CLOUDERA

Identifying and Mitigating Cloud Concentration Risk

How the Financial Services and Insurance industries, Cloud Service Providers and Regulators can work collaboratively towards a resilient cloud computing environment

Table of Contents

Emerging Risks

The Financial Services and Insurance industries, will be transformed by cloud computing in 5 years. This seismic change will drive new innovations while concurrently introducing new types of risks that need to be addressed by regulators, Financial Services and Insurance providers, and technology innovators.

This growth in cloud adoption has gained the attention of regulators at global, regional, and national levels. Regulators are evaluating the complexities involved in the "shared responsibility model" that exists between a cloud customer and the cloud service provider (CSP) to ensure sufficient oversight and controls are in place. A subset of these regulatory operational resiliency concerns is **Cloud Concentration Risk.**

Financial Services and Insurance have a prime opportunity to collaborate for a win-win across the industry to safely and securely leverage next generation technology to mitigate Cloud Concentration Risk exposures.

WHAT IS CLOUD CONCENTRATION RISK?

Cloud Concentration Risk concerns arise from an institution's over-reliance on one cloud service provider to support key banking and insurance services, or if a significant number of institutions have a key operational or market infrastructure capability (e.g. payment, settlement, and clearing systems) running on a single CSP.

© 2020 Cloudera, Inc. All rights reserved.

Industry Trends in Cloud Computing

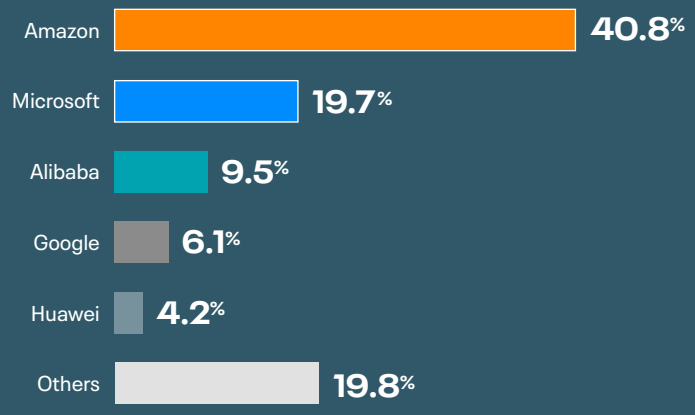
As with most industries in general, cloud adoption in Financial Services and Insurance has been accelerating over the past few years, seeking to capitalize on the speed, agility, simplicity, and lower costs that it provides.

Detailed CSP cloud market share estimates for the Financial Services and Insurance industries are not publicly released by the CSPs. The Bank of England published high-level results of an annual survey of the 30 largest banks and 27 largest insurers—that they supervise—to understand how these institutions utilize the cloud. This includes a good selection of some of the largest global banks[1].

- Top two CSPs have a combined market share of 60.5%
- 80% of global IaaS market share held by 5 providers
- Top 5 market share increased 3% from 2018 to 2020 (77% to 80%)
- Amazon continues to lead the worldwide IaaS market with an estimated revenue of $26.2 billion

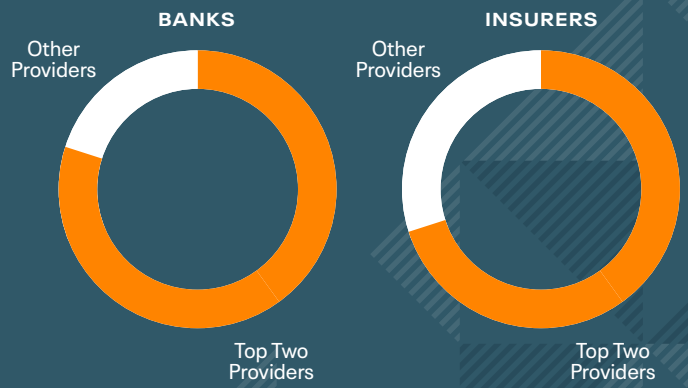
Worldwide IaaS Public Cloud Services Market Share, 2020

Across All Industries



Source: Gartner, June 2021

Bank of England CSP UK Market Share Estimates



Source: Bank of England survey, January 2020

© 2020 Cloudera, Inc. All rights reserved.

Risk Exposures

A diverse list of operational resiliency concerns has been identified across many regulator publications, the following items reflect critical factors in evaluating future risk exposures for an individual firm and across the industry.

Firm-Specific Cloud Concentration Risks

Risks that are directly under the control of any single firm.

1. **Lack of Unified Data Security & Governance**—Each cloud-native product re-creates its own silo of metadata making data management, security, and governance complex.
2. **Cyber Attack Resiliency**—The consolidation of multiple organizations within one CSP presents a more attractive target for cyber criminals than a single organization.
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 CSP.
4. **Operational Resiliency**—The "shared responsibility" model inherent in the relationship between a cloud customer and the CSP is a concern. Regulators are clear that institutions remain fully responsible for all functions they outsource to 3rd party providers.

Risk Exposures (continued)

Systemic Cloud Concentration Risks consist of risks that affect the stability of the larger, potentially worldwide financial system.

Systemic Cloud Concentration Risks

Risks that are not directly under the control of any single firm.

1. **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 regulators from full visibility on the applications that reside with a CSP.
2. **Systemic Risk Concerns**—Regulators are concerned about the systemic risk arising from a concentration of many large financial service firms' critical application(s) residing on the same CSP. These include applications such as payment, settlement, and clearing systems.

The oversight complexities of Cloud Concentration Risk highlight the need for the Financial Services and Insurance industries, the CSPs and Regulators to collaboratively work together to manage these risks.

EU Digital Operational Resilience Act (DORA)

"The proposed legislation will require all firms to ensure they can withstand all types of Information and Communication Technology (ICT)—related disruptions and threats.

Today's proposal also introduces an oversight framework for ICT providers, such as cloud computing service providers."

European Commission Press Release, September, 2020

> 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

© 2020 Cloudera, Inc. All rights reserved.

US Federal Reserve Study of Cyber Risk

The Federal Reserve Bank of New York recently used payment activity in Fedwire Funds to evaluate how a cyber-attack could be amplified throughout the financial system[4].

The baseline scenario looks at the impact of a top five bank halted from Fedwire access because its internal systems had been disrupted for a day.

They find that banks would continue to pay into the stricken bank's account, but no funds would be coming out, creating a "liquidity black hole." As other banks realize their interbank payments with the affected bank is one-sided, they would stop paying out to their counterparties to protect their own liquidity. The simulation study finds that on average **38% of all bank assets could be impacted** to a level that amounts to **more than 2.5 times the daily GDP of the United States.**

Another scenario looks at the impact reflective of an attack on a 3rd party service provider, analogous to a CSP:

"For a provider with multiple large and medium size bank clients, **an average of 60% of banks by assets become impaired.** In addition to highlighting the direct impact that a cyber-attack may have on its clients, this exercise reveals the importance of understanding operational linkages presented by 3rd party service providers."

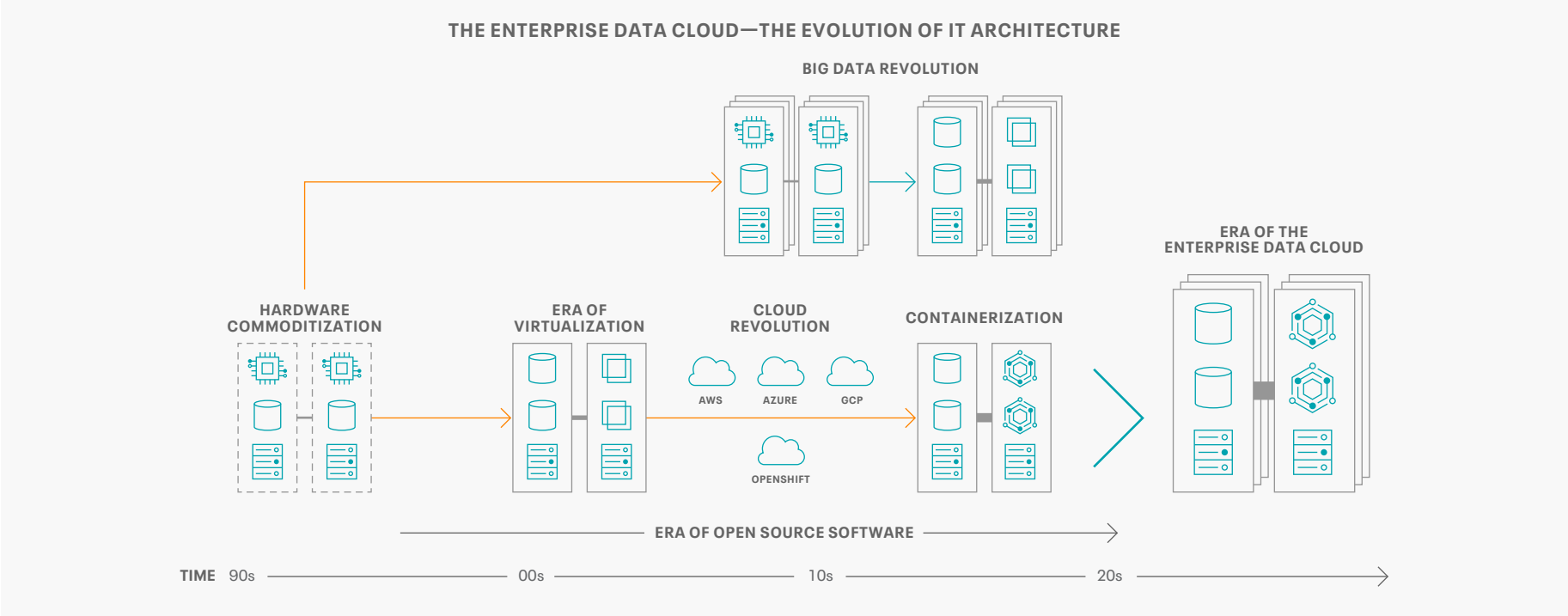
In addition to highlighting the direct impact that a cyber-attack may have on its clients, this exercise reveals the importance of understanding operational linkages presented by 3rd party service providers.

© 2020 Cloudera, Inc. All rights reserved.

Enterprise Data Cloud—the Future of Cloud Computing

The wide adoption of cloud computing and the need to manage data, workloads and security across many platforms has led Cloudera to develop the next generation Big Data platform, an Enterprise Data Cloud that unlocks the power of your data to serve customers better, operate with greater efficiency, and strengthen security to protect your business:

• Deployment options in any public or private cloud or on-premise providing choice and control.	• Separate compute and storage to maximize efficiency.	• Portability with container architecture to enable flexibility.	• Common governance to consistently manage security and compliance.



© 2020 Cloudera, Inc. All rights reserved.

Cloudera Data Platform

The Cloudera Data Platform (CDP) is a hybrid data cloud built for the enterprise. With CDP, financial services firms manage and secure the end-to-end data lifecycle to drive actionable insights and data-driven decision making.

Public, Private, and Hybrid Cloud

Optimized for hybrid cloud, CDP delivers the same data management and analytic capabilities seamlessly across private and public clouds. Companies can provision a data management and analytic solution in the environment of their choice.

End-to-end Data Lifecycle

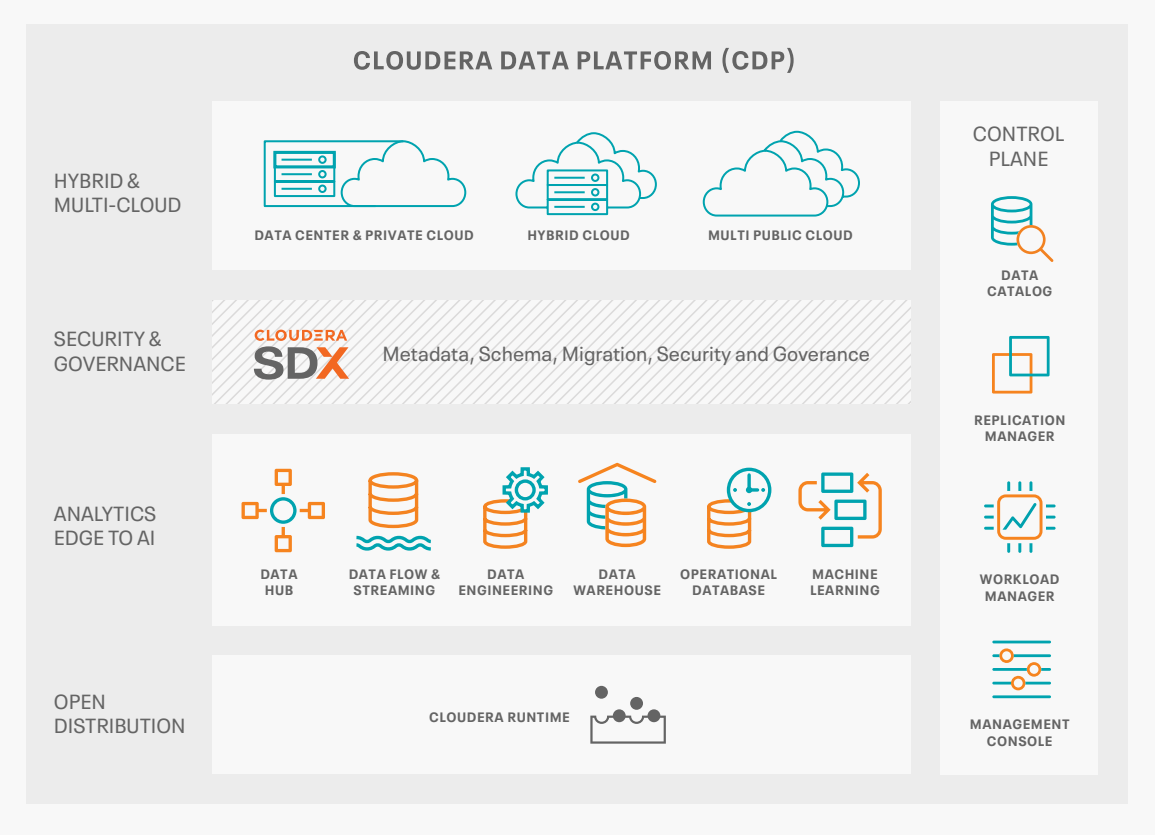
CDP enables companies to connect disparate workloads by integrating streaming, analytics, and machine learning to develop critical applications on one data management platform to address current and future workload needs.

Shared Data Experience (SDX)

The security framework ensures consistent data security, governance, and control across the data lifecycle and across all environments. Enterprises set data access controls and policies once and they are automatically enforced across data and analytics in hybrid and multi-cloud deployments, even as data and workloads move between them.

100% Open

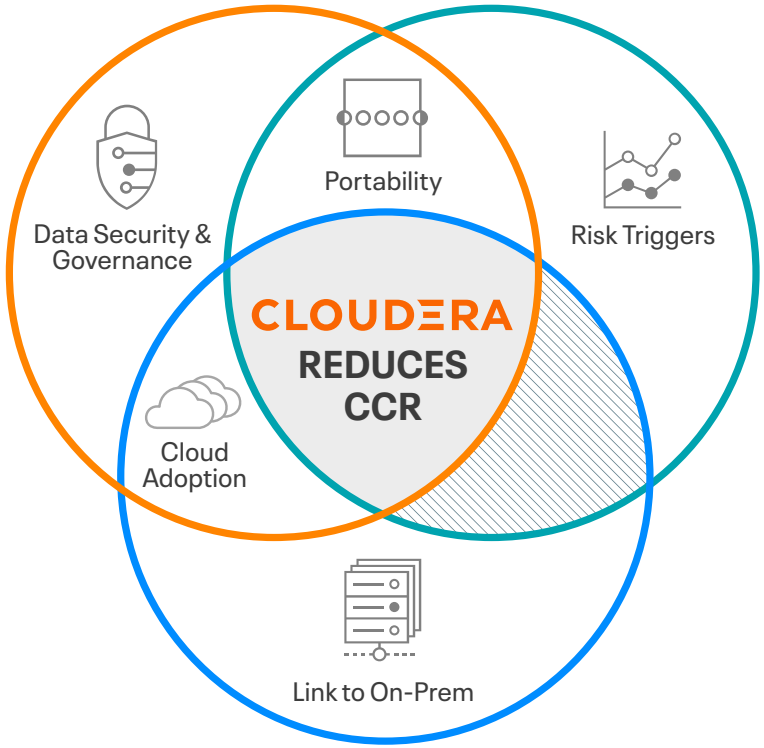
Open source software accelerates innovation and prevents vendor lock-in. Using open source ensures CDP is interoperable with a broad range of analytic and business applications.



© 2020 Cloudera, Inc. All rights reserved.

Cloudera Data Platform Reduces Cloud Concentration Risk (CCR)

CDP reduces several regulatory concerns for market participants



Financial Institutions and Insurers

- Avoid Cloud Lock-in
- Consistent Data Security & Governance
- Portability of Data & Applications
- Reduce Cloud Regulatory Concerns

Regulators

- Portability of Data & Applications
- Model Systemic Risk Triggers
- Reduce Cloud Regulatory Concerns

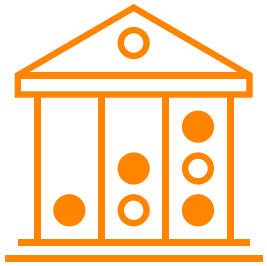
Cloud Service Providers

- Accelerate Cloud Adoption
- Linkage to On-Premise Landscape
- Reduce Cloud Regulatory Concerns

© 2020 Cloudera, Inc. All rights reserved.

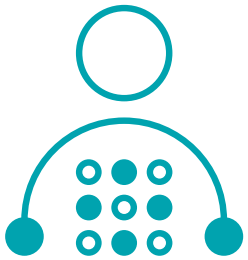
Mutual Benefits of Industry Collaboration

CDP Helps Reduce Firm-Specific and Systemic Cloud Concentration Risk



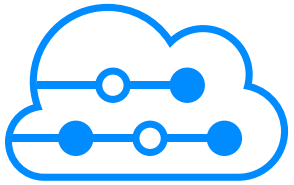
Financial Institutions and Insurers

- **Cloud Lock-In:** Avoids cloud lock-in with portability across any environment.
- **Data Security and Governance:** Shared Data Experience (SDX) maintains unified data security and data governance across all environments.
- **Portability of Data and Applications:** A container architecture enables flexibility while separate compute and storage maximizes efficiency.
- **Cloud Regulatory Concerns:** Reduces key concerns about a lack of unified data security and governance, cyber-attack resiliency, vendor lock-in, operational resiliency.



Regulators

- **Portability of Data and Applications:** A container architecture enables flexibility to move between environments.
- **Systemic Risk Triggers:** Enables ML, AI and Simulation capabilities to help identify systemic cloud concentration risk trigger points and evaluate policy and structural approaches.
- **Cloud Regulatory Concerns:** Reduces key concerns about a lack of unified data security and governance, cyber-attack resiliency, vendor lock-in, operational resiliency.



Cloud Service Providers

- **Cloud Adoption:** Helps accelerate cloud growth and workload migrations.
- **On-Premise Linkage:** Supports consistency across workloads and between environments.
- **Cloud Regulatory Concerns:** Reduces key concerns about a lack of unified data security and governance, cyber-attack resiliency, operational resiliency.

© 2020 Cloudera, Inc. All rights reserved.

Going Deeper

To learn more about how regulators globally are evaluating cloud operating risks and how a hybrid, multi-cloud platform can help reduce cloud concentration risk, read our related whitepaper, Cloud Concentration Risk II: What has changed in the past two years?

About Cloudera

At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world's largest enterprises.

Learn more at cloudera.com | US: +1 888 789 1488 | Outside the US: +1 650 362 0488

Sources

[1] Bank of England. "How reliant are banks and insurers on cloud outsourcing?" Bank Overground, January 17, 2020.

[2] Gartner Says Worldwide IaaS Public Cloud Services Market Grew 40.7% in 2020.

[3] ESRB: "Systemic cyber risk," February 2020.

[4] "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis." Federal Reserve Bank of New York, Staff Reports no.909, June 2020.

© 2020 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice. November 2020

Privacy Policy | Terms of Service

CLOUDERA