Enterprise Resilience Program Overview

Business Continuity and IT Disaster Recovery

August 2023

Table of Contents

Organization Overview

Morningstar, Inc. is a leading provider of independent investment research in North America, Europe, Australia, and Asia. The Company offers an extensive line of products and services for individual investors, financial advisors, asset managers and owners, retirement plan providers and sponsors, and institutional investors in the debt and private capital markets. Morningstar provides data and research insights on a wide range of investment offerings, including managed investment products, publicly listed companies, private capital markets, debt securities, and real-time global market data. Morningstar also offers investment management services through its investment advisory subsidiaries.

Governance

Morningstar is governed by the Board of Directors, which is currently composed of ten members, eight of whom are independent directors. The Board has three committees - Audit Committee, Compensation Committee, and the Nominating and Corporate Governance Committee - each of which is chaired by an independent director. Morningstar's daily operations are directed by eleven Executive Officers led by Morningstar's Executive Chairman and founder, Joe Mansueto. On January 1, 2017, Kunal Kapoor became Morningstar's Chief Executive Officer and a member of Morningstar's Board of Directors.

Organizational Structure

Morningstar's organizational structure supports the achievement of our corporate objectives. Reporting lines are sufficiently defined, and authorities and responsibilities are adequately controlled and monitored across the organization. Individuals are held accountable for their internal control responsibilities in pursuit of Morningstar's objectives.

Code of Ethics

Our Code of Ethics provides a framework to help make good decisions when faced with ethical questions. While not intended to be comprehensive, the Code of Ethics covers a broad range of topics including personal accountability, conflicts of interest, anti-bribery, confidential information, accounting standards, hiring practices, discrimination, business conduct, and compliance with law. Employees receive a copy of the Code of Ethics when they begin working for Morningstar, and it is distributed to them on an annual basis.

Morningstar has established a confidential Ethics Hotline that anyone may use to report complaints or concerns about ethics violations, including accounting irregularities, financial misstatements, problems with internal accounting controls, hostile work environment claims, or non-compliance with external rules and regulations.

Hiring Practices

Morningstar adheres to all local, state, and federal laws regarding hiring and employment practices. We strive to maintain a standard of excellence in its practices that minimizes risk associated with the employment relationship. Candidates often go through several rounds of interviews. The

experience and skill of candidates for employment are evaluated before they assume the responsibilities of their position. All employees are subject to a mandatory pre-employment background screening. Non-employees (e.g., consultants, vendors, etc.) who are granted certain access to Morningstar buildings, personnel, or technology go through a similar background screening process prior to providing services. Employees and non-employees in non-U.S. offices are subject to background screening as provided for by local law.

Audit and Compliance

Morningstar continuously monitors the effectiveness of its business processes, risk management, compliance requirements, and internal controls. Our independent internal audit function, Internal Audit Services, regularly performs financial, operational, and compliance reviews as well as process improvement consulting engagements. Internal Audit Services helps Morningstar achieve its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, controls, and governance processes. An annual enterprise-level risk assessment is conducted by Internal Audit covering the following areas: general business, financial, legal and compliance, operations, technology, and strategic initiatives. Management monitors changes in risk throughout the year and adjusts its risk strategy accordingly.

The Compliance Department has established compliance policies, training, and monitoring practices relevant to each of the business groups within its purview. The Chief Compliance Officer appears before the Audit Committee of the Board of Directors at least annually to review various aspects of the global compliance program and various compliance matters.

Enterprise Resilience

Morningstar recognizes the potential strategic, operational, financial and stakeholder support risks associated with service interruptions and the importance of maintaining capability to continue critical business processes, with minimum impact, after a business disruption event. The enterprise-wide goal after a major emergency or disaster is to restore all critical business activities and supporting technology in a timely manner. The Enterprise Resilience Program provides a framework to ensure that Morningstar can recover after a business disruption event that causes a loss of facilities, technology, staff, or vendors.

Resilience Program Scope and Structure

Enterprise Resilience Program is applicable to all Morningstar entities globally and applies to all locations, subsidiaries, business units, departments, information processing facilities, personnel, consultants, contractors, and third-party personnel.
The Program consists of two distinct but closely related parts: Business Continuity Management (BCM) and IT Disaster Recovery (ITDR) programs.

- **Business Continuity Management**
  Business Continuity Management program is focused on creating a system of prevention and recovery procedures that ensures that Morningstar's people, offices, and business processes they support, are protected and able to quickly recover when a business disruption event occurs.

- **IT Disaster Recovery**
  IT Disaster Recovery program focuses on the technology used to support Morningstar's internal operations and delivery of our products and services. It establishes and governs the processes by which disaster recovery plans are implemented and tested, with the ultimate goal to enable effective and timely recovery of our technology capabilities in the event of a disaster.

All-Hazards Approach to Enterprise Resilience

Morningstar's Enterprise Resilience Program is developed using all All-Hazards Approach to resilience. This risk-based approach begins with identifying potential hazards, their likelihood of occurring, and impacts they may have, while accounting for any existing hazard prevention, deterrence, and risk mitigation capabilities.

As it is impractical to develop a specific plan for every possible hazard for every location, All-Hazards Approach uses identified risks to inform the development of continuity strategies and a broad range of capacities and capabilities that enable recovery from a wide variety of business disruptive events that may impact Morningstar, such as acts of violence, pandemics, natural disaster, and any other natural, technological, or human-caused incidents.

Program Governance and Oversight

Enterprise Resilience Steering Committee

The Enterprise Resilience Steering Committee serves as the primary steering group for the development and continued enhancement of the Enterprise Resilience Program and is comprised of executive management from across the enterprise. The Steering Committee's primary responsibilities include:

- Oversight – Provide oversight and governance over the Enterprise Resilience Program
- Risk Mitigation – Provide direction and guidance for resilience-related risk mitigation
- Prioritization – Set priorities for Enterprise Resilience Program execution and risk mitigation
- Accountability – Ensure accountability for mitigation of Business Continuity and IT Disaster Recovery risks

Chief Financial Officer - Business Continuity Program Executive Sponsor

Provides support and oversight over development and implementation of the organization-wide Business Continuity program.

Chief Technology Officer – IT Disaster Recovery Program Executive Sponsor

Provides support and oversight over development and implementation of the organization-wide IT Disaster Recovery program.

Enterprise Resilience Policies and Standards

The purpose of Morningstar's Enterprise Resilience Policy is to define the scope and overall objectives of the resilience program. This policy is designed to establish a framework that outlines the responsibilities of each business unit and corporate group along with specific requirements each group must meet in order to ensure enterprise resilience. The key elements of Morningstar's resilience policy include:

- Roles and responsibilities
- Risk identification, classification, and mitigation process
- Planning requirements
- Plan review and maintenance requirements
- Exercise and testing requirements

Vendor Management

To ensure Morningstar's compliance with internal resilience standards and regulatory requirements, we have established a risk assessment and due diligence process for our vendors, aimed at ensuring that our vendors meet or exceed the same standards.

An initial risk assessment is conducted with each potential vendor and at that time vendor is assigned a risk rating. Risk rating is based on the potential business impact that vendor may have to Morningstar's processes in the event it faces a disruption, following the same standards that are applied to the internal applications and dependencies. Vendor is always assigned highest risk level attributable to the contract, or sum of all contracts, with that vendor. Vendor risk re-assessments is generally performed as part of contract renewal or anytime the relationship with the vendor changes in any significant way.

To ensure continued compliance with requirements and standards necessary for reliable provision of contracted services, periodic due diligence inquires may be performed on any of Morningstar's vendors. The degree and frequency of due diligence required will depend on the vendor's risk rating and applicable regulations.

Resilience Training

Resilience Training is divided in two different categories – all employee training and position-specific training.

All employee training is delivered and assigned to all company employees as a part of the enterprise-wide annual mandatory training curriculum. The purpose of this training is to ensure that all employees understand the Enterprise Resilience program, to know what to expect when a business disruption occurs, and to understand their roles and responsibilities in a disruption.

Position specific training is aimed at members of the Local and Corporate Incident Management Teams. This training covers topics such as incident management, emergency notification, and similar topics related to their responsibilities.

Client Communication

In the unlikely event of a service disruption, Morningstar has a dedicated internal incident management teams, as well as policies and procedures in place to track and manage incidents. Morningstar will notify impacted clients as soon as possible via the client relationship manager, and then continue to provide regular status updates to the affected clients until such time that service is restored to its normal state.

Business Continuity Management Program

The Business Continuity Management program is focused on creating a system of prevention and recovery procedures that ensures that Morningstar's people, offices, and business processes they support, are protected and able to quickly recover when a business disruption event occurs.

In order effectively protect our business and ensure minimal impact during and after an incident, Morningstar requires that all business units actively participate in the Business Continuity Management (BCM) Program.

Business Continuity Strategies

In accordance with the Enterprise Resilience policy and All-Hazards Approach, Morningstar formulates methods and strategies that ensure that critical business functions and services are restored within their recovery objectives following a business disruption event.

Morningstar's recovery strategies for incidents impacting people or locations enable recovery from:

- Short-term loss of staff or facility (up to 7 days)
- Long-term loss of staff or facility (7 to 31 days)
- Loss of critical vendors

Incidents impacting Morningstar's technology are addressed as a part of IT Disaster Recovery Program, detailed below.

Business Continuity Planning Process Overview

A strong planning process is at the core of Morningstar's approach to Business Continuity. This enables Morningstar to continuously improve based on ever changing client needs and business environment.

Business Continuity Planning is a continuous process, made up of five distinct phases.

- **Risk Assessment**
  Risk assessment is the process used for identification of hazards that could negatively impact the organization's ability to conduct business at any given location. These assessments help identify inherent business, technological, natural, and human caused risks and evaluate measures, processes and controls that were implemented to reduce the impact of these risks. Risk assessments inform all subsequent stages of continuity planning, and they are reviewed at least annually.

- **Business Impact Analysis**
  The Business Impact Analysis (BIA) identifies critical business functions, prioritizes order of recovery, and determines the impact to the organization if those functions become unavailable for a given period of time. The BIA includes all information necessary to classify critical locations, employees, processes, dependencies, and vendors. BIAs are completed for each business group represented at any given location and reviewed at

least annually. Once completed, BIAs become an integral part of the Business Continuity Plan.

- **Business Continuity Plan Development and Update**
  Business Continuity Plans are designed to mitigate potential impacts of threats facing Morningstar, by outlining recovery processes and procedures necessary to recover from a business disruption event. The plan development process is informed by the risks identified in the Risk Assessment and aim to mitigate business impacts quantified in the BIA. To ensure that plans remain actionable, they are reviewed at least annually, or whenever there is a significant change in business needs or requirements that may affect a plan's validity.

- **Business Continuity Exercises**
  While it is extremely important to have BC plans in place to ensure quick recovery, it is equally important to maintain these plans in a state of readiness. Morningstar does this through regular exercises, designed to validate the policies and procedures that are currently in place. Enterprise Resilience Policy, alongside the needs of individual business units, dictate the types and the frequency of BC Exercises. In general, exercises are conducted at least once per year.

- **Exercise Validation and Plan Review**
  Business Continuity Plans are living documents. Following an exercise or a real-life event, an evaluation is conducted to assess effectiveness of the plan and correct any deficiencies. Additionally, a plan may change because of lessons learned from incidents that occurred within the industry or nationally. Best practices and instructional guidance published by trade associations, professional societies, and government entities are also utilized to evaluate and improve Morningstar's BC plans. The outcome of every exercise is documented in the After-Action Review document, outlining the capabilities that were tested, any lessons learned, and improvements that may need to be implemented.

Plan Management and Access

To ensure that Business Continuity Plans, procedures, and other related documents are always available and accessible, copies are provided to those responsible for plan execution. Morningstar utilizes a specialized Resilience Management platform to facilitate effective Business Continuity planning process management. The platform standardizes all aspects of the plan lifecycle, while enabling centralized auditing. The platform itself is hosted outside of Morningstar's data centers, on a resilient infrastructure that is geographically diverse, ensuring access to recovery plans and procedures in the event of a disaster.

Incident Management

Incident Management process is a framework for responding to a disruption of day-to-day business operations, with the objective of returning to the state of "business as usual". Incident management focuses on determining the impact of the disruption, developing a strategy for response, and recovery of impacted systems or processes in a timely manner.

This process is activated whenever a natural or human-caused incident is affecting any of Morningstar's locations and said incident cannot be handled in the scope of day-to-day operations. The Incident Management process is designed to be sufficiently flexible to accommodate incidents of all types, magnitudes, and durations, using the All-Hazards Approach. Response principles used are based on the Incident Command System (ICS).

Different Morningstar locations will have different risk profiles and varying incident response needs. To ensure a timely and adequate response, specific procedures for local incident response will be created and managed by the Local Incident Management Team that is supported by Regional and Corporate Incident Management Team.

Crisis Communication and Management

Crisis Communication and Management are actions taken to protect and defend the reputation of the organization, its brand and its products/services. A crisis may result from an incident, however, not every incident will cause a crisis, and not every crisis will be an incident.

Morningstar's Corporate Crisis Communications Plan establishes a framework for effectively managing internal and external communications in the event of a crisis in any of Morningstar's offices. The Corporate Incident Management Team and the Local Incident Management Teams are responsible for the execution for the Crisis Communication Plan.

Emergency Notification

Morningstar is committed to ensuring that our employees receive timely, accurate, and useful information in the event of an emergency at one of our offices, or in the local area, that may pose a risk to their health and safety. To support this commitment, Morningstar uses several forms of communications that allow us to distribute notifications in the event of an incident.

IT Disaster Recovery Program

IT Disaster Recovery program focuses on the technology used to support Morningstar's internal operations and delivery of our products and services. It establishes and governs the processes by which disaster recovery plans are implemented and tested, with the ultimate goal to enable effective and timely recovery of our technology capabilities in the event of a disaster.

What is IT Disaster Recovery?

The IT Disaster Recovery Program is a component of the overall Enterprise Resilience Program, focusing on minimizing disruptions of internal and client-facing IT systems by setting standards and requirements for disaster recovery environment design, planning, testing, and accountability.

Disaster Recovery Strategies

Morningstar formulates methods and strategies that ensure that the systems and/or processes that are identified as being critical can be brought back online quickly with minimal impact to the business and client experience. Recovery strategies are further tailored for each product to meet specific recovery time objectives (RTO) and recovery point objectives (RPO).

Disaster Recovery Planning Process

Strong planning process is at the core of Morningstar's approach to disaster recovery, enabling continuous improvements based on ever changing client needs and business environment. Core components of the planning process are:

- **Risk Assessment –** perform a risk assessment to identify hazards that may threaten Morningstar's technology and infrastructure.
- **Application Assessment Process** – is similar to the Business Impact Analysis, but is tailored to assess applications as a whole, to understand its potential impacts to the business, and quantify recovery requirements.
- **Mitigation Strategies** – from the risk assessment and application assessment, mitigation strategies are identified and implemented in order to minimize potential impacts from assessed risks (e.g. backups, redundancy, data replication, geographic diversity, etc.)
- **Disaster Recovery (DR) Plan Development** – plans that meet RTO and RPO requirements are developed based on identified risks while taking the application assessment data and mitigation strategies into consideration.
- **Plan Testing and Validation** – after plan development is complete, DR plans are tested through regular exercises, at least annually.
- **Plan Updates –** plans are updated and improved regularly as result of past exercises, new business requirements, and/or significant changes in environment or business requirements, at least annually.

Risk Assessment

Risk Assessment is the first step in the planning process, and it drives all subsequent steps. During the assessment, existing processes and methodologies are reviewed with the goal to identify any risks and assess product's current resilience capability.

Application Assessment

Application Assessment is conducted based on the information from the risk assessment, as well as the product's technical details. This is a Business Impact Analysis process that is expanded to include information specific to applications and technology-based services. Application Assessment quantifies impacts that a potential product outage would have on our clients and internal dependencies. This process also identifies internal and external dependencies and defines recovery objectives, including RTO and RPO that need to be met to minimize identified impacts.

Mitigation Strategies

After identifying risks and quantifying their potential impacts on Morningstar's systems, variety of mitigation strategies are employed to minimize those impacts on our infrastructure, ensuring high levels of resilience and reduction in downtime. Currently, Morningstar employs fault tolerant design for our systems, redundant network infrastructure, n-tier platform architecture combined with geographic diversity and variety of data protection methods.

- **Geographic Diversity**
  Where appropriate, Morningstar leverages geographic diversity when deploying technology solutions and systems. The goal is to mitigate single points of failure and to minimize impacts in the event that production systems are impacted by a region-wide disruption. Morningstar maintains global technology presence and has datacenters and public cloud capabilities throughout North America, Europe, Australia, and Asia.

- **Redundancy**
  Morningstar systems are designed with scalability in mind and, where appropriate, critical systems are deployed as redundant and highly available. Deploying systems to be redundant and highly available allows system engineers to rapidly assess outage incidents and recover quickly following an incident.

- **Network Infrastructure**
  All network infrastructure deployed at Morningstar is high speed and fully redundant providing reliable and consistent service to all of Morningstar's product offerings. Where applicable, load balancers are utilized to distribute traffic evenly over highly available production applications, maximizing speed and availability.

- **Fault Tolerant Design**
  Morningstar applications are designed to be fault tolerant in nature, with a specific focus placed on ensuring availability, integrity, and security.

- **Platform Architecture**
  Where feasible, Morningstar implements an N-tier architecture in which the presentation, application processing and data management layers are logically separated. Access and security controls are individually tailored to meet the unique requirements of each layer.

Where technically feasible, each tier of the system is clustered across numerous servers to ensure that it remains highly available at all times.

Disaster Recovery Plan Development

After conducting the risk assessment, performing the Application Assessment, and employing variety of mitigation strategies, a Disaster Recovery Plan is developed based on the information and capabilities identified in those steps. Disaster Recovery Plans outline specific recovery objectives, procedures, priorities, and responsibilities, that are designed so that affected systems can be returned to full functionality within defined RTO and RPO.

Plan Testing and Validation

While it is extremely important to have recovery plans in place to ensure quick recovery, it is equally important to maintain these plans in a state of readiness. Morningstar does this through regular Disaster Recovery tests and exercises, designed to validate policies and recovery procedures that are currently in place. Policy dictates that DR testing is performed at least once per year or following any significant changes. The most common testing methodology is full application failover from production to disaster recovery data center or region, where appropriate. Following a disaster recovery test, any identified issues are documented and prioritized for mitigation.

Plan Updates

Disaster Recovery plan is a living document. Following an exercise or a real-life event, an evaluation is conducted to assess effectiveness of the plan and identify gap mitigation strategies to correct any deficiencies. Additionally, lessons learned from incidents that occurred within the industry or nationally can trigger a need for plan changes. Best practices and instructional guidance published by trade associations, professional societies, and government entities are also utilized to evaluate and improve Morningstar's disaster recovery plans. Policy dictates that all DR plans are reviewed at least once per year or following significant changes to recovery strategies or applications themselves.

Disaster Recovery Planning Process Management and Plan Access

Morningstar utilizes a specialized Resilience Management platform to facilitate effective Disaster Recovery planning process management. The platform standardizes all aspects of the plan lifecycle, while enabling centralized auditing. The platform itself is hosted outside of Morningstar's data centers, on a resilient infrastructure that is geographically diverse, ensuring access to recovery plans and procedures in the event of a disaster.

Data Backup and Recovery

All data required for the effective recovery of production systems at Morningstar is backed up in accordance with the Enterprise Resilience Policy. That same policy dictates backup types, locations, and retention requirements to ensure regulatory and contractual compliance.

- **Data Backups**
  Morningstar conducts backups of its critical systems, designed to support required RPO. Backups are encrypted and stored off-site using a globally recognized vendor, archived and retained to meet regulatory requirements, and up to 7 years.

- **Restoration Testing**
  Morningstar conducts regular file-level recovery and validation tests on a random sample of backup jobs, to ensure that backups are functioning correctly. Tests are performed on different schedules based on backup media type.