Cloud Computing in the Securities Industry[1]

Contents

Introduction

Cloud computing is transforming how broker-dealers operate by providing opportunities to enhance agility, efficiency, resiliency and security within firms' technology and business operations while potentially reducing costs. As a result, cloud computing is increasingly seen by many firms as an important architectural component to their infrastructure.

Worldwide, cloud computing has enjoyed rapid adoption. Measured by the revenues earned by public cloud providers, the size of the cloud market is projected to reach $307 billion in 2021,[2] from $182 billion in 2018,[3] constituting a 19% average annual growth rate from 2018 to 2021. Growth in cloud was particularly pronounced in the wake of the pandemic, as remote work surged, and is likely to remain robust as firms continue to seek to drive value from the cloud.[4]

Within the securities industry, broker-dealers are adopting or exploring the adoption of cloud computing services in multiple ways. Firms are looking at the cloud to be able to scale operations flexibly, build robust solutions for business continuity, and create an environment for launching products more quickly to market. However, when seeking to migrate to the cloud, firms are likely to want to consider the potential business, operational, and regulatory implications.

Considering both the opportunities and challenges presented by cloud computing, FINRA, through its Office of Financial Innovation (OFI), undertook a review to better understand the implications of cloud computing on the securities industry. As part of this initiative, FINRA staff engaged in an active dialogue with nearly 40 market participants operating in this space, including broker-dealer firms, cloud service providers, industry analysts, and technology consultants to learn more about the state of cloud adoption within the securities industry and the related implications.

FINRA staff discussions with market participants revealed that broker-dealers have taken different approaches with respect to the adoption of cloud computing. Some firms, such as fintech firms, that are relatively new entrants to the broker-dealer space, started natively in the cloud and built their entire technology stack in the cloud. Other firms are either in the process of preparing to move to the cloud, piloting workloads in the cloud, or scaling operations in the cloud, typically in an incremental fashion. Still others have yet to commence their cloud journey in any meaningful way and are taking a "wait-and-see" approach to gain additional information as cloud computing matures.

For firms that have already begun the cloud adoption journey, many reported having benefited from features such as: (i) cloud-based productivity and collaboration tools (particularly at the onset of the Covid-19 pandemic when remote work surged), (ii) cloud-based applications that permit the streamlining of databases, (iii) data analytic applications that can accommodate computationally-intensive calculations that may spike with market volatility or increased trading activity, and (iv) new automated workflows and cloud-based tools that enable a greater ability to quickly launch products and innovate, including through the use of technologies, such as machine learning and other forms of artificial intelligence.

Firms have also identified certain challenges they faced during their cloud migration, including: (i) developing the appropriate protocols and skill base to facilitate establishing and maintaining cloud security, (ii) sufficiently changing organizational processes and firm culture to take advantage of the offerings presented by a cloud platform (*e.g.,* viewing technology use as a variable expense instead of a fixed capital cost and taking advantage of the ability to scale up and down quickly to innovate), and (iii) limiting the potential for vendor lock-in risk with a cloud provider.

In order to provide greater insight into the information gathered from FINRA's review, this paper summarizes key findings from FINRA's review in three sections:

- Section I provides an overview of cloud computing, discussing various cloud deployment models and cloud service models.
- Section II summarizes firms' experiences with cloud adoption, highlighting the level of cloud adoption, applications being deployed on the cloud, common themes from cloud adoption, and certain benefits and challenges.
- Finally, Section III discusses some regulatory considerations for cloud computing.

The discussion below is intended to be an initial contribution to an ongoing dialogue with market participants about the use of cloud computing in the securities industry. Accordingly, FINRA requests comments on all areas covered by this paper.[5] FINRA also requests comments on any matters for which it would be appropriate to consider guidance, consistent with the principles of investor protection and market integrity, related to cloud computing applications and their implications for FINRA rules.

SECTION I: Overview of Cloud Computing

Cloud computing refers to the delivery of information technology (IT) services using internet technologies in a way that is elastic and scalable and may be priced on a pay-as-you-go basis. Core cloud computing services generally include data storage, processing capacity, networking and software applications. Many of these services are similar to utility services in that they are largely commoditized and can be consumed in small or large quantities as is needed. Because firms no longer own or manage physical infrastructure, such as data centers, when moving to the cloud, they move from a capital expenditure ("capex") to operating expenditure ("opex") mode of consuming IT resources.

The National Institute of Standards and Technology (NIST) developed a more formal definition of cloud computing, describing it as being composed of five essential characteristics:[6]

- **On-demand self-service:** A user can easily provision computational resources at will.
- **Broad network access:** Cloud resources are available over a network, such as an intranet or public internet, that promotes access via an array of clients, from smart phones to workstations.
- **Resource pooling:** The cloud provider pools computing resources, such as data storage, that are shared by multiple users in a "multi-tenancy" arrangement where resources are allocated in a dynamic fashion depending on user demand. Users may know the physical location of their data at some high level (*e.g.,* locality of the data center) but not necessarily with granular specificity beyond that.

- **Rapid elasticity:** Computing resources can be quickly scaled up and down as needs change. To most users, the availability of computing resources will appear unconstrained to the extent that resources can be appropriated in the quantity needed.
- **Measured service:** There exists metering capability that records resource usage transparently and enables better control and monitoring by both user and provider.

Historically, cloud computing has developed at the intersection of three different technological fronts: (i) computational capabilities offered as a utility, (ii) virtualization, which allows multiple users to simultaneously operate off the same physical server and (iii) ability to access services through a network.[7] These developments date back to the 1960s, when mainframe computers were being developed and the Advanced Research Projects Agency Network (ARPANET) was launched as a predecessor to the internet.[8] In 1972, IBM launched a virtualized operating system called the Virtual Machine (VM) to allow multiple users to timeshare the system.[9] Over the following decades, computational capabilities from networking to storage were built out and increasingly commoditized. Internet adoption boomed starting in the 1990s with the advent of the World Wide Web, and supporting infrastructure was built out and bandwidth expanded. Virtualization technologies simultaneously advanced, enabling complete virtual computers to be executed within the same physical computer. These developments laid the groundwork for the modern day "cloud computing" concept to be created around the turn of the century.[10] As mentioned previously, the public cloud has grown rapidly to become an over $300 billion global market.[11]

Cloud Deployment Models

Firms may adopt different cloud models, depending on their needs and preferences. Each model provides different features and implies different trade-offs. Models are generally categorized into the following:[12]

- **Public cloud:** In this model, cloud services are made available virtually over the internet to users and are operated by a cloud service provider. The cloud provider hosts and operates the physical servers and locates them in multiple locations to provide improved resiliency capabilities. Depending on the level of service, they may also manage the operating system, middleware, and various application layers on top of the physical infrastructure. In this model, because cloud providers run large data centers, users are able to quickly provision needed computational resources, including redundant resources. And because of the economies of scale cloud providers enjoy by operating such vast infrastructure, they are able to drive down the costs of services[13] while also investing heavily in leading cybersecurity practices and technologies.
- **Private cloud:** In the private cloud model, computing resources are dedicated to a single firm instead of shared across firms, as is the case in the public cloud. The servers can be hosted on-premise in the firm's own data center, or the service may also be provided by a third-party provider at their data center. Consumers of private cloud services plan and provide for their own dedicated resources instead of accessing a public cloud's pooled resources. The infrastructure may be owned, managed, and operated by the firm or by a third-party provider or some combination of both. Private clouds allow firms to make use of various cloud-based tools and provide a testing ground for becoming more familiar with a cloud environment before possibly pivoting to a public cloud. However, potential drawbacks from a private cloud include the higher cost of renting dedicated servers or the responsibilities and risks that come with owning and managing infrastructure.[14] In addition, firms are more limited in the amount of resources they can quickly tap into. To address some of these concerns, firms have begun the use of virtualization in the cloud to permit users to share physical hardware to drive down costs while isolating their data and systems to prevent unauthorized access between customers (known as virtual private cloud, or VPC).[15] In the VPC approach, customers may face some limitations in features relative to traditional multi-tenant public cloud users but will still enjoy the benefits of scalability.

- **Hybrid cloud:** Hybrid cloud combines private and public cloud capabilities, typically in an inter-operable and orchestrated way. A firm may elect to pursue a private cloud environment but pair this with public cloud capabilities for a number of reasons. For one, firms may "burst" computational resources into the public cloud in the case of demand spikes. Alternatively, firms may elect to hold more sensitive data within a private environment while allowing other less sensitive data to be hosted on a public cloud. Or, workflows or certain data may lend themselves better to a private or public setting, and this may lead to firms pursuing a hybrid model. Another common use of hybrid cloud is as a transition strategy while moving on-premise ("on-prem") private cloud systems and data to the public cloud. As outlined, the hybrid model provides firms greater flexibility for workflows and management of data. However, the management of multiple cloud arrangements can create greater complexity and diseconomies of scale from managing multiple environments and potentially lead to redundancies between systems.
- **Multi-cloud:** Firms may pursue a "multi-cloud" strategy in which an organization uses services from multiple public cloud providers. This can be distinguished from a hybrid approach, which generally refers to the pairing of a private and public option and furthermore does not necessarily imply the deployment of multiple public cloud platforms. A multi-cloud strategy has the advantage of allowing a firm to mitigate dependencies upon a single cloud provider. It also provides a more flexible platform to assign workflows to the best-suited environment. For example, a firm may run their email system in one cloud platform and their account management application or trading system in a different cloud platform. Similar to the hybrid model, though there is the potential for greater complexity, diseconomies of scale and redundancies between systems. A multi-cloud environment may also increase the overall costs of computing.

Cloud Service Models

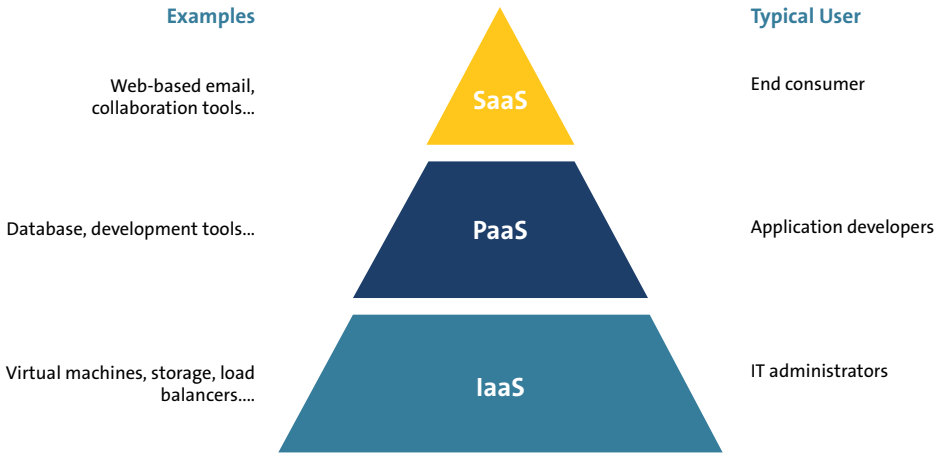
Firms that pursue public cloud technologies generally can pursue three different models depending on their needs: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Each type entails a different level of service provided by the cloud service provider:[16]

- **Infrastructure as a Service (IaaS):** IaaS refers to a self-service model for accessing basic IT services such as data storage, compute, and networking. These services are typically delivered over the internet via virtualization technology and are highly scalable. The user does not manage the underlying IT infrastructure but does control the layers of technology that run on top, such as the operating system and applications. IaaS essentially provides a flexible hardware resource that can scale rapidly and elastically in response to augmented storage and computational processing needs.[17]
- **Platform as a Service (PaaS):** PaaS builds upon IaaS, in which the cloud provider provides an on-demand environment of tools (such as programming languages and libraries) and software for application testing and development. PaaS is also delivered over the internet, thus enabling a virtual product development platform that resides on top of the IaaS layer. In this service model, again the user does not control the underlying infrastructural services nor some of the additional layers, such as the operating system and application tools, but has control over the applications that are being developed and deployed.[18]
- **Software as a Service (SaaS):** SaaS is a full-service model enabling firms to avail themselves of the full stack of cloud services to distribute software on-demand over the internet to end users. SaaS builds upon PaaS by completing the final step after application development to launch the final product over the web straight to users. In a SaaS model, the cloud provider manages all the layers of software and hardware necessary to host, develop and launch new applications. The firm has the least control of the underlying services and infrastructure and is effectively renting a full IT stack from the cloud provider.[19]

- **Other Services:** Many other types of services are emerging in the cloud computing environment. One example is Function as a Service (FaaS),[20] where applications can run in a "container"[21] that limits the need to account for complexities associated with separate operating systems (*e.g.,* Windows or Linux).

The following diagram sketches out the various layers of technology offered by cloud providers according to different models. As can be seen in the below Figure 1: Cloud Pyramid, cloud services form a stack, with SaaS built at the top. Division of responsibilities between user and provider also shifts as additional services are added between IaaS and SaaS. At the IaaS level, the cloud service provider manages the infrastructural services but manages the entire stack at the SaaS level. This division of responsibility has important implications for identifying who has what responsibility for securely operating in the cloud, as will be explored later.

Figure 1: Cloud Pyramid[22]



SECTION II: Firms Experiences with Cloud Adoption

Level of Cloud Adoption

Broker-dealers are at various stages in their cloud computing journey. Firms identified their size, business focus, existing IT infrastructure, and firm culture as some of the factors that influence their path to implementing cloud computing. While it is difficult to generalize for the entire industry, the following broad categories related to cloud migration may be helpful to understand broker-dealers' experiences:

- **Fully in the cloud:** Firms that are fully in the cloud generally fit into two groupings. The first group includes fintech start-ups that launched their businesses cloud natively (*i.e.,* built their technology systems around a cloud environment from inception). Founding team members may include technology leaders with previous cloud experiences, either in the securities industry or elsewhere, and could architect an IT environment in the public cloud for launching their product. These firms note that having a cloud native approach may enable them to get their product to market and respond to market demands more quickly while minimizing the start-up costs associated with establishing a private data center. The second group includes small firms that have been able to generally transfer workflows to the cloud by exclusively using off-the-shelf SaaS products or working with an IT service or cloud integrator to migrate their IT from an on-premise to a cloud-based one. Due to their small IT footprint, these firms may have fewer impediments to making a wholesale transition into the cloud.

- **Partially in the cloud:** Firms that are partially in the cloud include firms with different business models and sizes. These firms have typically begun the process of migrating certain applications, business domains or other workflows into the public cloud but are taking an incremental approach to cloud migration. Larger firms generally have an articulated enterprise strategy for moving towards the public cloud and are in the early stages of scaling their cloud presence. This enterprise strategy typically entails migrating an increasing share of their work onto the cloud over time, often implemented at the business unit level, as well as beginning certain new businesses in the cloud. Large firms also noted early work in pursuing multi-cloud platforms as a way to separate workloads and diversify cloud vendors. They also noted the adoption of private cloud, often as an initial foray into the cloud environment. Aside from the larger firms, other firms were pursuing more targeted use cases without necessarily making a commitment to expand their footprint in the cloud.

  For the broader category of firms that have begun the process of migrating into the cloud, it was sometimes the case that the more mission-critical work were the first ones to migrate, which made the footprint in the public cloud appear more pronounced. For others, lower-risk workflows involving less sensitive data (*e.g.,* public data or fund disclosures) were the first to go to the cloud. In addition, some firms took the approach of migrating client-facing aspects of their business early on to provide a better user experience. Generally, firms still ran legacy systems that needed to be accounted for when considering cloud migration, and the pace at which these legacy systems could be retired or the pace at which the data could be re-architected represented an important speed bump to the pace of moving to the cloud. The existence of legacy systems was one reason that developing a predominantly cloud environment for a firm might take a number of years.

- **Exploring or experimenting:** Many firms are in the category of exploring or experimenting in the cloud. These firms are typically evaluating cloud options and experimenting with potential use cases through pilot programs.[23] Some of these firms have defined an enterprise strategy for their cloud migration and were in the process of laying the groundwork for the migration (*e.g.,* setting up policies and governance structures). For others, the approach is less overarching and more targeted. Some firms contemplated migrating much of their work to the cloud, though many firms in this stage of cloud migration cited a more cautious "wait-and-see" approach, hoping to gain insight from their pilots and from others that are further along the cloud journey as the technology evolves. Many of these firms exploring cloud pilots typically elected to migrate lower-risk workloads. Some firms cited greater control or familiarity with existing systems and concerns over developing expertise or managing security in a new environment as reasons for proceeding more cautiously.

- **Principally on-prem:** Some firms—typically small-to-medium in size—maintain mostly on-prem systems and are not actively contemplating a move to the cloud. These firms may have, at most, ventured into some SaaS solutions for non-core functions. For firms remaining in these legacy systems, the rationale for not pursuing the public cloud did not necessarily reflect a conservatism towards new technology. Rather, part of it was a lack of urgency since there was not at the current time a pain point or compelling driver to move to a different environment. These firms indicated that despite the surge in remote work and surge in trading activity experienced at the outset of the pandemic, they were able to adapt using their existing technology infrastructure despite initial adjustment challenges. These firms also did not see a strong economic justification for migrating to the cloud at the current time, especially if existing infrastructure had not been fully depreciated. Many of these firms, however, are still considering migrating to the cloud in the future, being fully aware of the potential benefits.

Applications Being Deployed on the Cloud

When adopting cloud computing on a partial basis, firms typically targeted workloads that could be significantly improved because of the operational benefits provided by the cloud. Some of the key types of applications firms are beginning to deploy on the cloud include the following:

- **Productivity SaaS applications:** Firms migrating to the cloud often seek to become consumers of SaaS products for a variety of operational functions. For example, cloud-based SaaS products for productivity services (such as for email, file sharing, online chat or video conferencing capabilities) proved to be useful especially at the outset of the pandemic, given the reportedly easy and seamless way in which workers could continue working from a remote location. Firms also indicated a desire to find ways to help workers collaborate better, either in a remote work environment or geographically distributed work setting, with the use of these applications.
- **Data management applications:** Several firms are seeking to develop data management applications in the cloud that allow them to re-organize and streamline their databases across previously siloed business lines and functions onto a single platform or "data lake." For example, firms could seek to integrate data from previously siloed fixed income and equities businesses, seek to create a common platform from front-middle-back office trade/portfolio operations, or streamline data processes for customer on-boarding. The deployment of new cloud-based database architectures generally enabled more efficient workflows to query and use the data and also leveraged the ability to scale storage capacity into the cloud and facilitate data backup and disaster-recovery processes.
- **Data analytic applications:** Firms are also deploying cloud-based data analytics applications to analyze their data in many ways. Firms cited the rapid scalability of the cloud as an advantage for running computationally intensive workloads, for example running portfolio risk calculations, best execution possibilities, valuations and more. Using these applications, firms may be able to gain insight from the data, which was previously difficult or impractical to obtain, and the elasticity and scalability of the cloud mitigated the risk of interruptions during periods of high volatility or surges in trading activity. A few firms also noted that they were looking into cloud-based artificial intelligence and machine learning applications for data analysis, to enhance existing capabilities.
- **Client-facing applications:** Several firms are seeking to set up user interface applications in the cloud to be able to innovate and scale in a nimbler fashion. These applications could be browser- or-mobile based and generally are geared towards providing an intuitive and more personalized experience for clients to, among other things, access their account information, execute trades, and run portfolio analytics. These firms view using a cloud-based approach to client-facing applications as allowing their business to iterate more quickly in response to changing business needs and therefore be more competitive in areas of rapid innovation.

Common Themes from Cloud Adoption

A firm's journey to the cloud varied based on a given firm's specific facts and circumstances. Several firms noted that cloud migration was not a simple, linear process, even with adequate preparation, and there was no easy formulaic way to conduct a migration, given the unique circumstances of each firm. Despite the difference in each firm's journey, however, some common themes emerged regarding their experiences.

- **SaaS products are used broadly by firms:** Many firms, particularly smaller firms, interacted with the cloud by consuming mostly off-the-shelf SaaS products not directly related to their core business. This consumption is to be distinguished from those firms that build SaaS applications in the cloud. This "buy" over "build" approach constituted one of the earlier and more expeditious steps that firms took to move into the cloud. Most commonly, firms migrated certain operational functions using well-known, established SaaS applications. SaaS products for worker productivity and collaboration, such as email systems,[24] in particular, have seen considerable usage by firms. Use of other SaaS products for customer relationship management (CRM), financial account and human resources needs are also common.
- **Rollouts of cloud infrastructure tend to be targeted, incremental, and iterative:** Firms typically took a measured approach instead of launching a wholesale migration of the business to the cloud, with the realization that unexpected issues or challenges could emerge, requiring modifications to how a project was rolled out, what kind of talent was needed, or what the projected financial impact might be. Some firms took the route of identifying discrete workflows, applications or business domains to be refactored, rehosted and/or relaunched in the cloud. Examples included analytics platforms for wealth management clients, workflow and imaging systems, consolidation of a firm's data reporting infrastructure or setting up risk calculations in the cloud. Regardless of the scope, firms typically started with an initial pilot projects testing the use case before launch. As mentioned before, as a precautionary measure, some firms elected to send less sensitive data or less mission-critical workloads into the cloud first. Others, however, were more proactive in migrating mission-critical work to the cloud to gain a quicker competitive advantage.
- **Focus on governance, cloud security, and training:** Firms noted that it was beneficial to expend significant resources to develop governance and cloud security policies and procedures to help ensure a successful move to the cloud, with cloud security generally defined as encompassing the safeguarding of data and systems associated with cloud computing. The development of appropriate governance and cloud security protocols to attend to the necessary security requirements could take several months or even a few years. The use of experienced third-party providers, including cloud service providers, can assist with this development. Some large firms assembled governance committees across business functions to set broader policies for what kind of data or work could be moved and to set guidelines for implementing necessary controls to prevent loss or theft of sensitive data. A completion of a risk assessment can be useful when defining these cloud-based policies and controls. Firms noted that implementing training programs for staff of such policies and controls were labor-intensive but helpful steps to migrate to a new IT environment. They also noted the importance of training to maintain awareness of ongoing cybersecurity risks.
- **Organization and cultural changes often accompany cloud adoption:** Some firms noted that optimizing cloud capabilities required changes in the way people work, particularly as it relates to application development. Cloud adoption often coincided with firms reassessing their areas of technology expertise frequently, with existing staff being retrained or new staff with cloud expertise brought in. Firms also viewed enhanced cloud capabilities as enabling greater responsiveness to business needs and generally sought to implement agile workstreams that would more tightly weave software development and operations together.[25] With these changes, firms hoped to be able to enhance time-to-market capabilities and limit the potential for silos. Several firms also note that the organizational and cultural changes needed to embrace the disruptions to workforce and process that accompanied cloud migration were a key component to a successful cloud migration.

Benefits and Challenges

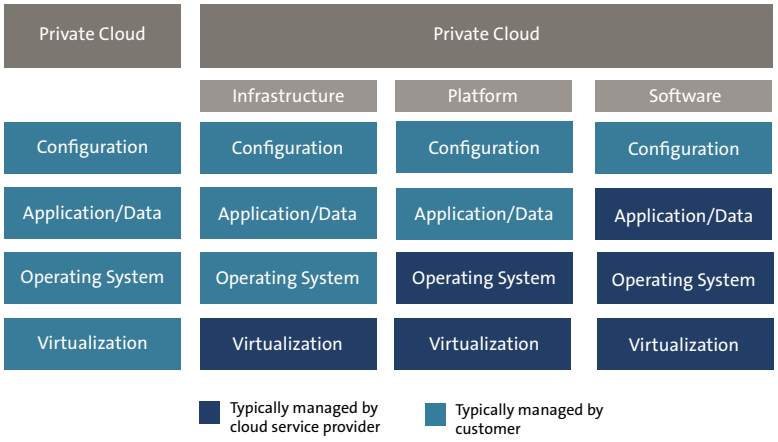
Firms cited several different benefits and challenges they encountered during their cloud journey.

In particular, firms noted that in assessing the potential benefits and challenges related to the use of cloud computing, it is important to assess them in comparison to the other alternatives available to firms, such on-prem environments (which carries its own relative benefits and challenges). The discussion that follows highlights some of these key benefits and challenges noted by firms related to their agility, resiliency, cost structure, cybersecurity, staffing, and operations.

- **Agility:** Several firms indicated that cloud-based technology infrastructure may allow them to be more innovative and nimbler in deploying new products and services. Some firms noted that time-to-market was improved in comparison to an on-prem environment because they did not have to provision for new servers and personnel to configure and maintain them. Instead, on the cloud, resources for new projects could be spun up within a day instead of within months and could be scaled up or down as needed. This enhanced ability to "fail fast" without incurring significant costs increased their capacity to develop new products and services. In addition, the cloud environment was cited by firms as being highly modular, enabling firms to select from a host of software and tools that can be customized to firms' needs. Cloud service providers noted the parallel of building in the cloud to building with LEGOs, with a much broader menu of tools and applications to use than might be available with existing legacy infrastructure. To fully leverage the cloud, however, firms also noted the importance of modifying workflows and the challenges involved in changing these workflows particularly in large organizations.
- **Resiliency:** Firms' views on resiliency generally focus on the ability to provide services in the face of any adverse external event or stress. The onset of the pandemic was an example of an adverse shock that tested firms' ability to accommodate surges in market activity and a shift to remote work for employees. Firms hosting or consuming applications on the cloud generally found comfort in the rapid scalability of cloud services as well as the geographically distributed nature of cloud providers' data centers so as to provide secure back-up storage and create more of a seamless failover solution should one data center or area suffer outages. The ease of scaling up computing usage within the cloud provided firms with high responsiveness to the surge in demand for IT resources that firms experienced during the pandemic. The ability to easily scale was noted as a benefit not only in the face of major external events but for day-to-day workloads, particularly for firms whose computational demands varied by time and had peak demands that were significantly larger than their average use. In addition to the resiliency benefits, however, firms also noted that cloud computing presented challenges with respect to resiliency as they considered issues related to lock-in risk to any cloud service provider.
- **Cost Structure:** Firms indicated that the potential cost implications of cloud migration were nuanced and dependent on factors such as activities conducted in the cloud, time horizon, resource governance and the condition of legacy system being retired. With respect to activities and time horizon, many firms considered that the financial benefit of migrating to the cloud might be felt only in the longer term, particularly with respect to activities where the computation and data storage needs of the firm did not fluctuate. In addition, firms noted challenges associated with closely monitoring, managing, and optimizing cloud usage, given that on-demand operating expenses could easily accumulate when opportunities for consumption are vast. In the short term, the costs associated with retraining staff and hiring new expertise also may present challenges for firms. Other transition costs include time and expenses needed to refashion existing workflows and rearchitect data and applications to take advantage of a cloud environment. The opportunity cost of foregoing existing infrastructure is also a consideration. Despite many of these structural and short term challenges, though, several firms noted that in the long term, they viewed a cloud-based infrastructure as being a cost benefit by better enabling them to align their costs to their needs on a real-time basis and by providing opportunities to create operational efficiencies. Firms also noted the potential opportunity to enhance revenues by more efficiently delivering competitive products and services.

- **Cybersecurity:** Firms cited cybersecurity as a potential benefit to cloud computing due to the many security features available in a cloud environment, in part, because of cloud service providers' ability to enjoy economies of scale in managing massive data centers. However, several firms noted challenges in making sure their systems are appropriately configured for security on the cloud and indicated that the cloud environment could be less secure than an on-prem environment if appropriate measures were not taken. For example, developing appropriate encryption and key management protocols were cited by firms as important components to developing comfort to committing sensitive data to the cloud. Automating certain processes was also cited as advantageous for minimizing human error. Firms also noted the importance of correctly identifying responsibilities for maintaining cloud security (*i.e.,* the safeguarding of data and systems associated with cloud computing) to limit the potential for security or control gaps or misconfiguration of cloud resources based on the mistaken assumption that the cloud service provider would take on cloud security tasks that the firm should be assuming. As seen below, firms perform a varying number of tasks for maintaining cloud security at different levels of service.[26]

Figure 2: Cloud Security Shared Responsibility Model



The challenges of maintaining a strong cloud security posture exists on many levels, and that was reflected by firms. Many firms noted the importance of well-designed governance policies that clearly laid out roles, processes, standards, and accountability around security in the cloud. Other firms noted the criticality of implementing appropriate user access rights to data and applications as well as developing strong authentication techniques for end-clients using cloud-based products.[27] Training users to avoid common traps, such as phishing,[28] was seen as a constant effort to protect the firm from external breaches. To help firms manage these risks, cloud service providers are bolstering the toolsets that help simplify firms' ability to track cloud security, by including offerings such as dashboards and scores related to security risk as well as consulting services to provide expertise related to cloud-based security. For those in the process of rolling out a pilot program or new applications on the cloud, "penetration tests"[29] are also regarded as a helpful exercise to identify potential vulnerabilities. Ensuring appropriate access management controls in the cloud environment is also critical.

- **Staffing:** The need to attract new staff with cloud expertise and train existing staff to operate in a cloud environment was cited by several firms as one of the challenges associated with cloud adoption. Many firms seeking to migrate to the cloud explored the potential of hiring new staff, re-training existing IT staff, and utilizing a third-party consultant or the cloud service provider. Firms noted that the demand for trained or certified cloud engineers has been outpacing supply, particularly considering the growth in cloud adoption in other industries. Despite these challenges, some of the fintech or larger firms that have heavily invested in building their cloud presence noted that their cloud-forward stance facilitated their ability to attract and retain staff with cloud expertise. They noted that engineering talent generally was migrating from traditional on-prem architectures to cloud-based ones. For several small firms, the primary option indicated was to outsource much, if not all, of their IT and cloud needs to a third-party cloud service vendor.

  Firms also noted challenges associated with developing processes to continually refresh, update, and train staff on the evolving offerings associated with cloud computing. This observation was relevant not only to understanding the growing ecosystem of cloud-native applications and technologies but also potential threats, which reinforced the need for constant training in the cybersecurity sphere to maintain an appropriately vigilant cybersecurity posture.

- **Operational:** One of the main operational challenges discussed by firms was "lock-in" risk, in which a firm is excessively dependent upon a specific cloud provider.[30] This is a risk that could compromise a firm's business resilience to external adverse events if the cloud service provider becomes less reliable. Overall, while no firms were significantly concerned that their cloud service provider would abruptly terminate service, firms did see the benefits of having a flexible stance towards the cloud so that it was possible to seamlessly move across providers as warranted by business demands and risks. The actual implementation of achieving portability across clouds, however, was a challenging task. For example, building expertise in multiple clouds added to the challenge of building the necessary human resource capabilities. In addition, the technology available to allow portability of data is complex and incomplete. Many firms spoke of "containerizing" data as a way to modularly manage data and applications such that they could be more easily ported to different cloud environments. However, most firms said that this was a task more easily said than done and may potentially introduce disruptions to business availability.

  Some firms seeking to mitigate lock-in risk are starting to leverage multiple clouds for different types of workloads, thus gaining aptitude in multiple cloud environments. Many industry participants, including cloud providers, have openly embraced open source software as a way to build out cloud applications that could be used across cloud environments. Some cloud providers are starting to focus on providing platforms that can enable firms to develop applications and launch them in any environment, thus bridging incompatible cloud architectures and helping firms run across hybrid or multiple clouds. To the extent warranted by each firm's risk considerations and to the extent practicable, firms are also developing "exit plans" that lay out a process for moving to another provider(s) over the course of a period of time. Firms may consider how long their service agreements allow them to remain with a service provider in the event the provider ends the agreement, and how much time would be required to switch to a different provider. In addition, the ability to potentially move data via application programming interfaces ("APIs") may offer some flexibility for firms looking to limit lock-in risk. Despite these offerings, some friction is likely to still exist in moving data across cloud environments, but the trend appears to be towards greater inter-operability across cloud providers.

SECTION III: Regulatory Considerations for Cloud Computing

There are several regulatory implications that firms may wish to consider when establishing a presence in the cloud. It is important to keep in mind that although a firm may shift its technology infrastructure to a cloud environment, all of the regulatory requirements that are applicable in an on-prem environment continue to apply. However, cloud-based applications may contain some unique features that securities market participants may wish to consider as they explore and adopt related technology tools. Specifically, where applicable, factors for market participants to consider when seeking to adopt a cloud environment include cybersecurity, data governance, outsourcing/vendor management, business continuity, and recordkeeping. This section provides a brief discussion of each of these factors and highlights certain related regulatory considerations.[31]

While this section highlights certain key thematic areas, it is not meant to be an exhaustive list of all factors or regulatory considerations associated with adopting cloud-based applications. Broker-dealers should conduct their own assessments of the implications of cloud computing, based on their business models and related use cases.

- **Cybersecurity:** Cloud technology is complex, and firms should consider any potential differences in cybersecurity management between cloud services and on-prem systems. Many best practices from an on-premise environment would still apply, though some may differ. For instance, insider risks may extend to the cloud service provider. Also, as mentioned previously, one important feature of cloud computing is the sharing of cloud security-related tasks between the firm and cloud service provider. As laid out in Figure 2 (above), a firm may undertake to perform more or less of certain cloud security-related tasks depending on the type of cloud deployment. When considering the division of cloud security-related tasks between itself and the cloud service provider, a firm may benefit from working to ensure cybersecurity is incorporated as a critical component of the evaluation, development, and testing process of any cloud-based application. The division of tasks should also be reflected in the contractual agreement between the firm and cloud services provider. For additional resources on this topic, including applicable rules, guidance, and FINRA's report on Cybersecurity Practices, refer to FINRA's webpage on cybersecurity.

  A cloud vulnerability report by the National Security Agency[32] also noted the following three functions where it is important to identify the party that will be performing the cloud security related task: (i) threat detection, (ii) incident response (iii) patching/updating. Typically with respect to each of these functions, the cloud service provider will undertake tasks for securing its own cloud resources, but the firm would still need to perform tasks for monitoring threats, responding to incidents and patching any vulnerabilities for the cloud resources they manage. The cloud service provider may have tools or services to help a firm perform these tasks, but it is important for firms to clearly understand the division of responsibilities to limit any potential gaps.

The NSA paper also cites two vulnerabilities related to cloud computing that may be beneficial for firms to monitor.

- **Misconfigurations**: Cloud misconfigurations have to do with improperly setting up a cloud-based system, which creates vulnerabilities that can lead to data breaches. Misconfigurations are common, since they can occur in many different areas and be caused by various people with access rights. They can also go unnoticed, which creates a potentially large opening for attackers to exploit a firm's cloud resources. Common misconfigurations vary but may include: publicly exposed cloud data and resources, unrestricted access to outbound/inbound traffic, or data encryption not being applied. Misconfigurations can result from anything from low awareness of security responsibilities and lack of proper controls and oversight, to simple insider negligence, and speak to the need for well-designed policies, layers of security controls, and mechanisms for monitoring potential breaches.

- **Poor access controls:** Poor access controls have to do with weak authentication methods that enable unauthorized entities to infiltrate cloud resources. Vulnerabilities may also exist such that authentication methods can be bypassed. Vulnerabilities may occur at a point of access to the cloud within the firm or at a client endpoint, namely a client's cloud-based account. FINRA issued a Cybersecurity Alert in October, 2019, warning about cloud-based email account takeovers ("ATOs"), in which perpetrators use various techniques to acquire client log-on credentials and from there acquire sensitive information, initiate a fraudulent transfer of funds or expand the attack footprint. ATOs can also occur with firm staff accounts that have administrative privileges, which provides a platform for a much larger attack. Such attacks could be prevented with stronger authentication techniques, namely 2FA, better retention of activity logs and more effective management of and controls over administrative accounts.

- **Data Privacy:** Related to the previous points on cybersecurity, firms are also subject to requirements to safeguard customer records and information. Such requirements are laid out in SEC Regulation S-P, and a reminder of Reg S-P's requirements are also spelled out in FINRA's Notice to Members 05-49. Regulation S-P requires firms to have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to: (i) ensure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Despite the firm's outsourcing of certain IT tasks to cloud service providers, the firm is ultimately responsible for compliance with the requirements of Regulation S-P.

  Moreover, if a firm's cloud adoption leads to changes in how it collects, stores, analyzes, and shares sensitive customer data, firms may need to update their policies and procedures related to customer data privacy to reflect such changes. Relatedly, firms may wish to consider whether appropriate consent from customers, as needed, has been obtained with respect to the collection of any new information that may be desired to facilitate or enhance the benefits associated with cloud adoption. In addition, firms may wish to consider whether appropriate policies and procedures exist with respect to sharing such data with cloud service providers or other vendors, including how and what level of access is provided to vendors; any parameters for storing the data; any restrictions on vendors sharing data with other third parties; and any restrictions on aggregating customer information with data from other vendor clients.

- **Outsourcing/Vendor Management:** To the extent that a cloud service provider or other cloud vendor is selected to perform certain tasks on behalf of the firm, firms should be mindful of applicable guidance on outsourcing.[33] Firms are reminded that outsourcing an activity or function to a cloud service provider or other cloud vendor does not relieve them of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA rules associated with the outsourced activity or function.

  The FINRA outsourcing guidance also notes in pertinent part: "After the member has selected a third-party service provider, the member has a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities. This requires the member to have in place specific policies and procedures that will monitor the service providers' compliance with the terms of any agreements and assess the service provider's continued fitness and ability to perform the covered activities being outsourced."[34] Therefore, firms are encouraged to conduct appropriate due diligence and testing of cloud service providers and vendors to help ensure that the vendors can conduct the activities being outsourced in a way that complies with FINRA and other relevant rules.

Firms may also consider the risks associated with vendor lock-in and the potential that cloud service providers might be unable to reliably provide services. Currently, platforms and technologies may not readily enable migration between cloud vendors should an existing cloud solution fail to meet the firm's requirements. Firms may wish to consider whether multi-cloud or hybrid cloud options are compatible with their business needs. Alternatively, they may wish to consider adoption of an exit strategy to mitigate against an unfavorable lock-in scenario. As mentioned before, certain services and technologies (*e.g.*, containerization, open source software) are making it easier to use different cloud service providers or switch between them.

Finally, firms also may want to consider whether a cloud vendor has undergone rigorous operational and financial audits (*e.g.*, SOC 1 and SOC 2) or has had third-party assessments or certifications to help demonstrate its ability to provide vital functions on an ongoing basis. Firms may also consider industry-recommended security best practices for working with a specific cloud service provider.

- **Business Continuity:** FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires firms to create, maintain, annually review and update written business continuity plans relating to an emergency or significant business disruption. Such plans must be reasonably designed to enable the firm to meet its existing obligations to customers and address the firm's existing relationships with other broker-dealers and counterparties. As mentioned before, the cloud offers the potential for greater business resiliency due to redundant storage and computing capacity across cloud service provider's data centers. Cloud providers typically host multiple data centers in different locations, and firms should consider the extent to which cloud service strategies may support their business continuity and disaster recovery plans and obligations. Firms should also be aware that latency issues may exist that impact real-time back-up of information or availability of services in case of a failover to the secondary location. Accordingly, firms may wish to consider testing the redundant configuration to ensure business services can continue in the face of a disruption, and update test plans and procedures accordingly. Firms may also wish to consider whether cloud services may support greater resiliency for their systems. For example, important applications can run in a live production mode across multiple cloud datacenters with highly available databases. In this scenario, if one of the cloud provider's data centers fails for any reason, the remaining data center continues to service the production load with no impact to customers.
- **Recordkeeping:** Broker-dealers are increasingly looking to utilize cloud storage for data and information maintained by the firm. FINRA and SEC rules require firms to preserve specified records for certain periods.[35] In addition, these rules require that such records be preserved during the retention period in a format and media that complies with Exchange Act Rule 17a-4, including, among other requirements, a requirement that records preserved on electronic storage media be stored exclusively in a non-rewriteable and non-erasable format.[36] Certain cloud providers have indicated that they provide products or services designed to be compliant with FINRA and SEC recordkeeping requirements. Firms should be aware of their recordkeeping obligations and assess any such recordkeeping products or services offered by their cloud providers.

SECTION IV: Request for Comments

FINRA encourages comments on this paper, including areas where guidance or modifications to FINRA rules may be desired to support cloud adoption while maintaining investor protection and market integrity. Comments are requested by October 16, 2021.

Member firms and other interested parties can submit their comments using the following methods:

- Online using FINRA's comment form for this Notice;
- Emailing comments to pubcom@finra.org; or
- Mailing comments in hard copy to:
  Jennifer Piorko Mitchell
  Office of the Corporate Secretary
  FINRA
  1735 K Street, NW
  Washington, DC 20006-1506

To help FINRA process comments more efficiently, persons should use only one method to comment on the proposal.

Important Notes: All comments received in response to this paper will be made available to the public on the FINRA website. In general, FINRA will post comments as they are received.[37]

Direct inquiries regarding this paper to Haimera Workie, Senior Director, Office of Financial Innovation, at (202) 728-8097; or Michael Oh, Director, Office of Financial Innovation, at (202) 728-8305.

ENDNOTES

1 This paper is not intended to express any legal position and does not create any new requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any regulatory obligations. While this paper summarizes key findings from FINRA's outreach and research on the use of cloud computing in the securities industry, it does not endorse or validate the use or effectiveness of any of these applications. Further, while the paper highlights certain regulatory and implementation areas that broker-dealers may wish to consider as they adopt a cloud environment, the paper does not cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules, and regulations to determine potential implications of implementing cloud-based applications.

2 Press Release, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020, Gartner (Jul. 23, 2020). https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020.

3 Press Release, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, Gartner (Apr. 2, 2019). https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.

4 Duncan Stewart, Patrick Jehu, Nobuo Okubo and Michael Liu, The Cloud Migration Forecast: Cloud with a Chance of Clouds, Deloitte Insights (Dec. 2020). https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/cloud-migration-trends-and-forecast.html

5 *See* Request for Comments section on 15 of this paper.

6 Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, 2, NIST Special Publication 800-145 (Sep. 2011). https://doi.org/10.6028/NIST.SP.800-145

7 Blesson Varghese, History of the Cloud, The Chartered Institute for IT (Mar 19, 2019). https://www.bcs.org/content-hub/history-of-the-cloud/

8 DARPA, ARPANET, https://www.darpa.mil/attachments/ARPANET_final.pdf.

9 IBM Cloud Team, A Brief History of Cloud Computing, IBM (Jan. 6, 2017). https://www.ibm.com/cloud/blog/cloud-computing-history

10 Antonio Regalado, Who Coined Cloud Computing? MIT Technology Review (Oct. 31, 2011) https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/#:~:text=The%20notion%20of%20network%2Dbased,term%20to%20an%20industry%20conference. In 2006, Amazon launched Amazon Web Services and its Elastic Compute (EC2) services, which allowed users to run their own computers and applications over the cloud. Press Release, Announcing Amazon Elastic Compute Cloud (Amazon EC2) – beta, AWS (Aug. 24, 2006).

11 Gartner (2020).

12 Mell and Grance (2011) lay out different cloud deployment models; *see also* cloud overviews by vendors and service providers, for instance: Accenture, Cloud Computing, https://www.accenture.com/us-en/insights/cloud-computing-index; *see also* Grace Lewis, Basics About Cloud Computing, Carnegie Mellon Software Engineering Institute (Sep. 2010). https://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28877.pdf.

13 James Hamilton, Cloud Computing Economies of Scale, Mix'10 Conference (Dec. 8, 2009). https://channel9.msdn.com/Events/MIX/MIX10/EX01.

14 Paul Diamond, Cloud storage vs. on-premises servers: 9 things to keep in mind, Microsoft Corporation (Sep. 25, 2020). https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

15 IBM Cloud Education, Virtual Private Cloud (VPC), IBM (Nov. 2019). https://www.ibm.com/cloud/learn/vpc.

16 Mell and Grance (2011) lay out main service models as do Accenture, Cloud Computing and Lewis, Basics of Cloud Computing.

17 Some of the major providers of IaaS include AWS, Azure, Google Compute Engine and Cisco Metapod.

18 PaaS service providers include AWS Elastic Beanstalk, OpenShift, Google App Engine.

19 Such applications include Google Docs, Office 365, Zoom and Symphony.

20 IBM Cloud Education, FaaS (Function-as-a-Service), IBM (July 2019). https://www.ibm.com/cloud/learn/faas#:~:text=FaaS%20(Function%2Das%2Da%2DService)%20is%20a,building%20and%20launching%20microservices%20applications.

21 Containerization is a way to encapsulate packages of software code so that the software can run as a portable unit across different cloud platforms.

22 The diagram depicts a standard cloud pyramid, as depicted, for example, in: Deloitte, Change the Way You Change: How Can Banks Stay Ahead of the Curve? (Aug. 2019), p. 29.

23 However, many of these firms had already experienced some adoption of cloud-based SaaS services for non-core functions like email or human resources, but there was less of a touchpoint with the cloud in terms of business workflows, applications or management of data related to their core brokerage business.

24 Other examples include Office 365, Zoom, Teams, Slack.

25 An agile workflow approach is a modern approach to project management that fosters shorter development cycles (sometimes called "sprints") while incorporating feedback at the end of each cycle to enable modifications and improvements before moving to the next cycle. Some firms similarly referred to improved "DevOps" for facilitating shorter application lifecycles.

26 National Security Agency, Mitigating Cloud Vulnerabilities (Jan. 20, 2020). https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

27 FINRA Information Notice, Cybersecurity Background: Authentication Methods (Oct. 15, 2020), https://www.finra.org/rules-guidance/notices/information-notice-101520.

28 Phishing is the fraudulent effort to obtain sensitive personal information, such as usernames or passwords or credit card details, by posing as a trustworthy entity in a digital communication.

29 Penetration tests, or "ethical hacking," entail the hiring of a third-party firm to conduct an authorized cyberattack on a firm's IT system to identify exploitable vulnerabilities. The utility of such tests also extends beyond the initial rollout and is often employed on a regular basis.

30 Some firms also noted that vendor lock-in risk is not unique to cloud and may exist for on-premise systems as well.

31 Supra note 1. While the paper highlights certain regulatory and implementation areas that broker-dealers may wish to consider as they adopt a cloud environment, the paper does not cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules, and regulations to determine potential implications of implementing cloud-based applications.

32 National Security Agency, Mitigating Cloud Vulnerabilities.

33 *See e.g.,* NASD/FINRA's Notice to Members 05-48: Members' Responsibilities When Outsourcing to Third Party Providers.

34 Id.

35 *See e.g.,* FINRA Rule 4511 (General Requirements) and Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 (Exchange Act). *See* also FINRA, Key Topics, Books and Records, https://www.finra.org/rules-guidance/key-topics/books-records.

36 *See* Exchange Act Rule 17a-4(f); *see* also SEC Interpretation: Electronic Storage of Broker-Dealer Records, Release No. 34-47806, available at https://www.sec.gov/rules/interp/34-47806.htm.

37 Parties should submit in their comments only personally identifiable information, such as phone numbers and addresses, that they wish to make available publicly. FINRA, however, reserves the right to redact or edit personally identifiable information from comment submissions. FINRA also reserves the right to redact, remove or decline to post comments that are inappropriate for publication, such as vulgar, abusive or potentially fraudulent comment letters.