of the important concern about CSP auditability, the authors perceive the following six items reflect the most critical factors in evaluating future systemic risk exposures.

1. Lack of Unified Data Security and Governance — Each cloud native product re-creates its own silo of metadata making data management, security and governance much more complex.

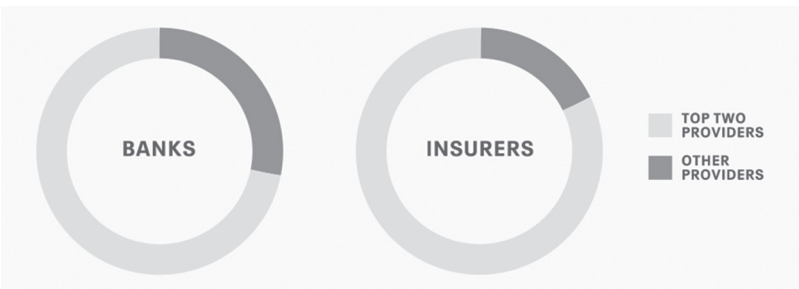


*Figure 3 Market share of providers of infrastructure as a service*
*Source: Bank of England, Bank Overground, January 17, 2020.*

Without a unified security and governance framework, institutions will be challenged to identify, monitor and address crucial issues in data management that are critical for proper measurement of risk exposures across different platforms. This is especially true for hybrid or multi-cloud environments.

2. Cyber Attack Resiliency — The consolidation of multiple organisations within one CSP presents a more attractive target for cybercriminals than a single organisation.[20] A further complication is that cloud security is a shared responsibility between the CSP and the institution.
3. Vendor Lock-In — The market share concentration of a small group of CSPs can result in significant lock-in effects, whereby an institution is unable to easily change its cloud provider either due to the terms of a contract, a lack of feasible alternatives, proprietary technical features or high switching costs.
4. Operational Resiliency — Much of the operational resiliency concerns by regulators is the 'shared responsibility' model inherent in the relationship between a cloud customer and the CSP. Regulators have consistently made it clear that institutions at all times remain fully responsible for all the operational functions they outsource to third-party providers. This addresses the liability but does not address the fundamental exposure that still exists.
5. Lack of Transparency — A CSP is unlikely to share detailed information about its processes, operations and controls. This restricts not only an individual institution but also the regulator from being able to fully ensure sufficient oversight to ensure very limited operational risk exposures as well as the ability of regulatory authorities to properly perform their oversight function. From a reporting perspective, the United Kingdom and Luxembourg regulators require institutions to periodically report all functions outsourced to the cloud, alongside requiring preauthorisation for critical activities. The EBA Outsourcing Guidelines provide that banks should gradually build an Outsourcing Register, which should be complete by 31st December, 2021.[21]
6. Cloud Concentration Risk — Regulators are concerned about institutions' overreliance on one service provider to support their banking services. This not only presents operational risks for individual institutions but creates financial stability risks for the financial system within a single country as well as globally. Concentration risks also arise if a significant number of institutions have a key operational or market infrastructure capability (eg payment, settlement and clearing systems) in a single CSP. For instance, there is abundant research and analysis on the potential systemic risk exposures from Central Counterparties and their default fund structures but little discussion among regulators on cloud concentration risk in these risk assessments.

Specifically, with regard to the issue of cloud concentration risk, one can segment this into two distinct categories:

- Firm-Specific Concentration Risks: These consist of risks due to cloud lock-in, a lack of unified data security and governance across CSPs and third-party operational resiliency concerns such as auditability, multi-cloud controls and cybersecurity exposures.
- Systemic Concentration Risks: These consist of risks that affect the stability of the financial system. This includes a lack of transparency in what critical applications currently reside on or will migrate to a specific CSP. Regulators are also concerned about the systemic risk of having a concentration of many large financial

service firms' critical application(s) all reside on the same CSP. For example, these include payment, settlement and clearing systems.

This bifurcation of oversight complexities of cloud concentration risk highlights the need for the financial services industry, the CSPs and regulators to collaboratively work towards resolving these issues.

Fortunately, recent innovations in developing a comprehensive hybrid, multi-cloud architecture, generically, referred to as the 'Enterprise Data Cloud', directly eliminates most of the concerns around vendor lock-in dangers as well as the lack of unified multi-cloud data security and governance capability that in turn helps address several key concerns of firm-specific cloud concentration risk.

## THE ENTERPRISE DATA CLOUD — THE FUTURE OF CLOUD COMPUTING

The original Big Data open source platform, Hadoop, has experienced continuous innovation throughout the past decade. The advent of the wide adoption of cloud computing and the need to manage data, workloads and security across many platforms have led to the development of the next-generation Big Data platform. At Cloudera, they call this next-generation hybrid, multi-cloud architecture the 'Enterprise Data Cloud'. Gartner calls this the emergence of 'Cloud Data Ecosystems'[22] while 451 Research describes this as 'Enterprise Intelligence Platforms'.[23] Regardless of the terminology chosen, the clear understanding is that the future of cloud computing will need to support an agile hybrid, multi-cloud environment that allows for the full portability of data and applications across all relevant platforms.

From a high-level perspective, an enterprise data cloud needs to support:

- Hybrid and multi-cloud — to provide data-management capabilities to manage, analyse and experiment with data in any public or private cloud or on-premise data centre for maximum choice and flexibility.
- Multifunction capabilities — to address the most demanding business use cases requires applying real-time stream processing, data warehousing, data science and iterative machine learning across shared data at scale.
- Secure and governed — simplifies data privacy, security and compliance for diverse enterprise data with a common security model to govern data on any cloud — public, private and hybrid.
- Open Source — facilitates innovation within the open source community, the choice of open storage and compute architectures without vendor lock-in, and the confidence and flexibility of a broad ecosystem supporting both legacy systems and innovative partners.

While hybrid cloud environments bring substantial advantages in terms of rapid deployment and reduced infrastructure costs, they bring a new set of data-management challenges. As cloud environments multiply, new cloud data silos can appear, some of which bypass IT (information technology) altogether. Securing and governing data that lives across multiple clouds, each with their own architecture is difficult. Furthermore, cloud vendor lock-in effects can make it difficult and costly to migrate applications or data.[24]

From a cloud migration perspective, it is important that institutions first develop an enterprise data strategy before finalising their cloud strategy. This allows institutions to implement their enterprise data strategy consistently in the cloud by focusing on data storage, data management and data protection requirements. This helps to ensure that a uniform multiplatform security and governance

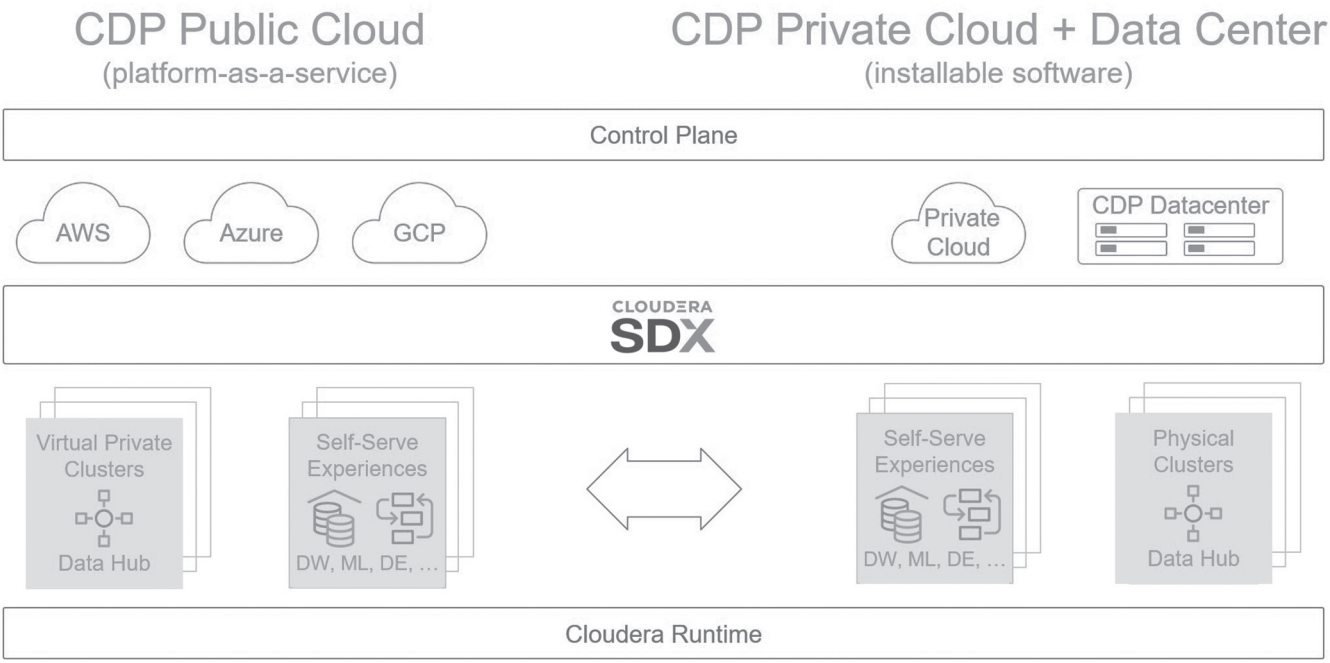


*Figure 4 One platform – three form factors*

framework is put into place that supports an institution's core business objectives — such as increasing revenue, improving customer satisfaction and protecting the business while driving profitability.

Cloudera is leading the industry in offering the world's first Enterprise Data Cloud. It is called the Cloudera Data Platform (CDP). As illustrated in Figure 4, the CDP provides three form factors; CDP Public Cloud, CDP Private Cloud and CDP Data Centre (the on-premises version of CDP) in a single unified platform that prevents cloud lock-in, supports the complete data life cycle, provides a single control plane to secure, govern and track data linages across all platforms and allows for the portability of data and applications as required.

## AN ABM FRAMEWORK FOR SYSTEMIC RISK ANALYSIS

The complex and emergent behaviour of financial markets, especially under stress, has proven difficult to model with traditional mathematical approaches. A simulation-based approach that comes out of the complexity science literature is starting to gain traction in financial services. This approach is referred to as agent-based modelling (ABM). ABM is a bottom-up approach to the modelling of complex and adaptive systems with heterogeneous agents.

A key factor that is not addressed by traditional machine learning-based approaches is that the sequencing of events within a period of time can be vitally important for capturing interconnecting effects that develop into trigger points for wider contagion effects. This allows ABMs to explain how the behaviour of individual institutions or agents can affect outcomes in complex systems and offers the opportunity to understand potential vulnerabilities and paths through which risks can propagate across the financial system. Additionally, such models offer the ability to


*Figure 5 Diebold-Yilmaz Total System Connectedness Index (System: 27 US & EU Banks)*

depict the heterogeneity of agents, as well as idiosyncratic rules for how financial institutions operate, which are important for replicating real market conditions.[25]

The ABM simulation framework allows regulators and financial service institutions to develop dynamic simulation environments that can evaluate thousands of stress test scenarios at the system-wide level. This can be an indispensable tool to identify and quantify emerging financial stability risks around third-party cloud outsourcing and cloud concentration. In this framework ABM, explicitly modelling a specific type of critical financial market infrastructure is not done, but they identify a generic situation that involves a flow of transactions that are critical to the bank and the wider financial system.

The authors utilise the Diebold–Yilmaz 'connectedness' approach[26,27,28] to provide a market-based measure of the strength of interrelationships between banks, focusing on the degree of volatility spillovers. The Diebold–Yilmaz connectedness framework measures connectedness from three perspectives: total connectedness, total directional connectedness and pairwise directional connectedness. Total connectedness is an overall description of the degree of system connectedness. Total directional connectedness from others represents the share of volatility shocks received from other institutions in the total forecast error variance of each bank's stock price, while total directional connectedness to other banks stands for each bank's stock price's contribution to the other banks' forecast error variances. Pairwise directional connectedness indicates the directional connectedness between two banks.

From a practical perspective, the perception that a bank's riskiness is likely to spillover to other banks should be reflected in high levels of comovement in their stock price volatility at high frequency, due to the implications of connectedness for bank profitability. For the authors' case, they utilised the median index value of the pairwise directional connectedness for the 12-months ending on 22nd May, 2020, as a proxy for the volume of transaction flow between banks.[29]

Figure 5 shows the Diebold–Yilmaz Connectedness Index from 23rd May, 2019, until 22nd May, 2020. One can see the elevated levels of connectedness that have

arisen out of the coronavirus disease-2019 pandemic.

### The authors' framework ABM structure

The authors' framework ABM is a discrete-step simulation consisting of a structural and a behavioural component. The structural component consists of two types of agents: Banks and CSPs. Banks are fully connected to each other and are connected to one or more CSPs as seen in Figure 6. Banks can send and receive transaction flows proportional to their bank connectedness, as measured by the Diebold–Yilmaz connectedness measure. The CSP provides the IaaS cloud environment that the bank utilises to run its critical financial infrastructure application which settles transactions received from the bank. In this framework ABM, the authors have 27 US and EU banks that coincide with the latest Diebold–Yilmaz (2017) connectedness estimates. They have three CSPs (CSP1 to CSP3) reflecting the cloud concentration risk that the regulators have noted as documented earlier. In both cases, this can be easily extended to as many banks and CSPs needed.

This general arrangement is illustrated in Figure 6.

Figure 6 provides a high-level overview of the model structure showing single and hybrid cloud banks connected to CSPs. Single cloud banks are restricted to the use of one CSP while hybrid cloud banks can switch between CSPs if there is a service interruption.

The behavioural component specifies how agents behave at each step of the simulation. The images in Figure 7 illustrate the full system view.

Image (A) shows the network of banks connected to each other and of each bank connected to 1, 2 or 3 CSPs. Image (B) shows the use of the Diebold–Yilmaz bank connectedness measure as a proxy for transaction flow between banks. Negative connectedness is modelled as zero transaction flow. Image (C) shows the total asset of each of the 27 banks.[30] The authors now outline how agents are specified in this framework ABM as well as how they are measuring two types of risk exposures: settlement risk exposures and credit risk exposures.

In this framework ABM setup, the authors are interested in bank-specific risk as well as systemic risk. While the authors implement a mechanism to propagate risk based on the transaction flow, they measure two types of risk: settlement risk,

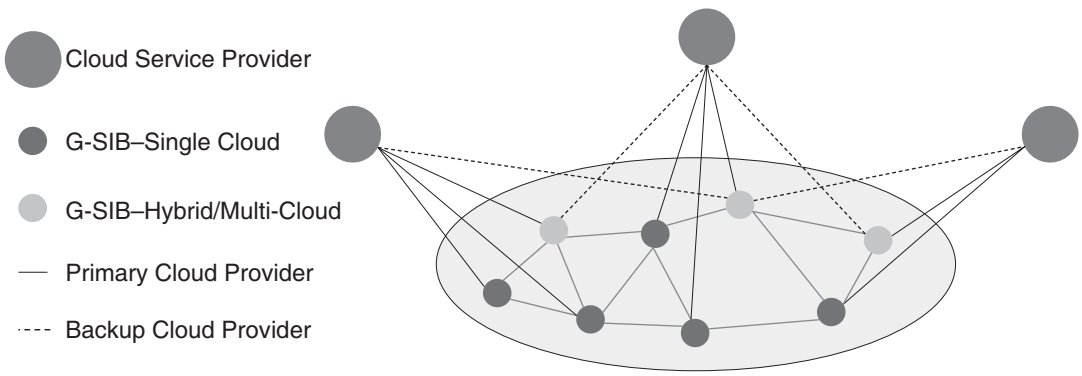


*Figure 6 ABM Framework Model Structure Between Banks and CSPs.*

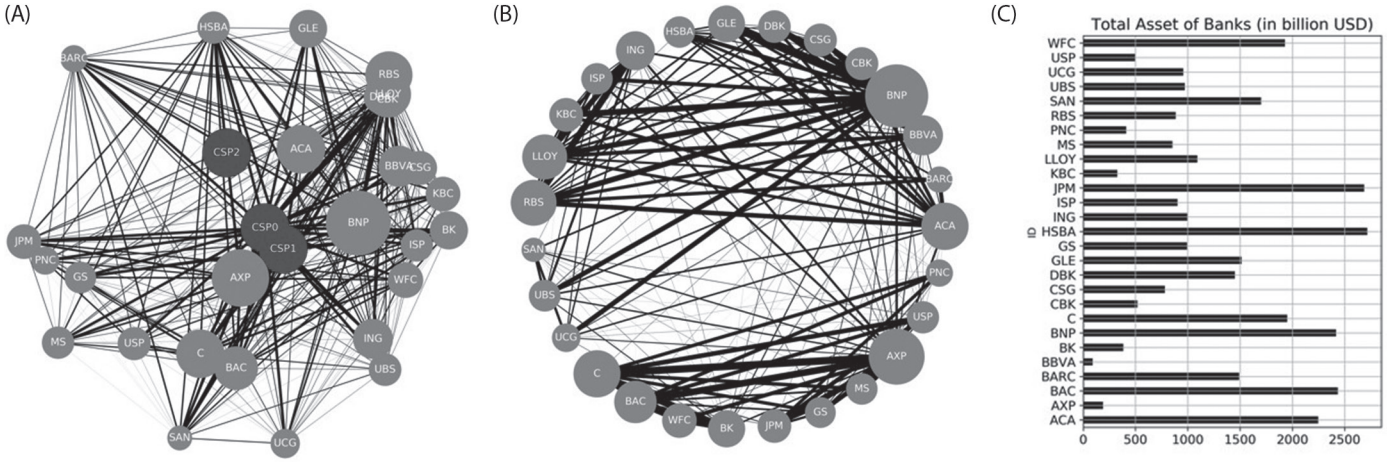


*Figure 7 Full System View: (A) Banks and CSPs; (B) Diebold–Yilmaz Bank Connectedness Measure; (C) Bank Size By Total Assets.*

which would more closely resemble an operational risk exposure in the real world, and credit risk. Given the system-wide bank connectedness, they measure the spill-over of risk across the system as credit risk exposure of a bank that depends on its interrelationship with other banks. Specifically, with a connected bank rejecting a transaction once they hit their specific settlement risk exposure limit, this translates to an increase in credit risk for the bank as the transaction remains pending and the bank is exposed to the risk of the transaction not being fulfilled.

While there are many more complex ways of calculating various types of systemic risk, these are, however, beyond the scope of this paper. The framework ABM uses a simple risk measure, the accumulation of individual bank credit risk exposure. This can result in emergent systemic risk exposures based upon the spread of rejected transactions emanating from the connected bank agents as the mechanism for disseminating risk throughout the system. The authors now describe how the agents are specified, how settlement risk exposures and credit risk exposures are created and how this propagates across the banking system.

## The agents

The CSP hosts critical financial infrastructure applications that settle transactions from the banks. There a probability of $P_k^{fail}$ that CSP k fails at each step. When the CSP fails, it sends a down status update to the connected banks, and when the CPS is back up, it sends an OK status to the banks. A CSP is down for a period of downtime that is drawn for each simulation from an exponential distribution:[31]

$$t_k^D \sim \mathrm{Exp}\left(\lambda_k^D\right).$$

The bank i sends and receives transactions $p_{s,i,j}$ from bank j and the bank settles $p_{s,i,j}$ through its critical financial infrastructure application hosted by CSPs, $\ell_i$, settling a proportion $\omega_k \forall k \in \ell_i$ where $\sum_{k\in\ell_i} \omega_k = 1$. As a default, transactions are settled equally across CSPs, where:

$$\omega_k = 1 \Big/ |\ell_i|$$

## Settlement risk exposure

### *Single CSP*

Now, if a CSP is down, any unsettled transaction is accumulated by bank i as

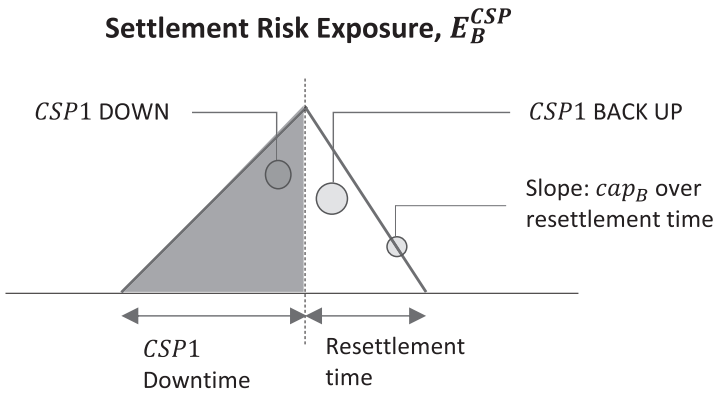


*Figure 8 Single CSP*

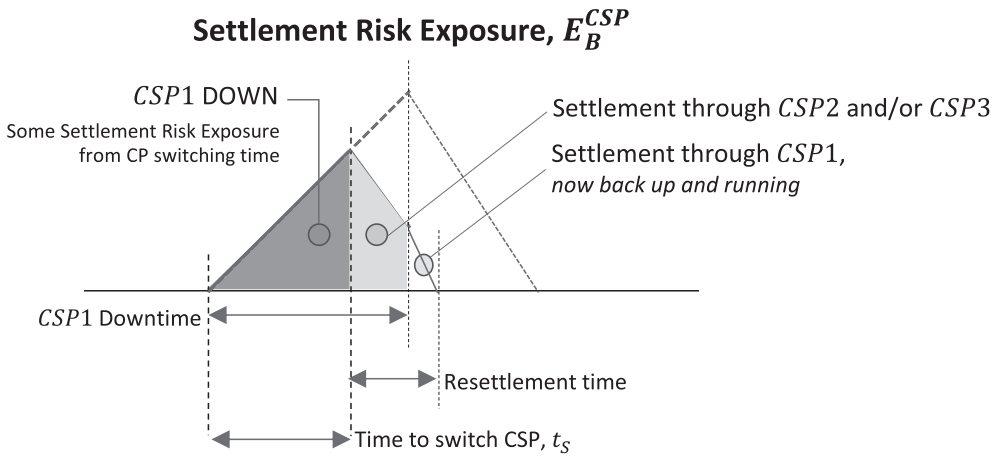


*Figure 9 Hybrid CSP*

settlement risk exposure $E_i^{SR}$ until the CSP is backup. When the CSP is back up, the unsettled transaction is then settled at a rate of $cap_i$ until $E_i^{SR} = 0$ during a resettlement time. Now, if there is more than one CSP, the bank i can switch to other CSPs with a delay, $t_i^S \sim \text{Exp}\left(\lambda_i^S\right)$ and the proportions are adjusted such that $\omega_k = 0$ for all CSPs that are down.

As illustrated in Figure 8, when CSP1 fails, the bank accumulates the (unsettled) transaction flow as settlement risk exposure (shown in red). Once CSP1 is back up, the unsettled transaction flow is settled by CSP1 at a resettlement rate, $cap_k$.

### *Hybrid CSP*

The hybrid CSP example has the bank utilising more than one CSP. While the authors have outlined a process where any switchover of the critical financial infrastructure application's transaction flow is done equally across more than one CSP, it is easy to adjust this settlement behaviour so that all transactions can be settled in a specific second CSP which sequentially can be switched to the third CSP should the second CSP fail.

Figure 9 illustrates the case where the bank has a hybrid CSP setup. In this case,

a bank has the option to switch its critical financial infrastructure application to another CSP when one is down, subject to some switching time, $t_i^S$ during which it accumulates settlement exposure risk. Once switched, the settlement is transferred to one or more other CSPs until the original CSP is back up where it takes over the settlement of the backed-up transaction flow. Again, one can easily allow for different operational situations where a bank might have a critical financial infrastructure application running in parallel on a second CSP, which would make the switching time very short while other banks would need additional time to switch a critical financial infrastructure application to a second CSP.

### *Settlement risk exposure limit*

When the settlement risk exposure breaches a limit $L_i^{SR}$, bank rejects transactions from all other banks until the settlement risk exposure goes below the limit.

In Figure 10, the authors illustrate the impact of the settlement risk exposure limit. This can be specified in many ways. In this framework ABM example, when the settlement risk exposure limit is breached, the bank rejects the transaction flow from other banks. This leads to the start of the accumulation of credit risk exposures by Bank A.

## Credit risk exposure

In this framework ABM, we are interested in bank-specific risks as well as systemic risk. While we implement a mechanism to propagate risk as a proxy for transaction flow, we measure an operational type of risk as settlement risk, which then accumulates to a bank's specific limit; this results in halted transactions and accumulation of credit exposure risk. We measure the spillover of risk across the banking system as credit risk exposure based of an individual bank's interrelationship with other banks. Specifically, with a connected bank rejecting a transaction, this translates to an increase in credit risk for the bank as the transaction remains pending and the bank is exposed to the risk of the transaction not being fulfilled.

While there are more complex ways of calculating various types of systemic risk, these are beyond the scope of this paper. This framework ABM uses a simple measure, the sum of individual bank credit risk exposure, which results in emergent systemic risk exposures coming from the agent-based interactions of connected bank agents and captures how risk is spreading through the system.

When bank i rejects a transaction from bank j, this transaction is accumulated as part of the bank j's credit risk exposure $E_j^{CR}$. When bank j's credit risk exposure breaches its credit risk exposure threshold

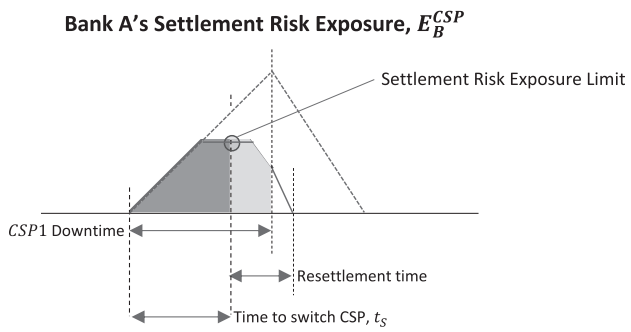


*Figure 10 Settlement risk exposure limit*

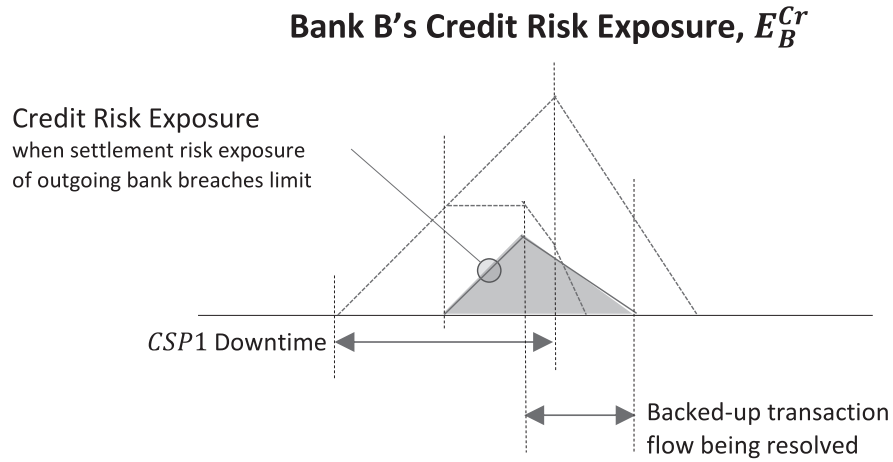


*Figure 11 Spillover Contagion Risk To Bank B When Bank A's Settlement Limit Exposure Is Breached.*

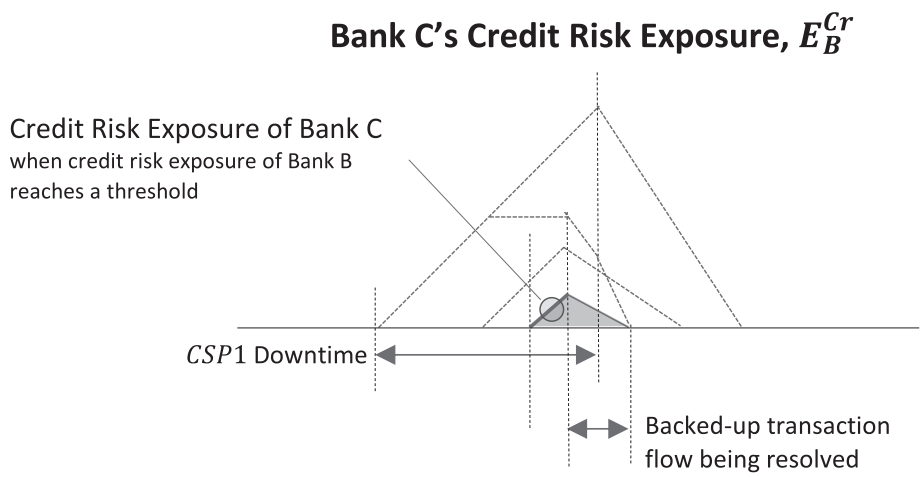


*Figure 12 Spillover Contagion Risk To Bank C When Bank B's Credit Risk Exposure Threshold Is Breached.*

$L_j^{CR}$, bank j rejects a proportion of transactions, $1-\gamma_j$, based upon how far the credit risk exposure is above the limit threshold. Bank j will attempt to settle, $\gamma_j$, if another CSP is available to support its critical financial infrastructure application in completing the outstanding transactions. The authors define $\gamma_j$ as the ratio of bank j's credit risk threshold relative to the bank's cumulative credit risk exposure:

$$\gamma_j = \frac{L_j^{CR}}{E_j^{CR}}$$

The cumulative effect of this mechanism is an indication of spillover contagion risk that can spread throughout the system as each bank rejects transactions on the basis of their credit risk exposure thresholds. An example of this type of contagion is shown in Figure 11.

In this case, when bank A's CSP fails and its settlement risk exposure limit is breached, bank A begins to reject transactions from bank B. Bank B subsequently rejects transactions from bank C when its credit risk exposure threshold is also breached. As illustrated in Figure 12, when

the transaction flow of bank B to bank C is interrupted, bank C accumulates credit risk exposure until the time that bank B accepts the backed-up transaction flow.

## SIMULATION OF THE FRAMEWORK ABM

As part of this work, the authors built a framework ABM to illustrate how this simulation approach can help understand factors impacting potential cloud concentration risk as well as evaluating the impact of the number of CSPs on settlement risk and credit risk. To demonstrate how this works, the authors use a simple subset example to illustrate how this works based upon just three banks and three CSPs. In this example, BARC is connected to CSP1, ACA is connected to CSP2 and BBVA is connected to CSP3. In this scaled down ABM, when CSP1 fails in simulation step 10, the downtime endures for further 50 simulation steps. As seen in Figure 13, the settlement risk exposure limit of BARC is breached at Step 18, BARC rejects transactions from ACA and BBVA causing credit risk exposure to spread through the system, including BARC.

As shown in Figure 14, one can look at this from a system perspective by examining the credit risk exposures of the three banks over time steps in the simulation.

Recall that at Step 20, CSP1 failed. This contributes to elevated credit risk exposures spreading from ACA to BARC and to BBVA. This illustrates in our framework ABM how credit risk is disseminated in this simplified three bank system.

The authors now simulate the entire system of 27 banks and 3 CSPs on the

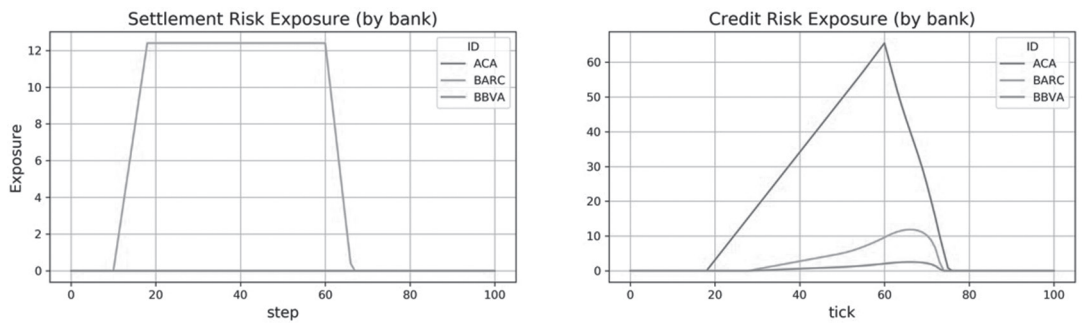


*Figure 13 Settlement and credit risk exposures from CSP1 failure*

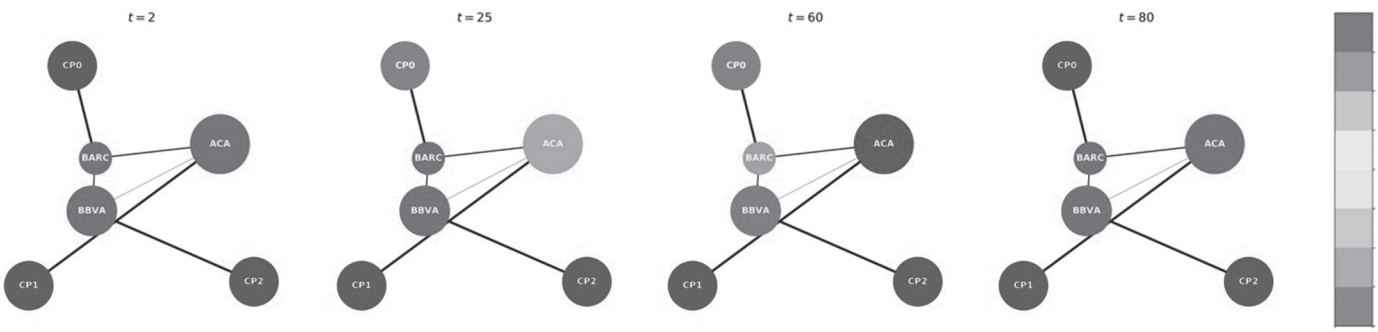


*Figure 14 Credit risk exposures by simulation time steps*

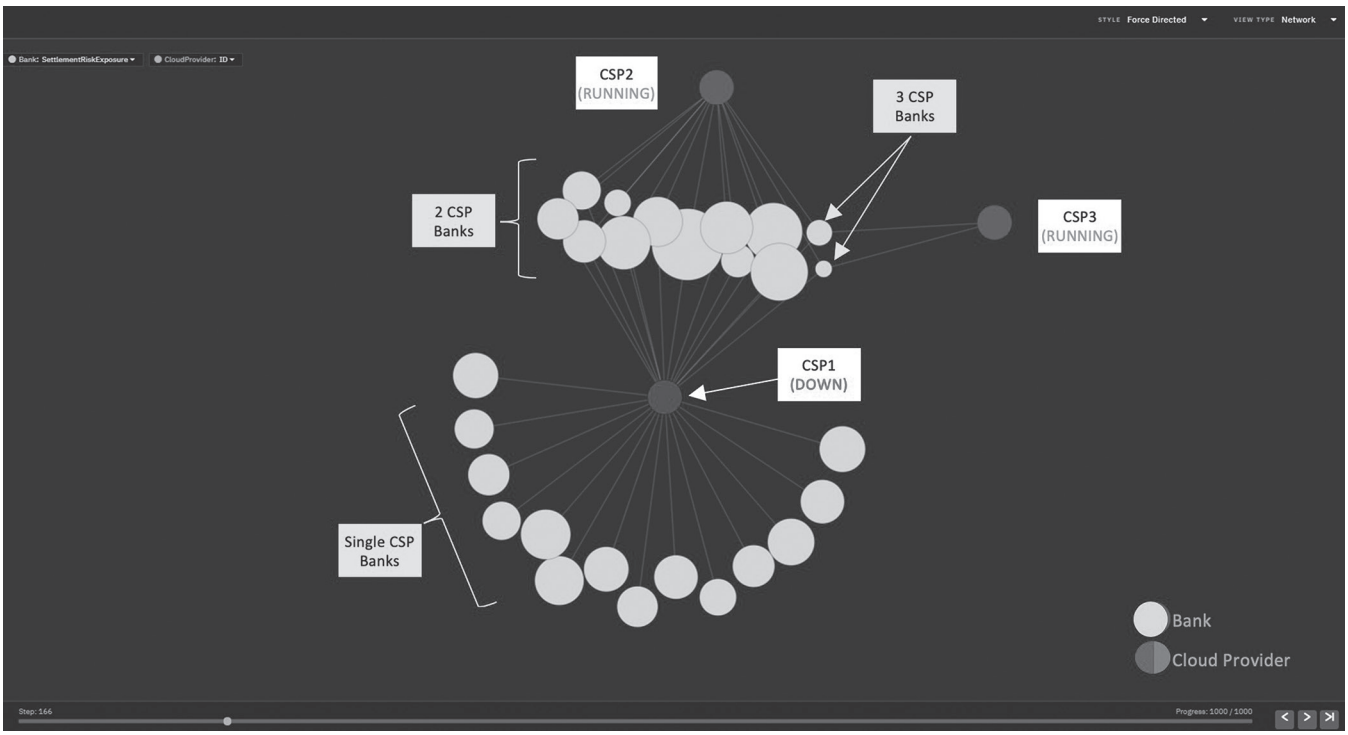


*Figure 15 Simudyne simulation dashboard of framework ABM — network view*

Simudyne ABM simulation platform. Given their limited access to data ie bank connectedness measures and bank total assets, they run a Monte-Carlo simulation, where model gaps are randomised over each simulation to capture their uncertainty. Figure 15 is a Simudyne Dashboard view of the system with a time step where CSP1 is down and the banking network with one group of banks solely on CSP1, a second group on CSP1 and CSP2. In this simulation, there are two banks that have all three CSPs in the cloud deployment.

The dashboard given in Figure 16 shows 4 views across the 27 banks of their settlement risk exposures, their credit risk exposure, their total exposure and aggregated downtime across the banking system.

First, given that the authors do not know the number of CSPs each bank has nor the details on how critical financial infrastructure applications are deployed on the CSPs, they make no assumption and instead analyse the impact given any number of CSPs by running Monte-Carlo simulations with randomly sampling the number of CSPs for each bank. They look at the maximum credit risk exposure of each bank, averaged over the Monte-Carlo runs and at the ratio of settlement risk exposure to the settlement risk exposure limit of each bank, where the limit is proportional to the total asset of the bank ie larger banks have higher limits. On average, we can see that credit risk exposure is highly dependent on bank connectedness as expected, while the smaller banks tend to be more exposed to breaching their settlement risk exposure limits.

Figure 17 provides an example of the types of analysis that one can do with the framework ABM. In this case, based upon 100 Monte-Carlo simulation runs, the


*Figure 16 Simudyne simulation dashboard of framework ABM — risk view*

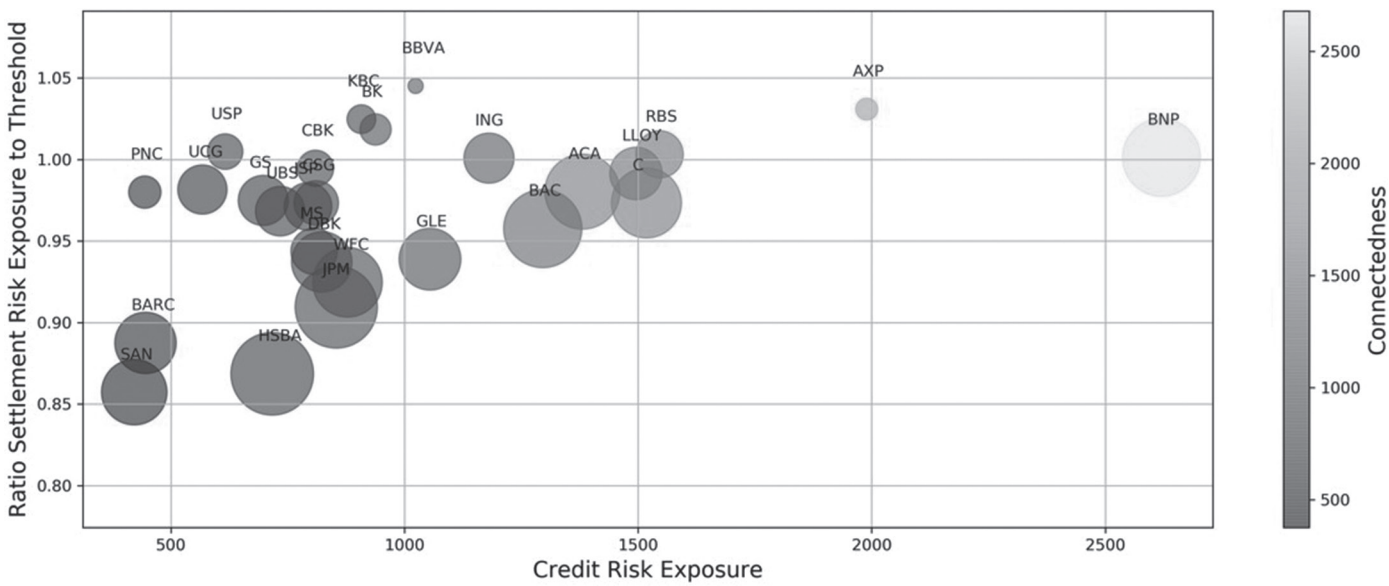


*Figure 17 Settlement and credit risk exposures from 100 Monte Carlo simulation run*

authors look at the relationship between credit risk exposure and the ratio of settlement risk exposure to each bank's threshold. The colour of each bank represents the degree of bank connectedness and the size represents the total assets of the bank. These have been randomised over how many cloud providers a bank might have as part of their cloud deployment. Note that the ratio shown earlier can be above 1 as

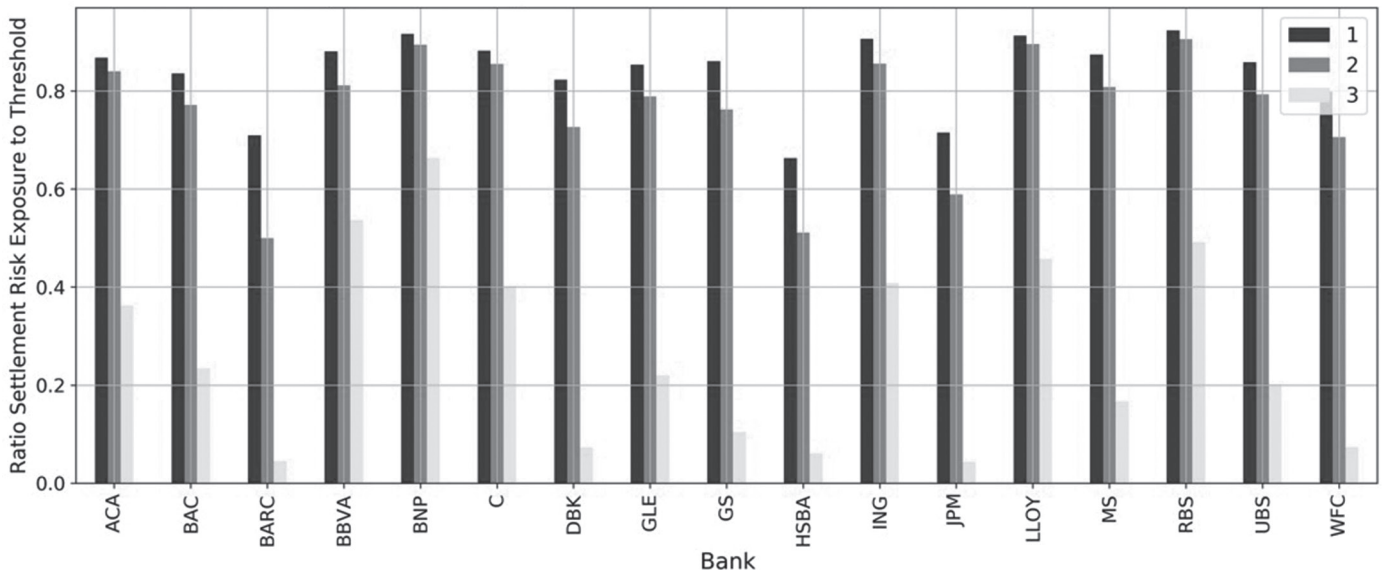


*Figure 18 Settlement risk exposure given a different number of CSPs deployed*

transactions are rejected only after the limit is breached.

Figure 18 provides an example of evaluating the settlement risk exposure impact of banks having a single vs hybrid cloud strategies. The authors do this by looking at the operational impact conditional on the number of CSPs deployed. As shown in Figure 9, having a hybrid cloud deployment capability will mitigate settlement risk exposure with the impact of having two or three CSPs varying across banks.

Averaged over 100 Monte-Carlo simulation runs, this type of analysis can be used to evaluate the beneficial impact on the ratio of settlement risk exposure to the bank's threshold by having a more CSPs. This ranges from a ratio level of 85 per cent for one CSP, 77 per cent for 2 CSPs to 27 per cent for deploying 3 CSPs.

Furthermore, The authors expect a saturation point where increasing the number of cloud providers would not significantly decrease the ratio of settlement risk exposure to the bank's threshold. Understanding this saturation point would allow a bank to adequately choose its number of CSPs given their risk preferences, but this not within the scope of this paper.

## Benefits of developing a cloud concentration risk ABM

This framework ABM is designed to help enable the use of ABMs for evaluation of cloud concentration risk exposures. This can be relevant to all market participants.

For Regulators, we see the following benefits:

1. Policy/Supervisory Strategies — Evaluate the effectiveness of policies in addressing systemic risk, quantify the range of possible costs and benefits to the banking system from a compliance and risk perspective.
2. Identify contagion trigger points that might yield systemic risk events, understand what types of critical financial infrastructure applications are most impacted by a bank's cloud deployment strategy.
3. Quantify impacts on the real economy and identify which sectors are impacted under a range of different macroeconomic scenarios and assumptions.

4. The ultimate objective is to leverage new approaches such as evolutionary game theory as a tool for determining optimal supervisory policies given a range of constraints and assumptions.

For Banks, the following benefits are seen:

1. Evaluate the benefits and costs of various hybrid cloud deployment strategies.
2. Evaluate which critical financial infrastructure application is most exposed to a single CSP deployment strategy.
3. Demonstrate to regulators how the bank has taken into account a wide range of possible future circumstances to improve their regulatory compliance and reduce their exposure to cloud concentration risk concerns.

For CSPs, the following benefits are seen:

1. Evaluate scenarios where specific example (eg., March 3, 2020: Microsoft Azure, US East Coast) can have a material impact on the organisation with retention across the regional and global businesses.
2. Optimise customer and regulator audit strategies with respect to cost, operational support and the effectiveness of compliance.
3. Determine which critical financial infrastructure application has the most damaging impact on the CSP's banking customers as well as for the CSP's reputation.
4. Evaluate competitor business, operational and pricing strategies with respect to retention of existing customers and acquiring target customers.

## Future work

As part of the authors' future work, they intend to analyse the competitive behaviours of CSPs and the banks. Using Game Theory and Evolutionary Game Theory [1], they can analyse the strategy of the banks to understand the dynamics of the system ie how systemic risk changes given the adaptive behaviour of the banks, which aim to mitigate their settlement and credit risk exposures. A regulator could also impose policies, understand the impact of those policies on competitive behaviours of the banks and CSPs and ensure systemic risk remains within risk adjusted limits.

In Figure 19, the authors speculate what the system dynamics and equilibrium might be in a simple game where banks

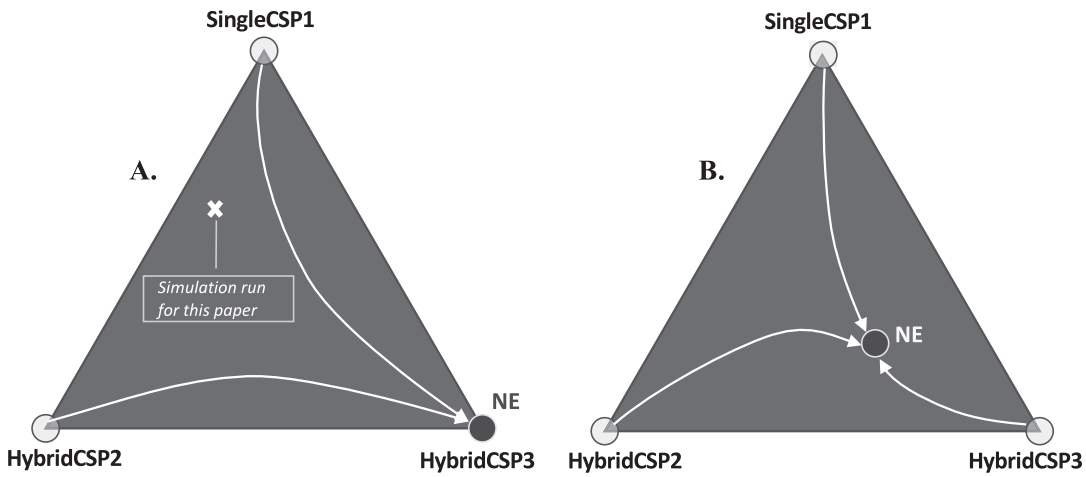


*Figure 19 Evolutionary game theory to analyse an ABM with agents with competitive behaviours*

can choose between 1, 2 or 3 CSPs, intending to minimise the settlement and credit risk exposure and the impact of the cost of hybrid CSPs on the Nash Equilibrium.

Following from this framework ABM, one can identify banks having three strategies:

1. SingleCSP1: Cloud deployment on a single CSP.
2. HybridCSP2: Cloud deployment with two CSPs.
3. HybridCSP3: Cloud deployment with three CSPs.

Within a world where there is no cost to having multiple CSPs, there would be an obvious Nash Equilibrium (NE) where all Banks adopt HybridCSP3 as shown in (A). With a cost to having hybrid CSPs, however, this NE will change — they speculate an NE in (B) that is different from (A). Note that in (A), they show the point at which they run the simulation for the paper, where 50 per cent of banks have 1 CSP, 40 per cent have 2 CSPs and 10 per cent have 3 CSPs. A game-theoretic analysis would require running Monte-Carlo simulation over the space of probabilities of having 1, 2 or 3 CSPs and is a focus area for our future research.

## ACKNOWLEDGMENT

We thank Professor Kamil Yilmaz for sharing his market-based estimates that are used to define the bank system network connectedness in this paper's framework agent based model (ABM).

## References and Notes

(1) Gulliver, S. (2019) 'Cloud computing in the financial sector: A global perspective' [Online], Program on International Financial Systems, available at: https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf (accessed 26th July, 2020).
(2) Financial Stability Board (2019) 'Third-party dependencies in cloud services: Considerations on financial stability implications' [Online], Financial Stability Board, available at: https://www.fsb.org/wp-content/uploads/P091219-2.pdf (accessed 26th July, 2020).
(3) Gartner (2019) 'Forecast: Public Cloud Services, Worldwide, 2017-2023, 3Q19 update' [Online], available at: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020 (accessed 26th July, 2020).
(4) Strachan, D. 'Financial services on the Cloud: the regulatory approach', Deloitte Blog. Weblog [Online], available at: https://blogs.deloitte.co.uk/financialservices/2019/09/the-regulatory-approach.html (accessed 26th July, 2020).
(5) Financial Stability Board, see ref. 2 above.
(6) European Securities and Markets Authority (2020) 'Draft guidelines on outsourcing to cloud service providers' [Online], European Securities and Markets Authority (ESMA50-164-3342), available at: https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf (accessed 26th July, 2020).
(7) European Banking Authority (2019) 'Final report on EBA guidelines on outsourcing arrangements' [Online], European Banking Authority, available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1 (accessed 26th July, 2020).
(8) Rakesh, M. (2019) 'At a glance: EBA issues revised guidelines on outsourcing' [Online], PWC, available at: https://www.pwc.co.uk/financial-services/assets/pdf/eba-issues-revised-guidelines-on-outsourcing.pdf (accessed 26th July, 2020).
(9) European Systemic Risk Board (2020) 'Systemic cyber risk' [Online], European Systemic Risk Board, available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf (accessed 26th July, 2020).
(10) UK House of Commons Treasury Committee (2019) 'IT failures in the Financial Services Sector' [Online], UK House of Commons, available at: https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf (accessed 26th July, 2020).
(11) Bank of England-Prudential Regulatory Authority (2019) 'Outsourcing and third-party risk management' [Online], Bank of England, available at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf (accessed 26th July, 2020).
(12) Gulliver, see ref. 1 above.
(13) The Financial Stability Oversight Council (FSOC) was established by the Dodd–Frank Wall Street Reform and Consumer Protection Act and created to address the fact that no single regulator had

responsibility for monitoring and addressing overall risks to financial stability. In their 2019 Annual Report, third-party outsourcing risks were not highlighted as a crucial systemic risk concern.

(14) Pederson, B. (2019) 'Does Amazon-Google-Microsoft hold on the cloud pose a risk to banking?' American Banker, September 30, 2019, available at: https://www.americanbanker.com/news/does-amazon-google-microsoft-hold-on-the-cloud-pose-a-risk-to-banking (accessed 21st June, 2020).

(15) *Ibid*.

(16) Asia Cloud Computing Association (2018) 'Asia's Financial Services on the cloud 2018: Regulatory landscape impacting the use of cloud by Financial Services Institutions in Asia' [Online], Asia Cloud Computing Association (ACCA), available at: https://www.slideshare.net/accacloud/asias-financial-services-on-the-cloud-2018-regulatory-landscape-impacting-the-use-of-cloud-by-financial-institutions-in-asia-by-the-asia-cloud-computing-association-227586958 (accessed 26th July, 2020).

(17) BitSight (2020) 'Managing risk in an increasingly regulated world' [Online], BitSight, available at: https://info.bitsight.com/managing-risk-increasingly-regulated-world (accessed 26th July, 2020).

(18) Australian Prudential Regulatory Authority (2018) 'Outsourcing involving cloud computing services' [Online], Australian Prudential Regulatory Authority (APRA), available at: https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf (accessed 26th July, 2020).

(19) Bank of England (2020) 'How reliant are banks and insurers on cloud outsourcing?' [Online], Bank of England Bank Overground, available at: https://www.bankofengland.co.uk/bank-overground/2020/how-reliant-are-banks-and-insurers-on-cloud-outsourcing (accessed 26th July, 2020).

(20) In 2017, the ESRB established the European Systemic Cyber Group (ESCG) to investigate systemic cyber risk and examine whether and how a cyber incident could cause a systemic crisis. The analysis conducted shows that a cyber incident could indeed evolve into a systemic cyber crisis that threatens financial stability with the potential to have serious negative consequences for the real economy. (Source: ESRB, see ref. 9 above)

(21) European Banking Authority (2019) 'Final report on EBA guidelines on outsourcing arrangements' (EBA/GL/2019/02), February 25, 2019, available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1 (accessed 21st June, 2020).

(22) Merv, A. (2020) 'Stop talking about "Hadoop"' [Internet], Gartner Blog Network, available at: https://blogs.gartner.com/merv-adrian/2020/03/04/its-time-to-stop-talking-about-the-hadoop-market/ (accessed 21st June, 2020).

(23) Ashlett, M. (2020) 'Don't call it a comeback: Cloudera accelerates its hybrid cloud strategy' [Internet], 451Research.com, available at: https://clients.451research.com/reportaction/99019/Toc (accessed 21st June, 2020).

(24) Cloudera (2020) 'Why a successful hybrid cloud strategy requires an enterprise data strategy: Five strategic considerations for hybrid cloud success' [Online], Cloudera, available at: https://www.cloudera.com/campaign/five-strategic-considerations-for-hybrid-cloud-success.html (accessed 26th July, 2020).

(25) There are many examples of ABM simulation models developed for systemic risk and policy evaluations. One example that would be similar in design is the following paper: Bookstaber, R., Paddrik, M. and Tivnan, B. (2018) 'An agent-based model for financial vulnerability', *Journal of Economic Interaction and Coordination* [Online], Vol. 13, No. 2, pp. 433–466, available at: https://www.springerprofessional.de/en/an-agent-based-model-for-financial-vulnerability/12064202 (accessed 26th July, 2020).

(26) Diebold, F. and Yilmaz, K. (2014) 'On the network topology of variance decompositions: Measuring the connectedness of financial firms', *Journal of Econometrics* [Online], Vol. 182, No. 1, pp. 119–134, available at: https://www.journals.elsevier.com/journal-of-econometrics (accessed 26th July, 2020).

(27) Diebold, F. and Yilmaz, K. (2016) 'Trans-Atlantic equity volatility connectedness: US and European Institutions, 2004–2014', *Journal of Financial Econometrics* [Online], Vol. 14, No. 1, pp. 81–127, available at: https://academic.oup.com/jfec (accessed 26th July, 2020).

(28) Demirer, M., Diebold, F., Liu, L. and Yilmaz, K. (2017) 'Estimating global bank network connectedness', *Journal of Applied Econometrics* [Online], Vol. 33, No. 1, pp. 1–15, available at: https://onlinelibrary.wiley.com/doi/full/10.1002/jae.2585 (accessed 26th July, 2020).

(29) These estimates were graciously provided to us by Professor Kamil Yilmaz.

(30) S&P Global Market Intelligence (2019) 'Top 100 Banks', April 5, 2019, available at: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/the-world-s-100-largest-banks-50964984 (accessed 21st June, 2020).

(31) The choice of an exponential distribution for the downtime is to emulate the likelihood of having a lot of short-lived failures, with decreasing probability of having critical failures lasting a significant number of steps. Similarly, switching time normally would not take a long time, with a decreasing probability that it takes a long time to complete.

## APPENDIX

| # | *Variable* | *Model Parameter Name* | *Notes* |
|---|---|---|---|
| 1 | $n_B$ | Number of banks | 27 US and EU Banks; can be changed from 1 to 27. |
| 2 | $n_{CSP}$ | Number of cloud service providers | 3 Cloud Service Providers (CSP1, CSP2, CSP3) |
| 3 | $A_B$ | Total asset of bank B | From Historical Data — 12-month median from daily estimates: May 23, 2019 to May 22, 2020. |
| 4 | $C_{i,j}$ | Bank connectedness between bank i and Bank j | From Historical Data — 12-month median from daily estimates: May 23, 2019 to May 22, 2020. |
| 5 | $P_j^{fail}$ | Probability cloud service provider j fails at each step | 10% CSP1 fails, 5% CSP2 fails and 2% CSP3 fails at each step. |
| 6 | $P_j^{CSP}$ | Probability bank has j cloud service providers | 50% a Bank has 1 CSP; 40% a Bank has 2 CSPs and 10% a Bank has 3 CSPs. |
| 7 | $cap_{CSP}$ | Capacity of cloud service provider to resettle backed-up transactions | 1 |
| 8 | $L_i^{CR}$ | Credit risk exposure threshold | 3000; the average across all banks, proportional to total asset of a bank. |
| 9 | $L_i^{SR}$ | Settlement risk exposure limit | 1000; the. average across all banks, proportional to total asset of a bank. |
| 10 | $cap_i$ | Rate at which bank *i* resolves backed-up transaction from credit risk exposure | 3 |
| 11 | $\lambda_j^D$ | Parameter of exponential distribution for downtime | 30 for all CSPs |
| 12 | $\lambda_i^S$ | Parameter of exponential distribution of time to switch a cloud service provider when one fails | 5 for all Banks |