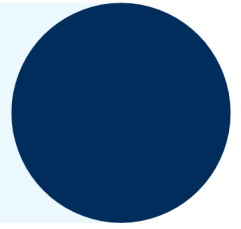


# Tradeweb Business Continuity & Disaster Recovery Fact Sheet



## Our Strategy, Approach, & Governance

Tradeweb Institutional, Tradeweb Direct, Dealerweb and Execution Access (collectively, “Tradeweb”) are committed to providing uninterrupted delivery of their products and services to clients. As a global institution, our organization is exposed to uncontrollable events that cause varying degrees of disruption to normal business processes. Our Business Continuity Management (“BCM”) program is a critical component of our enterprise resiliency strategy and is designed to plan for, respond to, and recover from business interruptions, with a view to minimize their impact and facilitate service continuity both within recovery time objectives and based on prioritization of business objectives and operations. Business Continuity is part of Tradeweb's operational resiliency program, which aligns, centralizes, and integrates disciplines and capabilities to deliver timely and effective incident identification, impact assessment, escalation, communication & resolution; and help Tradeweb businesses deliver resilient world-class products and services.

As a key component of Tradeweb’s system resiliency, we maintain a global program for BCM that facilitates activities designed to protect the firm during a business continuity event. A business continuity event is an interruption with potential impact to normal business activity of the firm’s people, operations, technology, suppliers, and/or facilities. The BCM program’s core functions include business continuity planning (with associated testing) and crisis management. Tradeweb has extensive governance and senior level oversight, focus, and support in place for managing this program. Governance groups include Executive Management, Tradeweb’s Risk Steering Committee and Tradeweb’s Business Continuity Steering Committee, which is comprised of key executives and senior members of Technology, Infrastructure, Risk Management, Cybersecurity, Marketing/ Communications, Human Resources, Corporate Services, Internal Audit, Legal, Regulatory Compliance and senior level Business Managers.

## Business Continuity Management

Tradeweb’s continuous and iterative BCM Framework comprises the activities and methods for identification, assessment, mitigation, and monitoring of Operational Risks including External Disruption Risk. Therefore, the BCM Framework supports timely, transparent, and well-informed management decisions to accept or mitigate the risk of disruption from an external event. Each BCM Framework component yields insights that inform risk- management reviews and lead to further improvements. Additionally, Tradeweb maintains Business Continuity Plans specific to locations, processes, and business requirements. These Business Continuity plans define a number of preventive (mitigation) strategies, crisis response strategies, and recovery strategies to ensure the continuity of Tradeweb's business operations, including:

- Capability to work from secure remote locations
- Capability to transfer responsibilities to an alternate location; this includes cross-training of employees
- Capability to relocate employees to a secure alternate location
- Capability to move technology processes to alternative locations
- A Pandemic Response Plan to ensure the safety of our staff and the continuation of business operations

## Disaster Recovery

Disaster Recovery (“DR”) is an integral part of our infrastructure, systems, and testing.

- Tradeweb utilizes the services of global leaders in data center colocation and interconnection services, who provide Tier 3 level, fully redundant, co-location environments serving as data center locations for all Tradeweb businesses
- Production and DR for geographically diverse locations are in completely physically separated data centers in excess of 750 miles of each other. Data Centers are located in the US, United Kingdom, and Japan
- Co-location services consist of physical and environmental protection controls, including but not limited to; physical security, heating ventilation and air conditioning, fire detection and suppression, and power
- Tradeweb systems operate in multiple Tier 3 equivalent data centers, acting as primary and secondary DR hot sites. Data is replicated real time across sites providing a hot site recovery strategy so that affected systems are re-directed from one site to the other with minimal disruptions
- If DR is invoked, sufficient redundancies and system capacity within the Tradeweb System have been built-in to handle the alternate location’s traffic and fully replicate all the data generated intra-day in all locations
- Data Center and Network failover is exercised during the annual SIFMA industry-wide Disaster Recovery Test and on a scheduled basis at a minimum

## Crisis Management

Crisis Management is the process of identifying and managing the firm’s operations during business continuity events. This is a critical component of Tradeweb’s Business Continuity Framework. Procedures include strategic goals and operational processes for responding to and managing incidents that may severely impact Tradeweb, its customers, employees, and/or other stakeholders.

In the event of a disruption, our dedicated Business Continuity and Disaster Recovery (“BCDR”) governance and support teams lead a coordinated and effective enterprise process to triage, assess impact, respond and recover, and glean lessons learned to improve our resiliency posture. Governance groups take charge of understanding the disaster and activating procedures for Tradeweb to continue business services amidst the disaster. Governance groups include Executive Management, Tradeweb’s Risk Steering Committee and the Business Continuity Steering Committee. The Business Continuity Steering Committee will meet regularly throughout a disaster to discuss the state of the event, make recommendations to Executive Management, and evaluate plan effectiveness. Support groups relay and execute planned procedures throughout the company to make resilient services a reality. Support groups include the Technology, Infrastructure, Risk Management, Cyber, Corporate Services and Marketing departments, who use guidance from governance groups to determine appropriate communication avenues, alternate employee work locations, access points to Tradeweb systems, and corporate communication. Collectively, these governance and support groups are vital to ensuring effective business execution during the BCDR situation as well as procedural improvements after the situation via post-mortem analysis of lessons learned.

## Pandemic Management

Tradeweb has a defined Pandemic Response plan that is designed to enable Tradeweb to meet the following objectives:

- Ensure the safety of our staff
- Ensure continuation of business operations and orderly markets
- Ensure that communication protocols are established and effective to clearly articulate necessary actions internally and as necessary, externally
- Creating a culture of infection control in the workplace
- Establishing contingency plans to maintain delivery of services during times of significant and sustained employee absenteeism
- Established and tested mechanisms allowing employees secure methods of alternate location connectivity

## Business Impact Analysis & Operational Risk Assessments

### Business Impact Analysis

A Business Impact Analysis (“BIA”) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. The BIA includes for each business unit and support function, an assessment of the processes in each location including the Recovery Time Objectives (“RTO”), the Recovery Point Objectives (“RPO”), and the systems and applications supporting these processes. This enables an assessment of the potential Financial, Operational, Regulatory and Reputational impact to the company.

Where applicable, a BIA may be periodically performed to determine which tasks, processes, systems, and applications are critical for Tradeweb to sustain service. In addition, a BIA may also be performed as part of our ongoing Risk Assessment process and in conjunction with the annual SIFMA industry-wide Disaster Recovery Test. Note that each business unit may also periodically conduct its own BIA to ascertain all required tools, technologies, applications, external connectivity, personnel, etc. that are necessary to continue operations.

### Operational Risk Assessments

Tradeweb’s Integrated Risk Assessment Program forms a holistic profile of risks stemming from external disruptions, prior incidents, Audits (internal & external), and collaboration with stakeholders. Information obtained from each component informs the other assessments, resulting in an integrated, repeatable, and scalable risk-assessment cycle. The Risk Assessment identifies the probability of risks to an organization and evaluates the impacts if these risks develop into an emergency. Tradeweb conducts Risk Assessments across the organization on an annual basis at a minimum. The results of Risk Assessments are utilized to inform Business Continuity and Disaster Recovery Planning.

Note that Risk Assessments and BIAs are performed periodically in order to ascertain the ability for resiliency during a BCDR event from a human resource and technology perspective.

## Business Continuity Supplier Risk

Tradeweb assesses and performs risk-based due diligence on third-party service providers’ resiliency and ability to continue to provide services during an event. As part of Tradeweb’s Enterprise Risk Management program, we perform thorough risk reviews of prospective vendors prior to onboarding, as well as ongoing & formal annual risk reviews of critical vendors. The scope of these reviews includes an assessment of our third-party service provider’s Business Continuity and Disaster Recovery Plans, including BCDR controls in place and results of testing performed. Additionally, technology testing with these vendors is conducted periodically, as appropriate by our Technology and Infrastructure teams.

## Telecommunications & Connectivity

Redundant connectivity and system resiliency are key components of Tradeweb's BCDR framework. Tradeweb's system network infrastructure is designed to provide a robust and fully redundant infrastructure for support of Tradeweb clients. Tradeweb's system infrastructure including telecommunications, power, uninterruptable power supply, environmental measures, and all network components including, but not limited to, servers, routers, switches, firewalls, etc. classified as critical components needs for support of the production systems have been designed with full redundancy, availability, and backup. All systems, applications, and databases are replicated in real time across Tradeweb's data center locations.

If Disaster Recovery is invoked, sufficient redundancies and system capacity within Tradeweb systems have been built-in to handle the alternate location's traffic and fully replicate all the data generated intra-day to all locations. All applications and database servers are run as hot backups and replicated real time so that affected systems are re-directed from one site to the other without any interruptions. Additionally, on a daily basis, backups are performed, encrypted, and archived to an alternate data center.

## Testing, Planning, & Reviews

Our resiliency posture is continuously enhanced through a rigorous BCDR planning, testing and review program. A variety of exercises enable us to challenge, verify, and demonstrate our ability to mitigate disruption risk/impact, identify improvements, and validate recovery capabilities. Our Business Continuity Plan establishes the requirements for the types of BCDR testing, their frequency, and test participant roles and responsibilities. Exercises include:

- Enterprise DR Testing: periodic, large-scale exercises to assess our ability to failover and maintain operations.
- Targeted DR Testing: frequent, targeted tests to assess the resilience of specific applications
- BCDR Emergency Notification Testing: to validate our ability to communicate instructions and ascertain staff well-being and availability
- Alternate Site Testing: demonstrating our ability to continue working from an alternate facility when the primary facility is unavailable
- Site-based Testing: to assess our ability to collectively move people and processes from one physical location to another
- Remote Capability Testing: to test our ability to work from home in the event of a loss or disruption to existing office locations
- Employee Cross Training Testing: to assess our ability to transfer work to employees across multiple locations
- Industry Collaboration and Testing: participation in global forums and sector exercises to ensure integration with industry and market partners

BCDR testing is conducted annually at a minimum. Note that Tradeweb is an active participant of the annual SIFMA and Regulation System Compliance Integrity industry-wide Disaster Recovery Failover test which includes registered clients across business units.

Tradeweb's BCDR Plan is formally reviewed and updated annually at a minimum and when necessary, to incorporate any changes in our business operations, personnel or organization, critical systems/infrastructure, and applications. Please also note that Tradeweb's Enterprise Risk Management Department manages and reviews all BCDR program policies and procedures as part of our document review process to ensure they are properly reviewed, updated and approved on an annual basis at a minimum.

### Control Testing

Controls are tested in an ongoing fashion by both internal, external and regulatory sources. Tradeweb employs a Three Line of Defense model. This model requires all Tradeweb employees to be Risk Mitigators as part of the first line of defense. The second line of defense is comprised of the Risk Management and Regulatory Compliance departments who are responsible for designing and monitoring Tradeweb's overall Risk Management Framework and compliance to the Framework, monitoring compliance with Regulations, compliance testing, and internal escalation and notification of any risks/incidents. Tradeweb is also required to remain in compliance with regulatory agency rules from regulators such as the SEC, FINRA and CFTC, to name

a few. The Internal Audit team as the third line of defense, performs on-going internal reviews of our controls. In addition, Tradeweb facilitates annual SOC 1 and SOC 2 audit reviews performed by a third-party accounting firm.

## **Employee Training & Awareness**

Tradeweb has developed a program for providing business continuity training, at least annually, to all required personnel. Training is designed to promote an understanding of business continuity, as well as the roles of BCM and personnel during a business continuity event and as the business recovers. Personnel are responsible for completing the training and familiarizing themselves with their Business Unit Coordinators and business continuity plans.

## **Communication Plans**

As part of Tradeweb's BCDR Policy and Procedures, we maintain communication plans (via appropriate teams) for notifying key client representatives, employees and regulators in the event of a disruption to Tradeweb's operations.

### **Client Communications and Questions**

Incidents that affect clients will be communicated to key client representatives as soon as possible by their respective Relationship Manager or Tradeweb Client Services Team. Should there be a significant operational disruption, clients are encouraged to visit the Tradeweb website (<http://www.Tradeweb.com>) for additional information.

For any additional questions regarding our BCDR program, please reach out to our Tradeweb Risk Management Team ([TWRM@tradeweb.com](mailto:TWRM@tradeweb.com)).