Microsoft

Addressing concentration risk and building practical exit strategies for Microsoft Cloud

TABLE OF CONTENTS

Executive summary

Financial institutions increasingly choose to strategically partner with major cloud and AI providers to support their mission-critical operations and gain competitive advantages. While this trend reflects a growing third-party dependency and introduces systemic concentration risk, it is not inherently negative. In fact, many firms strategically leverage Microsoft's cloud and AI platform for its ability to help address critical needs, such as improving resiliency, security, and regulatory alignment.[1] Rather than viewing concentration as a singular threat, many firms approach it as a natural consequence of choosing robust, scalable platforms that meet high standards for availability and compliance.

Concentration risk is addressed by reducing the likelihood and impact of failures through resilient design, distributed deployments, and robust security. This is achieved primarily by developing durable business continuity plans and complementing these with exit strategies where possible. Many regulators recognize that well-architected cloud solutions can offer greater resilience than traditional on-premises implementations, and that severing third-party vendor relationships entirely can be challenging. As such, the emphasis is shifting from enforcing diversification to encouraging firms to understand and manage their dependencies intelligently.

Still, in some jurisdictions, firms today are required to develop exit plans that can enable them to remove contracted critical Information and Communications Technology (ICT) services and securely transfer relevant data from a third-party provider to alternative providers or reincorporate them in-house. To accomplish this, the most forward-looking institutions adopt a balanced, risk-based approach. They begin by identifying critical or important functions or business services and, in a granular approach, mapping their third-party dependencies down to the service level. This way a concentration "heatmap" can be visualized. Next, for each area of high concentration, firms can evaluate likely threat scenarios and identify service-specific exit plan options that are proportionate to the risk.

Note here that simply shifting workloads to a different Microsoft region, while useful for business continuity, may not constitute a valid exit strategy under regulations such as the EU's Digital Operational Resilience Act (DORA), as it does not enable termination of the outsourcing arrangement. As a result, firms may encounter scenarios where an exit is either not feasible or desirable (for instance due to the sustained dependency on the same provider when exiting the service), mandating some level of risk acceptance. It is also common that no clear alternative can be found for a specific solution or service, making the exit plan therefore unrealistic and prohibitively expensive. Such risk acceptances should be clearly documented and formally approved.

In conclusion, the smartest firms are those that embrace the benefits of cloud while remaining clear-eyed about the risks. They build resilience first, prepare for contingencies second, and align their exit strategies with both business goals and regulatory expectations. This approach not only satisfies compliance requirements but also positions them to innovate confidently in a cloud-first world.

Getting started with exit planning

Regulatory expectations: DORA and UK PRA guidance

Under Article 28(8) of the EU's Digital Operational Resilience Act (DORA), financial entities must develop transition plans that enable them to remove contracted ICT services and relevant data from third-party providers and securely transfer them to alternative providers or reincorporate them in-house. These plans must be actionable, tested, and aligned with the institution's broader operational resilience framework.

Similarly, the UK Prudential Regulation Authority (PRA), through Supervisory Statement SS 2/21, requires firms to maintain documented exit strategies for material outsourcing arrangements. These strategies must differentiate between stressed and non-stressed exits, define roles and responsibilities, and ensure continuity of critical business services in the event of disruption.

Both DORA and PRA guidance emphasize the need for proportionality; exit planning should be risk-based, focused on critical or important functions or business services, and integrated into broader risk governance and business continuity planning.

Innovation, Frontier Firms, and the rise of concentration risk

The financial services industry is undergoing a profound transformation driven by AI, data-driven innovation, and the emergence of what analysts and industry leaders increasingly refer to as "Frontier Firms." These are institutions that leverage advanced AI and cloud technologies not only to optimize operations but to redefine their business models, create new revenue streams, and lead in digital finance. To become Frontier Firms, many financial entities are entering strategic partnerships with leading cloud providers—embedding AI capabilities, scalable infrastructure, and integrated data platforms into their core operations.

This shift, while essential for competitiveness, inevitably leads to higher levels of concentration risk at the vendor level. As more critical functions are migrated to cloud platforms, the dependency on a limited number of providers deepens. This is not inherently problematic—modern cloud architectures offer resilience, security, and agility that often exceed traditional on-premises setups—but it does require careful evaluation and planning.

The importance of adopting a practical, risk-based approach

Given the complexity of modern cloud environments and the strategic importance of many outsourced services, aiming for a perfect or universal exit plan is neither realistic nor required. Instead, institutions should adopt a pragmatic approach that begins with a structured analysis of their cloud dependencies.

The primary risk mitigation is to create highly robust and well-tested business continuity plans. The reason for this is that Microsoft cloud services have been designed from the ground up with business continuity in mind, providing extensive failover and data transfer capability both to other cloud regions and, in most cases, also to on-premises and third-party providers.

The business continuity plan (BCP) remains a firm's principal risk mitigation tool for addressing all sorts of threat events related to concentration risk. The exit plan is complementary to the BCP and addresses risks that a BCP does not cover (e.g., provider insolvency), as well as on longer-term risk mitigating measures if a BCP proves to be inadequate.

What, then, is a good approach to exit planning?

The first step is to develop a heatmap of concentration risk—identifying the most critical applications and corresponding business functions, and mapping their dependencies on specific cloud services. This analysis should be grounded in business impact assessments and reflect both technical and operational reliance. Once the concentration hotspots are identified, institutions should ensure that robust BCPs are in place for each. These BCPs should address short-term disruptions and include fallback mechanisms, failover strategies, and recovery procedures.

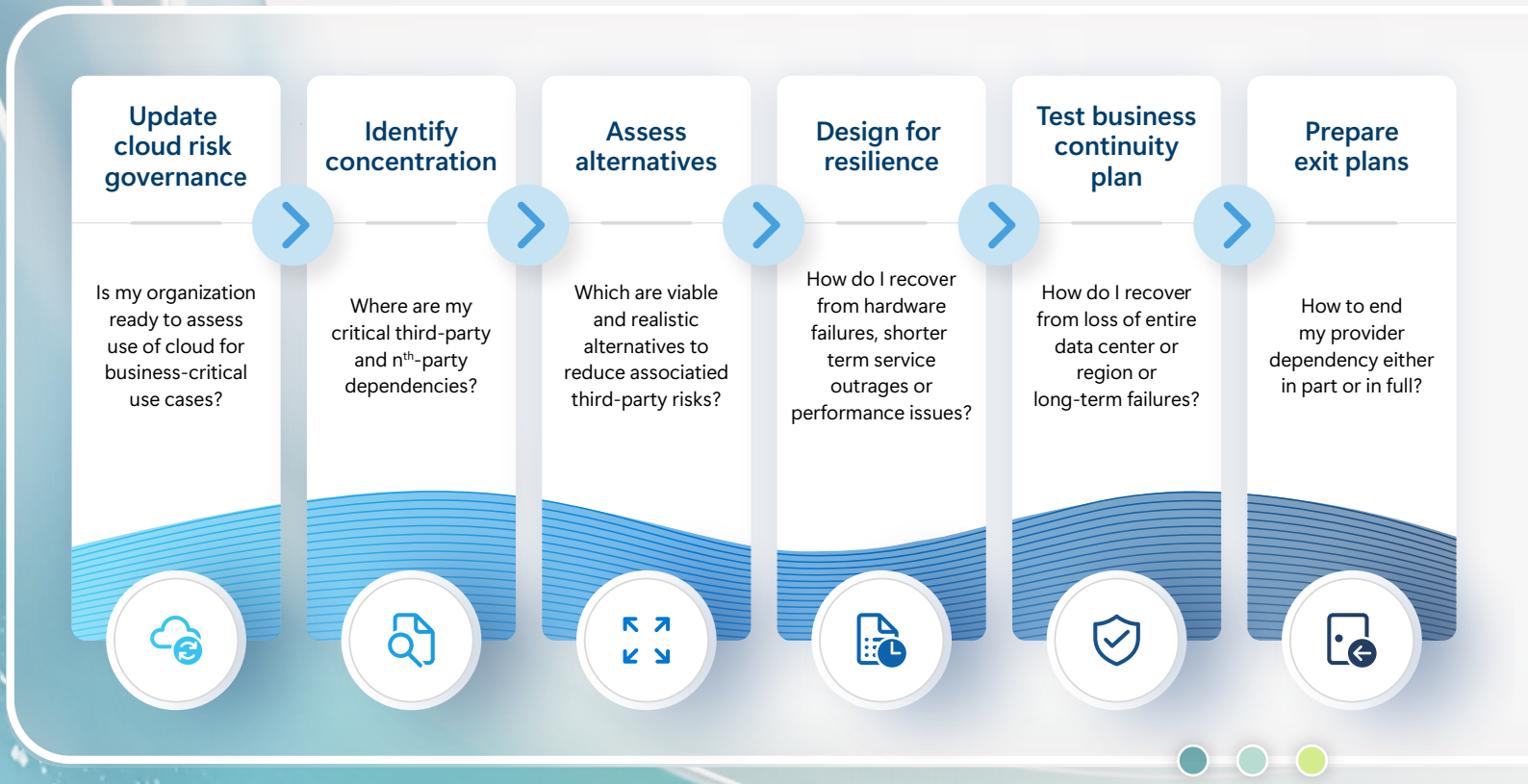
Next, firms should assess the residual risk that remains in light of exit planning. For each critical concentration hotspot, evaluate the feasibility of an exit that includes contractual termination, either in part or in full, imbued with a sense of realism. This may involve migrating services to alternative providers, transitioning workloads to on-premises environments, or modifying business processes to reduce reliance. The exit plans must be proportionate to the risk, avoiding unrealistic or undesirable plans where the third-party dependency remains in place after the exit (e.g., continued dependency on software products that require maintenance and security updates), and scenarios where the exit plan becomes prohibitively expensive and therefore unrealistic (e.g., where the provider is specifically chosen because of its unique capability to provide a service).

Where viable alternatives exist, these strategies should be documented and tested. Where no feasible alternative is available, institutions may need to introduce a formal risk acceptance, supported by a thorough risk evaluation and aligned to the organization's overall risk appetite.

Embedding exit planning within a broader resilience strategy

While exit planning is a critical component of regulatory compliance and operational preparedness, it should not be treated as a standalone exercise. Instead, it must be embedded within a broader, structured approach to strengthening operational resilience – one that addresses the full lifecycle of risk identification, mitigation, continuity, and recovery.

To support such an integrated approach, Microsoft developed a six-step resilience framework that aligns closely with the requirements of DORA.



These steps provide a structured pathway for institutions to assess their dependencies, evaluate alternatives, and build robust continuity plans and exit strategies. This is described in more detail in this article: "Strengthening operational resilience and reducing concentration risks in financial services."[2]

Exit plans fits seamlessly within this broader resilience context, ensuring they remain both practical and sustainable, and do not exist in isolation. This allows institutions to balance innovation with preparedness, and to demonstrate to regulators that they are managing concentration risk in a thoughtful, risk-based manner. The exit plan becomes one part of a larger system of controls and safeguards—complementing business continuity plans, architectural decisions, and governance processes.

Assessing risk: The impact of moving to cloud

An important dimension of the risk assessment may be to compare the "as-is" risk profile of legacy on-premises deployments with the "to-be" risk profile in a cloud configuration. In many cases, cloud adoption does not increase risk—it transforms it. Modern cloud platforms offer enhanced data portability, documented APIs, and standardized interfaces that can facilitate exit planning more effectively than proprietary on-premises systems. These features should be factored into the assessment, as they may reduce the operational and technical barriers when executing an exit.

Operationalizing your exit plans: Other considerations

Dynamics: Once the strategic direction for exit planning is established, institutions must turn their attention to the practical realities of implementation. Exit plans are not static documents; they evolve alongside the institution's cloud and AI innovation cycles. As new services are adopted, existing ones are modified, or regulatory expectations shift, the exit plan must be revisited and updated. This continuous lifecycle reflects the nature of cloud usage itself: Dynamic, iterative, and increasingly embedded in critical business functions.

Integration: A well-operationalized exit plan should incorporate elements of the institution's broader risk assessment strategy. This includes identifying the critical or important functions in scope, listing the dependencies on third-party services, and documenting the alternatives that have been considered. Where no viable alternative exists, the rationale for risk acceptance should be clearly stated and aligned with the institution's risk appetite. These assessments should be grounded in the same principles used for outsourcing and ICT risk management more broadly, ensuring consistency across governance frameworks.

Data and volumes: One of the most overlooked aspects of exit planning is the sheer volume and complexity of data stored in the cloud. For critical applications, this data may span multiple regions, formats, and services. Institutions must not only plan for how to migrate this data but also consider how it can be made operational in the target environment. This includes evaluating whether alternative solutions can process the data effectively, whether metadata and configuration details are preserved, and whether security controls (such as encryption keys and access policies) can be replicated or transitioned. Without these elements, data alone may not be sufficient to restore functionality.

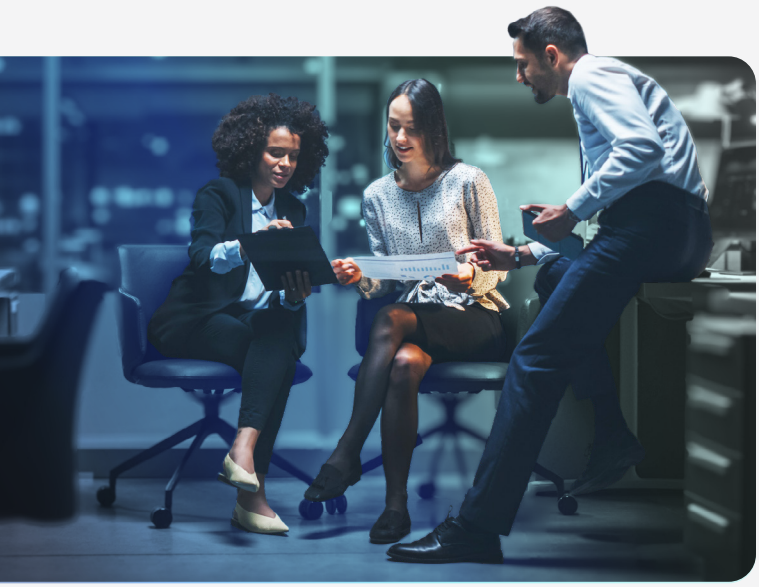
Human aspects: The human factor is especially important. Exit plans should include a communication strategy that addresses internal stakeholders, external partners, and customers as appropriate. Changes in service delivery, user experience, or support models must be clearly communicated and managed. This is particularly relevant in scenarios where the exit plan involves transitioning to unfamiliar platforms or workflows. Training, change management, and stakeholder engagement are essential to ensure continuity and confidence.

Contracts: Depending on the exit strategy, institutions may also consider pre-negotiated contractual arrangements with alternative providers. These can serve as contingency options in high-risk scenarios, offering a faster path to transition. However, such arrangements can be costly and complex to maintain, and may only be appropriate where the exit scenario has been worked out in great detail and is considered sufficiently probable. Institutions should weigh the benefits of these contracts against the operational and financial overhead they introduce.

Compliance: Regulatory frameworks such as DORA and PRA SS2/21 also call for specific elements to be included in exit plans. These include clearly defined roles and responsibilities, documented transition plans, and provisions for secure data transfer. Institutions should ensure that their plans meet these expectations, not only in structure but in substance. The exit plan must be actionable, proportionate, and aligned with the institution's operational resilience strategy.

The role of backups

Some regulatory interpretations, particularly within the ECB's supervisory perimeter, suggest that critical applications may require on-premises backups to support exit planning. While backups are essential for resilience and recovery, their role in exit planning should be carefully evaluated. A backup alone does not constitute an exit strategy unless it can be operationalized, meaning the institution must have access to the necessary hardware, software, business logic, metadata, and security keys to restore functionality, plus qualified personnel. Without these elements, the backup may preserve data but not enable continuity. Institutions should therefore assess the completeness and usability of their backup arrangements in the context of exit planning and ensure that any gaps are addressed through complementary strategies.



Microsoft-specific guidance and tools

Contractual safeguards supporting continuity and exit

Microsoft recognizes the criticality of continuity, reversibility, and secure data transfer in Financial Services Industry organizations (FSIs), particularly as mandated by regulatory authorities or in the event of restructuring, insolvency, or other resolution events. Our contractual commitments to FSIs include robust provisions to support business continuity in such scenarios and provide clear pathways for transition or exit.

Key safeguards:

Regulatory intervention support: If a regulator intervenes in the operations of an FSI, Microsoft commits to cooperating and to granting the regulator full administrative control over the institution's cloud environment.

Transfer and assignment of rights: Should an FSI undergo reorganization, acquisition, or similar events impacting its legal status, Microsoft contractually enables the assignment or transfer of service rights to a successor entity (such as an affiliate or acquirer).

Non-termination safeguard: Microsoft will not suspend or terminate service provision solely due to a transfer of rights to a regulator or authorized transferee, provided contractual obligations (including payment for services) are met. Additionally, there are built-in mechanisms to extend services month-to-month for up to 12 months post-termination or expiration, or longer if required by regulatory directive, allowing customers to retrieve their data and transition workloads.

Reversibility assurance: Microsoft Professional Services are available to assist with data migration upon exit, supporting smooth transitions to new environments at agreed-upon service rates. During any extended service period, customers have full access to standard data export tools for secure retrieval and migration of their information.

These safeguards are designed to provide institutions with operational flexibility, regulatory alignment, and the assurance that exit scenarios – whether planned or unplanned – can be executed without undue disruption or risk to critical business processes.

Technology tools to support data portability and migration

Microsoft also offers a suite of technical solutions to simplify and secure transitions during an exit:

Azure Arc: Microsoft Azure Arc enables hybrid and multi-cloud management, allowing FSIs to extend Azure services and management to on-premises or other cloud platforms. Workloads can be spread across different infrastructures, supporting flexible migration scenarios and reducing cloud concentration risk.

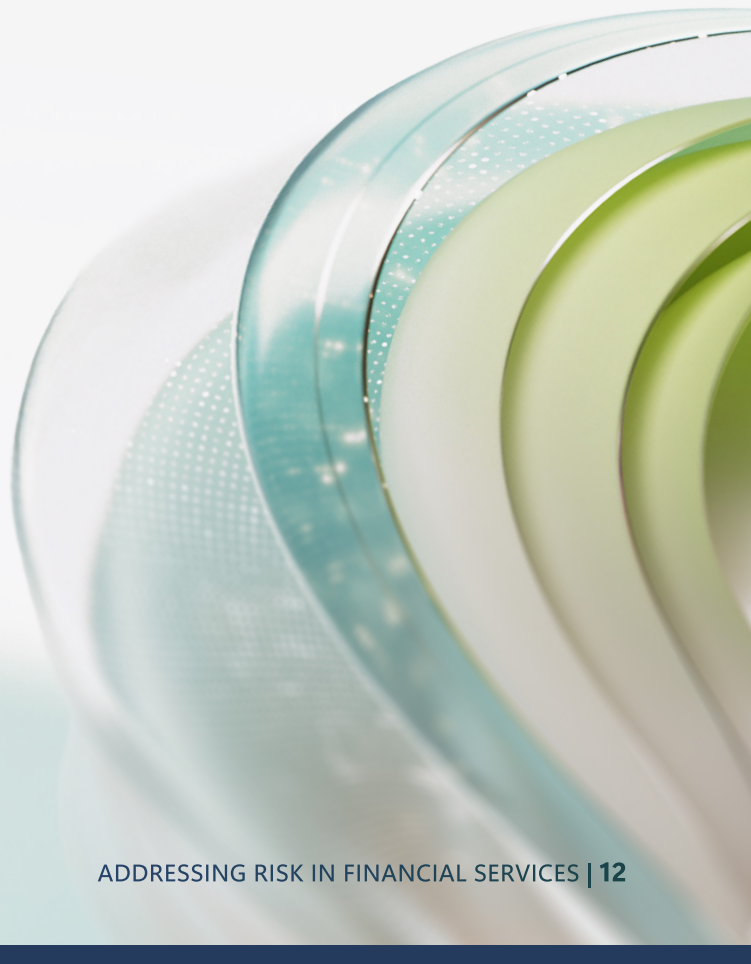
Containerization and platform portability: Leveraging containers (Kubernetes, Docker) and microservices architecture helps FSIs design application environments that are inherently portable. This approach facilitates the transfer of workloads between Microsoft Azure and other environments with minimal dependency on proprietary cloud services.

Automated data migration: Microsoft provides built-in tools for exporting and transferring structured and unstructured data. Azure Data Factory and related services automate extract-transform-load (ETL) processes, simplifying bulk data migration during an exit event.

Microsoft 365 data management

FSIs utilizing Microsoft 365 can leverage:

- **eDiscovery tools** for exporting copies of emails, documents, and collaboration data in standardized formats that are compatible with alternative platforms.
- **M365 backup solutions** to create and retain point-in-time snapshots of key data, supporting reversibility and continuity requirements.
- **Hybrid configuration and private cloud options** for Exchange, SharePoint/OneDrive, and Skype for Business, supporting migration between on-premises, private cloud, and Microsoft cloud as needed.



Data transfer considerations: Performance and throttling

Microsoft's public documentation indicates that data egress volumes for customer-controlled exports may be subject to throttling measures to ensure platform stability for all users, especially for very large datasets. However, in an exit scenario – particularly those necessitated by regulatory directive – Microsoft works with customers to **remove or adjust throttling controls** where feasible, to ensure expeditious and uninterrupted access to customer data and facilitate timely migrations. Customers can engage with Microsoft support or Microsoft Professional Services to coordinate large-scale transfers and minimize operational delays.

Summary

By combining clear contractual safeguards with advanced migration tools and flexible cloud architecture, Microsoft helps financial institutions to plan and execute exit strategies that comply with regulatory mandates, support business continuity, and secure their operational resilience in the cloud.[2] Our ongoing investment in hybrid cloud, open APIs, and data management solutions ensures FSIs can maintain control and portability of their critical workloads at all times.

Testing of exit plans

Testing is often the most challenging aspect of exit planning. While many institutions have made progress in documenting their strategies, fewer have developed robust mechanisms to validate them. Yet testing is essential—not only to satisfy regulatory expectations, but to ensure that the plan can be executed effectively if needed.

The most common form of testing is the tabletop exercise. These simulations bring together key stakeholders to walk through the exit plan in a structured setting, discussing roles, timelines, and decision points. Tabletop exercises are relatively low-cost yet can be highly effective and educational, making them a practical starting point for most institutions.

In some jurisdictions, there also is growing interest in performing joint scenario testing of failures and disruptions across an entire sector or between a provider and one or more of its users. These exercises focus on a specific disruption scenario, such as a prolonged outage or service degradation, and evaluate the institution's response from a business continuity perspective. While not explicitly designed to test exit plans, they often yield valuable insights that can inform exit planning in subsequent phases. For example, gaps in data recovery, stakeholder coordination, or alternative service readiness may surface and suggest areas for improvement.

More sophisticated testing may involve partial migrations, dry runs of data exports, or validation of alternative environments. These approaches require greater investment and coordination but can provide deeper assurance of exit readiness. Institutions should determine the appropriate level of testing based on the criticality of the function, the complexity of the exit strategy, and the feasibility of executing such tests without disrupting operations.

Ultimately, testing should be risk-based and proportionate. Not every service requires the same level of scrutiny, but all exit plans should be reviewed and validated to some degree. Institutions should also document the outcomes of these tests, including lessons learned and updates made to the plan. This creates a feedback loop that strengthens the plan over time and ensures it remains aligned with the institution's evolving risk landscape.

CONCLUSION:

Building confidence through pragmatic resilience

As financial institutions deepen their reliance on cloud technologies to drive innovation, operational efficiency, and strategic transformation, it becomes increasingly important to manage concentration risk and prepare for potential disengagement scenarios. Exit planning is no longer a theoretical exercise; it is a regulatory expectation and a practical necessity.

The most effective exit plans are those that evolve with the institution's cloud journey. They are embedded in governance frameworks, informed by realistic threat scenarios, and supported by robust testing and communication strategies. Where viable alternatives exist, they should be documented and prepared. Where no alternatives are available, risk acceptance must be justified and transparent.

Ultimately, exit planning is not about abandoning cloud innovation, it is about ensuring that innovation is sustainable, secure, and resilient. By operationalizing exit plans thoughtfully and embedding them within a broader resilience framework, financial institutions can meet regulatory expectations, protect critical services, and maintain the confidence to innovate boldly in a cloud-first world.

References and resources

1. Microsoft Azure Blog, "New options for AI-powered innovation, resiliency, and control with Microsoft Azure," December 3, 2025.

2. Microsoft Learn, Strengthening operational resilience and reducing concentration risk in financial services.

3. Microsoft Industry Blog, "Managing concentration risk and exit requirements: A framework for financial institutions," January 2026

4. Microsoft Industry, Microsoft for Financial Services, web page