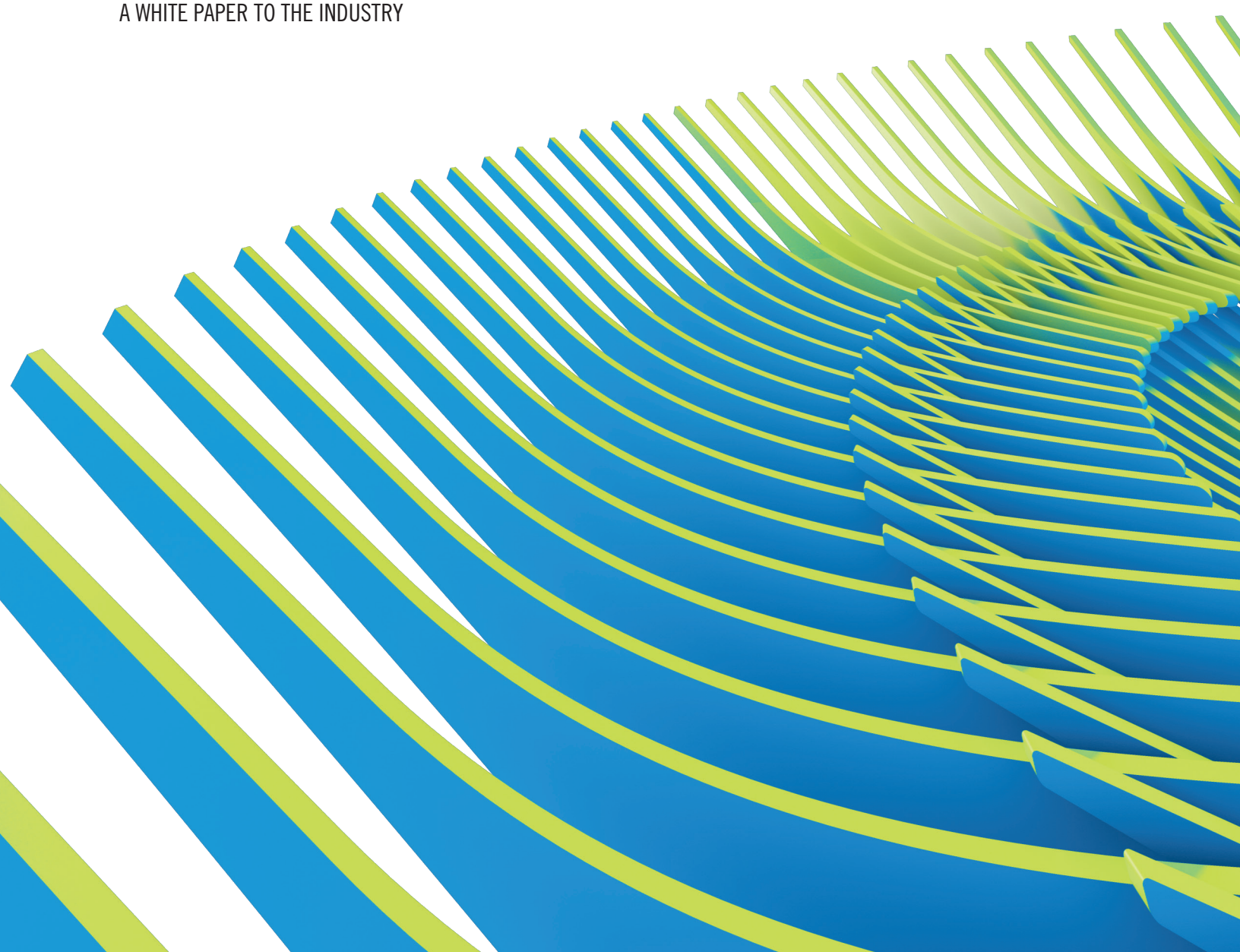
NOVEMBER 2020

CLOUD TECHNOLOGY: POWERFUL AND EVOLVING

A WHITE PAPER TO THE INDUSTRY



CONTENTS

EXECUTIVE SUMMARY

For decades, large financial institutions, including market infrastructure providers like DTCC, relied on private data centers to host and operate their core platforms and systems. But today, enterprises across the globe -- from new fintech startups to established regulated entities and from government agencies to regulatory authorities -- are increasingly outsourcing corporate and business applications to a public cloud service provider (CSP) using a shared, multi-tenant hosting infrastructure.

For some firms and applications, however, on-premises data centers continue to be used due to business, financial, network latency, application performance as well as regulatory considerations. Indeed, initial enthusiasm for large scale transitions of entire application portfolios to the public cloud has subsided to a more practical pace amid deeper consideration of the specific requirements for individual business solutions. Among the points in question: the state and cost of the existing solution supporting the business service, the appropriateness for business purposes, the maintenance of data security and privacy in accordance with relevant laws and the ability of the cloud to support business clients' resiliency and performance demands.

Indeed, initial enthusiasm for large scale transitions of entire application portfolios to the public cloud has subsided to a more practical pace amid deeper consideration of the specific requirements for individual business solutions.

The financial industry's understanding of cloud computing has evolved through many implementations with requirements for handling massive data sets, extremely low latency transaction processing, highly complex and integrated application portfolios and differing regulatory expectations across geographic regions. Meeting the highest thresholds of controls and monitoring, as established by market regulators, also raised the bar for CSPs. Financial institutions are held to high standards by regulators around the world and therefore, CSPs are now expected to provide infrastructure and services that meet or exceed expectations and requirements for cloud business continuity and resiliency. For years, those standards were enforced via capabilities established in on-premises data centers. CSPs that were unable to support these standards were historically not viable vendor options for the core processing applications of regulated entities.

The financial industry and CSPs have also learned from highly publicized security and control failures which resulted in financial and reputational damage. Enormous privacy failures exposing personal credentials, credit and health information from systems and data hosted at CSPs have occurred. The CSP provides the hosting services and infrastructure security capabilities, but it is the responsibility of the financial institution using the CSP to implement and monitor those capabilities. These breaches reminded financial institutions of the necessity for internal risk assessment and management processes in addition to robust audit functions and accountability within all levels of the organization. They also realized that there is no backstop for strong security practices on shared, multi-user infrastructure. CSPs have learned that reputations are built on client experiences and in the financial industry, trust and confidence are critical.

In 2017, DTCC released a white paper, Moving Financial Market Infrastructure to the Cloud, outlining its views on the benefits of public cloud platforms and relevant regulatory considerations for financial institutions. That was also the year DTCC embarked on a new technology strategy that included broader adoption of cloud as a primary hosting platform.

In the three years since our 2017 paper, financial industry use of cloud exploded as firms deployed a wide range of applications and services. For fintechs, the cloud removed an enormous barrier to entry and assisted in bringing client experiences to market at tremendous speed. For established financial institutions, the scale and processing power offered by CSPs cannot be matched, even by the largest enterprise data centers. Across the industry, firms are outsourcing undifferentiated commodity corporate functions to a few dominant SaaS providers.

Regulators and legislators globally have also advanced their own perspectives regarding cloud services. Cloud services are increasingly used by regulated entities, along with government agencies, including the policymaking community. Across jurisdictions, regulators are assessing challenges and working closely with regulated entities as the industry-wide use of cloud services expands. DTCC's 2017 white paper outlined regulatory responsibilities and policy guidance for financial market infrastructures. These responsibilities and guidance remain valid today and include a continued emphasis on financial institutions' engagement of CSPs.

Over the past three years, DTCC has made significant advances establishing cloud engineering as a core skill, and steadily shifted workloads to cloud hosting. Along the way, DTCC, like other institutions, has learned from its experience that cloud hosting can bring significant benefits to many classes of application.

Our cloud journey reinforced the importance of key considerations that have caused DTCC to adjust the pace with which we are approaching cloud adoption. Those considerations include:

A. The need for strong governance, controls, monitoring and alerting as table stakes.
B. A focus on extreme automation to eliminate manual steps for infrastructure provisioning as well as application releases.
C. Ensuring resiliency is engineered into the foundational application architecture.
D. Building out our resiliency testing through chaos engineering and failure mode analysis.
E. Developing clear enterprise guidance, based on business requirements and application suitability, for when to go to cloud, which cloud to go to, when to go portable and when to go cloud native.
F. Updating contracts, defining exit strategies and working with vendors as DTCC meets its regulatory responsibilities.

As we shared our experiences with clients, many suggested that others in the industry could learn and build better from our experience. We are pleased to share our experiences and best practices in this white paper. If you would like to discuss this white paper with DTCC's Technology and Research Innovation Team, please contact CloudInnovation@dtcc.com.

DTCC AND THE CLOUD

DTCC has played a pivotal role for more than 45 years in protecting and supporting the growth of the global financial markets, tackling some of the industry's biggest operational challenges while processing millions of securities transactions every day. User owned and governed, DTCC's clearing and depository subsidiaries are deemed Systemically Important Financial Market Utilities (SIFMU) in the U.S.[1] DTCC also provides a range of post-trade services, including trade repositories globally that provide compliance reporting for derivatives transactions across all asset classes.

DTCC began its cloud journey in 2012 with a CSP-hosted public data reporting application. The years since saw expanding usage of cloud services to run specific business applications, while at the same time, DTCC worked to develop and advance cloud-specific management and cloud governance capabilities. DTCC has incrementally advanced its cloud capabilities following that first step in 2012, primarily focusing on three broad categories of opportunity:

1. Corporate functions and services such as email, HR, finance and client relationship management have primarily been outsourced to leverage SaaS ("Software as a Service") cloud model.

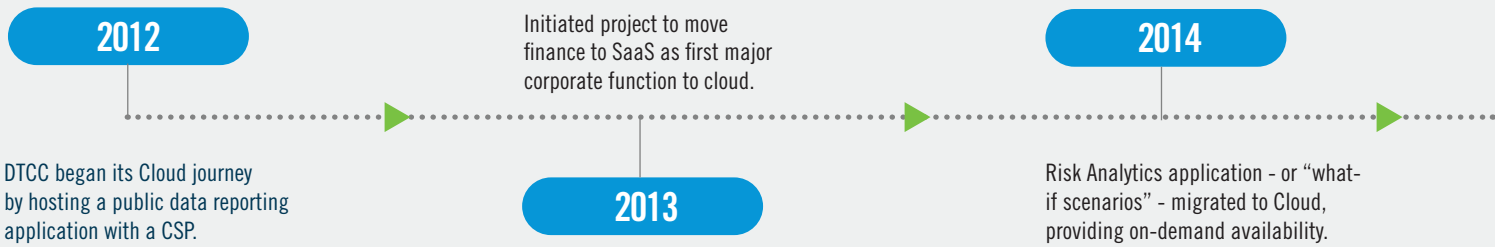
2. A priority for cloud migration has been data-oriented applications, including data storage, analytics, reporting and archiving. DTCC can manage massive amounts of data due to the benefits of CSP economies of scale – with virtually unlimited storage – and built-in encryption.

3. Development and testing environments for DTCC's distributed systems also migrated to the cloud. These environments, which support the development and testing of DTCC's business applications, constitute the large majority of demand on DTCC's IT infrastructure. Moving this demand to cloud hosting and automating the majority of provisioning using cloud automation tools removed a significant physical equipment and manual burden.

As part of these efforts, DTCC designed and prototyped a number of transaction processing applications for potential hosting in the public cloud. The team then evaluated the 'fit-for-purpose' characteristics of the cloud

1 On July 18, 2012, the U.S. Financial Stability Oversight Council (Council) designated, among others, DTCC subsidiaries National Securities Clearing Corporation (NSCC), The Depository Trust Company (DTC) and Fixed Income Clearing Corporation (FICC) as Systemically Important Financial Market Utilities (SIFMUs) under Title VIII of the U.S. Dodd-Frank Act.

DTCC CLOUD JOURNEY



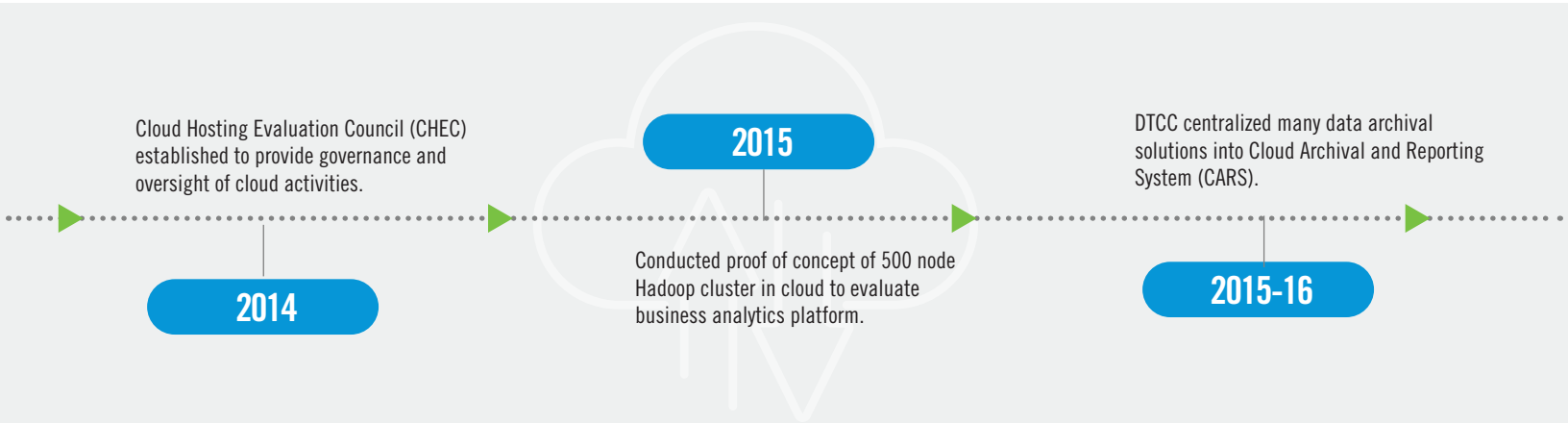
platforms to provide business value and meet DTCC's non-functional requirements for scale, performance, resiliency and security using the prototypes.

DTCC's approach to date has provided a foundational base upon which it intends to continue expanding enterprise-wide use of cloud. It has also created a model to allow DTCC to evaluate tangible business benefits of cloud adoption including potential risk reduction, capital efficiencies, improving time to market and introduction of new capabilities. This approach also allowed DTCC to test its governance processes, establish guidelines and support deployment hosting decisions where cloud is, and is not, the approved destination.

SPOTLIGHT: 2017 WHITE PAPER CONCLUDED THAT CLOUD COMPUTING MOVED PAST A TIPPING POINT OF MATURITY

In our 2017 white paper, "Moving Financial Market Infrastructure to the Cloud," DTCC asserted that the capabilities, resiliency and security of services provided by cloud vendors had surpassed on-premise capabilities. The paper shared our perspective on the benefits of the public cloud platform and relevant regulatory considerations to utilize cloud vendors and the related policy implications. The paper highlighted 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 – while underscoring that cloud strategies require examining each application to ensure that the proposed benefits are achievable.

Here, in our 2020 white paper, we share our experiences from our cloud journey to date.



BEST PRACTICES FOR EXTERNAL CLOUD HOSTING

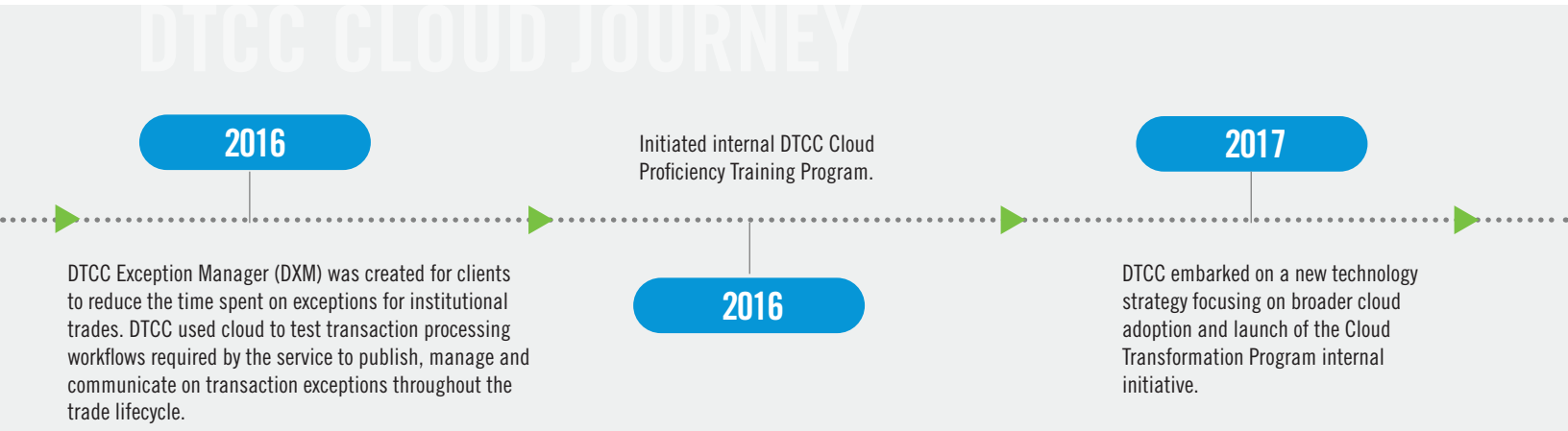
As the financial industry adopted cloud hosting, financial firms, industry advisory boards and associations (e.g., The Cloud Security Alliance) in addition to CSPs worked in coordination so that the core values underpinning financial markets – such as resiliency, security and privacy – are maintained while utilizing cloud services. These efforts led to the establishment of certain best practices critical to realizing the value of cloud, while putting in place the controls and management capabilities necessary to mitigate many risks. These practices can be categorized into four broad themes.

1. **Regulated Entity Obligations:** Cloud strategy, cloud governance, proactive security controls oversight and exit strategy.
2. **Foundational Technology Capabilities:** Architecture, automation, on-premises cloud options, lift and shift vs. design for cloud.
3. **Resilience and Resilience Verification Capabilities:** Failover and disaster recovery, resilience and chaos engineering.
4. **Cloud Vendor Obligations:** Contractual agreement considerations, security considerations, evidence of available capacity and data localization and privacy.

REGULATED ENTITY OBLIGATIONS

A regulated entity is responsible for the oversight, management and operation of its technology solutions. Although outsourcing any operational or technology function may re-locate the activity to third party providers, the entity cannot outsource its regulatory responsibilities. The entity should set the appropriate policies, governance structures and control regimes in place prior to outsourcing any regulated function. As varying regulatory statutes may apply across global jurisdictions, it is incumbent upon the entity to maintain a compliant technology solution, including any externally provided resources.

The regulated entity also has an obligation to its stakeholders to confirm that the technology used for any business process is appropriate to the regulatory and functional requirements of that process. For example, to assist in meeting its obligations DTCC established a *Cloud Business Value Framework* as an internal approach to evaluate whether applications or services are best suited for a cloud environment *[See Appendix B]*.



CLOUD STRATEGY

A firm should define a formal cloud strategy to establish the business purpose and goals of leveraging the cloud. Each financial institution's strategy is unique and may consider: criteria for cloud use, technology employed, services provided, risk posture and tolerance, required or desired functionality, data residency requirements, data classifications eligible for cloud, internal culture and support, time-to-market and financial considerations in addition to regulatory requirements.

GOVERNANCE

Internal oversight, control and management is mandatory for successful implementation of cloud-based applications and services. Governance activities include: cloud business management, vendor management, financial management, risk management, compliance oversight, monitoring and reporting. DTCC employs robust governance along with risk assessment and management practices around its pre-outsourcing process and use of public cloud environments.

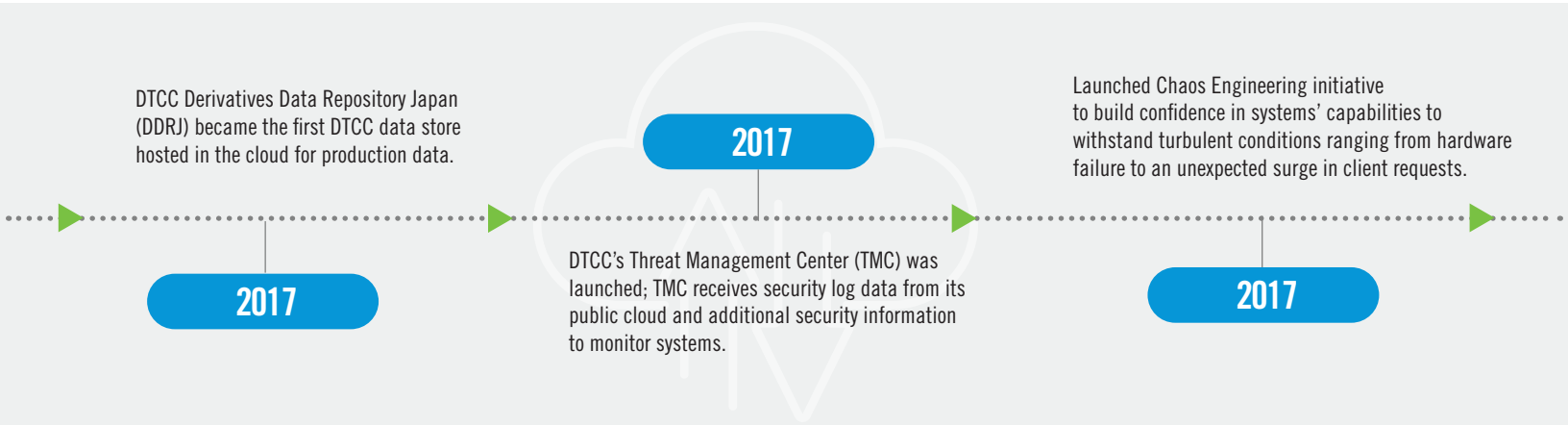
PROACTIVE SECURITY CONTROLS OVERSIGHT

For applications and services hosted in cloud environments, firms should apply their security policies against their cloud environment and define cloud-specific controls to satisfy policy obligations. Additional steps may include conducting ongoing cyber security policy adherence reviews, confirming that cloud resource access privileges are managed and limited to the minimum necessary, and automating controls and performance monitoring.[2]

EXIT STRATEGY

Exit strategies are a recommended best practice for business applications or services hosted externally and are included in regulatory requirements. Financial institutions have and continue to work with CSPs to develop new and innovative ways to build security and resilience into CSP service offerings. However, financial institutions own the resiliency of business services they provide to their clients and should consider including exit strategies in their business continuity planning, appropriate to the risk of the service provided by the CSP.

2 For example, regulated entities may use the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool, which was issued by the regulators in June 2015 as a voluntary self-assessment tool that regulated entities may use to help assess cyber risks and determine cybersecurity preparedness. The Assessment Tool incorporates baseline cybersecurity-related categories from the FFIEC IT Handbook and key concepts from the U.S. Department of Commerce Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as other industry best practices. The FFIEC is a formal U.S. government interagency body composed of the five U.S. federal banking regulators, and is empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions in the United States.



MULTI-CLOUD

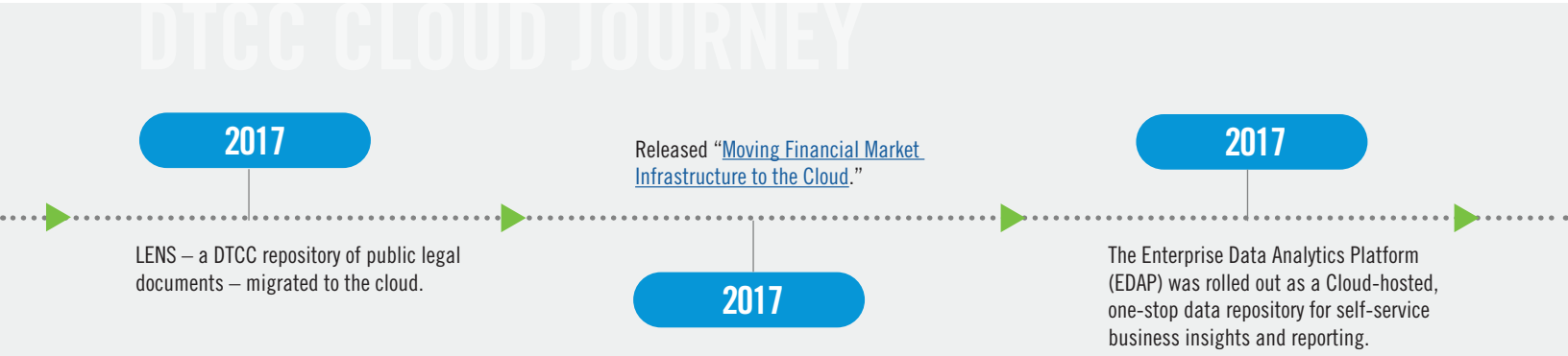
Multi-cloud is generally defined as the use of multiple Cloud platforms from different providers, which may include a combination of on-premises private cloud, and/or multiple public CSPs. The typical approach is to use different providers for different application workloads. While a proposed "aspirational ideal use of multi-cloud" is running the same production workloads on two vendor platforms concurrently, this is not a typical practice, as the complexity would likely increase risks of service disruption and the costs would likely exceed that of implementation in an on-premises data center. DTCC approaches multi-cloud as part of a broader strategy to assess and identify the appropriate cloud fit for specific services and offerings in addition to alignment with DTCC's strategic approach.

FOUNDATIONAL TECHNOLOGY CAPABILITIES

A core transformational feature of the cloud model is that every service is implemented through virtualization software, and every service is available through an API. Pre-cloud, deploying a new application required a lengthy physical infrastructure acquisition process. Cloud technology changed that model overnight and provisioning infrastructure resources is now a micro-second API call away. This provides tremendous power to the application developers, but also creates risks that cloud API's will be called, and cloud resources created, without adhering to the required policies and requirements. All cloud API's should be included in approved architectures and enabled through standard designs and tools to ensure they are used according to policy.

START WITH ARCHITECTURE

Cloud applications must start by leveraging designs and components architected to meet financial institutions' requirements. These designs should have resiliency and security baked into the component, and all modern best practices, such as error checking and retry logic, should be consistently used. Many CSPs provide best practice architecture guidance, which should be integrated into the financial firm's architecture models to create a library of reusable designs and patterns. Trained cloud architects should be available to guide the design of every cloud application. Cloud infrastructure engineers should be available to ensure the cloud application is hosted on appropriate, fit-for-purpose infrastructure resources that can meet pre-determined non-functional requirements, such as scale to peak volume and performance. Validation tools should be in place to require and verify use of approved application architectures and infrastructure components.



AUTOMATION IS BUILT-IN TO CLOUD PLATFORMS, AND IS NOT OPTIONAL

Automating cloud-hosted applications allows financial institutions to have built-in security policies, resiliency designs and management controls. For example, cloud configurations can be provisioned with infrastructure defined and security policies enforced through code. This creates cloud resources with mandated controls, the ability to restrict access and no unexpected privileges. Deployment of configurations that do not conform to policy can be prevented. The preprogrammed controls can be implemented to auto-respond to events or when processing flaws are detected, thereby adding processing resources and provisioning infrastructure when needed.

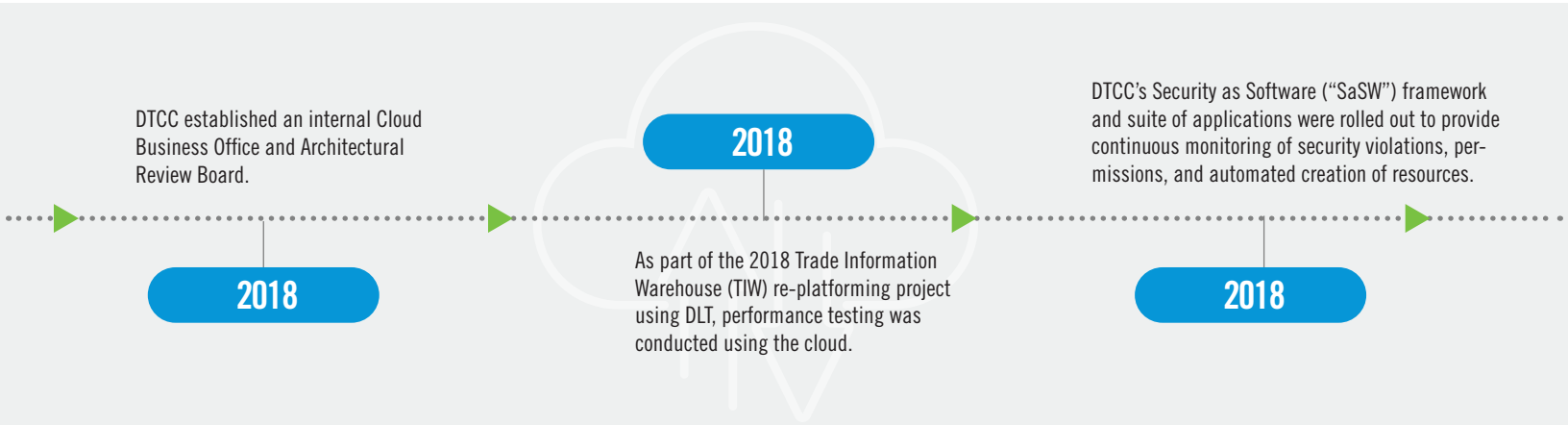
Automation does not come without its challenges. Many parts of infrastructure, including computing resources, storage resources and network resources, need to come together seamlessly for full environment automation, and security and compliance policy requirements must be built in. Another consideration is that "at cloud scale, infrastructure will fail." CSPs own and operate millions of servers and storage devices, and those devices may experience failures and require maintenance. Cloud hosted applications are not permanent and running applications should expect unplanned terminations. CSPs provide tools that can be configured to automatically add infrastructure in response to volume spikes or automate failover to an identical set of cloud infrastructure in response to an infrastructure failure. However, implementing automated responses to volume spikes or infrastructure disruptions requires clearly defined requirements, and management and testing of complex infrastructure configurations.

ON-PREMISES CLOUD OPTIONS

The maturity trend of the public cloud has aligned with the much broader "service oriented" ecosystem. CSPs themselves are built on top of a foundation based on virtualization that leverages commodity hardware, standardization and consistency around APIs and microservices. This virtualization also uses the maturity and standardization of automation and technology workflow orchestration software. As the "service oriented" ecosystem develops, traditional hardware vendors – along with some new entrants – have created on-premises platforms built as private cloud implementations. In addition, newer offerings from public CSPs offer an on-premises cabinet as a node of the public cloud (e.g., AWS Outposts). The service packaging and release management model of containers and self-service implementations through extreme workflow orchestration can be used to enable greater application independence from the underlying platform.

LIFT AND SHIFT VS. DESIGN FOR CLOUD

Cloud migration planning for an existing on-premises application requires design decisions that consider moving all or portions of an application to the public cloud "as is" (i.e., "lift and shift") or redesigning the application to



leverage the architectural advantages of the cloud. DTCC's experience is that the "lift and shift" approach may initially be viewed as easy, fast and inexpensive; however, this approach could introduce challenges due to the hidden complexities and interconnectedness of applications. Resource-intensive applications, especially those that expect dedicated high-performance processing and large memory resources, can introduce major performance issues if moved directly to the cloud without further considerations and appropriate adjustments. In addition, applications designed for on-premises data centers may not be able to optimize the features of public cloud-based services. DTCC has achieved best results with the migration of existing applications by re-architecting and/or redesigning them for efficient use of the services of the public cloud environment.

As DTCC has gained experience building applications for cloud hosting, it has increasingly leveraged container technology. Containers provide a standard way to package an application and its dependencies so that it can potentially be run in different environments. Containers can simplify moving components of an application to different hosting platforms without significant code changes.

PORTABILITY

As institutions consider the risks inherent in outsourcing specific business applications and potentially entire data centers, the key vendor dependencies and responsibilities to clients and regulators become their own source of risk. As a result, the topic of portability has taken on new meaning and importance for discussions regarding cloud services.[3] While it is often discussed as a simple, binary design decision and concept, portability is complex.

The concept of portability and minimizing dependency on a single vendor has been around nearly as long as the computing industry. Many standards that exist today - such as JAVA, web browsers, and the SQL database language - were earlier efforts to create software that could run without change on any platform. While these efforts achieved many of their goals, the complexity of vendors interpreting standards differently - in addition to vendors providing their own "value-add" enhancements - has resulted in the concept of complete portability being an aspirational and unachievable goal for the technology industry.

Financial institutions face a trade-off: any decision to prioritize portability with applications envisioned for the cloud vs. using a vendor's proprietary, or "cloud native," service must be balanced against the risk of vendor dependency. This balance should be determined through a full risk-versus-value evaluation in addition to consideration of applicable regulatory expectations. While complete portability is not a viable business model,

3 DTCC defines portability to indicate the ability for a component or an entire business application to move from one platform to another, ideally without change. In the cloud computing context, portability is often considered a goal to (1) allow an application built for one cloud platform to easily move to another, which minimizes dependence on a single CSP, or (2) allow an application built for a private cloud to move to a public cloud.

DTCC CLOUD JOURNEY

2018

The DevSecOps (DSO) function was established to drive self-service enablement of business application development, unlocking the power of Enterprise Agile, while incorporating quality, security and increased productivity through the automation of foundational IT services.

2019

DTCC progressed its use of new offerings including leveraging Containers-as-a-Service ("CaaS") and on-premises private cloud.

financial institutions should mitigate cloud use risks in a manner that aligns with their resilience strategy. For example, an institution might choose to port highly sensitive data back on premises as opposed to moving that data to a different CSP. DTCC has been using container technology to maximize application portability.

Portability and vendor dependency concerns are areas regulators have raised with regulated entities.[4] Financial institutions should engage closely with their regulators to develop a common understanding of these concerns and the intended impact on their use of CSPs. Financial institutions should continually monitor, assess and appropriately manage vendor risk and carefully consider the CSPs internal measures, procedures and supply chain.[5]

RESILIENCE AND RESILIENCE VERIFICATION CAPABILITIES

Resiliency is generally defined as an organization's ability to safeguard its critical business services against the threat of potentially disruptive events, regardless of their nature, and regardless of their origin. The past several years brought a heightened focus on building and enhancing the resiliency of the financial markets, due to the increased interconnectedness of the financial ecosystem, evolution of the cybersecurity threat landscape and increasingly sophisticated attacks and the pace of technology innovation.

Resilience is embedded in DTCC's culture and is a driving force behind its enterprise-wide initiatives. DTCC's multiple data centers were built to support its resilience objectives and enable the availability of critical services in the event of a significant regional disruption. The Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) requirements related to physical disaster recovery continue to inform DTCC's resiliency requirements, even as DTCC shifts workloads to cloud hosting. CSPs have been strengthening their service availability to meet RTO. DTCC currently employs multiple CSPs and SaaS vendors and continually works with these vendors regarding the appropriate testing and recovery procedures for DTCC services that operate in public cloud environments.

FAILOVER AND DISASTER RECOVERY

Financial institutions have business continuity requirements that must be maintained regardless of whether services are provided in house or outsourced. These entities must also consider if appropriate disaster recovery

4 The European Union has outlined concerns and challenges with multi-cloud interoperability and data portability in its European Strategy for Data (2020) as well as its Free Flow of Data Regulation (FFDR). As a result, a switching and porting code of conduct working group was launched in an effort to reduce the risk of vendor lock-in by CSPs.

5 For example, in July 2018, the UK's Financial Conduct Authority (FCA) published guidance for outsourcing to CSPs and made clear that firms are obliged to know whether the CSP is using other companies in supplying the service and for safeguarding regulatory compliance throughout the supply chain.

2020

Released Cloud Technology: Powerful And Evolving

measures are in place, regularly tested and maintained by any third-party vendor and any additional providers that the vendor itself may utilize.

The ability for a CSP to "fail over" within or across data centers is a critical disaster recovery measure. Financial institutions must be able to verify that ability to meet their requirements for business continuity. While CSPs offer extremely large scalability and focus on provisioning services based on business requirements, regulated entities may require evidence and metrics of the capacity available to a firm in the event of a disruption -- meaning the unused capacity provisioned by the CSP in their data centers and regions. While most CSPs currently do not report enough evidence of this capability, DTCC has been working with its own CSPs to deepen their understanding of the financial industry's regulatory requirements regarding evidence and metrics of failover capabilities and continue to coordinate with the industry and regulatory community.

SERVERLESS COMPUTING

An important innovation from CSPs, known as "serverless computing" has been challenging to existing regulation. With "serverless computing", the CSP client provides code and all of the details of executing that code is left to the CSP. The CSP provisions the infrastructure and handles scaling and maintenance, and the client does not need to manage any of the infrastructure resources. There are enormous efficiencies associated with serverless processing, and some of the greatest time-to-market and cost savings can be achieved with this processing model. However, existing regulatory requirements contemplate processing on known hardware and for hardware to be physical and visible. Furthermore, regulations require backup processing capacity to be available and deterministic (in other words, visible and measurable). For DTCC, it was not possible to reconcile the serverless processing model with its regulatory requirements, so despite the large business value, DTCC, at this point in time, has backed away from serverless computing for any of its regulated transaction processing applications.

The ability for a cloud service provider to "fail over" within or across data centers is a critical disaster recovery measure.

RESILIENCY

Financial institutions are responsible for maintaining continuity of service and developing formal policies regarding redundancy and availability of backup data. Considerations such as service level agreements (SLAs) regarding cloud outages and downtime, monitoring, reporting, escalations and control audits need to be thoroughly coordinated between the firm and its CSP.

DTCC undertakes a flexible approach and develops applications with an appropriate level of resilience and security, in addition to autonomy with respect to decoupling an application from its original environment if needed. Rather than solely focusing on whether applications are placed in a cloud environment, DTCC also concentrates on how applications are architected, to embed resiliency from the start and to enable future optionality.

A core aspect of DTCC's resiliency program is constant testing of failure scenarios. DTCC has integrated its CSP hosted and SaaS hosted applications into its regular testing cycles to verify business continuity and assist in the ability for on-premises and cloud-based systems to recover and reconcile with each other.

CHAOS ENGINEERING

Chaos engineering is an emerging engineering discipline that conducts a "failure mode analysis" to identify and evaluate the impact of component failures on a system, and then purposefully introduces failures into systems to test an application's ability to recognize and respond to disruptions. In 2017, DTCC launched its Chaos Engineering initiative to build confidence in its systems' capabilities to withstand turbulent conditions, ranging from a hardware failure to an unexpected surge in client requests. A team was established to devise and conduct a variety of experiments to assess the predictability of systems' performance, including those hosted in the cloud. The Chaos Engineering team simulates random CSP outages and disruptions and then analyzes DTCC systems' input and output to help build confidence that requirements are maintained. The Chaos Engineering team has challenged pre-existing assumptions and identified gaps regarding failure detection and response mechanism.

VENDOR CONTRACTUAL OBLIGATIONS

CONTRACTUAL AGREEMENT CONSIDERATIONS

DTCC has worked with CSPs for close to a decade and in doing so, has coordinated on a range of contractual considerations. Financial institutions should coordinate with CSPs to align their expectations regarding performance necessary to meet or exceed internal business continuity and regulatory requirements.

SECURITY CONSIDERATIONS

The implementation of effective security measures, especially regarding cyber security, is a top priority for CSPs and financial institutions using their services. While CSPs provide robust security capabilities, it is the responsibility of the public cloud client to implement security policies and controls. A guiding principle for cloud is that the CSP is responsible for the physical security of the data center and the client is responsible for securing the systems and resources built on top of the CSP services. Organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment. As part of ongoing security management, financial institutions should monitor CSPs to identify any potential service degradation or increased security risks. New information security risks, based on threat landscape and evolving business operations, should also be identified. As financial institutions maintain accountability for ownership and protection of their data, entities should carefully consider what data goes into cloud environments as sensitive, critical, or regulated information may require additional security measures. Financial institutions should also assess incidents, which may trigger varying levels of regulatory notification.[6]

CSP & CYBER SECURITY CONSIDERATIONS:

As noted in DTCC's 2017 paper, CSPs provide services and capabilities that can mitigate cybersecurity challenges presented by on-premises data centers. CSPs also provide security measures to protect against more traditional security risks through redundancy, geographical separation and personnel with up-to-date skills for responding to new cyber threats. While these benefits may drive users to cloud services, simply moving to a cloud environment does not automatically increase security. The appropriate governance and processes need to be in place to identify and mitigate those risks inherent with cloud computing. For financial market infrastructures and firms, cyber-specific considerations may include:

1. Contractual limitations, which may impact a user's ability to test CSP security and resilience controls or an authority's access to financial information held at a third party;
2. Potential cross-border issues, due to legal obligations under foreign law that govern access to, storage location, or use of data;
3. Lack of internal expertise and experience with cloud environments, which could result in security incidents such as those due to poor or incorrect configuration and lack of proper monitoring.

6 For example, in the U.S., breaches involving personal data might implicate state level notifications. This concept is also highlighted in the EU Network and Information Security (NIS) directive – which has been adopted by most EU Member States – that specifies "digital service providers" (DSPs), which includes CSPs, need to take appropriate security measures and to notify substantial incidents to the competent authority.

EVIDENCE OF AVAILABLE CAPACITY

As part of internal business continuity measures, firms may have controls in place that require CSP capacity to be available in varying regions to provide support during times of crisis and other scenarios. While providing on-demand capacity is a core benefit of using cloud services, the ability of CSPs to guarantee and evidence reserved capacity is an ongoing consideration for regulated entities. This could potentially be addressed by CSPs validating – for example, per contractual agreement and/or via regular reports – reserved capacity across regions, or by users' pre-provisioning capacity in varying regions at specific intervals. However, considerations such as the ability to validate capacity and potential costs associated with reserving capacity should be considered. An important consideration for financial institutions and their regulators is the ability to audit cloud services and performance, including reserved capacity.

DATA LOCALIZATION AND PRIVACY

Regulators globally take varying approaches to data storage or localization, which refers to regulatory requirements for specific data to be stored or processed within a particular region or country. Given that large CSPs have multiple data centers across geographic locations, data localization laws are a significant consideration for both CSPs and their clients. CSP users should assess vendors' geographic data center locations so that the regulated entities' use of cloud services remains compliant with any applicable requirements. CSP users should also consider contractual obligations for data to be stored in specified locations and what procedures their hosts have in place for moving compute or allocated storage across data centers, as this may be a factor in maintenance cycles and in the case of failure events.

Financial institutions should establish privacy safeguards in addition to procedures to safeguard the consistency, accuracy and trustworthiness of data held in cloud environments. Regulatory obligations regarding data privacy have emerged that may have a significant impact on CSPs and those utilizing their services.[7]

SOFTWARE AS A SERVICE

By most measures, the broadest adoption of cloud computing is the use of Software as a Service vendors providing non-differentiated "commodity" services for corporate functions, such as email, HR systems, financial reporting systems, client relationship management systems and technology management, tracking and reporting systems. Many firms moved those functions to SaaS providers, built the necessary linkages and data feeds and decommissioned internal platforms. This widespread shift removed significant infrastructure, complexity and maintenance responsibility from internal technology responsibilities. However, it also added a new dimension of risk related to the security, controls and resiliency of the chosen SaaS vendor, and potentially further levels of risk for the vendors – often including other CSPs – that the SaaS provider relies on. This creates new requirements for managing and securing the data exchanges between the firm and the SaaS vendor, and sometimes also between multiple SaaS vendors providing different services to the same firm. Many, if not all of the above best practices can be equally applied to the use of SaaS cloud service providers.

7 In May 2018, the EC's General Data Protection Regulation entered into force in an effort to protect personal data and ensure data flow. To help CSPs comply, the first EU Data Protection Code of Conduct for Cloud Service Providers was developed. In January 2020, NIST released a privacy framework regarding privacy engineering practices that support privacy by design concepts and help organizations protect individual privacy.

FUTURE CONSIDERATIONS

DTCC's Cloud journey is ongoing and we look to leverage our experiences to strengthen future efforts. Key considerations to date that have helped inform our evolution in leveraging cloud capabilities, in addition to recommended areas for further consideration, include:

1. **Applications should be developed using "cloud-ready" technologies and approaches.** These efforts enable improved efficiency, through architecting reuse, and simplification, through service-oriented design, as well as improved security and application deployment through technologies like containers.

2. **Focus on automation and layering of technologies** to best leverage cloud-hosted applications. End-to-end automation of application code delivery and infrastructure-as-code provisioning of entire environments is a prerequisite for secure and resilient cloud deployments. Additionally, the introduction of enterprise APIs and reconciliation services can help financial institutions better engage clients and improve capabilities against future potential disruptions.

3. **Alerting and monitoring are core elements of resilient and secure operations.** Financial institutions need to respond to changes in the environment in order to detect and address potential risks or attacks. Continued alerting and monitoring of applications and services involving third party vendors is recommended.

4. **Establishment of a principles-based, harmonized regulatory framework to better support adoption of cloud services.** Given the increasing importance of cloud services to the financial services industry, and to better support such adoption, policymakers should increase coordination efforts with the private sector to establish a principles-based, harmonized regulatory framework that incorporates the recommendations below:

    a) Adopt a **common lexicon of cloud terminology.** The creation and ongoing maintenance of a common lexicon of relevant cloud terminology would foster effective, cross-sector communication and

increased understanding of regulatory requirements within the financial industry. The cloud lexicon should be globally coordinated, principles based, updated as necessary, and aligned to financial industry standards and best practices. The undertaking should be aimed at supporting financial firms in the development and execution of comprehensive cloud strategies and risk management programs; avoiding regulatory misunderstandings, uncertainty and inconsistency across jurisdictions. By way of example, enclosed as *Appendix A* is a list of proposed terms that warrant consideration as part of any efforts to develop a cloud lexicon.

b) Facilitate international coordination on the **development of cloud specific harmonized principles and best practices**. Policymakers should support international standard-setting bodies in developing principles-based, harmonized regulatory standards and guidance for financial institutions' use of cloud services that apply uniformly across jurisdictions. The resulting regulatory framework should provide clear rules and guidance on key themes specific to the use of cloud services by financial firms, such as establishment of a cloud lexicon, as described above; critical elements of third-party risk management programs in relation to CSPs, and industry-level issues related to cloud services that are best addressed at the industry level. This approach should serve to eliminate unwarranted barriers to financial firms' use of cloud services and better enable adoption of cloud computing and other innovative technologies that are critical to the financial industry's success. Further, by bringing increased clarity and consistency by working on global regulatory expectations, policymakers likely will increase their success in achieving policy goals.

c) **Refresh legacy regulatory requirements in a technology-agnostic** manner. Recognizing that existing regulatory requirements largely were developed in the context of on-premises technology infrastructures and traditional outsourcing arrangements, policymakers should review and modernize rules and guidance so that they are technology neutral. This effort should be focused on eliminating unintentional impediments to the adoption of cloud services and other innovative technologies, without compromising the safety and soundness of individual firms and the broader financial system, market integrity and investor/client protection.

By leveraging cloud services and engaging with CSPs, industry participants can benefit from a more flexible environment, efficiently scaling technology to respond to fluctuating business volumes and demands. Firms should continue to assess and refine their cloud strategy to maintain ongoing collaboration with key stakeholders and meet the highest levels of resiliency and security. DTCC hopes this white paper encourages ongoing industry and regulatory dialogue on the benefits and considerations of responsibly utilizing Cloud services and engaging CSPs.

APPENDIX

APPENDIX A: SAMPLE CLOUD LEXICON

CLOUD LEXICON*	
No.	**TERM**
1	Cloud computing and/or cloud services
2	Cloud service provider
3	Resiliency
4	Service-level agreements
5	Reserved capacity
6	Portability
7	Interoperability
8	Fail over
9	Multi-cloud
10	Exit strategy

**The proposed terms are for discussion purposes only.*

APPENDIX B: CLOUD BUSINESS VALUE FRAMEWORK

During its ongoing cloud journey, DTCC evaluated if the potential use of public cloud was a best fit for specific use cases or applications, through a four-part framework:

1. Improving Time to Market:

Utilizing a CSP may provide a good fit for new business opportunities where a minimum investment is required to deliver technology requirements, and scaling capacity and infrastructure up and down is flexible.

- **When It's a Good Idea:** Public cloud may be a best fit for purpose if the business case requires a short lead-time for client on-boarding. The cloud also enables firms to avoid delays in ordering, installing and configuring equipment, in addition to providing timely availability of system resources to develop and test applications. Firms also have the option to "turn off" capabilities, providing limited risk and financial exposure if interest or adoption doesn't materialize.
- **When to Move Cautiously:** While the cloud offers improved time-to-market, if the application requires continual uptime of all resources, or there are regulatory considerations, it is important to look at long-term cost efficiencies to determine the optimal platform.

DTCC Examples in Action

- **DTCC Exception Manager:** This application went live in 2017 as a new portal for clients to view and assign trade exceptions for institutional trades which failed to settle and are in an "exception" state. Institutional Trade Processing (ITP) was able to move this product from concept to industry use in just nine months, with the flexibility to scale infrastructure for new client use.
- **Performance Testing of Distributed Ledger Technology (DLT):** As part of the 2018 Trade Information Warehouse (TIW) re-platforming project using DLT, performance testing was conducted using the AWS Cloud. IT engineers dynamically created an environment to test application capacity that far exceeds normal, predicted conditions to confirm scalability. To conduct this test using on-premises infrastructure, with the large capacity required, would have been cost- and time-prohibitive.

2. Introducing New Capabilities, Especially for Data

With cloud hosting, data can be used to conduct self-service analytics, reporting and business intelligence. Certain legacy constraints around infrastructure and capacity are minimized due to the cloud's ability to provide cost-effective data storage, as building these types of new, "big data" capabilities using on-premises infrastructure can be extremely cost prohibitive. The cloud also enables firms to more easily try out new analytic tools and other vendor offerings, eliminating many traditional barriers to innovation.

- **When It's a Good Idea:** Cloud is best used when a firm needs a fast solution with the ability to scale-up storage and processing capabilities to generate ad hoc, repeatable and/or custom reporting.
- **When to Move Cautiously:** The infrastructure flexibility gained from using cloud hosting is potentially attractive in terms of quick scalability, processing power and cost. However, delivery of big data capabilities should be closely monitored against original requirements to ensure the overall cost to host and run applications is commensurate with business expectations and budgets. Additionally, the controls, security and privacy required must be commensurate with the risk classification of the data and included in the cost vs. benefit analysis.

DTCC Example in Action

- **Enterprise Data Analytics Platform (EDAP):** This platform was introduced in 2017 as a cloud-hosted, one-stop data repository for self-service business insights and reporting. Delivering a platform like this, with its capacity and processing capabilities, would have required significant investment and scale using on-premises infrastructure. Even with the anticipated growth in data volume, cloud hosting remains the optimal approach to avoid annual cost impact to DTCC for an on-premises solution.

3. Reducing Risk Through SAAS

The best applications for a SaaS support model using cloud hosting are commodity third-party products for business functionality, which are better to buy "off the shelf" than to build internally. Examples include HR services, client relationship management, email servers and finance systems. By leveraging an SaaS model for these types of capabilities, firms can take advantage of best-in-class applications, reduce the need to build and maintain non-core capabilities, reduce their data center footprint and avoid impacting critical business applications if unplanned outages or unfavorable events arise.

- **When It's a Good Idea:** SaaS is a best fit for a "fully packaged solution" when vendors are responsible for

most upkeep and maintenance. This approach also helps lessen or eliminate entry points for potential cyber threats.

- **When to Move Cautiously:** Use of a SaaS model in support of critical business applications should be carefully considered from a range of viewpoints, including sensitivity of data, internal business continuity measures and regulatory requirements. Availability of alternate providers and complexity of the application should be considered to avoid significant business impact. SaaS provider dependencies on other CSPs, supply chain and concentration risks should be considered as well.

DTCC Example in Action:

- **Enterprise Collaboration Tools:** Specific collaboration tools are hosted on vendor-managed cloud infrastructure using a SaaS model. This migration allowed IT to reduce DTCC's potential "attack surface" in data centers and eliminated a significant entry point for cyber threats, moving corporate applications away from the on-premises infrastructure that hosts DTCC's most critical core business applications.
- **Client Relationship Management and Knowledge Base:** DTCC leverages out of the box cloud based applications for managing client interactions, support activities and knowledge management. These applications are very mature with robust, "off the shelf" capabilities. DTCC implemented these products with minimal customization, leveraging as much as possible the turnkey models. As a result, upgrades are virtually seamless, requiring minimal investment from the IT organization especially compared to the overall value these applications deliver to the business.

4. Potential for Capital Efficiencies

The use of cloud technology provides flexibility to run resources periodically when required, as opposed to continual use, in addition to scaling up infrastructure when needed. By choosing cloud hosting, firms can move away from an upfront capital investment model to an on-demand, pay-as-you-go operating expense model. This capability can introduce cost savings, especially for business applications with considerable downtime or variable volume usage.

- **When It's a Good Idea:** Using the cloud eliminates infrastructure sitting idly, waiting for one-off peak scenarios. Public cloud is a best fit for applications with flexible requirements for capacity and infrastructure and can be scaled as needed.
- **When to Move Cautiously:** If firms do not have clarity on how or when applications may be "spun down" in the cloud (e.g., during off-hours when no processing occurs), this may not be a good fit. Also, when requirements for resiliency and risk mitigation demand high complexity and add extensive engineering effort and ongoing testing, other models, including on-premises, should be considered. Value versus cost must be weighed when using cloud services.

DTCC Example in Action:

- **Cloud Archival & Retrieval System (CARS)**: DTCC has separate data archival systems across business lines, all formerly hosted using on-premises infrastructure. Data was infrequently accessed and retrieved, and new infrastructure was periodically purchased to address new capacity requirements. In 2017, DTCC centralized many data archival solutions into a service known as CARS. Between 2017 and 2020, storage costs were reduced, along with the data center footprint.

APPENDIX C: DEFINITIONS

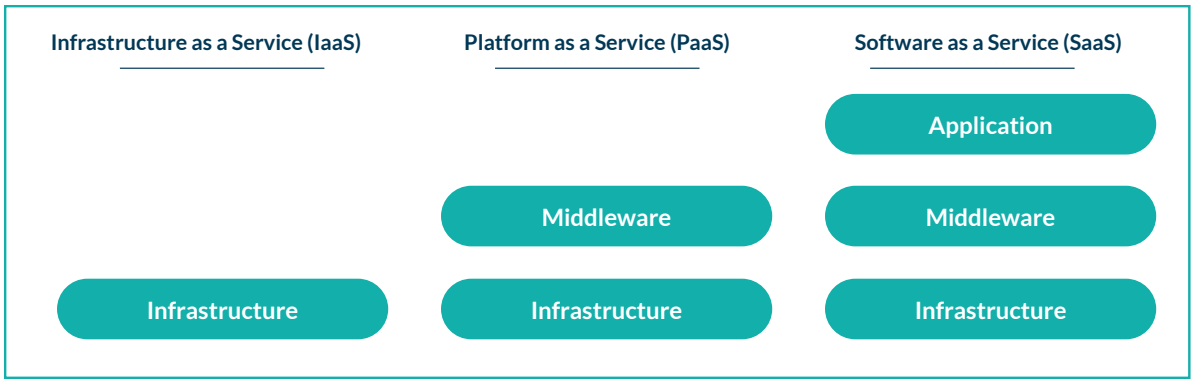
Deployment Models

- **Public cloud:** Resources (servers, storage and internal networking) are owned and operated by a third-party CSP and delivered over the internet or a private network connection. CSP could own hardware, software and supporting infrastructure, while users share hardware, storage and network devices with other users.
- **Private cloud:** Computing resources provisioned for an organization's exclusive use which can be physically owned and located at an organization's data center, hosted by a CSP or a combination of the two.
- **Hybrid cloud:** Combines on-premises infrastructure with public cloud.
- **Multi-Cloud:** Generally defined as the use of multiple cloud platforms from different providers, which may include a combination of on-premises private cloud, and/or multiple public CSPs.

SaaS, PaaS, IaaS

While the following are standard definitions of SaaS, PaaS, and IaaS, DTCC is finding CSPs blurring the lines across these dimensions. For example, some providers display attributes of both SaaS and PaaS, where DTCC uses a business service and directly controls aspects of that service's infrastructure. DTCC finds it increasingly difficult to use these terms to define controls, and instead looks at each solution in terms of what is within and outside of DTCC's control.

- **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, database 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 client. These tools, which include libraries, languages and components, allow the user to construct applications using the service providers' infrastructure. In this model, the client manages the applications and services using the vendor's components. Examples include specific and proprietary offerings from Amazon, Microsoft and IBM.
- **Infrastructure as a Service (IaaS):** Infrastructure components are provided to the client, 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 client 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.



For more information on our products and services, visit DTCC.com
For information on careers at DTCC, visit careers.dtcc.com

FOLLOW US ON

DTCC
ADVANCING FINANCIAL MARKETS. TOGETHER.™