DTCC

Securing Today. Shaping Tomorrow.®

MAY 2017

# MOVING FINANCIAL MARKET INFRASTRUCTURE TO THE CLOUD

## Realizing the Risk Reduction and Cost Efficiency Vision While Achieving Public Policy Goals

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

DTCC plays a critical role in protecting the integrity and stability of the global financial system. The firm stands at the center of the global marketplace, and in its role as the holding company for Systemically Important Financial Market Utilities (SIFMUs) in the United States, its services are deemed essential for the safe and efficient functioning of the marketplace. Historically, DTCC's core platforms and systems have been hosted in private data centers owned and operated by the firm – an approach that was consistent with many of its peers in the industry. However, as DTCC has been executing its IT Strategy to modernize its core platforms, it has also incrementally expanded its solutions delivery capability to externally-hosted platforms, including the use of public cloud vendors. A similar shift has been occurring across the industry as many financial institutions, including financial market utilities (FMUs), governmental agencies and regulators, have begun to leverage the public cloud. This change reflects both the ongoing maturation of cloud computing as well as a growing understanding and appreciation for the enormous security and operational benefits the cloud can provide.

Cloud computing has reached the tipping point as the capabilities, resiliency and security of services provided by cloud vendors now exceed those of many on-premises data centers. The combination of

**DTCC is an industry owned and governed financial market utility**, providing financial transaction and data processing services for the global financial industry. Three of DTCC's subsidiaries, National Securities Clearing Corporation (NSCC), Fixed Income Clearing Corporation (FICC) and The Depository Trust Company (DTC), are designated Systemically Important Financial Market Utilities (SIFMUs) by the US Financial Stability Oversight Council. In addition, DTC, as a New York limited purpose trust company and state member bank of the Federal Reserve System, is also subject to supervision and examination by the New York State Department of Financial Services and the Federal Reserve Bank of New York under delegated authority from the Federal Reserve. DTCC provides a wide range of post-trade services across the financial services industry, including central clearance and settlement and asset servicing for the majority of cash equity and fixed income trading in the U.S., services to support the wealth management and insurance industries, institutional matching and post-trade management services, and trade repositories that provide global compliance reporting for swaps transactions across all asset classes. DTCC also provides the governance, operations, technology applications and infrastructure to support these and other related services.

technology commoditization with the scale and competition from public cloud vendors is driving the unit price of computing, storage and network services toward zero. This gap will continue to grow at an accelerated rate, leaving laggards in cloud adoption at increased risk from a resiliency and cost perspective. The question of the past 10 years has been, "is it safe to move processing to the cloud?" Today, that question has become: "What compromises are market infrastructures making by maintaining processing in on-premises data centers?"

As a result, DTCC intends to strategically expand the leverage of cloud technology across a much greater range of its services and applications over the next 3-5 years. Due to the critical nature of the services provided by DTCC, we will execute our cloud strategy in collaboration with key stakeholders, including clients and supervisors.

DTCC recognizes that understanding and market acceptance of significant technology changes requires industry wide communication and open discussion. This paper provides DTCC's views on the benefits of the public cloud platform and discusses the relevant regulatory guidance and requirements to utilize cloud vendors and the related policy implications.

# BACKGROUND

Since DTCC's inception more than 40 years ago, the technology supporting the global financial markets has evolved dramatically. Previously, many market infrastructures built, maintained and housed mainframe technology in proprietary data centers. Today, they are leveraging a combination of these data centers and internet-hosted services to support both internal and customer-facing business applications. However, a new utility model of computing has emerged over the past decade – cloud computing – which has been enabled by a combination of commoditized hardware, such as high-capacity networks, low cost computers and network devices and widespread adoption of software capabilities, including open source, service-oriented architectures, virtualization and automation. A key contributor to this trend is the global access to commercial cloud computing offered via the public internet. As a result, global demand for cloud services has increased dramatically, driving exponential expansion in the range and depth of solutions offered by vendors. The cost savings and benefits of cloud computing are now challenging the longstanding justifications for provisioning and/or sustaining individually-owned and managed data centers.

## Service Models of Cloud Computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

There are three basic cloud service models available today:

- Software as a Service (SaaS):

  A software application that provides a business service that is offered directly to the consumer, typically using a web browser. The Service Provider manages the application, middleware and infrastructure, with limited customization options. The consumer administers the application data and users. Examples include client relationship management (Salesforce), human resource applications (e.g. PeopleSoft) and service management (ServiceNow).

- Platform as a Service (PaaS):

  A set of tools for building applications is provided to the consumer. These tools, which include libraries, languages and components, allow the user to construct applications using the Service Providers' infrastructure. In this model, the consumer manages the applications and services using the vendor's components. Examples include specific and proprietary offerings from Amazon, Microsoft and IBM.

1 NIST NIST, Glossary of Key Information Security Terms (May 2013), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810.

- Infrastructure as a Service (IaaS):

  Infrastructure components are provided to the consumer, but the data center facilities and physical technology components are managed and operated by the Service Provider. Virtual environments, which typically include processing, storage and networking resources, are managed by the consumer to run operating systems, databases, middleware and applications of their own choosing. In the IaaS model, the consumer manages the entire infrastructure above the resources provisioned by the cloud vendor.

## Public cloud vendors have matured and expanded offerings

The first commercial cloud vendors began providing commercial services over 10 years ago. As the largest of these vendors have matured and reached enormous scale, they now serve millions of customers from dozens of data centers globally. They have built highly-automated, client-focused offerings using their own hardware components, which are tailor-made for cloud requirements of security, scalability, multi-tenancy and high availability. In addition, they support their own internal networks and, in some cases, even build their own power plants. These operations have become so robust and sophisticated that the biggest individual companies cannot achieve the scale of these large vendors with respect to key performance requirements.

Public cloud vendors have also built into their systems critical capabilities, such as strong and granular access management, the ability to scale capacity up and down instantly based on demand and resiliency by designing systems to expect failure. Included in this impressive toolkit is functionality for monitoring and logging all activities, even programmatic API calls, as well as built-in security with data encryption in transit, during compute and at rest and encryption key management by either the customer or provider.

The primary business objective of public cloud vendors today is to operate a secure global infrastructure for millions of customers. The leading cloud vendors are at the forefront of security implementation and research, enabling them to attract and retain the top global talent. In contrast, many enterprises address security as a necessary operating requirement to support business priorities and, as a result, they craft customized, defensive security measures that cannot approach the scale or resources of solutions offered by the largest public cloud vendors. Very few companies can replicate the reliability and built-in automation and processes of a public vendor that is installing tens of thousands of individual servers every day and monitoring and trouble-shooting tens of millions of active network components.

## The Benefits and Challenges of Modern Corporate Data Centers

Most large financial firms, including financial market infrastructures, have invested in and continue to operate corporate data centers that were designed as fit-for-purpose for the specific needs of a particular business. Unlike a newly formed start-up that can make an initial investment in an enterprise infrastruc-

ture, existing corporations must weigh the costs and benefits of leveraging a corporate data center or using the cloud.

There are advantages and benefits to private, corporate infrastructure that may compel some companies to maintain or expand their own data centers. These include:

- Proprietary configurations or specialized systems that are not available at public cloud vendors
- Dedicated resources
- Situations that require highest performance requirements, extremely low latency or massive data processing

It is also true that for some existing applications, the on-premises systems may have already been optimized and given this increased efficiency, may not gain any benefits from moving to the cloud.

However, many modern corporate data centers present a common set of challenges. Much of today's legacy infrastructure was built with a purposeful and intentional design to support a set of applications at a given point in time. As a result, firms face increasing financial, security and other issues because the simplicity of the initial designs have become enormously complex due to continuous waves of mergers, integrations, enhanced security requirements and rushed additions or modifications.

**Complexity Challenge:** This is the result of the ever-expanding portfolio of hardware components, network segments and software products created, purchased or acquired over the course of years. Retiring or removing technology is difficult and often results in unexpected disruptions, so many firms have an inventory of applications and hardware that are unused but still online. Business continuity requirements, which are typically achieved through multiple data centers, replication schemes and tightly orchestrated recovery scripts, add to the complexity.

**Security Challenge:** Legacy infrastructures were often not architected with centralized controls or logging and management consoles. In addition, they typically provide limited, if any, information about their running status. The challenges are compounded with older networks that were not designed and built with network and end point security, which put them at increasing risk from external access and unknown actors. Patching mixed environments to prevent the latest security exposures is time consuming and difficult.

**Cost Challenge:** Maintaining a corporate data center has become an expensive proposition for many financial market infrastructures as they are forced to invest limited resources into: hardware refresh and their related depreciation, purchasing and maintaining unused excess capacity to support the highest-ever projected volume requirements, purchasing and maintaining unused excess capacity to support local

component failure and out-of-region disaster recovery and all of the human and organizational resources to manage and maintain these assets.

## Public Cloud Transforms the Model

The public cloud provides services and capabilities that mitigate many of the challenges discussed above. It is a utility-based model of near-infinite resources that are available immediately on demand, with cost only for resources that are actually utilized.

| | |
|---|---|
| **Scale:** | The cloud provides the impression of nearly unlimited capacity as a result of vast resource shared across millions of users. Cloud vendors have implemented "auto-scaling," to enable users to automatically scale up when additional capacity or performance is needed and scale down when demand subsides. Storage is provided at the time it is needed, with the required performance and cost. Overprovisioning is eliminated, potentially saving users a significant amount of money. |
| **Resiliency:** | The cloud provides expanded models for building applications that must be constantly online, and designing systems resilient to disruption when components fail or changes are introduced. Some examples include auto-scaling; load balancing applications across data centers and geographic regions; distributing copies of applications to multiple domestic and global locations and turning them on or off as needed; changing and pre-validating in isolation, testing and scheduling the release. Furthermore, every location can be identically configured and automatically verify the same code and data. Operating from a "backup copy" of an application can turn into an every day standard operating model instead of the complex, orchestrated event it is today. |

| | |
|---|---|
| **Privacy:** | The privacy design features of the public cloud enable financial market infrastructures to protect client data and address local jurisdictional rules regarding privacy. For example, the foundation of the cloud is the internal walls that allow pooled (multi-tenancy) and shared resources (virtualization) to keep individual environments separate, independent and isolated from and unaware of each other, even if the same physical resources are shared. In addition, unlimited "private" segments can be created for network, compute and/or data resources while giving users access to a wide range of encryption technologies and tools that can be tailored to their specific requirements. Cloud vendors also provide data centers in many regional and global geographic areas to address regulatory requirements. Encryption keys can be managed by the financial market infrastructures, further securing access to client data. |
| **Security:** | The public cloud is built to support the most stringent security requirements at every level. Security models can be established and enforced within applications using best practices, standards, data encryption, and API logging – all required and validated. The use of public cloud vendors allows an enterprise to distribute encrypted applications and data across millions of servers in dozens of data centers, making it almost impossible to identify the physical resources being used by a specific firm. |
| **Cost & Time to Market:** | For most applications and configurations, the cloud will cost less. The scale, resource sharing, automation and metering of resources consumed contribute to lowering the costs of technology infrastructure for typical system requirements. This allows for instant experimentation, immediate results and an efficient exit, creating a dynamic culture where the user can test virtually any scenario, new software tool or alternative configuration without a lengthy purchase and provisioning cycle. These features support faster time to market, more reliable products and lower requirements for support and maintenance. |

## How the Public Cloud Improves Security

**Email:** The cloud can improve security by isolating corporate email, a primary entry point for malware and other cyber-threats. Moving email to the cloud severs the link to other internal resources, such as central authorization, and entitlement systems and collaboration tools. In addition, email attachments can be put into an isolated file system to prevent exposing other internal file systems to malware.

**Isolated production environments:** Leveraging the cloud allows development and testing environments to be created completely separate from production networks and applications. Security and stability of production environments can be significantly improved by removing all contact with non-production applications and users.

**On demand testing:** The cloud improves the agility of an organization to test new technologies with alternative hardware configurations in minutes, which is not possible in most on-premises data centers. As an example, DTCC conducted a big data tool evaluation using Hadoop technology in the cloud, and executed testing with 8 core machines, then 16, 32 and 64 core machines, all on demand, all within a few days.

In summary, there are many benefits of building applications in the cloud, including faster time to market, lower development costs, expanded testing, enhanced controls, automatic scaling and failover and quicker provisioning. However, just moving applications that were originally developed within the corporate data center to the cloud, a model known as "lift and shift," will not immediately deliver these benefits. In fact, it is possible migrating to the cloud could introduce additional complexity. Therefore, a cloud strategy requires examining each application carefully to ensure that the proposed benefits are achievable. DTCC believes that re-architecting applications so they are native to the cloud is the best approach.

# PUBLIC POLICY AND REGULATORY CONSIDERATIONS FOR USING CLOUD VENDORS

DTCC and other market infrastructures provide clearing and settlement services that support risk management and proper completion of securities transactions in the U.S. capital markets. Additionally, DTCC provides a variety of data services, such as regulatory trade reporting required of market participants in the derivatives markets.[2]

Due to the systemic importance of market infrastructures, public policy and compliance considerations must be addressed when considering whether to move processing functions to an outsourced or public cloud environment. In addition, a market infrastructure's use of a cloud vendor is similar to its use of any third-party vendor and raises many of the same issues. In this respect, these considerations are familiar to the regulatory community.

## Regulatory Responsibilities of Market Infrastructures

Broadly speaking, governance of cloud services expands upon guidance previously provided by relevant market and prudential regulators to regulated market infrastructures. The overall responsibility for the services and the data reside with the market infrastructure, so the governance, such as policy definition, management (including contracts, service levels, and monitoring), SLA reviews and control audits, all continue to be owned completely by the market infrastructure. With these principles in mind, the following issues reflect the primary policy and regulatory considerations, as well as security factors a market infrastructure must address when leveraging the cloud.

- **Data protection and sensitivity.** The regulated market infrastructure's security policy for outsourcing and cloud services must ensure adequate safeguards to protect the confidentiality of data. Among the issues the policy needs to cover is whether the cloud adequately protects and/or encrypts sensitive data and encryption key management concerns. Market infrastructures must recognize that, regardless of the rigor of a cloud vendor's data security, it holds complete responsibility for ownership and protection of its data.

2 DTCC has three legal entities that are registered with the Securities and Exchange Commission (SEC) as a "covered clearing agency," and another registered with the U.S. Commodity Futures Trading Commission (CFTC) as a "swap data repository," respectively, with additional regulatory registration in other global regions. In each of those jurisdictions, DTCC must comply with a host of regulatory responsibilities that reflect the importance of these services from a market integrity and functionality perspective, among other reasons. Regarding its responsibilities as a covered clearing agency, DTCC's provision of services must be consistent with the Securities Exchange Act. Among other things, the Securities Exchange Act provides that the Commission must have due regard for the public interest, the protection of investors, the safeguarding of securities and funds, and maintenance of fair competition among brokers and dealers, clearing agencies, and transfer agents in supervising the U.S. clearance and settlement system. See 15 U.S.C. 78q-1(a)(2)(A). DTCC also provides some services that are not considered activities subject to regulatory oversight by U.S. or non-U.S. market regulators.

- **Data integrity.** Market infrastructures must take steps to ensure data integrity to prevent data from being altered or destroyed under all circumstances. The market infrastructure must be able to establish procedures to validate and verify the integrity of its outsourced and cloud hosted data, in addition to controlling data retention periods.
- **Continuity of Service.** Market infrastructures must ensure that data is available when needed. The cloud vendor must have adequate plans to respond to disasters and provide continuous service and pledge to make available essential communications links. It is incumbent on the market infrastructure to develop formal policies related to redundancy and the availability of backup data.
- **Auditing issues.** The compliance function of market infrastructures should require that cloud vendors have familiarity complying with the demands of regulated entities and can contractually meet current requirements, particularly related to required reporting and safeguarding of sensitive information. The regulated market infrastructure should use appropriate audit tools in order to ensure that the cloud vendor's internal controls are adequate.

Again, these issues stem from specific regulatory obligations within each jurisdiction in which a market infrastructure operates.

## Policy and Compliance Guidance from Relevant Authorities

In recent years, financial regulators globally have issued general guidance for addressing cyber security risk, including matters specific to public cloud computing. The various guidance documents represent best practices, and the guidelines aimed at cloud computing demonstrate a clear precedent for a financial institution's practice of outsourcing relevant operations to a public cloud provider. By issuing this guidance, the authorities are acknowledging the appropriateness of using cloud vendors so long as best practices are being followed and compliance obligations are being met.[3]

While cloud vendors and their related software services may have the most sophisticated security capabilities, the controls, configurations and access management are still overseen by the customer. In other words, the security responsibility is not outsourced. Fortunately, the decade-long maturing of cloud services, along with the active engagement of many regulatory and security experts have produced an abundance of guidance for securing cloud implementations.

The following discussion covers the various guidance documents issued by authorities globally. It's import-

3 For example, the SEC promulgated Regulatory Systems Compliance and Integrity (Reg SCI), and the CFTC promulgated a "systems safeguards" regulation that applies to SDRs. Many of the requirements that follow from these regulations also would be impacted by a market infrastructure's use of cloud vendors, and generally fall into the same key categories outlined above. Likewise, non-U.S. supervisors also impose cyber-specific regulatory responsibilities.

ant to note that some jurisdictions recommend "in-region" data residence and processing, which can often be met by global vendors that have deployed data centers in-region, sometimes in collaboration with a local partner. Some jurisdictions, however, have issued guidance that is clearly intended to require the use of a local, domestic "cloud vendor." These vendors are often limited by the size of their local audience and less likely to achieve the scale and efficiencies of global vendors, which could negatively impact the reliability and resiliency of the vendor's service offering.

## Guidance from U.S. Authorities

**National Institute of Standards and Technology (NIST).** The NIST issued guidelines in January 2012 aimed at users of public cloud computing services, specifically addressing security and privacy issues. The document offers recommendations that firms should consider when outsourcing data, applications and infrastructure to a public cloud environment. According to the NIST, financial institutions should plan and understand the public cloud computing environment and the solutions offered by a provider – similar to how they engage with other third-party service providers. The guidance notes that the cloud providers' default offerings generally do not reflect an organization's security and privacy needs and they should require that solutions are configured, deployed and managed to meet their security, privacy and other requirements.

The NIST guidance contemplates the client-side environment, noting that the service provider side of the arrangement typically is emphasized. The guidance states that organizations should review existing security and privacy measures and employ additional ones, if necessary, to secure the client side. As discussed, this problem may be mitigated if the institution maintains private communication connections to the cloud and does not use public internet access. Finally, the guidance notes that organizations employing cloud vendors maintain accountability over the privacy and security of data and applications deployed in public cloud computing environments. This is a crucial issue that ensures that institutions are incentivized to find the best, most secure cloud service provider and environment possible.

**Federal Financial Institutions Examination Council (FFIEC).** In July 2012, the FFIEC released a public statement for financial institutions on outsourced cloud computing. The document detailed comprehensive risk management controls for third-party cloud service providers including:

(i) conducting adequate due diligence to assess the provider's controls;

(ii) properly managing the cloud vendor, implementing additional controls where necessary to protect sensitive data, and implementing contracts and service-level agreements that are specific as to dispute resolution and the ownership, location, and format of the data;

(iii) determining the adequacy of a provider's internal controls and assessing whether those controls are functioning appropriately;

(iv) revising information security policies and practices to incorporate the activities related to a cloud computing service provider, and continuously monitoring the provider if necessary;

(v) mitigating legal, regulatory, and reputational considerations, including by specifying the providers' obligations with respect to institutions' responsibilities for compliance with privacy laws, for responding to and reporting security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches; and

(vi) determining whether the provider and the provider's network carriers have adequate plans and resources to ensure an institution's continuity of operations.

**Federal Reserve Guidance on Managing Outsourcing Risk.** In December 2013, the Federal Reserve issued Guidance on Managing Outsourcing Risk, which lists guidelines for ensuring that third-party service providers, including cloud vendors, comply with applicable regulatory obligations. According to the Guidance, the financial institution should conduct a risk assessment prior to engaging with a vendor to determine whether outsourcing is consistent with its overall strategy. Proper due diligence of the provider should include a review of its background, reputation, strategy, financial performance and condition, and operations and internal controls.

The Guidance also notes that the contract should include provisions related to confidentiality and data security and emphasizes the importance of the protection of consumer information and the financial institution's confidential information. Service providers, including cloud vendors, should provide the same customer information protections as provided by the financial institution, and their information security processes should map directly to the institution's processes. In addition, a service provider's use of information should be limited to what is necessary to provide the service.

Furthermore, the Guidance states that financial institutions should have processes and procedures in place to oversee and monitor their service providers and develop contingency plans for outsourced activities. In addition, providers should have adequate and effective disaster recovery and business continuity plans that align with the institution's protocols.

**Federal Risk and Authorization Management Program ("FedRAMP").** In 2014, FedRAMP was established to provide a standardized approach to security assessment, authorization and continuous monitoring of cloud products and services. One of its goals is to accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations. FedRAMP is the result of close collaboration

with cyber-security and cloud experts from General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officers Council, and its working groups, as well as private industry.

## Special U.S. considerations: Reg. SCI and CFTC Systems Safeguards

Reg. SCI is a disclosure-based rule that applies to certain market infrastructures and other self-regulatory organizations. Under the rule, market infrastructures are required to report to its members and/or to the SEC, significant systems disruptions, material changes to systems and an annual review of their compliance with Reg. SCI. Market infrastructures also may have to report data breaches experienced by their cloud service providers. After its adoption, the SEC issued Staff Guidance that relied on an expansive set of industry guidance to clarify some of the rule requirements, including the NIST guidelines on security and privacy in public cloud computing.

The CFTC's system-safeguards rules for swap data dovetail with these practices and contemplate oversight of service providers, potentially including cloud vendors, as part of an operational risk management program.

## Guidance from Non-U.S. Authorities and Consortia

**European Union Agency for Network and Information Security (ENISA).** "Cloud Standards and Security," a document posted by ENISA in August 2014, provides a broad overview of different technologies supporting cloud computing and the security standards associated with them. This document includes a mapping of the standards and cloud models and the application of those standards across the procurement lifecycle. It also includes an overview description of the standards and an index of relevant links into the standards documents.

In 2015, ENISA noted that many data protection authorities across the EU have issued compliance information on cloud computing and personal data legislation in their jurisdictions, including the UK, France, Sweden, Italy, Ireland and Germany, according to its guide on cloud security for SMEs[4]. ENISA gives examples of different types of legal requirements that may have an impact on cloud service providers, such as on-site audits, physically separated systems, third party outsourcing conditions, cross-border data processing and use of specific hardware for certain operations.

**U.K. Financial Conduct Authority.** The Financial Conduct Authority of the United Kingdom issued

4 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes/at_download/fullReport

"FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services,"[5] in July 2016 with an update in November 2016. This document includes "finalized guidance" with intent to clarify requirements on firms when outsourcing to the cloud and other third-party IT services. The document addresses feedback by financial institutions over uncertainty about the rules becoming a barrier to using the cloud. For example, the "Access to business premises" section clarifies the requirement on the need to "see the servers:"

> SYSC 8 requires relevant firms to have "effective access to data related to the outsourcing activities, as well as to the business premises of the service provider."
>
> We regard "business premises" as a broad term, encompassing a range of premises. This may include head offices, operations centres, but does not necessarily include data centres.

**Singapore.** In July 2016, the Monetary Authority of Singapore (MAS) issued new guidelines that specify that public cloud computing is a form of outsourcing. Accordingly, the guidelines state that financial institutions must perform the necessary due diligence and apply sound governance and risk management practices. For cloud service providers in particular, institutions should take active steps to address risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing.

**Hong Kong.** In November 2013, the Office of the Government Chief Information Officer (OGCIO) published a practice guide for procuring cloud services to assist companies in understanding and evaluating the risks and benefits of cloud computing. The guide explains the different types of cloud computing service models (SaaS, PaaS, and IaaS) as well as the deployment models (public cloud, private cloud, community cloud and hybrid cloud). The guide states that cloud computing can be viewed as an extended form of traditional outsourcing activity and sets forth security controls for both cloud users and cloud service providers to consider. The document also includes guidance on executing a service-level agreement and how to compare a service provider against industry best practices.

## Official Sector and SRO Use of Cloud

As noted above, the public cloud ecosystem has been deployed in many global locations by the largest commercial vendors. The public sector and quasi-government entities, particularly in the U.S., have become users of the public cloud as well. In fact, U.S. government agencies that have supervisory responsibility over market infrastructures and the self-regulatory organization, the Financial Industry Regulatory

5 https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

Authority (FINRA), have begun using the public cloud. This precedent is instructive given the fact that, in many cases, the data ingested by government agencies is sensitive and confidential. Consequently, the official sector's interest in protecting the confidentiality and integrity of data, as well as continuity of service of the vendor, are much the same. Appendix A describes the government agencies around the globe that use cloud services.

## DTCC's Strategy to Leverage the Cloud

DTCC has been leveraging cloud services for almost five years and believes the cloud represents a viable alternative to corporate data centers. The maturation, expanded offerings and enormous scale of the technology, resolve the privacy and security challenges of cyber-threats, potential flash crash type market disruptions and the cost challenges facing many financial firms today. DTCC believes cloud computing has moved past a tipping point, prompting the firm to pursue a strategy of building a cloud ecosystem with partner vendors that support best practices and standards. DTCC is taking this step because it is confident that the security, scalability, resiliency, recoverability and cost of applications in the cloud are better than almost any private enterprise could achieve on its own. DTCC also believes that business services, delivered by applications written to take advantage of the infinite resources, resiliency, and global reach of the cloud, have a significant advantage over legacy applications using traditional models in private data centers. We believe that gap will continue to widen over time.

As a critical provider of market infrastructure, DTCC is required by regulatory mandate to comply with the highest and strictest levels of recommended controls and best practices for the use of outsourced technology, including its cloud vendor relationships. DTCC, which owns responsibility for the data it holds and its related processing, regards cloud vendors as operations and technology providers subject to contractual and service level agreements. DTCC takes seriously its responsibility to be in full compliance with all relevant regulatory requirements and pledges to work in collaboration with its supervisors to achieve this. In short, DTCC will undertake this work with a singular focus on ensuring its actions support the highest level of market safety and soundness.

# APPENDIX A – OFFICIAL SECTOR AND SRO USE OF THE CLOUD

## U.S. Agencies Using the Cloud

**Obama Administration Policy.** On February 8, 2011, U.S. Chief Information Officer Vivek Kundra published the Obama Administration's Federal Cloud Computing Strategy, which empowered federal agencies to provide reliable, innovative services quickly within budget constraints. In response, the Obama Administration issued a Cloud First policy, which sought to accelerate the adoption of cloud computing services by government agencies by directing them to evaluate cloud computing options before making new IT investments. A key advantage of the policy is that it enabled the agencies to rapidly access IT innovations developed in the private sector without having to obtain significant hardware to access these services.

The Federal Cloud Computing Strategy was designed to "articulate the benefits, considerations, and trade-offs of cloud computing and provide a decision framework and case examples to support agencies in migrating towards cloud computing; highlight cloud computing implementation resources; and identify federal government activities and roles and responsibilities for catalyzing cloud adoption." While the cloud first policy requires agencies to migrate activities to the cloud, they have a responsibility to determine whether the cloud environment offers adequate security safeguards.

At the time of this writing, there has been no indication that the Trump Administration will reverse or change the Cloud First policy outlined by the previous administration.

**U.S. Government General Services Administration (GSA).** The U.S. Government General Services Administration (GSA) provides direct access to Cloud IT Services for all U.S. agencies and offers support and guidelines for moving to the cloud. This includes corporate services that are provisioned in bulk (e.g. email) as well as access to IaaS and PaaS that are in compliance with guidelines and best practices. Many U.S. government agencies, including the U.S. Army, Air Force, Navy, Department of Justice, National Security Agency, U.S. Department of Agriculture, U.S. Department of Education, National Aeronautics and Space Administration (NASA) and more have moved portions of their services to the cloud.

**SEC's Use of Cloud.** The SEC has complied with its obligation to consider cloud computing by migrating a number of applications to the cloud, including its response tracking system, a CRM application, and the MIDAS tool. In the agency's 2015 Annual Report, the SEC's Office of Information Technology (OIT) reported that it "is continuing to develop and add value to existing advanced data analytics capabilities and the underlying storage and compute infrastructure." The 2015 Annual Report also notes that "OIT is supporting the Enforcement Division and Office of Compliance Inspections and Examinations in developing a FedRAMP-certified, cloud deployment of a High Performance Compute Infrastructure (HPCI) for 'Big Data' analytics." These initiatives will undoubtedly rely on sensitive and proprietary data, suggesting that

SEC staff have become comfortable with security on large public cloud vendors.

In an April 2015 interview, Pam Dyson, SEC CIO, discussed data security on the cloud, noting that "all information is stored securely in the clouds so I know that there's some personal information there, but we have secure parameters around the information to ensure that it's secure at all times." Similar to Tony Scott, Dyson also has observed that data stored on the cloud is secure. In a September 2016 article regarding the SEC's migration to the cloud, Dyson stated,

> *"We continue to take a very pragmatic approach to the cloud. Two years ago, the discussion was all around security, is data as secure in the cloud as it is on-prem? I think we've overcome that across the federal government. FedRAMP has certainly helped put us in that space where we understand that data is secure. For us it's more about the business use of the data and the business use of the cloud. Can we use the same tools and get the same performance from a cloud instance that we can on-prem?"*

**CFTC's Use of the Cloud.** The CFTC plans to move some of its activities to a private cloud, according to its 2014-2018 Information Technology Strategic Plan (ITSP), which noted that "a private cloud computing environment will enable CFTC to consolidate processing and networking services in a highly virtualized environment. This environment will deliver high levels of availability, redundancy, and business continuity, while also allowing all information to be managed and made available centrally."

Unlike most initiatives that are hosted on a public cloud, the CFTC plans to utilize public and private clouds. Although a private cloud can be expensive if it replicates an existing on-premises infrastructure, the CFTC can take advantage of a private cloud configuration because the size of its operations is sufficiently large that many of the advantages associated with public cloud computing can be realized in a private cloud. By contrast, market infrastructures are unlikely to find private clouds cost-effective because they operate on much smaller scales.

**FINRA's Use of Cloud.** Perhaps more than any other entity – official or commercial – FINRA's use of the cloud is instructive as it relates for market infrastructures. Like a covered clearing agency in the U.S., FINRA is a self- regulated organization (SRO) and also subject to the SEC's Reg SCI requirements. Notwithstanding these obligations, FINRA has moved about 75-percent of its operations to Amazon Web

Services (AWS) to capture, analyze and store a daily influx of 75 billion records. AWS has created a flexible platform for FINRA that can be used to develop tools so that its analysts can query multi-petabyte data sets, thereby enabling them to efficiently monitor and regulate financial trading practices.

In a speech at the 2016 AWS "re:Invent" Conference, Steve Randich, Executive Vice President and Chief Information Officer at FINRA, stated, "private cloud [is] often pushed by people that want to stay in their comfort zone." He also observed that "cyber security is better in the [public] cloud than it is in private data centers." With respect to resiliency and disaster recovery, Randich further stated, "Given that our data is replicated and processed ubiquitously and virtuously across tens of data centers, the whole model about resiliency and disaster recovery is changed. And with public cloud computing done right, the resiliency, you just can't compare to a public [on-prem] data center."

As a part of FINRA's substantial migration to the cloud, it has indicated that, if it ultimately becomes responsible for maintaining and operating the Consolidated Audit Trail (CAT), it plans to host it in the cloud. The CAT is a comprehensive audit trail that will track orders throughout their lifecycle and identify the broker-dealers handling them, allowing regulators to track activity throughout U.S. securities markets. Broker-dealers will be required to report into the CAT quotes, orders, executions, and allocations, as well as customer data associated with these orders. To ensure that it is secure, the CAT plan processor will adopt all relevant standards from the NIST Cyber Security Framework and align with current industry standards and best practices as they evolve. The CAT processor's information security program will be reviewed at least annually by the Operating Committee.

## Non-U.S. Agencies in the Cloud

U.S.-based deployments meet the local security, privacy and jurisdictional requirements for cloud data hosting and processing. While the U.S. government and markets have been the most pro-active adopters of cloud computing, regional governments and markets globally have been slower to tap these services.

**European Union.** The current European policy on cloud computing is contained in the EU's Digital Market Strategy. Under this policy, the EU launched two cloud computing projects: the European Cloud Initiative and the Initiative on Building a European Data Economy. These two programs support the use of the cloud for storing scientific data and building a digital infrastructure for the free flow of data in Europe. The EU hopes the Digital Single Market will accelerate the use of cloud computing across all economic sectors and unlock the scale necessary for cloud computing to reach its full potential in Europe. According to the latest Eurostat data available, as of the end of 2014, 19-percent of EU enterprises used cloud computing. Estimates indicate that the European cloud market could grow from €9.5bn in 2013 to €44.8bn by 2020—or five times the market size.

ENISA recently published a report identifying EU member states with operational government cloud

infrastructures.[6] In 2013, ENISA noted that it expected around 80% of organizations to be dependent on cloud computing in a few years. Of the countries that have cloud strategies, ENISA classified the U.K., Spain and France as "early adopters," meaning they have a cloud strategy, they have made specific decisions on how to implement the governmental cloud and they have a initiatives already running on the cloud. The U.K. is using a public cloud, while France and Spain are using a private cloud. The Netherlands, Denmark, Sweden, and Greece—classified as "well-informed"—also are planning to adopt some services from public cloud providers, although cloud implementation was at the design or prototype stage as of November 2013. Finally, the report identifies Italy, Turkey, and Portugal as "innovators" that already have a few cloud-based services running at a local level or in specific sectors.

ENISA published a report in February 2015 on four case studies for national cloud security approaches: Estonia, Greece, Spain, and the U.K. The report outlines a security framework containing actions that each member state should follow when implementing a secure government cloud. The report states that the framework has been validated through the four case studies.

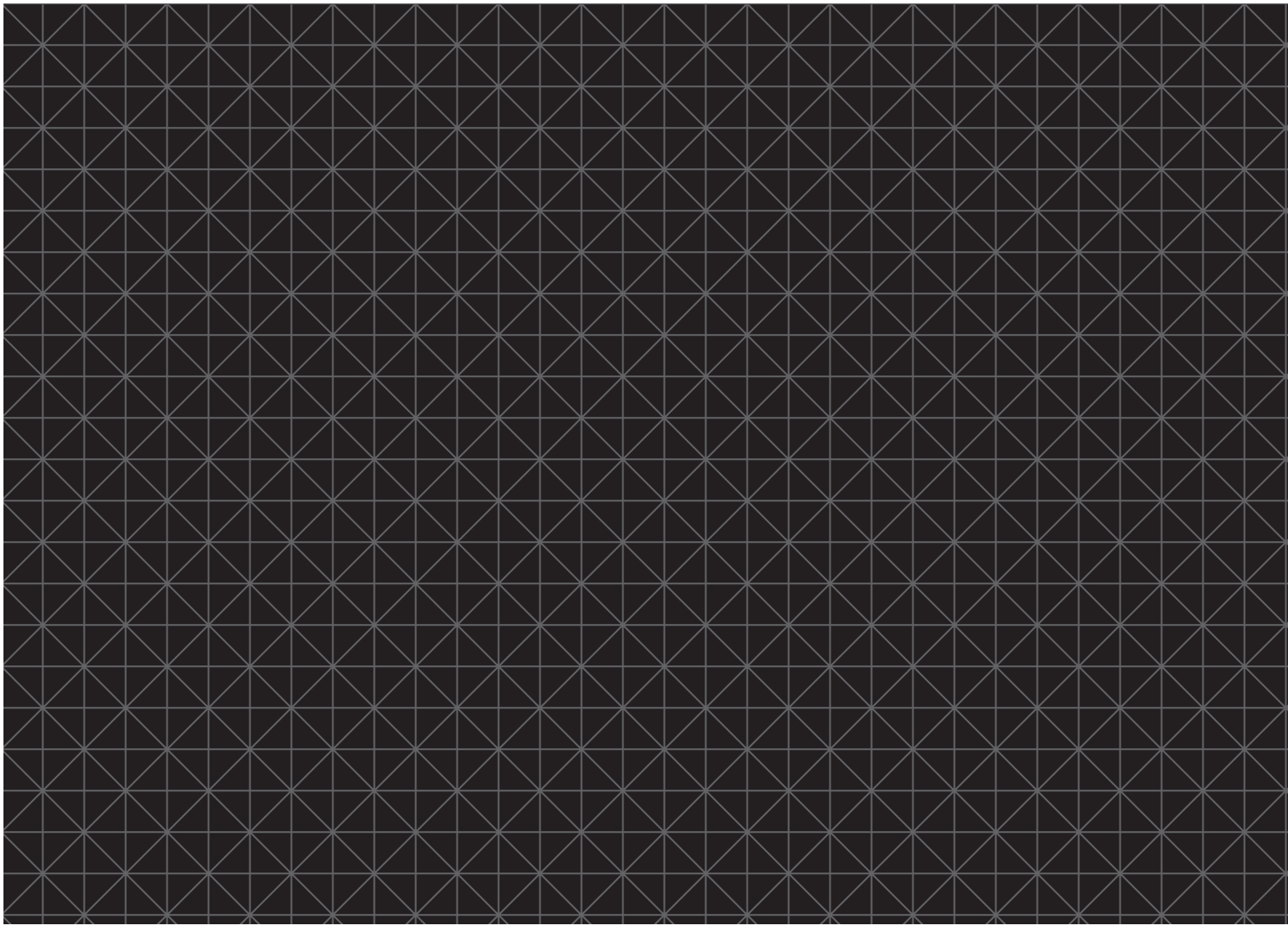
**Canada.** In October 2016, the Canadian government launched the Cloud Adoption Strategy aimed at ensuring the successful adoption of cloud computing services and usage within the Canadian public and private sector. The Strategy describes the future vision for a Canadian public sector community cloud, which would bring together Canadian public sector buyers with public cloud service providers, brokered and security-assessed by the government. The Strategy sets out the security approach for firms and government to adopt use of the cloud. It also seeks to create a cloud workforce to educate and promote understanding of cloud computing.

**Singapore.** The Singapore government has created the Infocomm Media Development Authority (IMDA), which, among other things, develops strategies for the use of cloud computing. The IMDA publishes a booklet annually that provides an overview of Singapore's cloud computing ecosystem and strategies the government intends to develop to promote and further adopt use of the cloud.

**Hong Kong.** The Office of the Government of Hong Kong Special Administrative Region has a cloud computing policy, a forum of cloud computing standards and experts and a listing of vendors providing public cloud services for government bureaus and departments. The list of vendors, which was established in May 2012, allows government agencies to acquire public cloud services from over 40 service providers with over 300 cloud service options. Government public cloud service providers must have at least one year of cloud service experience and apply for inclusion as an approved vendor.

---

6 See, e.g., "Good Practice Guide for Securely Deploying Government Clouds" (Nov. 2013), available at https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds.



13161 ER 052017