Migration to Public Cloud: Risks and Regulatory Requirements for Clearing and Settlement Facilities

Oscar Douglas, Elizabeth Kandelas and Ed Orum[*]

Photo: Dragan Todorovic – Getty Images

Abstract

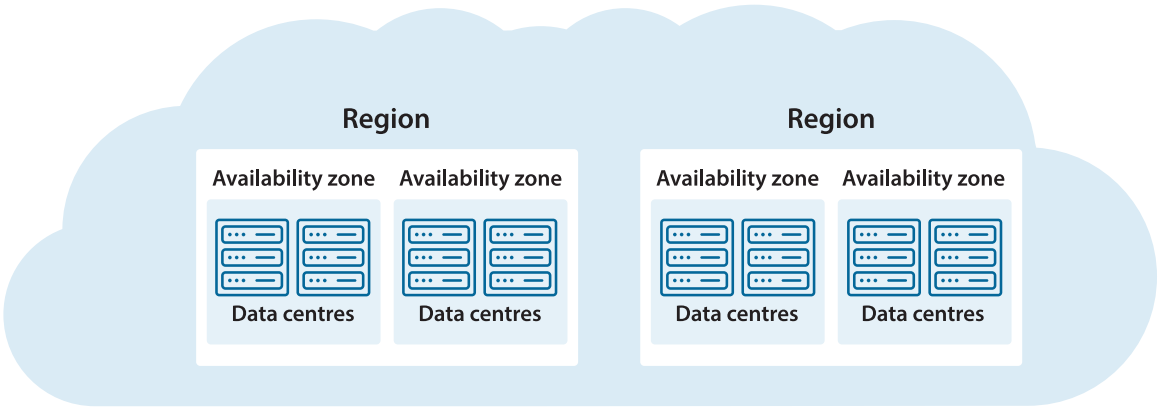
Public cloud technologies are increasingly being adopted by firms in the financial industry, including clearing and settlement facilities (CS facilities). Using public cloud offers a range of opportunities, but also presents risks for a CS facility's operations. Because CS facilities play a critical role in supporting the smooth functioning of financial markets, they need to manage these risks to ensure that they continue to provide resilient and secure services. This article discusses the opportunities and risks for CS facilities in using public cloud, and outlines the related regulatory requirements that apply to CS facilities in their management of risks, consistent with their obligations to promote efficiency and stability in the financial system.

Introduction

Adoption of public cloud is increasing among firms in the financial industry,[1] including clearing and settlement facilities (CS facilities) that are regulated by the RBA. CS facilities provide services that are critical to the operational efficiency and stability of financial markets. These services fall into two broad categories:

1. **Central counterparties (CCPs)**. These facilities act as the legal counterparty to all transactions, becoming the buyer to every seller and the seller to every buyer in the markets in which they operate. This intermediary function helps to manage the risk that buyers and sellers would otherwise face from credit exposures to each other.

Figure 1: Example of a Public Cloud Arrangement



2. **Securities settlement facilities (SSFs).** These facilities enable the final settlement of securities transactions, mitigating the risks associated with the exchange of securities and cash.

CCPs and SSFs also run a range of other services that support their clearing and settlement functions, such as facilitating securities issuances, the registration of trades, and managing collateral held by a CCP to cover certain exposures to its participants.

Operational failures that have an effect on the clearing and settlement services provided by CS facilities can significantly disrupt the functioning of financial markets. CS facilities therefore need to operate their services in a manner that is highly resilient and secure.

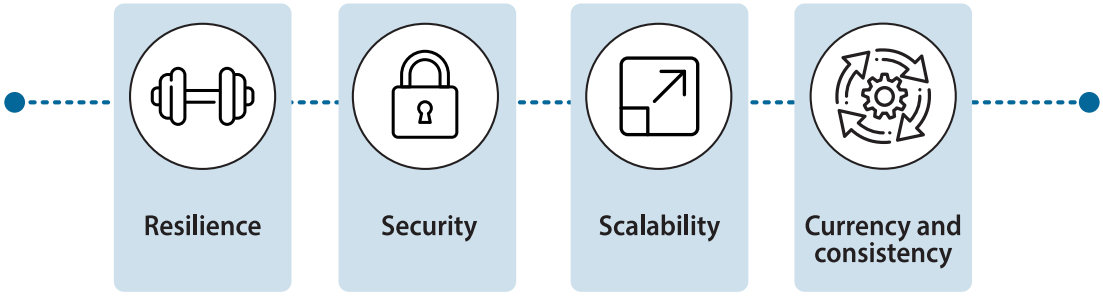
CS facilities have traditionally provided their services using on-premises data centres. Increasingly, however, CS facilities are looking to adopt public cloud technology to support the provision of these services, which are critical to the stable operation of financial markets. Using public cloud offers a number of potential benefits – including greater security, resilience and scalability – but also poses a range of risks related to cloud technology and an increased reliance on third-party providers. Before migrating services to the cloud, CS facilities need to ensure that appropriate design and testing activities are conducted. After migrating services, CS facilities need to carefully manage the services to ensure they remain resilient and secure, thereby supporting the orderly functioning of financial markets.

This article discusses some of the key opportunities and risks arising from CS facilities using public cloud and outlines the Australian regulations that require CS facilities to manage risks in a manner that supports the stability of the financial system.

What is public cloud

A public cloud is a collection of computer servers that are accessed over the internet, as well as the databases and applications that run on those servers. A public cloud is usually owned and operated by a technology company, with a common set of hardware, software and networks used to provide services to a large number of customers. Public cloud is typically hosted in numerous interconnected data centres, situated in multiple places across the world (Figure 1). Specialised software is used to optimise the use of computing resources, and to separate the data and applications of each cloud customer so that they are not visible or accessible by others (Cloudflare undated).

Figure 2: Potential Benefits of Public Cloud



Organisations may choose to use a single cloud vendor for all their needs, or different vendors for different services. They may also maintain relationships with multiple vendors as a contingency in case the services provided by their primary vendor become unavailable. There are potential benefits and risks associated with the use of public clouds, which are discussed in the following sections.

Potential benefits of CS facilities using public cloud

For CS facilities, the use of cloud technology offers several potential benefits over the use of physical data centres. If realised, the benefits outlined below could also support financial stability (Figure 2).

Resilience

CS facilities using public cloud technology can elect to have their data and applications run across multiple data centres located in different availability zones and geographical regions. The distances between these zones and regions reduces the likelihood of them all being disrupted simultaneously by physical incidents (e.g. natural disasters or power outages). This set-up provides greater resilience than traditional CS facility infrastructures, which typically comprise two or three data centres that may be situated close to each other (e.g. in the same city). Public cloud can help reduce the risk of a single point of failure and support higher availability than traditional data centres.

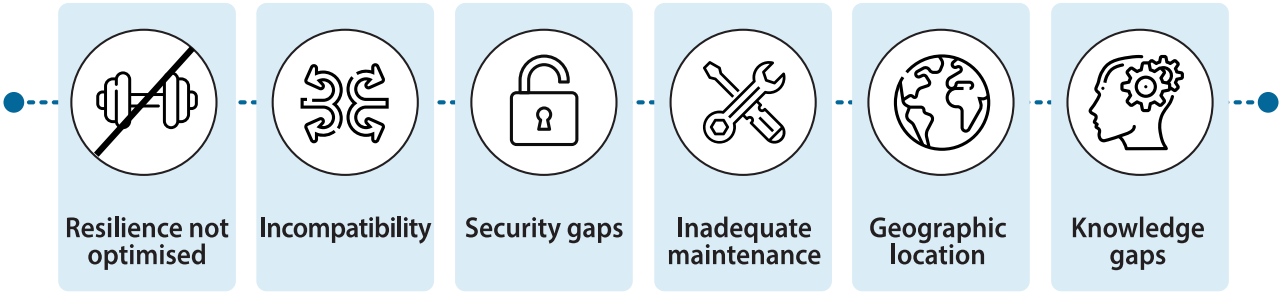
Security

Public cloud services can provide enhanced security solutions to protect against the loss or compromise of data and disruption to operations due to malicious activities such as cyber-attacks. The resourcing, specialisation and economies of scale of third-party providers enables them to develop and maintain security features that keep abreast of best practice and evolving security threats in a way that may not be possible for individual CS facilities. They also have the capacity to keep their infrastructure up to date and patch any security vulnerabilities as soon as possible.

Scalability

Public cloud environments provide vast potential amounts of computing power, due to the large scale of available resources and the technologies used to optimise the use of those resources. CS facilities can purchase access to additional computing power on-demand when using public cloud. This allows CS facilities to increase their processing capacity quickly and easily as required – for example, to respond to a significant market event that leads to substantial growth in transaction

Figure 3: Public Cloud Risks related to Technology



volumes. In contrast, capacity in traditional data centres is limited by the resources owned by the CS facility and scaling up requires significant planning and capital expenditure (US Department of the Treasury 2023).

Currency and consistency of infrastructure

Public cloud provides common sets of technology infrastructure and tools that are kept up to date by the cloud provider. Migrating systems from traditional data centres onto public cloud platforms alleviates the need for CS facilities to update many infrastructure components in physical data centres. It also provides opportunities for CS facilities to consolidate disparate legacy infrastructures and systems, thereby simplifying and standardising their technology environments.

Risks of migrating to and operating critical services in public cloud

While public cloud technology offers potential advantages over traditional data centres, migrating to and operating critical services in the cloud also poses a range of risks (Koh and Prenio 2023). CS facilities need to:

- identify and assess these risks in detail
- put in place and regularly assess the effectiveness of controls to mitigate the risks, to ensure that their critical services continue to support the stability of the financial markets they serve.

Some of the key technology and outsourcing risks associated with using public cloud are outlined in the following sections.

Technology-related risks

Transitioning from an on-premises operating model to a public cloud-based operating model is a significant and complex technology transformation. While there are broader change management risks associated with adopting, and operating in any new technology environment (e.g. introducing a new system), there are additional risks that are specific to the use of public cloud. The additional risks that CS facilities should consider are outlined below (Figure 3).

Resilience not optimised

While public cloud can offer benefits to resilience and reliability, realising these benefits requires proactive planning, design and investment by the CS facility. A CS facility without a well-defined cloud strategy and resilience objectives is unlikely to fully realise the benefits and appropriately manage the risks of public cloud. For example, if a CS facility pursues cost savings over resilience, it may make design choices that do not take advantage of the capabilities of public cloud, such as locating data centres in multiple availability zones and regions.

This could result in the CS facility's public cloud environment being no more resilient (or even becoming less resilient) than its existing on-premises environment.

Additionally, applications running in public cloud need to be designed to take advantage of its resilience features. A 'lift and shift' approach of moving existing applications to the cloud without appropriate redesign and testing is unlikely to result in the realisation of the resilience opportunities of cloud (O 2023; Pekkarinen undated). For example, legacy applications may not be able to operate effectively across multiple availability zones.

Resilience risks would also arise from CS facilities underinvesting in business continuity arrangements for their critical services in a public cloud environment. While extended outages that affect multiple cloud availability zones and regions are rare, they could still occur. If a CS facility operates multiple critical systems in a public cloud, all of these systems could be disrupted simultaneously. CS facilities that have not understood and tested the outage response arrangements of their public cloud providers, and do not have complementary business continuity plans, risk being unable to resume operation in a timely manner.

Incompatibility with on-premises systems

Without appropriate design and testing, CS facilities risk their public cloud-based services being incompatible with related systems that remain in their on-premises environment. This risk can be particularly prevalent during a CS facility's transition to a public cloud. It is important that CS facilities understand how their technologies will interact throughout all of the transition stages to avoid operational incidents and service unavailability.

Security gaps

While public cloud vendors can provide enhanced baseline security arrangements, CS facilities have a significant role to play in protecting their own services running in a public cloud. CS facilities need to build and configure their systems in a way that is compatible with, and takes advantage of, the vendor's security features. They are also responsible for implementing security controls and applying security patches to their applications, to protect their services within the cloud from hostile actors, including malicious insiders. A CS facility that fails to understand and fulfil its role in ensuring the security of its public cloud operations, or misconfigures security settings, could leave its critical services exposed to inadvertent, hostile or malicious compromise. Misconfiguration by cloud users has been reported as the most common source of data breaches in the cloud (US Department of the Treasury 2023).

Additionally, taking a 'lift and shift' strategy to migrating legacy applications can affect security, because it can result in on-premises security vulnerabilities being transferred to the public cloud (Pekkarinen undated). In practice, CS facilities would need to apply the same level of cyber-risk analysis and monitoring to the cloud-based systems, as they would for on-premises solutions.

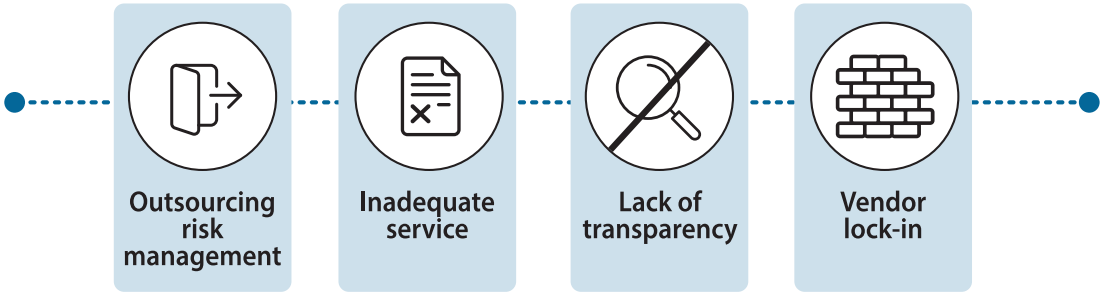
Inadequate maintenance

Once established, cloud-based systems need to continue to be updated and tested for security and resilience. Public cloud environments are continually evolving, for example, in response to emerging security threats or changes required by their customers. If a CS facility fails to maintain cloud-based systems in line with the cloud provider's upgrade schedule, this could create gaps and incompatibilities that pose a risk to the security and reliability of critical services.

Geographic location of data

Duplication of data across geographically diverse cloud locations can support resilience. However, if a CS facility chooses to use a cloud region located in another jurisdiction, it may be exposed to the legal or regulatory systems of that jurisdiction. Some governments place ownership and access restrictions on data held within their jurisdiction, which could limit a CS facility's control over its own data and systems. Issues with accessing data could be exacerbated by national crisis measures such as those taken by some jurisdictions during the COVID-19 pandemic.

Figure 4: Public Cloud Risks related to Outsourcing to Third-party Vendors



Insufficient cloud knowledge

The migration and operation of services in a public cloud requires staff at CS facilities to have different technical skills and operating mindsets to the skills associated with operating and maintaining on-premises systems. Similarly, a CS facility's board of directors and management need sufficient understanding of public cloud to provide effective oversight and governance for cloud migrations and operations. As with all technologies, insufficient cloud skills at the staff, management and board levels could lead to poor design decisions and sub-optimal operational, resilience and security outcomes.

Risks relating to outsourcing services to a third party

CS facilities typically use the technology products and services of a variety of third-party vendors in delivering their critical services. However, moving these critical services to operate in a public cloud significantly increases a CS facility's reliance on a single external provider, which heightens vendor-related risks as outlined below (Figure 4).

Outsourcing the management of risks

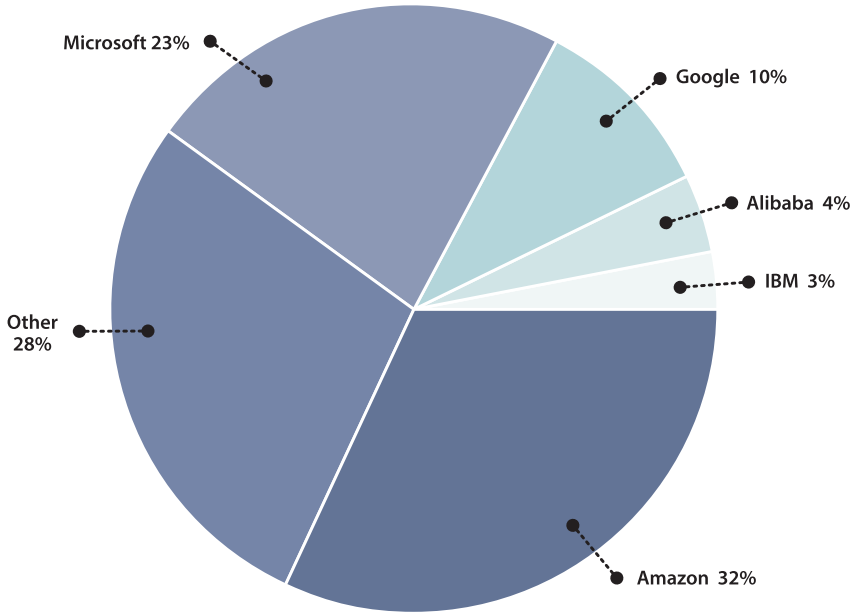
Public cloud providers might not manage risks in a manner appropriate to the operation of critical market infrastructure. The stability of a CS facility's critical services can be compromised if it does not validate the sufficiency of a vendor's risk management practices, or if it leaves risk management entirely to the third party. There are also technology-related risks that can only be managed by the CS facility itself, and not by the provider.

Inadequate levels of service

Although public cloud infrastructure can support high availability, resilience and security, there remains a risk that the public cloud provider fails to deliver a level of service commensurate with the criticality of a CS facility's services. This could occur for a variety of reasons. For example:

- The public cloud provider may not meet appropriate levels of availability, resilience and security set out in contractual arrangements. For instance, in the event of an operational disruption, the provider may not respond with sufficient urgency to restore services used by the CS facility.
- There may be deficiencies in the contractual service agreement. Public cloud providers have significant market power and may not agree to contractual arrangements that meet the needs of CS facilities.

Figure 5: Share of Infrastructure and Platform Cloud Services in 2023



Source: Synergy Research Group.

Lack of transparency

CS facilities may have limited visibility of the public cloud provider's operations, security arrangements and potential points of failure. This can make it difficult for a CS facility to determine if the cloud provider is delivering a reliable, secure and resilient service. Transparency may be further reduced where the cloud provider sub-contracts parts of its operations to fourth-party vendors.

Vendor lock-in

If the public cloud provider is no longer able to deliver an appropriate service (e.g. if the provider becomes insolvent), a CS facility may need to exit the arrangement. This exit could mean the CS facility needs to migrate its services to a different provider or bring the services back on premises. A CS facility's critical services could be severely disrupted if it does not have an effective plan and sufficient funding to exit and transition from its cloud provider.

Concentration risks

The public cloud market is dominated by Amazon Web Services, Microsoft Azure, and Google Cloud. Together, these providers accounted for almost two-thirds of the world market for cloud infrastructure and platform services in 2023 (Saarinen 2023) (Figure 5).

The limited number of public cloud providers means that many CS facilities, as well as their participants and clients, are also likely to be reliant on services from the same providers. This concentration means that an outage at a service provider could cause widespread disruption to the financial system. This issue is broader than CS facilities – concentration risk affects the whole financial industry, as well as other sectors, and has attracted increasing attention by regulators in Australia and internationally.

Regulations requiring CS facilities to manage risks posed by cloud

CS facilities are required to comply with the Financial Stability Standards (FSS) set by the RBA (RBA 2012a; RBA 2012b). These standards are based on the CPMI-IOSCO Principles for Financial Market Infrastructures, and are designed to ensure that CS facilities conduct their affairs in a manner that is consistent with financial stability.[2] The RBA assesses CS facilities against the FSS on a regular basis.

The FSS require CS facilities to identify the operational risks (including technology and third-party risks) to their critical services, and manage these risks in a manner that supports the stability of the financial system. The requirements apply equally to a CS facility's use of public cloud and traditional technologies, and provide a framework for ensuring that operational risks are addressed appropriately.

CS facilities are required to have in place robust systems, policies, procedures and controls to monitor and mitigate sources of operational risk. To meet the FSS requirements in the context of using public cloud, CS facilities must develop a thorough and detailed understanding of the potential risks, including to resilience and security. They also need to address these risks through the design, migration and subsequent operation of their cloud solutions.

Management of technology risks

The FSS require CS facilities to design the technology systems supporting critical services to be highly resilient and secure. CS facilities are also required to have the following:

- **Availability targets.** CS facilities must set clear and exacting targets for the reliability and availability of their critical systems.
- **Business continuity and recovery arrangements.** CS facilities must have arrangements in place to ensure that critical operations can resume within two hours following an operational or security disruption, and by no later than the end of the day, even in extreme circumstances. Systems should be able to resume with a high degree of confidence that data has not been lost.
- **Security.** CS facilities must implement safeguards to defend against current and potential future threats to the security of their systems and data (e.g. cyber-attacks). These controls should be regularly updated and tested to ensure their ongoing effectiveness.
- **Access to skilled resources.** CS facilities must have access to staff with appropriate skills to ensure that their critical services operate reliably and securely in all circumstances.

Management of third-party vendor risks

CS facilities that outsource key systems to third-party cloud vendors ultimately remain responsible for ensuring that their services meet the resilience and security requirements of the FSS. CS facilities are required to have the following:

- **Formal outsourcing policies.** These policies should include robust arrangements for selecting and monitoring vendors (including cloud providers) to ensure that the services provided meet all regulatory requirements. The FSS contain guidance on the scrutiny CS facilities should exercise over the risk management processes of third-party providers, particularly in relation to service availability, business continuity and recovery, and the confidentiality and integrity of data.
- **Access to information.** Contractual arrangements with vendors must provide CS facilities access to the information needed to assess the vendor's performance. Access to information must similarly be provided to the RBA. Contractual arrangements with vendors also must provide CS facilities with information about, and control over, the use of sub-contractors.
- **Formal policies for exiting outsourcing arrangements.** Exit arrangements (such as those relating to exiting a cloud provider) must ensure the continuity of critical services even in the event of a crisis.

The FSS do not directly address risks posed by the concentration of cloud vendors. However, management of technology and third-party risks in accordance with the FSS helps to ensure that CS facilities are more resilient to issues with their cloud providers. CS facility participants are also typically subject to prudential regulations that require them to manage third-party risks.

Governance

The FSS recognise the importance of sound board oversight and senior management leadership in managing operational risks. A CS facility's board of directors and management must have appropriate skills to discharge these responsibilities. For a CS facility looking to use cloud technologies, this would include skills to oversee and manage the risks associated with migrating to and operating critical systems in a public cloud. The FSS also set out specific governance responsibilities for a CS facility's board and board committees, including in relation to the approval of third-party outsourcing arrangements and receiving regular reporting on the performance of critical services.

Conclusion

CS facilities play a critical role in ensuring the stability and effectiveness of the financial system. The adoption of public cloud provides opportunities for CS facilities to enhance the technologies they use to deliver their critical services. However, there are also notable risks with migrating to and operating in a public cloud, relating to the appropriate and competent use of the technology, and to increased reliance on third-party vendors. The FSS require CS facilities to carefully identify and appropriately manage these risks so that critical services that are housed in a public cloud environment operate in a manner that is consistent with financial stability.

Endnotes

[*] The authors are from Payments Policy Department. This article draws on information from the following sources: APRA (2018), AWS (2023), CBA (undated), Crozier (2023), IBM (undated), Microsoft (undated), NAB (2022), O (2023), Perry (2020), Pekkarinen (undated), Saarinen (2023) and Westpac (2017). The authors would like to thank Benn Robertson, John Kenyon and James Macnaughton for their insight and input into this article.

[1] For example, the major Australian banks are pursuing technology strategies to migrate services progressively to cloud environments, with some banks now using cloud to run more than 70 per cent of their applications (CBA undated); (NAB 2022). Some newer neobanks are almost entirely cloud-based.

[2] In interpreting relevant requirements under the FSS, the RBA also applies the guidance on cyber resilience for financial market infrastructures from CPMI-IOSCO (2016).

References

APRA (Australian Prudential Regulation Authority) (2018), 'Outsourcing Involving Cloud Computing Services', Information Paper.

CBA (Commonwealth Bank of Australia) (undated), 'Making the Move to Public Cloud'. Available at <https://www.commbank.com.au/articles/careers/making-move-to-public-cloud.html>.

Cloudflare, 'What is the Cloud? | Cloud Definition'. Available at <https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud/>.

CPMI-IOSCO (Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions) (2016), 'Guidance on Cyber Resilience for Financial Market Infrastructures', CPMI Paper No 146, June.

Crozier R (2023), 'ANZ Finds Its Feet to Hit Cloud Migration Milestones Quicker', itnews, 1 August. Available at <https://www.itnews.com.au/news/anz-finds-its-feet-to-hit-cloud-migration-milestones-quicker-598479>.

IBM (International Business Machines) (undated), 'What is Cloud Security? Cloud Security Defined'. Available at <https://www.ibm.com/topics/cloud-security>.

IBM (undated), 'What is Virtualization?'. Available at <https://www.ibm.com/topics/virtualization>.

Koh T and J Prenio (2023), 'Managing Cloud Risk – Some Considerations for the Oversight of Critical Cloud Service Providers in the Financial Sector', Bank of International Settlements FSI Insights No 53, November.

Microsoft (undated), 'Security Implications of Logical Separation in the Cloud', Policy Paper. Available at <https://www.microsoft.com/en-us/cybersecurity/content-hub/security-implications-logical-separation-in-cloud>.

NAB (National Australia Bank) (2022), 'NAB Announces Long-term Cloud Deal with AWS', 29 November. Available at <https://news.nab.com.au/news/nab-announces-long-term-cloud-deal-with-aws/>.

O H (2023), 'New Cloud Guidance: How to "Lift and Shift" Successfully', National Cyber Security Centre (UK) Blog, 28 November. Available at <https://www.ncsc.gov.uk/blog-post/new-cloud-guidance-lift-shift-successfully>.

Pekkarinen P (undated), 'Benefits and Risks of Lift and Shift Migration to Public Cloud', Nordcloud. Available at <https://nordcloud.com/blog/benefits-and-risks-of-lift-shift-migration-to-public-cloud/>.

Perry Y (2020) '3 Cloud Migration Approaches and their Pros and Cons', NetApp.com, 18 September. Available at <https://bluexp.netapp.com/blog/cvo-blg-cloud-migration-approach-rehost-refactor-or-replatform#H_H4>.

RBA (Reserve Bank of Australia) (2012a), 'Financial Stability Standards for Central Counterparties', December.

RBA (2012b), 'Financial Stability Standards for Securities Settlement Facilities', December.

Saarinen J (2023), 'AWS, Microsoft and Google Hold 65 Per Cent of Cloud Market', CRN, 1 May. Available at <https://www.crn.com.au/news/aws-microsoft-and-google-hold-65-per-cent-of-cloud-market-593825>.

US Department of the Treasury (2023), 'The Financial Services Sector's Adoption of Cloud Services', Report.

Westpac (2017), 'Westpac Signs Five-year Agreement with AWS to Bolster Cloud Capabilities', Media Release, 27 February.