protiviti®

Face the Future with Confidence

Fortified in the Cloud

The Risk Management Strengths of Cloud Service Providers for the Financial Services Industry

Internal Audit, Risk, Business & Technology Consulting

Introduction

Cloud is on the rise in financial services and regulators are taking note.

The widespread use of cloud service providers (CSPs) in the financial services industry continues to grow. According to a recent study by the Cloud Security Alliance (CSA), 91% of financial services organisations are actively using cloud services today or plan to employ them within six to nine months. That is double the number reported in CSA's prior study on this topic from four years ago.[1]

After having evaluated the benefits, large, well-known financial institutions are embracing the cloud, resulting in its exponential growth in the industry. While the cloud delivers a raft of benefits, the pace of cloud adoption in the industry also has provoked questions regarding the efficacy of risk management and compliance practices within CSPs. However, CSPs are well-positioned and, in fact, when it comes to the cloud, highly experienced in practicing effective risk management. As we detail in this paper, mature and robust risk management practices and processes are embedded in every vertical and product line in leading CSPs, frequently aligning with the traditional three lines of defence in financial services institutions: management control, risk and compliance oversight, and internal audit.

Regulators, who count CSPs among a broad category of emerging technology organisations that also includes fintechs and regtechs, among other companies, have been publishing guidance on the use of these various technology organisations and providers for nearly a decade. Until recently, however, this guidance has not been very detailed.

Ultimately, the burden of providing regulators with greater comfort regarding the use of CSPs rests with the regulated financial services industry. The challenge with emerging technologies, including cloud, is to prove to the regulators that CSPs and the financial services firms that use them really do understand and have accounted for effective risk management in their organisations.

At the same time, regulators are still developing and introducing guidelines for how best to examine organisations like CSPs. In 2020, for example, the Federal Financial Institutions Examination Council (FFIEC) released its guidance around cloud computing. The CSPs themselves, as well as independent third party groups such as the CSA and the Centre for Internet Security, had previously recommended similar guidelines.

The bottom line is that as cloud adoption in the financial services industry has increased, regulators are becoming more knowledgeable about how financial institutions are relying on CSPs without sacrificing the rigour required in risk management and compliance practices within the financial services industry.

Mature and robust risk management practices and processes are embedded in every vertical and product line in leading CSPs, frequently aligning with the traditional three lines of defence in financial services institutions.

[1] *Cloud Usage in the Financial Services Sector,* Cloud Security Alliance, February 2020.

Current Perceptions — Strengths and Opportunities

Regulators of the financial services industry generally focus on risk issues related to the safety and soundness of the financial institution as well as protection for their customers and the public.

Customer data and privacy, together with broader areas of risk management, are always fundamental to an examiner's concerns, regardless of the platform. With regard to CSPs, other areas of regulatory focus include information security and resiliency. In their attention to those priorities, regulators increasingly recognise how CSPs are supporting the security controls of financial services organisations by enabling a complete, real-time inventory of assets and how they are protected.

Cloud technology directly addresses the security concerns of regulators and others while providing significant operating benefits. For banks, cloud technology represents a disruption from years past, when they would have infrastructure on premises or co-located with one or more service providers. Moving data and services from a financial institution's dedicated legacy infrastructure to a multi-tenant cloud environment, if properly configured, can provide additional layers of security for the financial institution and decrease that institution's systemic risk.

Among other key security benefits financial institutions gain from their CSPs are that these providers are world-class experts in security and protection, with highly skilled teams dedicated to ensuring privacy and effective controls. Amid the surge in cyber attacks in recent years, financial institutions understand, from a security perspective, the difficulty of achieving internally the scale of what CSPs are investing in securing the bank's infrastructure. For example, considering the potentially systemic impact of denial-of-service attacks, a CSP's defensive mechanisms are immense compared to those of any individual bank.

In terms of specific standards, CSPs follow leading industry principles such as those outlined by the CSA, ISO standards, PCI standards, and AICPA's System and Organisation Controls (SOC) reports.

Capacity is another key CSP benefit. Financial services organisations need to be competitive in the marketplace. By leveraging the greater processing capacity and power that CSPs deliver, financial services organisations can release new cutting-edge technologies quickly and scale their environment up and down as needed. For instance, a CSP can expand capacity in seconds, instead of the weeks or months that it may take a traditional bank. Another significant benefit is the money saved from changing the model from a fixed-cost to a variable-cost basis. Banks can retire their networks of large, costly and inefficient data centres and pay only for the processing and storage capacity they actually need at the time.

In addition, CSPs serve multiple customers, providing scale and cost savings. CSPs leverage that scale to keep their systems on the cutting edge of technology, providing the latest in infrastructure and security technology. They tend to have the latest architecture and access to the most relevant expertise. Financial institutions, on the other hand, often are trapped in legacy architecture that can necessitate an inefficient use of computing power and data storage. Smaller banks, in particular, may lack the capacity to hire the highest calibre technology resources or to be able to convert to newer technologies. Those institutions can, however, gain access immediately to the best capabilities from a CSP and on a comparatively low-cost basis.

Accordingly, regulators have come to appreciate that the basket of risk for financial services organisations has shifted and, in many cases, diminished with the advent of CSP involvement. In particular, they note the benefits of end-to-end security and remain attentive to coordination of incident responses between CSPs and financial institutions.

However, regulators have questions about the overall risk management approach and practices among CSPs, which tend to approach risk management and compliance via both bottom-up and top-down approaches (i.e., 360 degrees), versus the traditional top-down, hierarchical model in financial services organisations, and with greater use of automation. The bottom-up approach differs from that of financial institutions, with which regulators have a high level of familiarity. (This approach is detailed further in the next section.)

It reverts to the regulatory bodies and the specific examiners on the ground to consider whether the questions they ask of financial institutions still make sense in the context of cloud-based services. If not, will they begin modifying those questions? For example, regulators may ask: Given that CSPs are providing services with different technologies and different risks, do the banks understand what those risks are? Are they establishing the right kind of controls? If a bank has decided to replicate its data across a CSP's infrastructure, what sort of different controls should the bank put in place to make sure its data remains secured?

These and other questions are addressed in the next section, which provides greater detail on the risk management and compliance practices in CSPs, including but not limited to issues such as operational resilience and third party vendors.

"Cloud service providers have completely disrupted financial institutions' ability to deliver cost-effective digital experiences that are both secure and scalable. Cloud service providers pride themselves on their cutting-edge security, governance and risk management techniques, and financial institutions that are architecting cloud environments with an understanding of the various cloud shared responsibility models are greatly benefiting."

— Noah Kessler, Managing Director, IT Audit, Protiviti

A Robust, Proven Approach by CSPs to Compliance and Risk Management

A systemic relationship prevails between the bank community and CSPs. Just as with any third party service provider, regulators recognise that if a CSP suffers a significant adverse event, a trickle-down effect will potentially impact the banks.

These regulatory activities call for a different type of examination, with a different lens on control environments and how they work. These new perspectives add complexity, compared to the traditional on-premise technology provided by a bank's own IT division. And as noted earlier, regulators may have greater familiarity with examining on-premise technology systems and processes, as well as third party tools and software that historically have been housed within a financial institution's data centres, compared with a CSP's technology systems.

CSPs' robust risk management practices are evident when assessing them in five categories:

Operational resilience

Risk management and controls

Three lines of defence

Automation

Innovation

Focus on Operational Resilience

A critical component of risk management in financial services is operational resilience. Regulators have been very clear that operational resilience plans must account for financial institutions' material use of third party providers. Moreover, once an agreement is in place and significant workloads are moved to the CSP, arrangements may be complicated to unwind.

Roles and responsibilities need to be delineated clearly between financial institutions and the CSPs they use — typically referred to as a shared responsibility model. Being unique, these roles and responsibilities will not conform easily to a standard list. Nevertheless, a clear contract that details the activities and obligations of each party is a prerequisite; CSP service documentation also helps illuminate the shared responsibility model across a CSP's services. Keep in mind that in the eyes of the regulators, any issue that arises ultimately is the responsibility of the financial institution. That risk ups the ante on financial institutions' third party risk management programmes and the need to provide evidence of management of third party risks.

Keep in mind that in the eyes of the regulators, any issue that arises ultimately is the responsibility of the financial institution. That risk ups the ante on financial institutions' third party risk management programmes and the need to provide evidence of management of third party risks.

Why? Banks and CSPs are seeing different sides of the overall picture. CSPs cannot assess the criticality of a service for a financial institution. For example, a CSP would not generally be aware of whether the workload

is so significant that it is underpinning all of a bank's payment systems. The criticality rating has to come to the examiners from the financial institution, which, unlike the CSP, knows how reliant it is on specific cloud products and services.

On one hand, every CSP with which a financial institution has a relationship is responsible for a piece of operational resilience. As the CSP is providing the infrastructure, the recoverability of that infrastructure is its responsibility. On the other hand, banks must apply that shared resiliency model to their systems that are placed in the cloud. Additionally, interdependencies between services present a potential risk. If there were an outage for one service, it might have downstream effects on other services.

Resilience poses further questions. Regulators may ask, how does the bank deploy a resilient architecture for its workloads on the CSP's infrastructure? How is the bank handling disaster recovery? How is it handling backups? Regulators must understand the measures that the bank has taken to protect its resilience when parts of a bank or CSP's infrastructure are not available.

Above all, using and relying on a CSP that provides resilient and fault-tolerant infrastructure and services does not mean that the financial institution has abdicated responsibility around resilience. Regardless of what CSP an organisation is using, it is the responsibility of the organisation to manage its own space within the cloud. This is a key component of the shared responsibility model. The cloud provider will maintain the contracted digital space, but the organisation must deploy and ensure diligence of use within the space. This starts with proper architecture within the cloud. Systems in the cloud that are not architected properly will not enjoy the benefit of the CSP's resilience advantages and could be perceived by regulators as a red flag.

Focus on Risk Management and Controls

Both CSPs and financial institutions employ numerous controls and practices to minimise risk. There are pros and cons in each model, which exemplify divergent approaches. Regulators are far more familiar with the model employed in financial institutions.

The business model for CSPs is predicated on a model of increased autonomy, security guardrails and Agile development. Financial services organisations adhere to a centralised, top-down approach to compliance, whereas CSPs also take a more federated, bottom-up view (i.e., 360 degrees) that ensures all key business and process owners are engaged in compliance and risk management.

Within CSPs, a pervading culture of ownership drives risk management. That dynamic environment is supported by automated controls and mechanisms. Although governance reporting flows to senior leadership and executive management who exercise all of the roles and responsibilities that regulators expect in terms of oversight and risk management, service/product teams still retain a high amount of accountability.

CSPs empower every individual within their organisations to regard risk as if they personally own it — a risk management concept that regulators have used for many years.

CSPs empower every individual within their organisations to regard risk as if they personally own it — a risk management concept that regulators have used for many years. In other words, CSPs have created their own framework for risk control. They can take an unfettered view toward risk control — this autonomy cuts through layers of bureaucracy.

In a belt-and-suspenders approach, executive management oversees the commonalities and dives deep into service and product development, and each service is essentially treated as its own business unit. That independence provides the flexibility to develop processes and operations that best support the needs of each service. Each of these groups is mandated to ensure that risks are being managed, controls are being adhered to and security is paramount. Although the chief information security officer (CISO) organisation puts in place security guardrails, these groups are empowered to do what makes the most sense for their products.

A key point here is that a CSP's products are designed for customers for whom security and risk focus are vital. For each product group, security and effective risk management are critical components of their operations and team members assume responsibility for them. In fact, leading CSPs employ robust risk management and compliance practices comparable to those of financial institutions. They just do so with a different approach and model (bottom-up and top-down, or 360 degrees) compared to financial institutions (top-down).

Some typical dimensions of differences in risk mitigation are illustrated in the following examples:

- **Architecture:** CSPs anticipate failure of hardware and software by building in automated resilience; financial institutions focus on resilience through traditional disaster recovery sites, with human intervention required to bring them online.
- **Service delivery:** CSPs conduct service requests via application programming interfaces (APIs); financial institutions conduct service requests via human workflow.
- **Operability:** CSPs' programmatic and automated operations require fewer human operators as demand increases; within financial institutions, human-intensive operations grow linearly with demand.

The shared responsibility model noted earlier outlines certain aspects for which the CSP is responsible and others for which their clients — in this case, financial institutions — are responsible, and that shared responsibility differs per service. For instance, while the CSP may provide an API for a customer's access to storage devices, the CSP will not be responsible for the data the customer puts there. Its controls are intended to provide only virtual segmentation of the customer's data and the physical environment networking around it, as well as to prevent attackers from accessing it through the CSP's network. It remains the role of the customer (i.e., the financial institution) to protect access to that data through proper access controls and encryption. This underscores the importance of understanding and clearly defining the shared responsibility model between the financial institution and CSP.

Focusing on the Three Lines of Defence

The three lines of defence model — management/business line, risk and compliance oversight, and internal audit — is an accepted framework in financial services and other industries. This model is used to provide a standardised and comprehensive risk management process. It defines responsibilities for management, risk oversight and independent assurance.

Within a CSP, similar to financial institutions, independent credible challenge is performed to ensure that product and service teams are accountable. Separately, a CISO is responsible for overall plenary security in the cloud.

Consider how the following breakdown is applicable to CSPs:

First line: Product development teams create and manage cloud services. These teams are comparable to business lines at a bank, and they focus on areas

like security practices (e.g., secure code scans, patch management), capacity and availability. Many service teams incorporate services within services (e.g., storage). Each, however, is responsible for owning its risk activities, as well as for understanding how its function interacts with the other services.

Second line: Compliance or security assurance groups, comparable to the risk or compliance function in a financial institution, are in place at CSPs. The second line governance reporting oversees the enforcement of the teams' risk management at a detailed level.

In a CSP, the comparable second line function tends to be a hybrid between the first and second lines in a financial institution, so that amalgamation of functions may in fact diverge from those in a large bank. More than in a financial institution, CSP senior executives actively oversee processes. Within a CSP, similar to financial institutions, independent credible challenge is performed to ensure that product and service teams are accountable. Separately, a CISO is responsible for overall plenary security in the cloud.

Second line staff in a CSP, who are typically engineers and security experts, provide continuous validation checks to ensure service teams are meeting a high bar for security and operational resilience. Other formal groups conduct penetration testing, security reviews and onboard services into different client programmes.

Third line: A robust internal audit function in CSPs is comparable to the internal audit department in financial institutions. Very large customer audit teams operate within the CSP. To a greater extent than banks, they can release dozens of assurance reports on a regular basis to provide evidence of their control posture to their customers.

The CSPs are also heavily audited by third parties in terms of their standards, controls and processes. CSPs, which are developing services for customers worldwide, go beyond internal assessments, using independent auditors to produce SOC reports on a regular basis.

CSP customers regard these SOC reports as more compelling than internal assurance alone as evidence that CSPs have raised their level of risk management assurance.

Focus on Automation

CSPs leverage leading-edge automation in their risk management and compliance practices. They minimise manual controls in their organisations — as many controls as possible are automated, scripted and focused on security and efficiency. Unless something really must be performed manually, it will be automated so that the organisation can run leanly, with relatively few employees.

For CSPs, automation is essential to provide services at scale, such as detecting and alleviating security events rapidly, redirecting traffic, or load balancing. In the past, such activities required manual decisions, which are inevitably slower. Consider, for instance, failing to initiate a transition to an alternate site in the event of server failure.

Automated controls generate significant benefits, including improved accuracy, a clear audit trail, centralisation, and harmonisation among organisational silos, such as finance and risk.

Automated controls generate significant benefits, including improved accuracy, a clear audit trail, centralisation, and harmonisation among organisational silos, such as finance and risk. Manual processes, by comparison, are prone to error. With the aid of automation, CSPs are able to address certain technology concerns more effectively than financial

institutions, including evergreen (always patched) databases, deep and comprehensive logging, one-click threat analysis, and access to multiple geographic regions for resource deployment.

Financial institutions, in turn, benefit from a CSP's automated collection of evidence and mapping. Automated services continuously collect and organise IT configuration and logs in a streamlined fashion. The automated collection of evidence can then be delivered to the bank's risk management group. As another illustration, a CSP can memorialise responses to service attacks or other events, and can then automate the responses for a future occurrence.

One of the great powers of the cloud is automated remediation. Another one is compliance as code. Rather than standard on-premises practices consisting of a manual process that an infrastructure team must configure, CSPs do not need to touch the systems and configuration. Instead, they use code to automate. Doing so guarantees consistency and comprehensiveness of their compliance controls. Another advantage is continuous integration and continuous deployment pipelines, which IT deploys programmatically. Deployment through CI/CD ensures that the environment stays consistent, with everything automated and codified.

Focus on Innovation

CSPs are among the top innovators in the world. They continuously leverage leading-edge technologies and automation to drive effective risk management. Generally, they invest more in pursuing and achieving these innovations than in additional personnel.

Century-old financial institutions may be slowed down by a legacy organisational structure based around risk and control. Compare that to a more recently established and entrepreneurial CSP. The latter is willing to break the traditional model around, say, purchasing or installing equipment. CSPs, which don't have legacy debt or business incentives to keep over time, are willing to build more efficiently from scratch and remain more efficient over the long run. The CSP, therefore, armed with new ideas, can deliver its products much faster than traditional banks can.

CSPs are among the top innovators in the world. They continuously leverage leading-edge technologies and automation to drive effective risk management.

In Closing

Regulatory engagements with CSPs increasingly reflect regulators' growing understanding not only of the benefits and risks of cloud computing services, but also of how CSPs effectively operate their risk management and compliance programmes. When it comes to risk management, one of the stark differences between a CSP and a financial institution is that a CSP has the ability to empower its employees to be innovative in terms of managing risk.

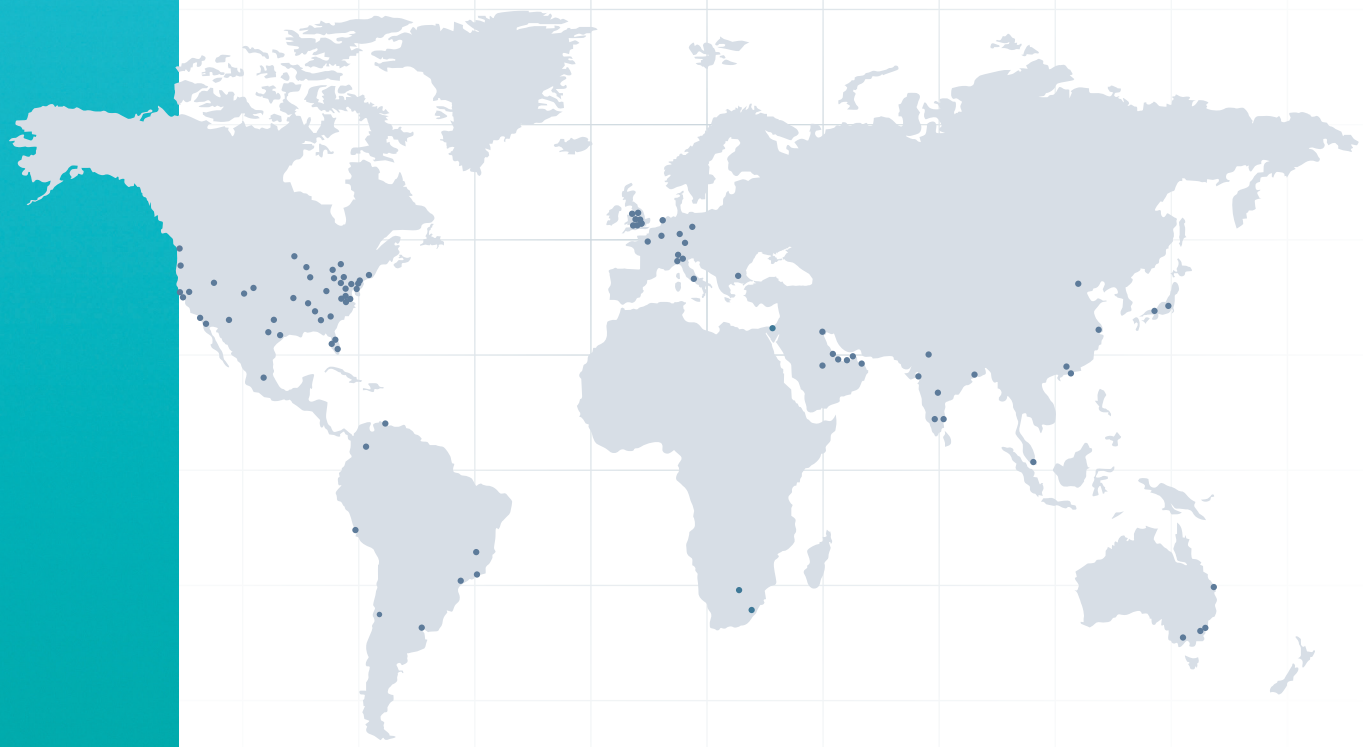
Since the onset of the COVID-19 global pandemic, financial institutions have accelerated their use of cloud capabilities — to support scale up, remote work, customer service and higher transaction volume. At the same time, regulators have become more conversant with how CSPs work and more comfortable with their risk management practices.

The overarching goal of the regulators remains the safety and soundness of their supervised financial institution, along with the protection of the end customer. As regulators grow increasingly familiar with the new efficiencies and culture of the cloud service provider industry, there should be increasing customisation in their oversight of CSPs.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.



THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®