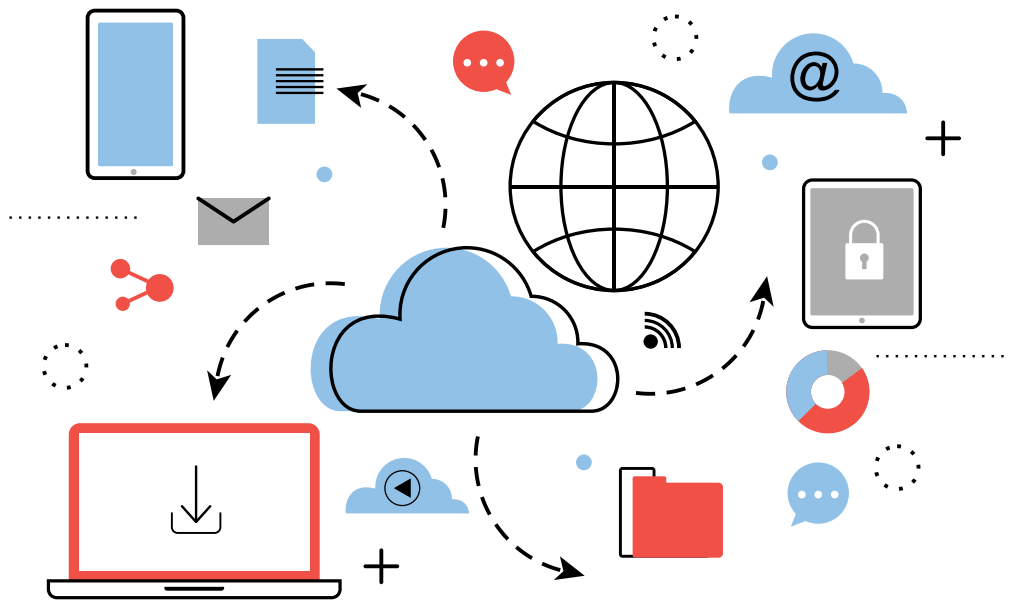

CLOUD COMPUTING FOR BANKS:

EMBRACING INNOVATION SECURELY

by Chris Couch and Drew Patty

The past decade has brought an explosion of innovation and development for financial technology. Crusty core processors now face competition from nimble start-ups, third-parties are integrating with established systems to create best-in-class solutions for consumer and commercial customers, and almost everything is mobile.

But banks are not "fintechs." They occupy a special role in communities and the national economy. Their goal is not to "move fast and break things." The tension inherent between rapid evolution and the need for reliability begs the question: **Can banks harness rapid innovation safely?**

Cloud Computing as the Basis for Rapid Innovation

This renaissance in community banking technology is not generally home-grown. While bankers are great risk managers, they are not known for innovation. The recent advances in financial technology and services are premised largely on "cloud computing," which allows companies to use third-party computing resources on-demand over the Internet to scale operations without investing in huge data rooms and IT resources. By relying on computing behemoths such as Amazon Web Services, Microsoft Azure and others, banks and service providers have been able to shift focus from physical asset management to innovation, allowing banks to expand and evolve product offerings quickly while maintaining a high degree of process reliability. Banks are leaning on third parties to maintain the currency, operability, and security of the system infrastructure, freeing bankers to service customers.

Cloud Computing From a Regulatory Perspective

Whether the bank is moving operations directly onto the cloud, or entrusting data to a vendor who processes in the cloud, the bank is outsourcing a function to a technology service provider ("TSP"). In its IT Examination Handbook, the Federal Financial Institutions Examination Council ("FFIEC") recognizes that banks may outsource any service, process, or system operation, including those relating to payments, customer accounts, loan and deposit processing, and security monitoring and testing. Indeed, the FFIEC recognizes that outsourcing may in fact "improve quality, reduce costs, strengthen controls." However, the FFIEC notes that (i) outsourcing does not diminish the Board of Directors' responsibility for any outsourced function, and (ii) the activities of TSPs on behalf of the bank are subject to examination. Banks must realize that TSPs are viewed as an extension of the bank, under the supervision of the board.

Board and Management Responsibilities in Cloud Computing

The board's primary responsibility with respect to cloud computing is ends-oriented: To ensure that cloud computing supports the bank's strategic goals, including considerations of risk tolerance, which necessarily requires the board to appreciate the risk associated with cloud-based processes. Cloud-based outsourcing differs from traditional outsourcing in several respects, not least of which are the use of shared computing resources. Cloud providers typically maintain specific servers and equipment only for extremely large customers. For all others, data is separated from other customers through technological – rather than physical – means, and may be transferred across multiple jurisdictions during processing. If not properly maintained, the technological separation could result in data leakage (erroneous or intentional exposure of data to unintended or unauthorized third parties), the risk of which increases upon transfer. Additionally, the nature of services that are often "cloud processed" – payments-related transactions, data aggregation and reporting – increase the bank's business continuity risk. The higher the degree of integration with the bank, the higher the reliance of the institution on the provider's business continuity. In a "distributed" or cloud environment, each cloud processor

processing facility represents a potential point of failure in business continuity.

The board's remaining responsibilities become means-oriented: Ensure the bank has the expertise to manage the relationship; evaluate providers based on the scope and criticality of the services outsourced; adjust the bank's risk management systems to accommodate the new relationship; and notify regulators, as necessary. These means-oriented considerations, while the responsibility of the board, are commonly delegated to the bank's management subject to board supervision.

Evaluating Cloud Vendors

TSPs who themselves rely on cloud service providers are no different from "traditional" TSPs, but should be assessed with a critical eye on the cloud provider through whom they process data. A bank should also assess and review the vendor's agreement with that second-order service provider .

Structuring Agreements for Safety and Soundness

As with any new vendor contract, a bank's agreement with cloud-based TSPs should scope the relationship properly and with precision, identifying the parties' respective rights and responsibilities, and the standards for performance and exercise of each. Banks should, of course, keep in mind the economic, operational, and regulatory implications, but should also particularly consider:

1. **SECURITY AND CONFIDENTIALITY.** A given bank's requirements will differ depending upon the location of their customer base. Similarly, the TSP's rights and obligations may differ depending upon where the data is processed. The same holds true with reporting and responding to information security incidents: TSPs may have obligations that are narrower or broader than the bank's. As the bank's reputation and customer base is primarily at stake, the bank's regulatory and commercial obligations should take precedence over the TSP's.

2. **INDEMNITY AND INSURANCE.** Because of the opportunity for claims against the bank for the TSP's actions (or inaction), the agreement should expressly consider issues of indemnity and insurance. These issues directly bear upon price, so these issues are most easily – though almost never – dealt with during the vendor evaluation process. The bank should also appreciate the quality and quantity of insurance carried by the TSP, and consider whether it appropriately covers the activity conducted and the likely points of loss. Finally, he bank should consider whether it should be added as an additional insured, a covered contract, or similar covered party.

3. **SERVICE LEVEL.** As noted, the more reliant the bank is on the cloud-based vendor, the more closely tied the bank's business continuity plan is to the TSP's; thus, service level becomes increasingly important. Banks should address service level directly, agreeing upon clearly defined performance standards, escalation and response procedures, and incentives (positive and negative) for performance. Many agreements exclude from the calculation of "downtime" events beyond the TSP's control, which may include the availability of their cloud-services provider where the vendor processes through a third-party. Banks should take particular care to exorcise such terms.

4. **ACCESS TO DATA; COOPERATION WITH EXAMINATION.** When considering cloud-based arrangements, banks also should bear

in mind FFIEC's express reminder in its IT Examination Handbook that "the examination and supervision of a financial institution should not be hindered by a transfer of the institution's records to another organization or by having another organization carry out all or part of the financial institution's functions." For cloud-based arrangements, this really means two things: First, the bank must have full access to its data, regardless of where maintained and by whom processed. Second, TSPs must agree to participate in the bank's examinations. Both of these elements should be reflected in the contract. Typically, data access is addressed through regular data backup and handover routines, rights to access data regardless of the status of payment on account, and for more critical services, escrow arrangements. Given the potentially devastating impacts of ransomware and the like, vendor backup protocols and incident response plans must be reviewed periodically over the life of the contract. Whether there are costs associated with ownership and access, on one hand, and participation, on theother, is a matter of negotiation, but both elements should be addressed.

5. **TERMINATION.** Any agreement with a cloud-based TSP needs a robust suite of termination triggers and post-termination provisions. Unlike many traditional bank service providers, many cloud-based TSP are innovative growth companies still figuring themselves out. That may or may not work great. And it may not in unexpected ways, like failing to register as a money transmitter, or sharing bank APIs outside of the bank's license. Banks should consider enhanced rights to terminate the agreement and transition their data in an expedited,orderly fashion.

Monitor, Report and Re-evaluate

The final component of reliance on cloud-based TSPs is the same as for all vendors: Monitor performance on a regular basis (through audit and otherwise), report any issues or developments, and re-evaluate over time. Re-evaluation may lead to expansion, contraction, or termination. Because of the increased risk of reliance upon cloud-based vendors, the quality and quantity of monitoring and reporting may be heightened relative to that for most vendors, and the frequency of re-evaluation may be greater.

Taking these steps, banks can responsibly work with cloud-based service providers to take advantage of the rapid innovation and operational flexibility and convenience that they provide – to the bank and its customers.

Chris Couch is a partner in McGlinchey's Financial Institutions Practice, resident in Birmingham. He advises banks, bank affiliates, and holding companies in regulatory and operational matters, including technology contracts, payment systems, BSA/AML, information security and privacy matters.

Drew Patty is a partner in McGlinchey's Baton Rouge officea, serving as the Intellectual Property Practice Group Team Leader and co-Leader of the firm's Cybersecurity and Data Privacy Practice. He advises financial institutions on technology product development, licensing and vendor services agreements, and related litigation.