Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 4, Issue 3, 2026

STRATEGIC TECHNOLOGY PROCUREMENT AND OPERATIONAL RESILIENCE: A MULTIPLE-CASE STUDY OF CLOUD CONCENTRATION AND EXIT READINESS IN FINANCIAL INSTITUTIONS

Syed Ahsan Raza Kazmi

AVP – Manager Technology Procurement, Mashreq Bank, UAE

Kazmiahsan1@gmail.com

DOI: https://doi.org/10.5281/zenodo.23834773

Keywords
cloud computing; technology procurement; operational resilience; concentration risk; third-party risk management; financial services; exit readiness; outsourcing governance

Article History
Received: 23 January 2026
Accepted: 11 March 2026
Published: 25 March 2026

Copyright @Author
Corresponding Author: *
Syed Ahsan Raza Kazmi

Abstract
Financial institutions are increasingly relying on cloud service providers (CSPs) to support critical technology, processing capabilities and customer-facing services. While embracing cloud can benefit scalability, access to additional security features, and improved operating efficiency, it can also present dependencies that are hard to find, manage, and unwind. The challenges are especially great if there are a number of providers in the shared space or if, for example, they use the same technology, software, and subcontractors. This paper explores the synergy of technology procurement strategy, together with provider selection, concentration risk assessment, contractual governance, dependency mapping and exit readiness, and how they can help achieve operational resilience. It uses a qualitative documentary multiple case study approach with analysis of regulatory and policy documents, a professional banking case study and peer-reviewed research. Some of the sources in the evidence corpus are from the Financial Stability Board, the U.S. Department of the Treasury, the Financial Conduct Authority, the European Banking Authority, Grant Thornton and Parchimowicz. The five interconnected governance issues identified by the thematic analysis are concentration risk extends beyond the number of contracted providers, procurement decisions impact on resilience throughout the technology lifecycle, contractual exit provisions does not automatically mean that practical portability is achieved, dependency visibility is key to continuity planning and exit readiness is all about regular testing and accountable ownership. The paper introduces an integrated governance model for procuring critical services from the perspective of the provider, contractual safeguards, architectural and dependency management, resilience testing and controlled exit execution. The study focuses on providing a governance-based synthesis for financial institutions to help them achieve a balance between cloud-based innovation and service continuity and regulatory responsibility.

1. INTRODUCTION

Cloud computing has become an important component of financial institutions' technology strategies. Cloud solutions enable banks, insurers, payment providers and other financial services companies to store data, power software applications, enable analysis, protect against cyber threats, deliver customer services, and increasingly, to power complex operations. Cloud adoption can offer access to infrastructure that is scalable as well as to certain specialised capabilities that would be costly to develop on their own. The Financial Stability Board (FSB, 2019) acknowledges that cloud services could enhance the resilience and

flexibility within individual institutions, and raises issues of governance, oversight, cross-border and concentration.

The cost, speed and technical functionality of cloud technology implementation, therefore, cannot be the only indicators for assessing its value. If a relationship is negatively impacted, procurement decisions will affect the institution's ability to monitor a provider, recover from disruption, transfer workloads, access data and maintain critical services in the future. These factors can be more significant if the services that critical banking functions rely on are few and large, or if they are based on interdependent technologies that cannot be replaced easily on their own.

Treasury (2023) points out that there are a number of challenges with financial-sector cloud adoption, such as the absence of specialized expertise, lack of transparency, incident-response coordination, market concentration, and contract negotiation imbalance. These concerns suggest that cloud risk isn't just an information-technology concern. It also involves the governance of commercial relationships, contractual rights allocations, supplier alternative assessment, and institution's ability to make credible decisions in times of disruption.

This broader view is reflected more and more in the regulatory approaches. The FSB's third-party risk management toolkit includes the critical services identification process and the management of third-party relationships over their lifecycle (FSB, 2023). The Financial Conduct Authority (FCA) is providing guidance on cloud and other third party IT outsourcing, covering topics such as due diligence, access to data, concentration risk and exit planning (FCA, 2016). The Digital Operational Resilience Act (DORA) (European Parliament & Council of the European Union, 2022) introduces obligations for in-scope financial entities (ISFEs) that include ICT risk management guidelines and ICT third-party arrangements. Parchimowicz (2024) discusses the legal and practical hurdles that cloud can create with the adoption of DORA, such as the selection of cloud providers, outsourcing of critical functions, contracting terms and conditions, data security and the concentration risk.

Even with this emerging guidance, a practical governance issue still remains: How can financial institutions define what it takes to meet the requirements for procurement and outsourcing, and ensure they can effectively withstand, respond to, and recover from a disruption to the cloud services? The termination rights in a contract do not necessarily guarantee that data can be provided in an acceptable format, applications can run on another platform, or replacement can be found within an acceptable time. Likewise, multiple contracts do not eliminate concentration risk when the multiple providers share a common infrastructure, software, identity services, connectivity or subcontractors.

This paper uses multiple-case study, a qualitative method, to explore the relationship between technological strategies to be purchased and operational resilience. It combines the regulatory guidance, policy analysis, academic study and published banking migration case. The aim is not to suggest that the sources are representative of all financial institutions but to highlight the common governance mechanisms and tensions that might be applicable to financial institutions' procurement practices.

The paper addresses three research questions:

1. How do cloud concentration and third-party dependencies challenge operational resilience in financial institutions?
2. How can technology procurement and contractual governance reduce the gap between formal exit rights and practical exit capability?
3. What integrated governance framework can connect provider selection, ongoing oversight, resilience testing, and exit readiness?

The paper offers a framework of the lifecycle approach that views procurement as not only a purchasing process, but rather as the starting point of an on-going governance process.

2. LITERATURE AND REGULATORY CONTEXT

2.1 Cloud adoption and concentration risk

Cloud services can deliver economies of scale, agility in application scaling, and the ability to scale up to specialized security and technology services. But their ubiquity also can create a focus of operational dependencies. The FSB (2019) distinguishes the benefits that individual institutions might derive from the other concerns that could arise if a large number of institutions rely on the same providers. Disruptions impacting a widely-used provider could impact multiple financial entities, especially those that rely on a

shared technology infrastructure to serve critical services.

Therefore, concentration needs to be appraised at several different levels. Direct concentration is related to the number and significance of services received from a specific service-provider. A functional concentration is when multiple critical business processes rely on a single provider or highly interdependent services. A form of subcontracting concentration is when two or more seemingly distinct suppliers share the same basic technology or infrastructure. Financial market concentration is a general issue around the weak supplier base in finance. These are analytically separate categories that also can reinforce each other.

The U.S. Department of the Treasury (2023) identifies concerns that increased concentration by cloud service providers can have a greater impact if an incident occurs and affect contractual bargaining power. It also identifies the challenges in measuring the sector-wide exposure in the absence of information on sector-level dependencies and provider arrangements. These considerations are good reasons for basing procurement decisions on analyzing the entire dependency chain instead of relying on a supplier's name as a proxy for risk.

2.2 Procurement as a resilience mechanism

The evaluation of a traditional procurement process will typically be based on the cost, service, technical match, delivery capacity, and terms of contract. In the case of critical technology the above criteria will still be required but alone would not be sufficient if they are not supported by a systematic evaluation of operational consequences. Procurement needs to think about whether the service proposed will allow for the institution to meet its continuity goals, whether the provider will provide adequate assurance information and whether the institution will be able to maintain adequate control over its regulatory responsibilities.

Firms continue to have responsibility for fulfilling the relevant obligations when outsourcing (cloud) or third party IT services (FCA, 2016). In the FSB's toolkit, third-party risk is a lifecycle issue, as it is identified and assessed, monitored and terminated throughout the process (FSB, 2023). These sources enable a governance model where procurement, information security, legal, architecture, operational resilience and business ownership have a say in determining who are the critical technology suppliers.

The cross-functional model is significant as procurement teams can negotiate contractual rights without having the technical information to be able to determine whether exit is possible or not. This is where technology teams can grasp the migration relationships and not have control over commercial commitments. Business owners can specify which services are more critical to them than others without knowing how costly it will be to move data and/or workloads and how long it will take to do so. Resilience then relies on linking up these roles and responsibilities rather than having them in separate departments.

2.3 Contractual governance and exit readiness

Contracts provide significant rights and obligations such as access to information, service-level obligations and commitments, audit, incident notification, subcontracting controls, data returns, transition assistance, and termination. But, a contractual right is not necessarily a proven technical ability. Proprietary data formats, application dependencies, specialist staffing needs, network requirements and limited capacity of replacement providers will only be addressed by an exit clause.

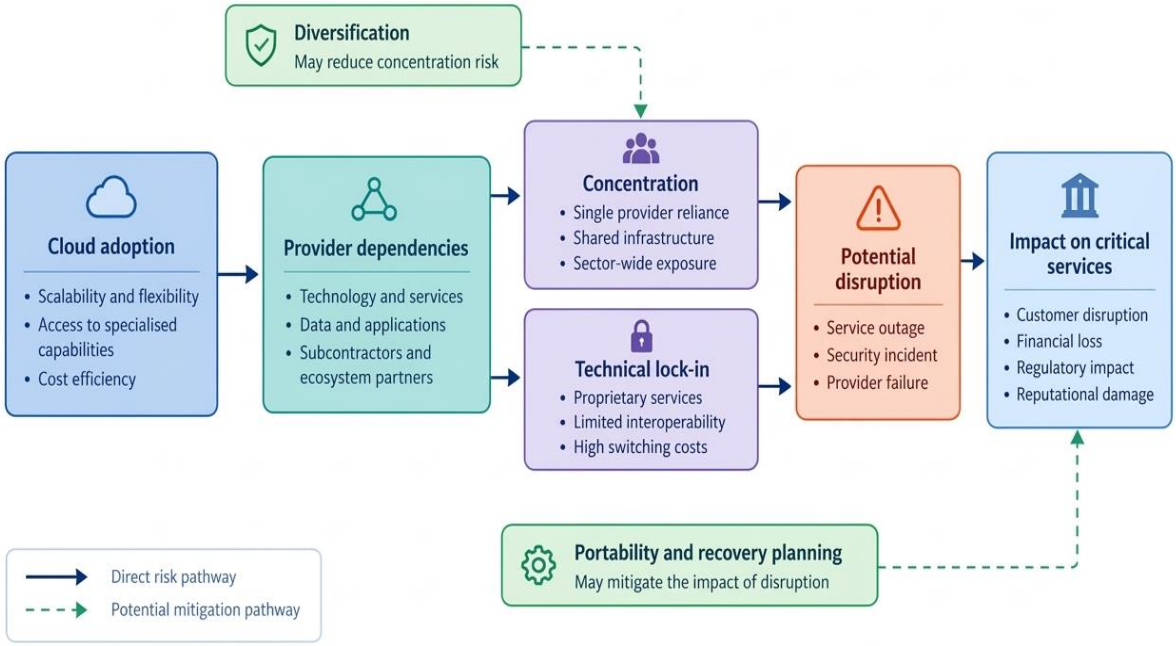
Parchimowicz (2024) outlines the provider selection, decisions on critical/important functions, contractual terms and conditions, data security and concentration risk as interrelated issues in the context of DORA for financial institutions. This reinforces the idea that exit factors must be taken into account at the selection and contracting process and not when a supplier relationship comes to an end.

The real-world implications of "exit readiness" is therefore more than just having a written exit plan. It requires a good understanding of the services being depended upon, an evaluation of available options, clear responsibilities, available data-export options, credible timeline for transition, and evidence based on simulation or testing. The amount of assurance will vary, depending on the nature of the service and the impact that would be caused by a disruption in the service.

2.4 Operational resilience and third-party oversight

Operational resilience is not just about not having any failures; it's about continuing to provide crucial services in the event of disruption. Particularly in a cloud environment, it is important for an institution to know which business services rely on a provider, how disruptions might be passed down, what alternative arrangements are available and how recovery actions will be determined.

The FSB (2023) has offered a toolkit for financial institutions and authorities that helps to enhance their third-party risk management and supervision in a lifecycle perspective. Due diligence, data access, risk management and exit planning are also covered in cloud outsourcing in the FCA (2016). While the rules vary from one jurisdiction to another, as well as from institution type to institution type, all these sources boil down to a single rule of good governance: Outsourcing will not absolve the institution of its responsibility to understand and manage the risks for its critical services.



Note: This figure presents a conceptual model of how cloud dependencies can create concentration and resilience risks in financial institutions and how certain governance actions may mitigate these risks. It is not a representation of a specific organisation.

Figure 1. Conceptual relationship between cloud concentration, procurement governance, and operational resilience.

3. METHODOLOGY

3.1 Research design

This study uses a qualitative documentary multiple-case-study design. Documentary Analysis is appropriate given that the research questions are related to governance expectations, published institutional experience and scholarly analysis of cloud concentration, cloud procurement controls and readiness for exit. The unit of analysis is not the individual employee or financial institution interview that is the focus of the study, but the document or source.

The study is a blend of three types of evidence: regulatory documents and policy documents, a professional banking case study, and peer-reviewed academic literature. The sources are used for various reasons. The governance expectations outlined in regulatory documents, the interpretation of legal and practical challenges contained in academic research and the professional case is a reported cloud migration programme are examples of the latter. The evidence is not considered methodologically interchangeable, but is synthesised.

3.2 Documentary corpus and selection

Sources were chosen based on their relevance with financial-sector cloud adoption, dependency on third-party providers, concentration of providers, financial-sector procurement governance, financial-sector operational resilience, and exit planning.

The corpus comprised the following seven sources

Source	Evidence type	Analytical contribution
FSB (2019)	Financial-stability policy report	Cloud dependencies, concentration, cross-border oversight, portability
FCA (2016)	Regulatory guidance	Due diligence, data access, concentration risk, exit planning
EBA (2019)	Regulatory guidelines	Governance of outsourcing arrangements and critical functions
U.S. Department of the Treasury (2023)	Government policy report	Provider transparency, concentration, bargaining power, incident response
FSB (2023)	Third-party risk management toolkit	Lifecycle governance and critical-service identification
Parchimowicz (2024)	Peer-reviewed academic article	Cloud adoption under DORA, provider selection, contract design, concentration
Grant Thornton (2025)	Professional banking case study	Cloud migration planning, application inventory, testing, transition, post-migration review

The Grant Thornton case is about a regional bank, migrating its core technology platform to managed cloud services. According to the published story, the transfer of assets and account information was accomplished for $16 billion, the end-of-day job runs were reduced by 20% and the computer operations department was eliminated in the process because of the elimination of execution work. It also covers the planning aspects of the activities including infrastructure assessment, application inventory, transition planning, testing, migration playbooks and post-implementation review (Grant Thornton, 2025). The information provided is based on claims made by the case study publisher, and is not the result of independent research.

3.3 Analytical procedure

Thematic analysis was used as a structured method to analyze the data, which followed the approach of Braun and Clarke (2006). Firstly, the documents were read for what they were intended for, the institutional context and if they were relevant to the research questions. Secondly, content related to provider selection, critical service identification, provider concentration, provider contract, provider dependency visibility, testing for resilience and exit arrangements were conceptually coded. Third, codes that are related were grouped together to form provisional themes. Fourth, the themes were examined in order to see how they resonate with the various type of evidence and how they are different and how they are limited. Lastly, a framework for integrated governance was developed based on the themes.

Analysis was not of a statistical nature. There is no indication on the frequency of themes across financial sectors. Nor does the study make any claim to access to the confidential supplier contracts, internal risk registers, interviews, or proprietary records of migrations. The results are the result of an analysis of the documents that were selected.

3.4 Credibility and limitations of the evidence

The credibility was reinforced through providing policy guidance alongside academic analyses and the reported migration experience. But, the purposes and independence of sources are not the same. There are three types of regulatory reports, one in the form of a consultancy case study and a scholarly article that outline legal and analytical arguments. Consensus among these sources can help to build a reasoned interpretation, but cannot provide statistical validation.

The documentary corpus is purposive and limited. It has no way of knowing how often any individual practice is used in all the financial institutions, nor can the Grant Thornton case show that the same results would be received in other banks. The

study thus seeks to be analytic in order to find governance questions and mechanisms which institutions can evaluate in other contexts.

4. FINDINGS AND CROSS-CASE ANALYSIS

The analysis revealed five interconnected themes: prioritising more than just a number of suppliers; procurement as the governance of the lifecycle; the difference between contractual rights and real exit options; dependency visibility as a precondition for resilience; and the need for testing instead of documentation of exit options.



Figure 2. Cross-source evidence map linking documentary cases to the principal analytical themes.

4.1 Theme 1: Concentration extends beyond the number of suppliers

The FSB (2019) and the U.S. Department of the Treasury (2023) both point to the possibilities that widespread reliance on cloud services could have systemic effects. They believe supplier numbers is not a reliable indicator of resilience, as their analysis shows. If the critical services are hosted on a common infrastructure, software dependency, identity provider or subcontractor, an institution could be vulnerable if it contracts with multiple providers.

This distinction has direct implications for procurement. Depending on the institution, vendor diversification may not be considered a risk reduction until the institution has investigated the dependencies under each contract. Questions are: Do alternatives have their own infrastructure, is workload dependent on the primary's proprietary services, and does there exist realistically some capacity to replace in the event of an event affecting a sector-wide portion of the population? No evidence is provided that all institutions need to employ more than one cloud provider. There could be extra complexity, cost, integration, and operational overheads when adopting multi-cloud. It's a more defensible argument, however, that procurement should evaluate concentration in relation to critical service needs and reasonable alternatives. Resilience can be better supported through a well tested recovery environment, portable workloads or through an alternative operating arrangement than by simply adding another provider with no separation of dependencies.

4.2 Theme 2: Procurement decisions establish the conditions for future resilience

Regulatory sources consider the role of a third party as a continuous one, and not an approval of the supplier. The FSB (2023) highlights the concept of lifecycle risk management, and the FCA (2016) mentions expectations on areas such as due diligence, access to data, concentration and exit planning. Parchimowicz (2024) also relates the choice of cloud provider and contractual terms to the risks stemming from DORA.

The banking case of Grant Thornton (2025) is an example of the need to be well prepared prior to migration. The approach it had was to assess infrastructure, inventory applications, put a transition plan together, create a testing plan, develop a playbook for migration, provide vendor support before and after go-live, and have a lessons-learned review. The activities illustrate the importance of planning and coordination in a migration programme. In the case, the bank did not however prove to have a full exit from its cloud provider or removed the concentration risk. It has a more limited contribution as it shows how structured planning and preparation of the application level can help with controlled technology transition.

Overall, this evidence indicates that resilience needs should be part of the request-for-proposal process, the evaluation process, the contract approval process and the contract governance. The procurement process should ensure that there is evidence that the proposed service will be able to support the operational needs of the institution, and that the critical assumptions (such as data portability, recovery time and transition support) are testable.

4.3 Theme 3: Contractual exit rights do not guarantee practical exit capability

A recurring tension across the sources is the difference between formal governance arrangements and operational feasibility. Contracts may provide rights to access data, end a service, provide transition assistance or provide information on incidents. However, the actual usefulness of these rights relies on the technical compatibility, co-operation of the providers, availability of skills, complexity of the migration process and availability of alternatives.

Parchimowicz (2024) notes that contract and provider selection is important when selecting cloud solutions. Similarly, FCA (2016) refers to the availability of data and exit arrangements as issues in outsourcing. The FSB's work on the portability and lifecycle management aspect of cloud dependency and third-party risk also continues to drive attention to portability and lifecycle management. (FSB, 2019, 2023)

From the procurement perspective, this means exit terms need to be translated into operational (acceptance) criteria. For a data-return clause, for instance, the data formats, how it's exported, metadata, integrity checks, access rights, and deletion confirmation should all be specified. A transition-assistance clause should point out what is expected of the school, what the student needs, what is expected of costs, and the duration of support. If a service continuity is critical, then the institution shall also define a replacement environment configuration, security, testing and authorisation for use.

A plan to exit, therefore, should be considered as a "handled" function, and not an appendix of a contract. The plan should be appropriate for the level of criticality of the service and should be periodically reviewed in light of any changes in applications, service architecture, provider arrangements or business requirements.

4.4 Theme 4: Dependency visibility is essential to resilience

The evidence shows that risks that are not mapped cannot be effectively managed in an institution. Throughout the lifetime of the relationship, the FSB (2023) emphasises identification of critical third-party services and management of related risk. The Treasury report (2023) outlines the problems with information and transparency in the financial services sector's relationship with cloud service providers. The Grant Thornton (2025) case also mentions the following as a part of the migration planning: Application inventory and infrastructure assessment.

Dependency mapping should identify business services that are dependent on applications, data stores, cloud services, providers, subcontractors, identity and access systems, network connectivity and specialist operational capabilities. This allows the institution to identify failures which might affect a critical service and dependencies they will need to be replaced or restored when transitioning.

It's not enough just to have a supplier register. May disclose the existence of an existing counterparty to a contract, but not disclose technology services that rely on it, or the potential impact of disruption. A valuable dependency record should take into account the provider, their criticality to the service, business ownership, the recovery objectives, data location and portability, sub-contracting agreements as well as exit assumptions. Also, the analysis indicates that dependency mapping needs to be carried out over time. Business Services evolve, new subcontractors are added, software is changed and cloud architectures change. It is likely that mapping will rapidly become a weak tool if it is focused on the scope of the initial due diligence rather than change management and periodic assurance.

4.5 Theme 5: Exit readiness requires testing and accountability

A documented exit strategy can be helpful to get started, but does not constitute an executable exit strategy. The sources as a whole support a more robust understanding of readiness: they should be able to tell who would have to do the decision making, which services would be prioritised, what they would need to take care of, how data and applications would be transferred, what resources would be needed, and how critical services would be continued.

Testing need not always involve a full production migration. The type of exercise an institution will use depends on the importance of the service and the cost of the service.An institution may choose to have tabletop exercises, data-export tests, restoration exercises, technical portability tests, or controlled migration rehearsals, depending on the importance of the service and the cost of the service. The test should, however, explore material assumptions and not just the documentation.

There's also accountability, spelled out. Business owners should set the acceptable level of service disruptions; technology teams should ensure the technology is viable; procurement and legal teams should continue to have contractual safeguards; information-security specialists should determine access and data risks; and operational-resilience should consider implications of continuity and recovery. Senior governance bodies have a role to play in deciding what material risk acceptances should be and to ensure that exit plans are funded and kept in place.

The conclusion is that exit readiness is not a specific technical characteristic. It's an integrated capability, which features contractual rights, architectural options, operational knowledge, available resources, and decision-making authority.

5. AN INTEGRATED PROCUREMENT-TO-EXIT GOVERNANCE FRAMEWORK

The cross-source synthesis provides for a unified framework in six stages of connection. This paper introduces a proposed framework, rather than an existing regulatory model and/or an empirically tested maturity standard.

Stage 1: Identify critical services and establish impact requirements. The institution needs to identify the business services that the proposed technology will support and understand the impact of disruption. Documentation should occur prior to provider selection of: Recovery Objectives, Service Tolerances, Customer Impacts, Regulatory Requirements, and Dependencies.

Stage 2: Assess providers and concentration exposure. Financial and operational capacity, security measures, transparency, subcontracting, geographic factors, legal factors, provider substitutability and market concentration are factors to consider in due diligence. Assessment should cover the technology dependencies of what is more or less independent suppliers.

Stage 3: Embed resilience and exit requirements in contracts. Data access and portability, notification of incidents, audit and assurance, transparency of subcontractors, service level commitments, transition support, termination rights, data return, data deletion and exit costs allocation should be a part of the contract. Clauses should be considered for their operational value, rather than their legal completeness.

Stage 4: Sustain the visibility of architecture and dependencies. The institution should keep an up-to-date list of critical business services and the applications, data, cloud services, providers, subcontractors and recovery plans that are required to maintain those services. As long as the architectural changes and the supplier changes are affecting the concentration and exit assumptions, they should be reevaluated.

Stage 5: Monitor, test and remediate. Ongoing assurance activities should include: Service performance, incidents, changes of providers, Control Reports, Dependency Updates and

periodic exit exercises. Results should result in remediation with owners and timeframes.
Stage 6: Execute exit or transition and reassess. Institutions should have a controlled plan in place when exit is required, which should include responsibility for the decision, sequencing of the transition, data integrity, security, continuity, replacement, contractual support and post transition validation. The lessons learned should be incorporated into the next steps of the procurement and architecture.



Figure 3. Integrated procurement-to-exit governance lifecycle.

The framework should be applied proportionately. Assessment and testing of a low-criticality productivity service could be different from that of a cloud service for payment processing or core banking operations. The principle of proportionality should affect the intensity of the control, not eliminate the need to establish who is owning the control, what their requirements are, and what is feasible to exit the control and how.

6. DISCUSSION

The results situate strategic technology acquisition as a key element of operational resiliency. The procurement process influences the institution's dependency profile prior to entering into the production of a service. The cost and complexity of changing to another provider may rise if a critical workload relies on the provider's proprietary technologies, data structures and operating practices. Resilience needs to be therefore part of the selection and contracting process and not added afterwards once it has been entrenched.
The first implication is about the extent to which suppliers can be diversified. Some diversifications can decrease some dependency, but can also bring about operational complexity. The goal of the relevant objective isn't to seek to maximize the number of providers rather, to determine if there are critical services with alternative, independent,

supportable, and credible alternatives. The technical dependencies, substitutability, contractual considerations, and feasibility of workload transfer should therefore be taken into account for a concentration assessment.

The second one relates to the impact of contract design on architecture of technology. The portability and the obligations to transition can be negotiated during procurement but whether the obligations can be delivered is determined by architecture. Contractual rights may be less useful where the workload is highly reliant on proprietary services, undocumented interfaces or special capabilities of the provider. A consideration of contractual and architectural options should thus be conducted concurrently.

The third implication relates to what it means to be "ready to exit. Exiting is not a call to action for customers to move away from a cloud provider and does not imply that customers should have a full replica of all services in their environment. These types of agreements could be costly and might add extra risks. Instead, readiness should involve the ability to have a defendable understanding of the options available for response and then to be able to carry out the option appropriately. These options can involve restoring backups, transferring workloads, moving to a pre-arranged replacement, or selecting to move the operations in-house, or managed transition period.

The fourth one relates to accountability of governance. While the technology teams and a cloud provider can do this, it is not solely their responsibility to provide operational resilience. It needs to be a coordinated decision, both in the business ownership, procurement, legal, information security, architecture, and risk management. Senior management need to grasp material dependencies, accept or mitigate any residual risks and monitor for any sufficiency in resources for resilience plans.

Lastly, the results show that regulation should be made evident in the capability. Policies, contractual clauses and registers are governance artefacts that are required, but records of operations, test results, decisions about remediation work and ownership of a policy should back this up. This interpretation aligns with the lifecycle focus of the FSB toolkit and with some concerns raised with provider selection, contracts, and concentration raised by Parchimowicz (2024).

7. PRACTICAL AND REGULATORY IMPLICATIONS

The framework suggests that financial institutions should start with a business-service analysis before starting to consider technical features during financial-procurement of critical cloud services. Procurement documents should include the service-criticality assumptions, recovery outcomes that are expected, data portability requirements, transparency requirements, and exit scenarios. Cost and feasibility of transition should be part of the provider evaluation and not just the cost and efficiency in the first instance.

Institution-based contract managers should ensure that the usage of a service does not change in the course of the contract, and is still as per the original risk assessment. A review should be conducted when there is a change in the material to the workloads, subcontractor(s) involved, data flows, or the service architecture. It is also important for institutions to have clear ownership for keeping plans for exits, and for records of what is found from testing.

The study highlights the importance of transparent communication of incidents, providing clear details about the subcontracting arrangements, providing easy access to data-export processes, and providing effective transition support to cloud-service providers. These capabilities can be used to enable customers to evaluate risk and plan for disruption. Increased transparency can also help to facilitate better collaboration among providers, financial institutions and relevant authorities.

The results for regulators and supervisory authorities will serve as a platform for focussing on firms' third-party risk management in practice. They might refer to evidence relating to the institution's capacity to identify critical dependencies, clarify the concept of concentration exposure, and have access to evidence and data, and have shown credible evidence of considering or testing transition arrangements. Standardization of the terms and cross-border coordination could also help in ensuring oversight between several institutions, which rely on the same providers.

8. LIMITATIONS AND FUTURE RESEARCH

This study does not include interviews, internal risk registers, confidential contracts or direct observation of exit exercises, it is based upon a

purposive documentary corpus. The professional banking case is a published consultancy case that may highlight programme outcomes/achievements instead of all implementation challenges. The regulatory and policy documents outline expectations and concerns for the sector but do not indicate the extent to which practices are found throughout the sector. The interpretations of findings should therefore be understood as being a qualitative synthesis of the results and not a representative statistical analysis.

The framework could be further explored in future research by undertaking interviews with financial institutions' procurement, operational-resilience, legal and technology leaders. Comparative analyses might be conducted to determine if there are differences in exit readiness across institution size, service criticality, jurisdiction or cloud deployment model. Other research might also be able to provide some quantifiable outcomes of exit capability, including the percentage of critical services for which data-export procedures have been validated, the time needed to bring workloads back to the environment, or the percentage of problems identified during the exit exercises that are closed. Any such metrics would need to be carefully operationalized and tested in the field before they could be considered as general metrics.

9. CONCLUSION

Financial institutions can leverage cloud to gain more scalability, access to specialised technology, and modernise vital services. But these benefits are accompanied by dependencies that can make the overseeing, continuance and exit more difficult. The evidence examined in this paper suggests that a supplier count is not enough to understand the concentration risk, as procurement can influence resilience during the entire technology lifecycle, and that exit risks in the contracts are not enough when lacking the capability to exit through operations.

An integrated governance framework from procurement to exit, linking critical service identification, provider and concentration assessment, contractual safeguards, dependency mapping, ongoing testing and controlled transition is the main contribution of the paper. The framework is not a document that is completed at the end of the contract, but is an institutional capability that needs to be developed throughout the contract. It also puts the importance of proportionability: the level of confidence should be commensurate with the importance of the service and the impact if it is disrupted.

Strategic procurement therefore should also be judged based on the level of control, transparency, substitutability and continuity that can be maintained during the procurement relationship for financial institutions. The incorporation of these factors in a procurement decision and their continued management as part of the governance process increases operational resilience.

REFERENCES

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

European Banking Authority. (2019). EBA guidelines on outsourcing arrangements (EBA/GL/2019/02). https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Financial Conduct Authority. (2016). FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services. https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it

Financial Stability Board. (2019). Third-party dependencies in cloud services: Considerations on financial stability implications. https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/

Financial Stability Board. (2023). Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities. https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/

Grant Thornton. (2025). A regional bank earns dividends from cloud strategy. https://www.grantthornton.com/insights/case-studies/banking/2025/a-regional-bank-earns-dividends-from-cloud-strategy

Parchimowicz, K. (2024). Do not get lost in the cloud: How EU financial institutions could avoid problems with cloud services arising under DORA. Law, Innovation and Technology, 16(2), 463–487. https://doi.org/10.1080/17579961.2024.2392935

U.S. Department of the Treasury. (2023). The financial services sector's adoption of cloud services. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

IEER
Institute for Excellence in Education & Research