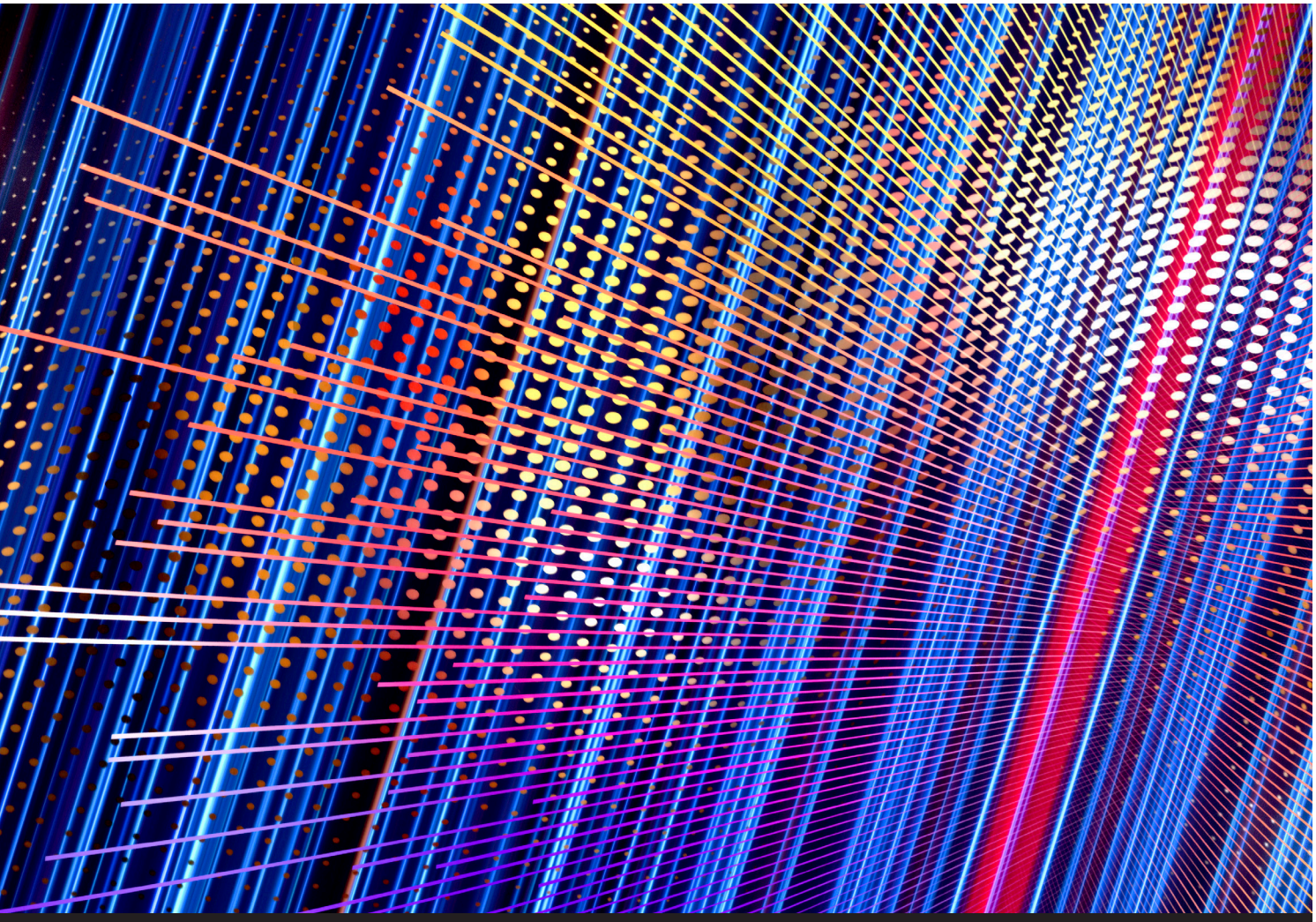
DTCC

SEPTEMBER 2019

# RESILIENCE FIRST

## Promoting Financial Stability by Planning for Disruption



A SYSTEMIC RISK WHITE PAPER TO THE INDUSTRY

# TABLE OF CONTENTS

# FOREWORD

Disruption has always been a key focus area in financial services. In today's highly interconnected and digital world, it can have far-reaching implications with the potential to undermine the safety, stability and integrity of an individual firm or, more broadly, the global financial system. As the nature of risk has evolved over time, this reality has taken on greater significance for market participants and the regulatory community.

As we noted in our 2015 white paper, *Understanding Interconnectedness Risks*, "the openness and complexity of the financial ecosystem and the likelihood that breakdowns will occur mean that firms must do more than monitor and mitigate these risks – they also need to focus on building resilience, so they can detect potential systemic shocks before they strike or recover from them as quickly as possible."

We specifically highlighted the need for enhancing industry-wide resilience due to ever-increasing cybersecurity threats in a report we published jointly with Oliver Wyman in 2018, *Large-Scale Cyber-Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies.*

The complexity of the threats we face continues to grow, not only as a result of rising cybersecurity concerns, but also because of the rapid development and adoption of new technologies, the increased interconnectedness of the financial ecosystem and growing industry-wide concentration risks.

It is no surprise that financial institutions, regulators and other stakeholders are placing an increased emphasis on building resilience, which is generally defined as the ability to prevent, withstand and quickly recover from disruptive events to continue providing critical business services.

Since DTCC's founding more than 45 years ago, resilience has been at the heart of our value proposition. It is embedded in our services, it is a central component of our culture and it is among our most important priorities given our systemically important role.

In light of the heightened focus on resilience, we have written this new white paper, *Resilience First,* to share our views on this important topic. We hope it will galvanize stakeholders to collaborate on enhanced global resilience practices that will help safeguard the industry from disruptions to better protect all market participants, including the end investor.

We hope that you will join us in an active and robust dialogue on resilience-related topics. We invite you to participate in our external outreach efforts and we encourage you to provide feedback on this paper and share it with your colleagues.

# EXECUTIVE SUMMARY

- DTCC is committed to leveraging its considerable experience to lead the discussion on the evolution of industry-wide resilience. This is a key strategic enabler that is consistent with our mission to deliver the world's most resilient and secure post-trade infrastructure for our clients.

- The proliferation of cyber-attacks and rising concerns about the highly interconnected nature of the financial ecosystem are among the main drivers of the industry's heightened focus on resilience.

- This increasingly complex environment requires a new approach to enhancing resilience that is holistic, forward-looking and highly collaborative. Initiatives to strengthen resilience touch on all aspects of a firm, including business services, applications and processes, training, communications and stress testing. As such, they should start at the board level and carry through to senior management and across the entire organization.

- Rather than narrowly focusing on *systems*, resilience initiatives should aim to safeguard *critical business services* against a wide range of technical, physical, logical or financial disruptions, regardless of their cause or origin. To consider impacts on, and interdependencies with, the broader ecosystem, resilience efforts should use an end-to-end perspective that starts with the customer and includes service providers, regulators, third parties, industry associations, as well as any other partners and stakeholders.

- Other paradigm shifts that are essential to increasing resilience include the ability to anticipate issues, as well as a willingness to prioritize resilience over efficiency in certain cases. Resilience must be established as a business-owned strategic initiative that is supported at the highest levels of the organization.

- As resilience-enhancing initiatives are further refined and implemented, industry coordination will be a key measure of success. Ongoing sector-wide collaboration and testing will be necessary to ensure all firms understand their roles and have the appropriate level of readiness to mitigate the impact of shocks that could disrupt their critical business services.

- Regulatory harmonization efforts to establish uniform and consistent internationally agreed upon standards with respect to resilience are equally important to promote global financial stability. International standard-setting bodies, such as the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organisation of Securities Commissions (IOSCO) and the Financial Stability Board (FSB) are in a unique position to coordinate global regulatory initiatives in this regard.

- Given that enhancing resilience is a multi-year journey that requires a structured and consistent approach, we have articulated a formal vision that is underpinned by core principles and supporting guidelines. These principles and guidelines are broad enough to be of interest to other entities that want to strengthen the resilience of their critical business services.

- The goal of this paper is to introduce, explain and share this vision. As we continue to develop our thinking, we will publish additional details and disseminate more specific information to further the conversation with our stakeholders.

# A GLOBAL FOCUS ON RESILIENCE

## KEY TAKEAWAY

- **Many factors contribute to the rising focus on resilience worldwide, but two stand out: the increasing threat of cyber-attacks and the growing interconnectedness of the global financial sector.**

Achieving and maintaining appropriate levels of resilience in today's complex global marketplace is a difficult balancing act that involves myriad trade-offs between competing objectives. Identifying potential sources of disruption and preparing for extreme but plausible events are never-ending challenges in an environment that is continually and rapidly changing. Budgetary constraints and other resource limitations also come into play, as corporate decisions to improve resilience may require foregoing other investment opportunities.

As of late, the topic of resilience has received widespread attention, largely because of two global trends:

**1) The growing frequency, sophistication and complexity of cyber-attacks have significantly changed the nature of systemic threats.**

Cyber risk consistently has been ranked as the number one concern by respondents to DTCC's Systemic Risk Barometer since the inception of the survey in 2013. The ever-increasing sophistication and frequency of cyber threats only intensifies concerns over their potential impact. Targeted attacks by well-funded state actors and other cyber criminals have the potential to cause massive and widespread disruptions, which could result in prolonged outages of critical infrastructure components or critical data to be held hostage. In addition to causing outright system failures and other types of damage, cyber-attacks also could create large-scale data integrity issues that could have a systemic impact.[1] While industry-wide investment in cyber defenses continues to grow and public-private partnership support greater levels of information sharing, existing solutions may be insufficient to address these threats and may even be counterproductive in certain cases. For example, data replication strategies designed to protect against physical disaster could end up worsening the impact of a cyber-attack by rapidly spreading malicious code or compromised data across datacenters.

**2) The expanding interconnectedness of the financial ecosystem has heightened its vulnerability to disruption and contagion.**

Economies of scale in the financial sector have generated tremendous efficiency gains, resulting in substantial industry-wide cost savings. However, these advances have also reduced the number of critical service providers, which creates significant consolidation and increases concentration risk. Meanwhile, greater automation and continuous advances in IT systems have increased reliance on technology and accelerated the speed at which the impact of a disruptive event can spread. Additionally, increased interconnectedness between IT systems of financial institutions and third parties has further heightened the potential for contagion.[2]

1 This is a key theme of a white paper we published jointly with Oliver Wyman in 2018, *Large-Scale Cyber-Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies.*

2 For a more extensive overview of how interconnectedness risks relate to financial stability, see also: DTCC (2015, October). *Understanding Interconnectedness Risks to Build a More Resilient Financial System – A White Paper to the Industry.*

## RECOVERING FROM A CYBER-ATTACK – AN INDUSTRY-WIDE CHALLENGE

Recovering from a cyber-attack that would compromise the integrity of critical business data on an industry-wide scale is a challenge that illustrates the need for coordination in today's highly interconnected financial sector. To mitigate this type of threat successfully, all affected parties must have the ability to revert to uncompromised data. This is one of the objectives of the coordinated development of the Sheltered Harbor standard, an industry-wide initiative that is supported by DTCC and a group of industry trade associations and financial services firms. DTCC's implementation of data protection capabilities to accelerate recovery efforts after a major cyber-event, which is being developed in close coordination with clients and other external parties that would play a key role in resuming the provision of critical business services in a safe and rapid manner, is another example of this type of initiative.

Given these trends, regulatory interest in resilience has understandably intensified. Following the 9/11 terrorist attacks, resilience initiatives primarily centered on improving contingency plans and safeguarding business operations against the risk of wide-area physical disruption. After the Lehman insolvency and the subsequent financial crisis, regulators shifted their focus to strengthening financial resilience by concentrating on recovery and resolution planning, increasing capital and liquidity requirements and the adequacy of stress tests. Lately, regulators have started looking more closely at operational resilience, especially in the wake of high-profile outages and other technology-related incidents at several major financial firms and third-party service providers.[3]

The combined effect of these changes creates an unprecedented set of challenges that require several **paradigm shifts:**

- In today's threat environment organizations cannot focus exclusively on strengthening their defensive capabilities to avoid a disruption from materializing. Instead, they must complement their defensive efforts by developing additional strategies to recover quickly from disruptive events and minimize their impact.
- Financial institutions need to adopt an all-encompassing approach that addresses disruptive threats holistically, regardless of their nature or origin. Firms can no longer afford to focus on disaster recovery, business continuity management and cybersecurity in isolation. In line with this thinking, DTCC created a Chief Security Office four years ago to centralize and align technology risk, information security, physical security, business continuity, disaster recovery and crisis management functions into a single organizational structure to ensure a comprehensive and cohesive approach to risk management and resilience across the company.
- The long-held notion that resilience is a back-office IT concern that taxes business development is outdated. Instead, enhancing resilience must be established as a business imperative and an enabler of company-wide strategic goals.
- While firms will continue to identify efficiency gains, it may be necessary at times to prioritize resilience because highly integrated, straight-through processes may increase the impact of a disruption or shock. As such, organizations may need to consider disaggregating certain IT applications or operational processes to increase the resilience of their critical business services.

To address these challenges and meet the heightened expectations of regulators, **the industry needs to adopt a new approach to resilience that is holistic, forward-looking and highly collaborative.** Firms must establish resilience as a core competency and embed resilience in all their critical business services.

3 In late 2018, the UK's Financial Conduct Authority (FCA) announced that financial institutions under its jurisdiction had reported a 187% year-over-year increase in technology outages (see https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services).

# BUSINESS RESILIENCE – AN OVERARCHING CONCEPT

## KEY TAKEAWAYS

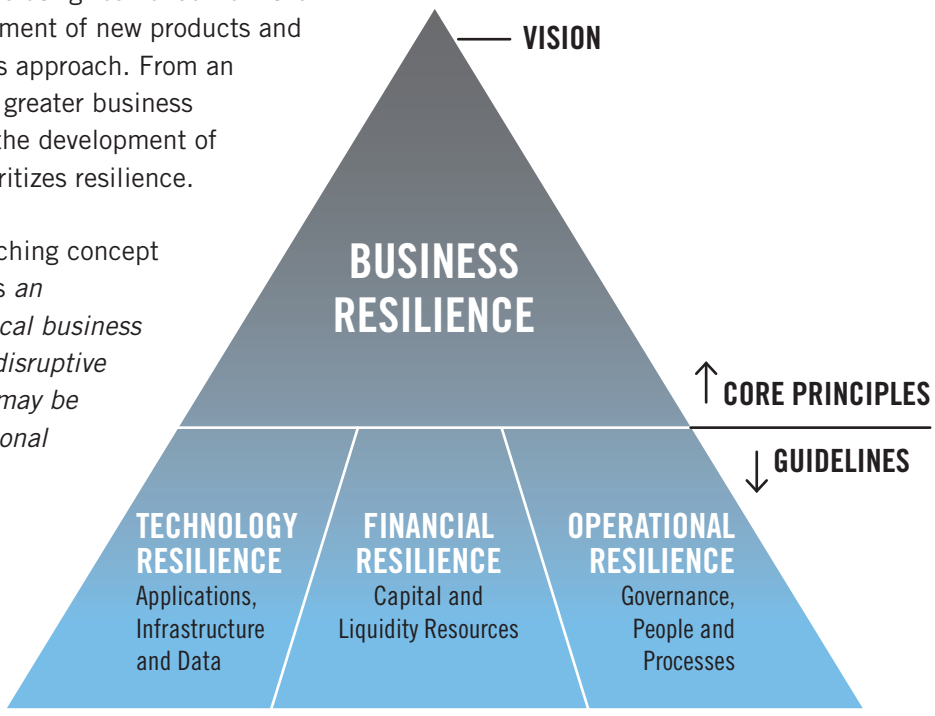
- **Business resilience is an overarching concept that refers to an organization's ability to safeguard its critical business services against the threat of potentially disruptive events, regardless of their nature or origin.**
- **DTCC's business resilience vision reflects its continued commitment to protect the post-trade ecosystem and create lasting value for its clients as well as the wider industry.**

Resilience has been an essential part of DTCC's value proposition since our founding more than 45 years ago and over these past four decades we have safeguarded financial stability during times of uncertainty. For example, we maintained critical business services after the 9/11 terrorist attacks, through the 2003 Northeast blackout and Hurricane Sandy in 2012 – not to mention the successful close-out of more than $500 billion in market participants' exposure in the wake of the Lehman insolvency in 2008, illustrating the robustness and the systemic importance of our risk management processes.

While we are proud of this track record, **our vision is to leverage our experience and market position to lead the evolution of resilience to protect and enable the post-trade ecosystem.**

The complex events that may disrupt today's interconnected markets demand that organizations develop a holistic approach to resilience that focuses on the continued, end-to-end provision of *critical business services*, rather than individual processes or operations. Incorporating resilience from the ground up into every stage of the development of new products and services is the logical consequence of this approach. From an organizational point of view, this requires greater business ownership and accountability, as well as the development of a corporate culture and mindset that prioritizes resilience.

As such, this paper introduces the overarching concept of **business resilience**, which we define as *an organization's ability to safeguard its critical business services against the threat of potentially disruptive events, regardless of their nature (which may be related to technology and/or other operational issues, as well as financial events) and regardless of their origin (which may be internal or external), by planning and executing a company-wide strategy to reduce their probability as well as their impact.*




As financial resilience has been a topic of significant focus for the industry and regulators since the 2008 crisis, we chose to create guidelines for operational and technology resilience as these areas are less mature.

# BUSINESS RESILIENCE PRINCIPLES

## KEY TAKEAWAY

- **DTCC's business resilience vision is supported by six core principles that can be adopted by a wide range of entities that are interested in making their critical business services more robust.**

We have adopted **six core principles** to support our business resilience vision. While these high-level principles have relevance for many business initiatives, we believe they are particularly helpful to achieve consistent and repeatable enhancements to business resilience across the industry.

**1) Business Resilience Efforts Must be Holistic**

Enhancing business resilience must be a comprehensive undertaking that considers key dependencies and potential vulnerabilities. To ensure that resilience-enhancing initiatives are based on a thorough understanding of critical business services, a broad range of potential impacts and solutions must be reviewed that:

- Include an end-to-end analysis of critical business services that considers regulatory requirements, client activities, dependencies on third parties and other touchpoints with all internal and external parties that use or contribute to the service being analyzed.
- Consider a wide array of operational, technical and financial risks and their impacts, in conjunction with concentration risk and other aspects of market structure.
- Extend to all critical business services across geographies, regardless of functional and departmental boundaries.

**2) Building A Resilience-Centric Culture and Mindset is Essential**

Embedding resilience into the corporate-wide risk culture and mindset improves risk and response management throughout an organization. It also fosters greater cross-functional alignment on a shared approach and common objectives. Successfully promoting a "resilience-centric" corporate culture and mindset that focuses on continuous improvement is achieved by:

- Emphasizing enhancements as a long-term corporate objective – supported by the board and senior management – rather than a short-term goal.
- Encouraging employees to challenge the status quo as a way to address resilience weaknesses and mitigate associated risks.
- Creating a mindset that is based on continuous learning – from previous incidents; from scenario analysis; and, more generally, from peers and the industry – to gain greater insight into resilience-related issues.
- Coordinating with senior executives and managers throughout an organization to change everyday behaviors and identify potential problems before a disruptive event occurs.

**3) Enable Resilience through Governance**

Create a governance structure that effectively supports resilience by:

- Enabling the board and senior management to oversee the planning and execution of resilience activities so they can ensure these activities receive the appropriate level of prioritization and funding.
- Creating and maintaining a comprehensive set of policies and procedures with respect to any additional resilience capabilities that are being created.

**4) Transparency and Measurability are Key**

To make thoroughly informed strategic decisions with respect to resilience, transparency and measurability are key prerequisites that can be achieved by:

- Creating impact tolerance statements to clearly define objectives and expectations.
- Using a comprehensive set of metrics and business indicators to measure resilience outcomes and report progress to senior management.

**5) Resilience Must be Sustainable and Adaptable**

Initiatives to address evolving resilience challenges will only be sustainable if they:

- Adapt to changing market and business conditions, as well as new threats and advances in technology.
- Encourage creative thinking and empower staff members who are involved in planning and executing resilience programs.
- Adopt a principles-based approach to provide guidance and direction without being unnecessarily prescriptive, given that each event will be unique.

**6) Resilience Requires Eliminating Complexities**

Improvements to resilience must seek to remove or avoid unnecessary complexity, which can create risk and make recovery more difficult. This can be achieved by:

- Minimizing touchpoints and removing intermediaries wherever possible.
- Using industry-accepted standards and practices rather than proprietary solutions.

Business resilience, and the principles above, subsume financial, operational and technology resilience. However, the remainder of this paper will focus solely on operational and technology resilience since financial market infrastructures have substantially improved their financial resilience during the past decade – thanks to efforts related to recovery and resolution planning, stress testing, loss allocation model enhancements, diversifying and expanding liquidity resources and increasing capital resources.[4]

4 See also: DTCC (2015, June). *CCP Resiliency and Resources – A White Paper to the Industry.*

# OPERATIONAL RESILIENCE

## KEY TAKEAWAYS

- **We have adopted a series of operational resilience guidelines that are consistent with the core principles that underpin our overall business resilience vision.**
- **These guidelines incorporate a wide range of factors to ensure that they are highly adaptable to changing circumstances and that they support business development goals.**

DTCC has adopted a series of **operational resilience guidelines** to make the core principles mentioned previously applicable to the challenge of creating or redesigning operational processes, defining decision points and developing escalation procedures.

Given that threats to operational resilience will continue to evolve over time, these guidelines are sufficiently flexible so that they can grow and adapt as external dynamics change. Additionally, they are designed to support, rather than hinder, business objectives and product development processes.

Based on these considerations, we believe that the following guidelines can help firms strengthen their operational resilience:

**1) Design for Resilience by Planning for Failure**

Build for eventual failure and subsequent recovery, based on a clear understanding of the interaction between critical business services, supporting processes and staffing. Clearly document agreed upon policies and procedures that govern how to respond to disruption and/or failure. Prepare internal and external communications plans to inform and update key stakeholders in case of a disruption.

**2) Assess 'Ecosystem' Resilience**

Actively assess resilience capabilities and weaknesses for all critical business services and operations, including impacts on clients and reliance on third parties. To address operational vulnerabilities, make sure to include both: (i) controls to prevent disruptive events; and (ii) processes designed to minimize the impact of such events, such as workarounds to deliver critical business services when key systems are unavailable and other plans to help ensure a rapid and safe recovery.

**3) Actively Monitor Resilience**

Track resilience metrics to monitor and assess the robustness of operational processes on an ongoing basis. Ensure that there is meaningful and measurable intelligence available to provide insights and trends regarding operational resilience performance to better inform strategic management and investment decisions.

**4) Continually Test Resilience Capabilities**

Test resilience-related processes with all relevant parties on a regular basis, confirm that policies and procedures are thoroughly understood and promote a learning-based environment to improve the ability to measure, monitor and manage risks. Give adequate attention to the human element of testing – by making sure that the appropriate experts are available, including exercises to build muscle memory and addressing key person risk.

## OPERATIONAL RESILIENCE – A GLOBAL FOCUS AREA

While operational resilience isn't a new concept, the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) turned the spotlight on this topic in 2018 when they jointly published the discussion paper *Building the UK Financial Sector's Operational Resilience.* In that paper, they underscored the importance of:

- Focusing on the continued delivery of critical business services
- Defining impact tolerance levels with respect to resilience
- Assuming that failure is inevitable
- Having full support from the board and senior management

The paper resonated on a global scale and sparked a wave of additional thinking on the ideas listed above, as well as a series of follow-up publications by consultants and other interested parties.

In March 2019, the Monetary Authority of Singapore (MAS) published two consultation papers, in which it invited interested parties to comment on a series of proposed revisions to its Technology Risk Management Guidelines and its Business Continuity Management Guidelines.

In June 2019, the Australian Securities & Investments Commission (ASIC) published a consultation paper on *Market Integrity Rules for Technological and Operational Resilience.*

Resilience also is an important topic on the regulatory agenda in the European Union, with the European Banking Authority (EBA) undertaking several initiatives to promote consistent supervisory practices.

Initiatives of other EU and global bodies related to operational resilience include, among others: the G7 Cyber Expert Group work; the Basel Committee on Banking Supervision (BCBS) work on operational resilience; the European Central Bank's European Framework for Threat Intelligence-based Ethical Red Teaming (ECB TIBER-EU); and the Euro Cyber Resilience Board (ECRB).

We expect that the current consultation papers and related efforts will eventually be converted into specific jurisdictional requirements. While these initiatives are in different stages of progress, however, none of them seem to have matured to the point where such conversion is forthcoming.

DTCC believes that global regulatory harmonization in this area is the most effective way to promote financial stability. As such, we believe the BCBS, the Financial Stability Board (FSB), the Committee on Payments and Market Infrastructures (CPMI), the International Organisation of Securities Commissions (IOSCO) and other international standard-setting bodies are in a unique position to coordinate global regulatory initiatives to promulgate uniform and consistent internationally agreed standards for operational resilience.

# TECHNOLOGY RESILIENCE

## KEY TAKEAWAYS

- **Ever-changing physical and cyber threats necessitate continuous enhancements with respect to technology resilience.**
- **To ensure that these enhancements are being implemented consistently, DTCC uses a number of widely applicable technology resilience guidelines that leverage leading-edge design concepts.**

Given the high degree of automation and the associated reliance on IT systems within the industry, technology resilience is a key element of business resilience. The pace of change in technology developments and the rapid introduction of new technologies further reinforce the need to continuously augment technology resilience capabilities to safeguard critical business services.

Legacy technology, while still used by many financial firms to support some of their key processes, may not be optimized to perform more advanced functionalities that are required to keep up with evolving business demands. Additionally, relying on older platforms also makes it challenging to find and retain specialists with the requisite knowledge base and to ensure continued vendor support.

### DTCC'S TECHNOLOGY MODERNIZATION INITIATIVE

DTCC has embarked on a multi-year modernization initiative to enhance its business offerings as well as any underlying systems and operational processes. While the primary goal of this initiative is to improve the client experience, embedding resilience from the inception phase of the new business development process is a key component. Other focus areas include opportunities to streamline processes and develop reusable IT components that are designed to support a uniform set of business services across a variety of markets and products.

Redesigning processes and building reusable IT components to perform common capabilities that are shared across business lines will reduce time-to-market and allow innovative solutions and enhancements to be implemented iteratively. For example, the creation of Application Programming Interfaces (APIs) will facilitate flexible and consistent data access across channels and devices. These APIs will enable clients to build self-service analytical capabilities while insulating them from changes to underlying applications and infrastructure. Furthermore, the new architecture will support artificial intelligence, robotics and other emerging technologies to provide innovative solutions.

DTCC's technology modernization initiative will build a future-state strategic IT architecture that is resilient by design. This means that the initial business requirements will include additional cyber-based and application-specific recovery capabilities, based on the assumption that such disruptions inevitably will occur at some point. Supplementary risk-reducing efforts will focus on extending out-of-region recovery capabilities, while simultaneously improving the resilience of on-premises systems. Other measures will include developing workarounds – such as alternative settlement capabilities – to deliver critical business services when key systems are not available. Strategic initiatives will be aligned with the new IT architecture, leveraging cloud and advanced on-premise distributed hosting capabilities.

As such, implementing modern technology capabilities is a key part of enhancing technology resilience and an important component of strengthening business resilience. Even though DTCC's current IT architecture is already highly resilient, designing and implementing new and enhanced technology capabilities remains a priority. Toward that end, we have decided to use a number of guidelines to help ensure that IT applications, platforms and components can optimally respond to, and recover from, disruptive events of varying severity. Similar to other principles and guidelines discussed in this paper, we believe that these **technology resilience guidelines** can be applied or adapted by a wide variety of organizations to ensure they have robust IT applications and infrastructure, as well as adequate data protection:

**1) Design for Resilient IT Capabilities**

Firms should anticipate that disruptions will inevitably occur at some point. As a result, systems and software should incorporate capabilities that are specifically aimed at recovering from a wide array of potential internal and external events, including cyber-attacks and application-specific incidents. For example, applications should be designed to operate independently of each other, where practicable, to help isolate and limit the impact of software issues and data outages. Each application should have its own resilience capabilities, which should be included as early as possible in the initial systems design stage. To further enhance resilience, software applications also should be developed to reduce infrastructure and other hardware dependencies as much as possible.

**2) Ensure Regional Availability**

Business service availability is typically defined as the percentage of time that operations are running normally. To build highly available critical business services, the IT architecture must be designed to include redundancy and autocorrect capabilities for each component within and across local sites by leveraging multiple instances of local data, computers and networks. These requirements will guide the implementation of resilience capabilities into all layers of a solution design.

**3) Leverage Out-of-Region Recovery**

Although out-of-region capabilities are primarily designed for physical disaster recovery purposes, they also can be leveraged to recover from logical disruption incidents that involve the corruption or destruction of data within a single region. Specifically, it is important to maintain cross-regional data consistency to ensure the viability of these capabilities. This may require the use of software to minimize any potential data loss and the implementation of reconciliation and/or replay capabilities to supplement hardware-based data replication technologies.

**4) Ensure Resilience Success**

All solution designs will require adequate validation processes to help ensure that each critical business service can determine its health and that resilience success can be verified upon recovery. These validation processes will be based on key performance indicators that are both monitored and responded to via automation, minimizing human intervention to the extent practicable. Automation can also be used to support the verification of application availability and operational readiness to support critical business services. Controls should be created to help prevent the corruption and/or destruction of production or reference data, source code and configuration data.

## CHAOS ENGINEERING AND RELATED INITIATIVES

DTCC established a Chaos Engineering function in 2018. Chaos Engineering is the discipline of experimenting failure conditions on a distributed system to build confidence in the system's capability to withstand a wide variety of turbulent conditions – anything from a hardware failure to an unexpected surge in client requests or a malformed value in a runtime condition.

This function is supplemented by the Critical Application Resilience Engineering (CARE) Program, which is designed to engineer solutions that address and minimize fault impacts identified by Chaos testing. DTCC launched CARE in 2019 to adopt and apply a proactive and consistent application resilience engineering methodology to model application failures, engineer solutions to respond to failures and perform operational resilience drills.

These initiatives, combined with a framework to automate testing efforts, supplement each other and measure resilience capabilities across in-region, out-of-region and hybrid failure scenarios.

# EXECUTING DTCC'S BUSINESS RESILIENCE VISION

## KEY TAKEAWAYS

- **The most effective and pragmatic way to implement DTCC's business resilience vision is through a federated model that is organized around a Business Resilience Center of Excellence.**
- **To prepare an effective implementation process, DTCC will focus on: an assessment of existing business services; a more detailed operating model design; further engagement with DTCC's Business Architecture team; and continued external outreach and validation efforts.**

While creating principles is a critical initial step to improving resilience-related objectives, we also need to harness the capabilities – or build new ones – to implement our business resilience vision and achieve the desired outcomes. After assessing several options, we believe that the most effective implementation approach for DTCC is a federated model organized around a Business Resilience Center of Excellence.

The primary benefit of this model is that it facilitates pragmatic, rapid deployment that leverages existing resilience-related activities. It also centralizes talent and expertise firm-wide to ensure that best practices are applied consistently across business lines.

To prepare for the implementation of the operating model, we will focus on the following areas as immediate next steps:

- **Continue to engage with the Business Architecture team** to explore how design principles can be effectively applied.
- **Ensure an appropriate governance model is established** that is integrated within the broader company-wide governance structure.
- **Assess existing business services** to determine initial priorities based on a high-level application of the principles and guidelines described above, while evaluating service and application criticality.
- **Conduct external outreach efforts** through industry forums and relationship management functions to obtain new insights and ideas to refine and validate our resilience approach.

# CONCLUSION

Business resilience is foundational to DTCC's value proposition. We are committed to improving industry resilience to enhance financial stability.

Our business resilience vision is designed to improve strategic decision making, promote greater alignment between IT and business groups and build upon our longstanding legacy of trust with our clients and partners.

We have adopted a series of principles and guidelines to promote a consistent and pragmatic approach to enhancing business resilience. We will continue to refine those concepts through further assessments, as well as industry outreach and feedback.

This white paper is a key component of that outreach and is intended to foster dialogue and discussion on this important topic. As such, we encourage you to share your comments and feedback with us.

Input can be provided to:

**Murray Pozmanter**
*Managing Director, Chief Operations Officer & Head of Clearing Agency Services and Global Operations and Client Services*
mpozmanter@dtcc.com
001-212-855-7522

**Dan Thieke**
*Managing Director, Business Risk & Resilience Management*
dthieke@dtcc.com
001-212-855-4162

**Stephen Pecchia**
*Managing Director, Head of Recovery and Resolution Planning & Product Risk Management*
specchia@dtcc.com
001-212-855-3356

# BIBLIOGRAPHY


Australian Securities & Investments Commission. (2019, June). *Market integrity rules for technological and operational resilience – Consultation paper 314.*

Bank of England/Financial Conduct Authority. (2018, July). *Building the UK financial sector's operational resilience – Discussion paper.*

Basel Committee on Banking Supervision. (2018, November). *Cyber-security and operational resilience (workshop 6).*

Basel Committee on Banking Supervision. (2018, December). *Cyber-resilience: Range of practices.*

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency & Securities and Exchange Commission. (2003, June). *Interagency paper on sound practices to strengthen the resilience of the U.S. financial system.*

Committee on Payments and Market Infrastructures/Board of the International Organization of Securities Commissions. (2016, June). *Guidance on cyber resilience for financial market infrastructures.*

Committee on Payments and Market Infrastructures/Board of the International Organization of Securities Commissions. (2016, August). *Resilience of central counterparties (CCPs): Further guidance on the PFMI – Consultative report.*

DTCC. (2015, June). *CCP resiliency and resources – A white paper to the Industry.*

DTCC. (2015, October). *Understanding interconnectedness risks to build a more resilient financial system – A white paper to the industry.*

DTCC & Oliver Wyman. (2018, March). *Large-scale cyber-attacks on the financial system: A case for better coordinated response and recovery strategies.*

Ernst & Young LLP. (2018). *Getting serious about resilience: A multiyear journey ahead.*

European Banking Authority. (2018, September). *Regulatory framework for mitigating key resilience risks.*

Federal Reserve Bank of Philadelphia. (2018, February). *The interplay among financial regulations, resilience, and growth.*

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). (2019, April). *Business services resilience and restoration – Building operationally resilient business services in the financial sector.*

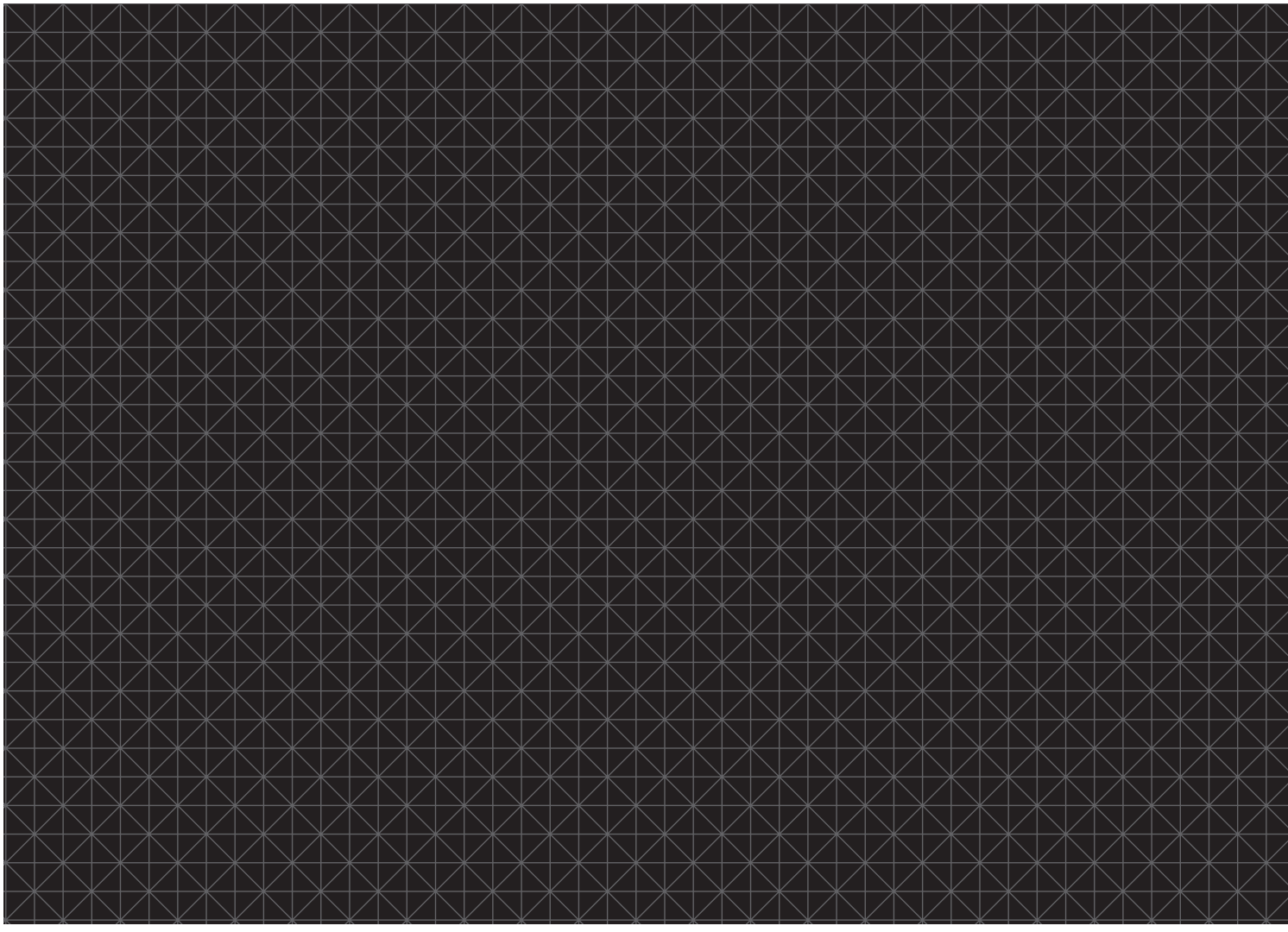
Infosys. (2019). *Designing for operational resilience.*

Monetary Authority of Singapore. (2019, March). *Proposed revisions to guidelines on business continuity management – Consultation paper.*

Monetary Authority of Singapore. (2019, March). *Technology risk management guidelines – Consultation paper.*

PWC. (2019). *Operational resilience – Your Swiss army knife to survive the next crisis.*

TheCityUK. (2019, June). *Operational resilience in financial services – Time to act.*



15251 TC092019