economymatters

ANNUAL REPORT

ECONOMIC RESEARCH

BANKING & FINANCE

REGIONAL ECONOMICS

COMM/ECON DEV

INSIDE THE FED

DEPARTMENTS

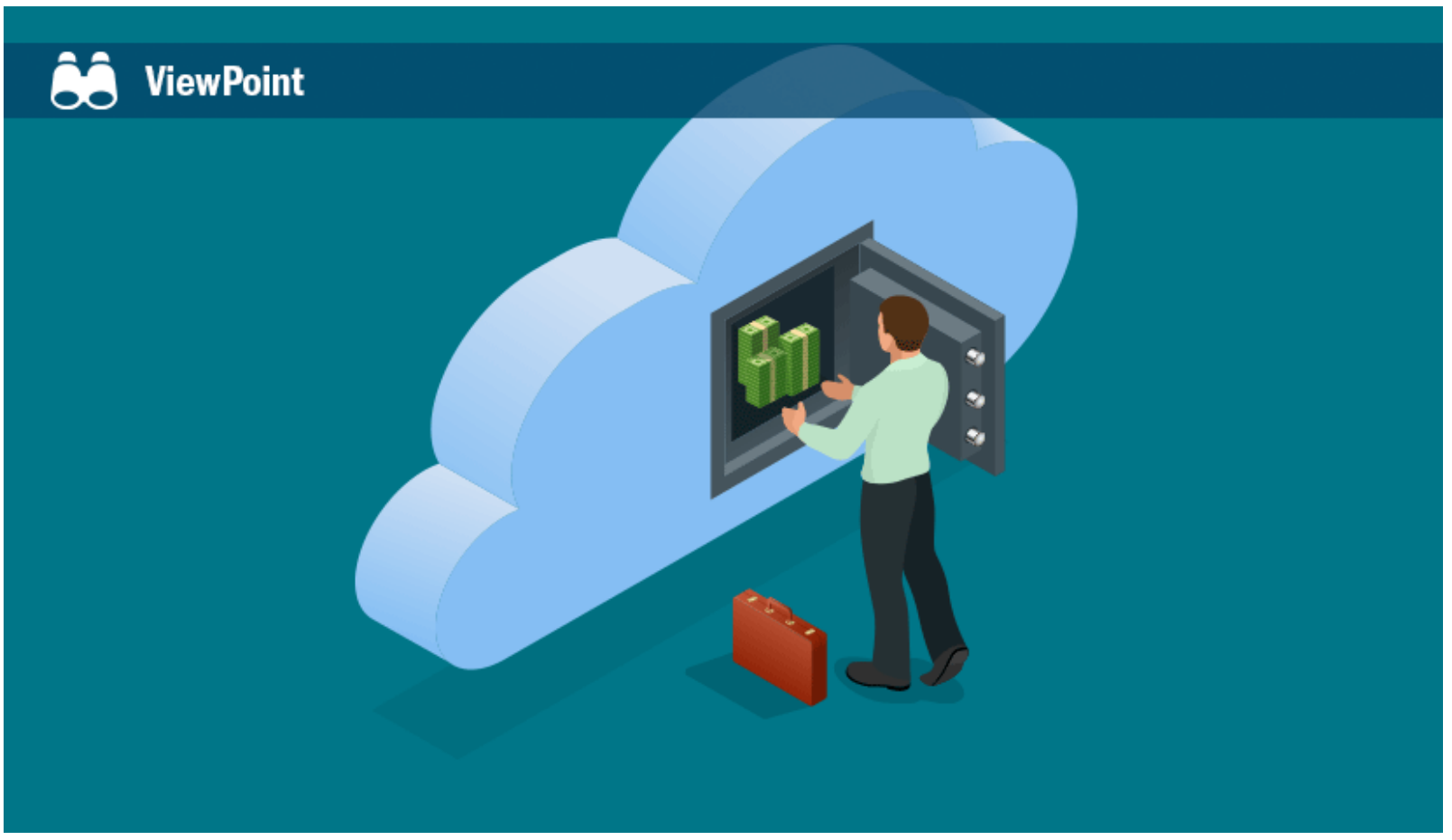
Financial Tips
Podcast
Quizzes
Staff & Credits

Subscribe to e-mail updates

BANKING & FINANCE

Supervisory Considerations in Cloud Computing in the Financial Services Industry

May 8, 2018



Technology has brought a host of benefits and challenges to the financial industry. Increasingly, banks depend on technology to provide services for customers, including online banking, financial advice, and mortgages. One type of technology banks have started to embrace is cloud computing. Cloud computing creates an opportunity to reduce capital investment and increase operational flexibility. Banks had been slower than other industries to adopt cloud computing due to security and regulatory concerns. However, improvements in technology and additional guidance from regulators have bank managements starting to see the cloud as the future for their companies.

According to the Federal Financial Institutions Examination Council's (FFIEC) handbook, cloud computing involves the use of shared IT resources from third-party service providers via the internet. For example, one model of cloud computing is Infrastructure as a Service (IaaS), where data are stored in the cloud service provider's network. This model provides processing capability, storage, networks, and other computing resources to run software. The end user does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications. The end user also possibly has limited control of select networking components (such as host firewalls).

Though the cloud offers opportunities, it also introduces risks not posed by in-house processing and is an area of focus for regulatory supervisors and industry groups. Successful use of a cloud environment depends on management's knowledge and understanding of the platforms they are using. Moving data outside the institution's physical environment creates additional risk-management considerations.

From the supervision perspective, SR Letter 13-19, Guidance on Managing Outsourcing Risk, defines regulatory expectations governing third-party oversight. Supervisory requirements cover both due diligence for new vendors and ongoing monitoring for existing third-party providers. Because an external third party provides cloud services, these providers should be incorporated into a financial institution's vendor management program with appropriate oversight for identified risks, including contracts, controls, cybersecurity, and disaster recovery.

Supervisory Expectations

Contracts

Management should regularly evaluate cloud provider service performance versus defined performance targets for metrics given in service-level agreements, including standards for measuring performance and the effectiveness of information security management. At a minimum, organizations should document their current metrics and how providers might use different

measurements when operations move to the cloud.

Management should monitor compliance with key contractual provisions to confirm that cloud providers comply with their obligations. In other words, when a cloud service provider is contractually required to perform a specific activity, management needs to confirm it actually occurs as defined in the contract. Examples include compliance with data retention requirements through data backups, and testing of the cloud service provider's business continuity program to support data availability and receipt of required control (such as the System and Organization Controls or SOC) reports.

In addition to business considerations, data retention is governed by regulation (including, but not limited to, numerous anti–money laundering statutes) and legal requirements arising from future civil litigation, including the ability to comply with court-issued subpoenas. Since the cloud will become the repository of most electronically stored information needed in litigation or an investigation, management must carefully plan with their cloud service providers how they will be able to identify all documents that pertain to a case so they can fulfill statutory and regulatory requirements. For institutions operating or storing information outside the United States, legal jurisdiction and governing law are additional considerations.

Controls
The effectiveness of cloud provider controls should be evaluated as if the activity were performed internally by the financial institution. In addition to internal due diligence and ongoing monitoring, management should also review SOC reports or equivalents prepared by an independent third party. The SOC Type 2 report is management's description of a service organization's system and the suitability of the design and operating effectiveness of controls. Management should periodically validate that applicable controls are in place within their financial institution and operating effectively.

Because of the on-demand provisioning and multi-tenant aspects of cloud computing, traditional forms of audit and assessment might not be available or might require modification. For example, some providers restrict vulnerability assessments and penetration testing, while others limit availability of audit logs and activity monitoring. If an institution's internal policies require these items, management might need to seek either alternative assessment options or an alternative provider.

Cybersecurity
All aspects of cybersecurity applicable within a financial institution's internal network must be considered in the cloud environment. To the extent a financial institution's existing cybersecurity program does not fully support migration to the cloud, Security as a Service (SECaaS) is available as a supplement to one of the three industry standard service models. SECaaS is a business model in which a cloud service provider integrates its security services into a corporate infrastructure on a subscription basis. In evaluating the appropriateness of SECaaS, the financial institution will need to consider its security posture and the ability to negotiate specific contract exceptions to resolve potential conflicts with internal security policy.

The Cloud Security Alliance (CSA)—the world's leading organization dedicated to defining and raising awareness of sound practices to help ensure a secure cloud computing environment—has defined 10 service categories within SECaaS. These definitions include business continuity and disaster recovery, continuous monitoring, data loss prevention, email security, encryption, identity and access management, intrusion management, network security, security assessments, security information and event management, vulnerability scanning, and web security.

The objective of the sound practices covered by these categories is to secure the financial institution's data from security breaches and vulnerabilities. This effort includes the two recently reported security flaws, Meltdown and Spectre, which Google's Project Zero identified in conjunction with academic and industry researchers from several countries. Together, these security flaws affect virtually every modern computer, including smartphones, tablets, and PCs from all vendors running almost any operating system. The Meltdown and Spectre vulnerabilities also work in the cloud, and—depending on the infrastructure—it might be possible to steal data from other customers. Security firms and vendors are releasing patches to mitigate these vulnerabilities and prevent any damage.

Disaster recovery
In continuity planning, cloud services are limited to disaster recovery of the technology supported by the service and deployment model. The financial institution is responsible for the operational aspects associated with business continuity planning. The financial institution is also responsible for defining the recovery strategy including risk assessment and recovery prioritization. It must also identify interdependencies and define recovery metrics, including recovery time objectives (RTO) and recovery point objectives (RPO).

Management will need to communicate the disaster recovery plan requirements to the cloud service provider and periodically confirm the cloud service provider's ability to support the plan's objectives through testing. Testing might include participating in the cloud service provider's test exercises or reviewing ongoing monitoring as part of the vendor management program, or both. The financial institution's recovery objectives should be specified in the contract with consideration of the recovery priority versus other cloud service provider clients.

Additional guidance: Sound practices
Financial institutions must comply with FFIEC guidance as well as meet industry standards, such as those developed by the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA). These standards include shared principles and provide a benchmark of sound practices that could aid institutions in meeting FFIEC requirements.

For example, NIST Special Publication 800-145 defines cloud computing and provides a framework over important aspects of cloud computing, including service models and deployment strategies. NIST 800-145 also defines three service models and four deployment models for cloud computing. Service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Deployment models include private for exclusive use by a single organization; community

for organizations with shared concerns; public, which is available to anyone; and hybrid, which combines elements of both public and private models.

By Ernesto Mendivil
A senior examiner in the Atlanta Fed's Supervision and Regulation division