JUNE 2022

THE POWER OF TECHNOLOGY RESILIENCE: A FRAMEWORK FOR THE INDUSTRY

CONTENTS

INTRODUCTION

For the past four decades, DTCC, in partnership with the financial services industry, has navigated through extreme events, evolving business continuity planning needs and data center redundancy expectations, and increased transaction processing capacity requirements for critical products and services.

DTCC has led the financial services industry through disasters and market disruption events, remaining operational during some of the most difficult periods of US history. In the aftermath of the September 11th terrorist attacks, numerous brokers were faced with the fallout of hosting both their primary and back-up data centers in the World Trade Center. Following the Northeast blackout of 2003, many firms burned through fuel reserves for their data centers before power was restored. The 2008 credit crisis and Lehman Brothers failure massively changed volume profiles. In 2012, a technical glitch at Knight Capital created a significant trading disruption and Superstorm Sandy shut down entire buildings in lower Manhattan for months. The volume spikes and circumstances driven by these events have challenged DTCC's scale and performance, but ultimately our robust planning and business resilience helped protect the financial services industry. Most recently, DTCC navigated the industry through significant market volatility in January 2021, processing just under half a billion transactions in a single day.

DTCC has led the financial services industry through disasters and market disruption events, remaining operational during some of the most difficult periods of US history.

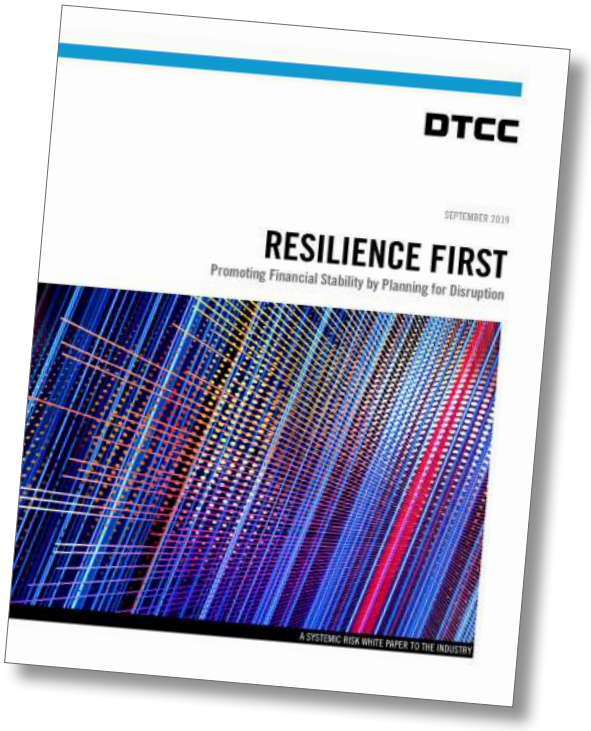
DTCC understands the importance of its position as a critical infrastructure and service provider for the global capital markets, resulting in a heightened focus on risk management and mitigation. In fact, we follow some of the most stringent resumption and recovery requirements for most of our critical services – meeting the regulatory required two-hour recovery time objective, and a data recovery point objective of just 30 seconds. Our out-of-region recovery locations must be hundreds of miles away from our primary data center and on completely separate power transmission interconnections with a separate physical telecommunications path. Regulators and supervisors are laser-focused on testing our resilience capabilities, consistently raising expectations for how we implement our most critical systems and software.

DTCC shared its overarching resilience imperative through the 2019 white paper, Resilience First. This paper describes the principles we use to prepare for and practice our response to all types of scenarios, including pandemics. Resilience is built into everything we do, so that we can endure, continue to execute seamlessly, and provide access to critical business services.

This paper goes a level deeper and designs, and shares how DTCC is building the concept of "resilience first" into our technology principles, designs, and the foundation of our applications and platforms through reusable patterns and enterprise capabilities. As the industry's landscape evolves and becomes increasingly complex, DTCC remains focused on preparing for disruptions and failures, moving beyond the long-held notion that resilience is primarily a back-office IT concern. DTCC believes that enhancing resilience must be established as an industry-wide business and strategic imperative to ensure the continued safety and soundness of financial industry markets in the face of ever-evolving risks.

VISION FOR BUSINESS RESILIENCE

In our 2019 white paper, we shared our overarching vision of **business resilience**, a foundational component of DTCC's value proposition. To turn that vision into action, we described our set of six core **business resilience principles**, which then further informed the next level of functional resilience principles covering the operational, technical, and financial considerations at DTCC. In this document we delve into how these are applied to our technology resilience.



Technology Resilience at DTCC

More than ever, financial institutions are reliant on automation and IT systems to deliver critical business functions. Traditionally, resilience has been platform-centric, but as business systems and processes are modernized, it's imperative that resilient capabilities are built in at the application level. Given this, technology resilience is a key enabler of business resilience, and DTCC strives to deliver IT solutions that increase service uptime and keep our business operational. This paper shares the technical resilience capabilities we developed as part of our modernization efforts, as well as our Plan-Build-Test-Operate model for application delivery, and provides a framework for other financial services firms to consider in their own strategic roadmaps.

For many years, we leveraged our Disaster Recovery (DR) program to prove that we can recover and resume business at our alternate out-of-region data center(s). However, in recent years, the heightened pace of change in the financial services landscape coupled with the rapid introduction of new technologies has further reinforced the need to continuously augment technology resilience capabilities to safeguard critical business services in new ways.

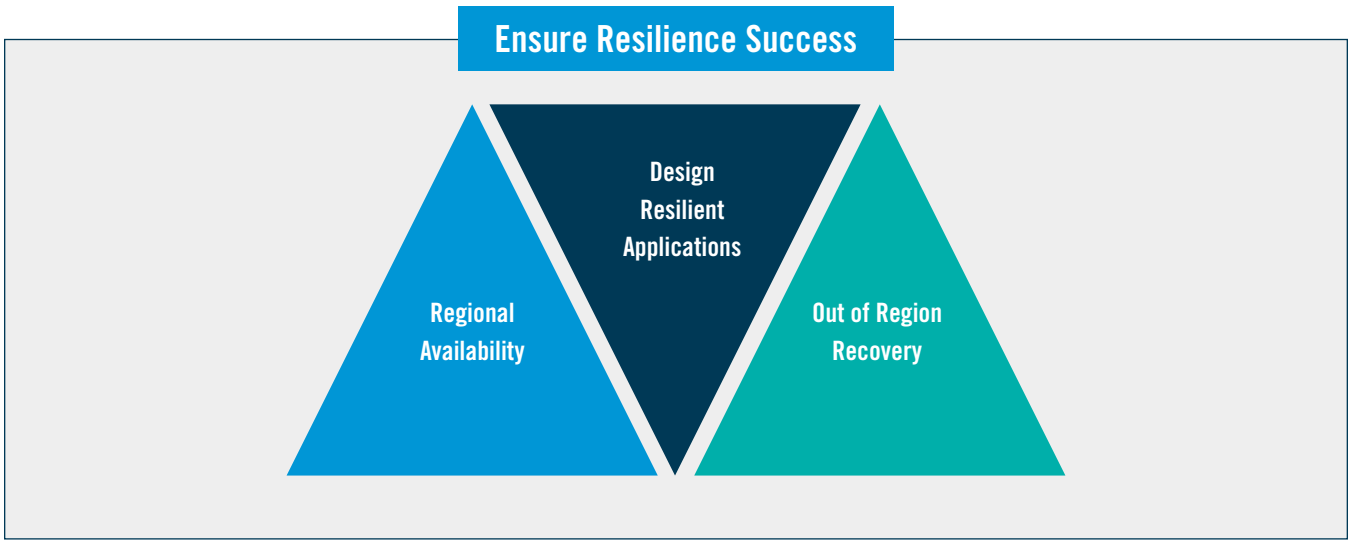
Across the industry, modern technology ecosystems now operate in multiple physical and virtual environments, including cloud. Increasing modularization of code components and supporting architectures, enabled by micro-services, have resulted in complex interactions and dependencies among multiple applications. Before, resilience was important at the singular application level, but now, these changes

The following principles were introduced in DTCC's 2019 Business Resilience White Paper and continue to inform the strategic direction of the capabilities we deliver to strengthen resilience for the industry:

1. Business Resilience Efforts Must Be Holistic
2. Building a Resilience-Centric Culture and Mindset is Essential
3. Enable Resilience Through Governance
4. Transparency and Measurability Are Key
5. Resilience Must Be Sustainable and Adaptable
6. Eliminating Complexities Improves Resilience

require that the design of modern architectures embed resilience into both applications and infrastructure to meet availability and reliability demands.

A set of Technology Resilience Principles were leveraged as enterprise guidance, informing the end-to-end application delivery process, as detailed in our 2019 white paper. These principles keep technology resilience at the center of everything we do, and identify and define resilience considerations that should be applied across infrastructure and applications during the delivery lifecycle.



Technology Resilience Principles

The following key categories encompass DTCC's technology resilience principles, applying considerations consistently during the application delivery lifecycle with reusable capabilities and components leveraged as much as possible.

- **Regional Availability:** Architecture must be designed for redundancy with auto-correct capabilities for each component within and across local sites by leveraging multiple instances of data, compute, and networks. Applications and infrastructure need to perform under all circumstances, and require targeted planning for capacity needs.

- **Design Resilient Applications:** Applications should be designed to detect internal and external failures and incorporate capabilities to recover from such failures, safely leveraging automation whenever possible. Resilient applications are also designed to be independent of other applications to help isolate data & compute failures. Applications should also be capable of having their workloads rotated across multiple data centers.

- **Leverage Out-of-Region Recovery:** Applications should be able to recover from disruptions and incidents at an alternate region to protect from local region failure scenarios affecting service availability. Augment capabilities to maintain data consistency across regions, like data reconciliation tools to identify and remediate gaps.

- **Resilience Success:** All solution designs require adequate validation processes so that each critical business service can determine its health and resilience success can be verified upon recovery, leveraging key performance indicators and automated responses when possible. Controls should be created to help prevent the corruption and/or destruction of production or reference data, source code and configuration data.

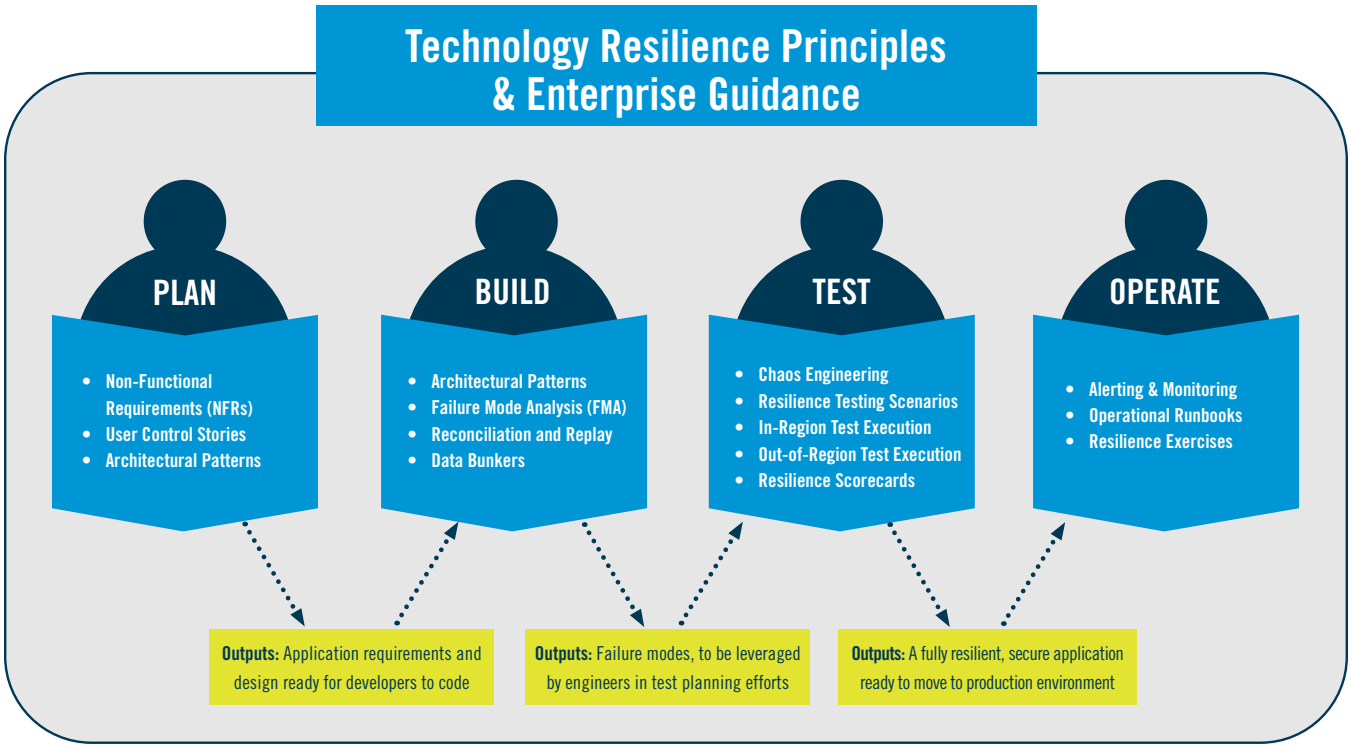
OUR APPROACH TO DELIVERING RESILIENCE

As DTCC modernizes, our IT governance processes have been adapted to enable our enterprise goal of delivering resilient applications while improving speed-to-market and creating efficiencies. We have developed a standard set of repeatable practices and capabilities for Agile squads and project teams to leverage, organized across a multi-phase application delivery lifecycle of Plan-Build-Test-Operate. These processes help reduce traditional reliance on physical infrastructure to enable resilience and yield key outputs that enable delivery of common, repeatable resilient applications.

As part of this framework, we recommend the system delivery process includes enterprise-wide artifacts like resilience principles, non-functional requirements, user control stories, and resilience scoring templates for accurate planning. In totality, these guidance documents result in a shared repository of resilience best practices and recommendations on how to implement technical capabilities, consume enterprise services, enhance coding specifications, influence test planning and drive automation. With the practice of 'build once, use many' at top of mind, these shared artifacts will enable firms to rapidly – and predictably – deliver high quality software solutions and resilient services to clients.

To help an application meet resilience goals, every team should start by including the resilience user stories (based on non-functional requirements) at project initiation. At DTCC, these stories influence the backlog items created in planning phases as well as the creation of an application's logical architecture, which captures the required business processes and data flows. As the logical architecture gets translated into a technical design, it is enabled by a catalog of resilient patterns, vetted by a failure mode analysis process, followed by a resilience scoring exercise. All application designs leverage reusable capabilities (e.g., reconciliation and data replication) to improve time to market and efficiency. Once the application has been built, we designed a testing framework to confirm that it meets all technology resilience characteristics in addition to performance and functional requirements. These efforts drive operational considerations, including enhancements to system alerting and monitoring capabilities to generate early warnings of degraded or failed services.

The following diagram illustrates each aspect of this process implemented as part of DTCC's overarching resilience workflow, enabling agile delivery of resilient and secure applications, with the ability to measure against the resilience principles at each step. Subsequent sections of this paper provide more details on capability objectives and the key outputs from the lifecycle phases.



Technology Resilience Capabilities

PLAN

Principles, Non-Functional Requirements, and User Control Stories

The evolution of our resilience practices started with the development of enterprise guidance, defining the criteria that supports delivery of resilient solutions to clients in a repeatable, standardized manner, fit for purpose and consumable by teams for various needs – including project planning and definition of test scenarios.

Firms should establish a set of technology resilience principles to guide the development of all software, services, and components. This exercise helps developers and engineers design and architect resilient applications, which can be later derived into non-functional requirements (NFRs) to enable teams to design and measure a solution in the context of resilience.

Further translating NFRs into a set of project-friendly user control stories and testing objectives allows Agile squads and project teams to leverage these as user control stories during planning and design phases. Test engineers will use the defined testing objectives to make sure test scenarios sufficiently confirm an application meets the spirit of the resilience principles.

BUILD

Architectural Patterns

Architectural patterns are a library of common patterns – like reference architectures[1] and use case architectures[2]

1 **Reference architecture** is a model for implementation of a business architecture which specifies technical architecture, key components, functional requirements, and non-functional requirements.

2 **Use case architecture** is a detailed, technology-specific architecture by our engineers to satisfy non-functional requirements such as resilience, disaster recovery, and business continuity.

– that can be leveraged by all teams. Originally created to enable faster time-to-market for our applications, at DTCC, these patterns have quickly evolved as the go-to assets required to help deliver repeatable, resilient solutions. Firms should consider storing these assets in a central, internal IT Marketplace, where all developers and engineers can be readily equipped with consistent, common patterns that have been tested and proven.

Failure Mode Analysis (FMA)

Failure Mode Analysis is a collaborative exercise conducted by architects, engineers, test engineers, and developers to investigate the application's technical design with the goal of identifying failure points in the system and their resulting effects.

PATTERNS IN ACTION

At DTCC, we have designed an architecture pattern that enables individual applications to rotate between regional data centers. This allows any business to schedule the move of production processing in advance of a potential disruption due to impending regional power or environmental conditions.

The process begins by understanding the business workflow and technical design of an application and identifying what could go wrong – a failure mode – with each component, interaction, and dependency. For each failure mode, the team consults the developer(s) to discuss potential impacts, as well as how to detect and mitigate the failure mode. As there are many moving parts in a modernized application architecture, at DTCC, we have implemented a comprehensive FMA process that brings resilience considerations to the forefront in the design stage. As new, critical failure modes are identified, we recommend documenting these in a centralized catalog with previously discovered failure modes. The results of FMA can be addressed through design changes to architecture patterns and/or code enhancements, then made available to a firm's IT community as reusable assets.

TEST

Chaos Engineering

Chaos engineering is the discipline of experimenting on a distributed system to build confidence in the system's capability to withstand turbulent conditions. These conditions could be anything from a hardware failure, to an unexpected surge in client requests, to a malformed value in a runtime configuration. Firms should consider implementing chaos engineering practices in their resilience practices, to confirm new technologies and services meet standard resilience principles and are compatible with the reusable patterns and capabilities already in use. As part of standard operating procedures at DTCC, when we apply chaos conditions to experiment with new technology and systems, we measure and document results to advance our alerting and monitoring indicators, inform new operational recovery steps, and better align patterns for target use case opportunities.

Technology Resilience Testing

Testing for technology resilience starts as soon as a technical diagram is produced. DTCC built a robust testing framework that leverages automation and standard processes to confirm applications are consistently tested against our resilience principles. With the failure modes identified earlier in our software development lifecycle, as well as previously identified failure modes for other applications, IT leverages a centralized catalog of resilience test scenarios to plan testing efforts, and builds new scenarios when needed. In doing so, this confirms testability (ways to simulate failure modes and findings from chaos engineering) and acceptance criteria (for observability / measurement). When applications complete the build phase and are fully functional, teams are ready to develop test scenarios and scripts and conduct resilience testing. There are few components of resilience testing that firms should contemplate including in their application delivery lifecycle to ensure delivery of secure and resilient code:

- **Resilience Scorecard:** This is a review process of the application architecture that scores the implementation plan against the resilience principles and resilience NFRs. This process also considers the results of failure mode analysis during scorecard grading. The output is a series of findings that are assessed for risk prioritization as the solution is planned.
- **Resilience Testing Scenario Creation:** Enterprise test engineers determine a set of critical business scenarios based on discussions with product owners and stakeholders. Additionally, failure modes identified through the earlier failure mode analysis process are leveraged to create additional resilience testing scenarios. Testing teams create the appropriate test data sets to execute this comprehensive set of testing scenarios.
- **In-region Test Execution:** In this step, engineers execute the defined resilience test scenarios leveraging failure conditions from which the application is expected to recover within the region of operation.
- **Out-of-region Test Execution:** Test engineers further execute resilience test scenarios with failure conditions which mandate recovery in the alternate region with verification of operational runbook procedures.

DTCC recommends investing in the following technology capabilities to deliver resilient solutions in new ways:

- Reconciliation service with data replay to confirm data consistency has been achieved before and after a Disaster Recovery (DR) or rotation event.
- Data bunkers that deliver synchronous copies of data, mitigating the risk of single copies and helping reduce Recovery Point Objectives.
- Immutable data copies that allow for business resumption from extreme cyber events targeting our most critical data.
- Global and local traffic management along with automated health checks to dynamically redirect traffic based on service availability.

OPERATE

Beyond designing new solutions and capabilities to advance our technology resilience strategy, a change in operational processes is essential to success. To support granular levels of resilience, we augmented the following capabilities and recommend these components be part of technology resilience frameworks across the industry:

- **Alerting and monitoring** should be enhanced to be more dynamic and location aware, enabling engineers to quickly determine if an environmental failure condition affects service availability so they can take appropriate steps to remediate, including relocation to an alternate data center.
- **Operational runbooks** must evolve to support enhanced resilience. Applications are decoupled from each other and, as a result, require individual automation and orchestration steps covering procedures like graceful shutdown and rotation as well as data validation and processing verification. In addition, there will be new steps needed to re-protect (e.g., reverse data replication flow) all applications so they can be DR and rotation-ready in the alternate region.
- **Resilience exercises** are also constantly evolving. Traditionally, at DTCC, we have performed monolithic DR

exercises on a regular schedule. Now, reimagined resilience exercises will help achieve a more continuous state of readiness for a disaster event. Our end state of loosely coupled applications that can independently operate in either region will allow us to test production applications more proactively by relocating them to alternate regions. It is critical to increase pre-production readiness testing capabilities with chaos engineering, failure mode analysis, and other framework practices.

LOOKING AHEAD

Our technology resilience vision is key to enabling overall business resilience and central to DTCC's value proposition. Reflective of our commitment to improving resilience to enhance financial stability, we share our experience and best practices in an effort to collectively safeguard post-trade processing for the financial services industry.

Through partnership across the enterprise, we translated our technology principles into guidance, reusable patterns, and created enterprise capabilities to build and operate resilient technology. We will continue to build on this foundation to expand the coverage of these patterns and capabilities to a broader set of our core applications. As industry expectations around resilience evolve, we remain focused on enabling enhanced capabilities that cover use cases on cyber and operational resilience, embedded in both our application and infrastructure layers.

Modern software applications are composed of applications, infrastructure components, and services sourced by critical partners and vendors. DTCC's technology resilience framework recognizes the importance of engaging vendors in the processes described in this paper, ultimately yielding benefits from the varied experiences and disciplines each vendor represents, while overlaying our resilience requirements to enrich our vendor-powered products.

Improving technology resilience is a journey that requires collaboration with clients and partners to calibrate and refine our approach. It is our intent for this white paper to create valuable discussion and dialogue on this important topic.

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.™