Organization &
Security Practice Overview

November 2017

Table of Contents

Our mission is to create great products that help investors reach their financialgoals.

We have 4,820 employees in 27 countries worldwide, providing local market expertise.

Our clients range in size from individual investors to the world’s top asset management firms.

Financial Advisors	Asset Managers	Retirement	Individual Investors
250,000 Independents & Affiliates	1,300+ Global Firms	300,000+ Plans	10.9 mil Website Users
$35.0 bil Managed Portfolios	$63.3 bil Investment Management	$114.2 bil Retirement Solutions	

Global Regulators	Media Companies	Alliances & Redistributors
50+	95+	590+

Organization Overview

Morningstar is a leading provider of independent investment research to investors around the world. Since its founding in 1984, the Company's mission has been to create great products that help investors reach their financial goals. The Company offers an extensive line of products and services for financial advisors, asset managers, retirement plan providers and sponsors, and institutional investors in the private capital markets.

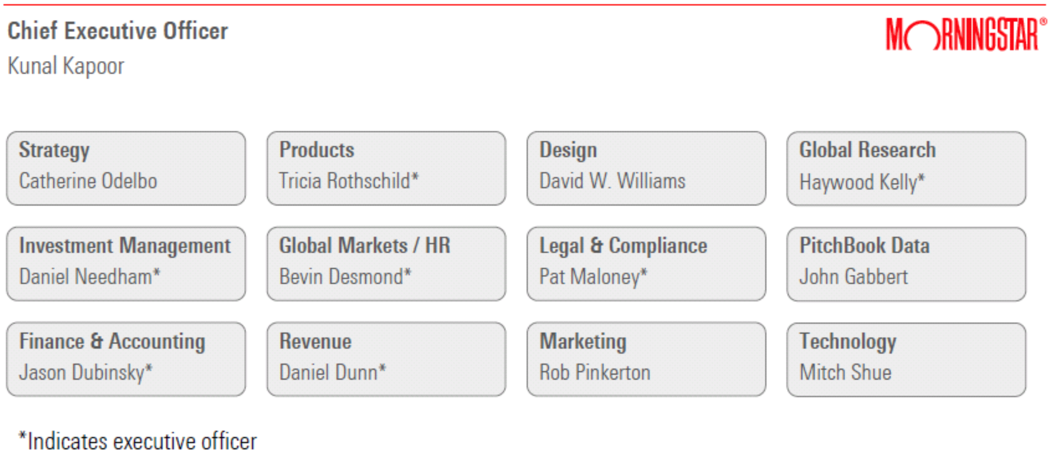
In addition to its U.S.-based products and services, Morningstar offers local versions of products designed for investors in Asia, Australia, Canada, Europe, Latin America, and South Africa. Morningstar provides data and research insights on a wide range of investment offerings, including managed investment products, publicly listed companies, private capital markets, and real-time global market data. Morningstar also offers investment management services through its investment advisory subsidiaries, with more than $220 billion in assets under advisement and management as of Sept. 30, 2017. We have operations in 27 countries.

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. The Executive Chairman of the Board is Joe Mansueto. Morningstar's daily operations are directed by eight Executive Officers led by Chief Executive Officer Kunal Kapoor.

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. The chart reflects Morningstar's organizational structure as of November 2017:



Chief Executive Officer
Kunal Kapoor

Strategy Catherine Odelbo	**Products** Tricia Rothschild*	**Design** David W. Williams	**Global Research** Haywood Kelly*
Investment Management Daniel Needham*	**Global Markets / HR** Bevin Desmond*	**Legal & Compliance** Pat Maloney*	**PitchBook Data** John Gabbert
Finance & Accounting Jason Dubinsky*	**Revenue** Daniel Dunn*	**Marketing** Rob Pinkerton	**Technology** Mitch Shue

*Indicates executive officer

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 pertaining to Morningstar Credit Ratings, LLC.

Information Security Practices

Morningstar is committed to taking reasonable efforts to secure the confidential information, assets, and intellectual property that belong to Morningstar and its clients. A number of different threats exist that endanger the confidentiality, integrity, and availability of Morningstar information. In order to be effective at protecting our information assets, employees, contractors, vendors, and third parties with access to the Morningstar network or Morningstar owned/managed facilities are required to abide by Morningstar information security policies.

Information Security Policies

Morningstar's Information Security Policies and Standards define information classification, appropriate data handling and usage, roles and responsibilities, access controls and provisioning, logging, monitoring, cryptography and key management, security awareness, virus prevention, risk assessments, physical security, mobile device policy, vulnerability management, policy enforcement, and handling of exceptions. Policies are aligned with ISO 27001:2013 and NIST SP-800 publications. Each year the Information Security Officer reviews and approves the Information Security policies.

Information Classification

Morningstar’s Information Classification Policy establishes requirements for classifying and handling information across Morningstar regardless of the form it takes (physical, digital, etc.). Information is grouped into one of the following four categories: Restricted, Confidential, Internal, or Public. Handling requirements include, but are not limited to, acceptable encryption, distribution, transmission, and storage methods depending on the classification level. The Information Classification policy prohibits transferring sensitive, non-public information unencrypted over public networks (e.g. Internet).

Acceptable Use

This policy outlines the acceptable use of Morningstar’s computing resources. The scope of the policy includes, but is not limited to, use of Internet, email systems, bulletin board systems, social networking systems, news groups, discussion forums, Morningstar’s Intranet, instant messaging applications, and all other company electronic communications mediums. The policy applies to all employees, contractors, consultants, and other individuals at Morningstar, including all personnel affiliated with third parties. It covers all equipment that is owned or leased by Morningstar or connected to Morningstar’s network.

Asset Classification and Management

Morningstar has procedures in place to approve and maintain hardware and software inventories to minimize loss due to theft, destruction or other damage. Distributed assets are identified with owners and maintained in Morningstar’s IT Catalog, a system inventory application. Asset type, format, location, ownership, installed software versions and information classification is documented where applicable. Technology Managers and/or asset owners are responsible for updating and maintaining the accuracy of inventories (such as ownership, asset retirement/decommissioning, software versions) and reporting loss, theft or damage of assets.

Policy Communication

Morningstar communicates security and confidentiality obligations including security policies, security awareness training, and ethics guidelines to employees on an annual basis. Policies and procedures related to security and confidentiality are made available to employees through email, training, and internal websites. Management promotes these policies in management meetings, communications, and leading by example.

Failure to comply with policies and procedures can result in disciplinary action, up to and including termination of employment, removal of contract personnel and/or initiation of appropriate legal action.

Security Awareness Training

At least once annually, we require Morningstar employees to complete security awareness training. Awareness topics addressed in training include company security policies, acceptable use, physical security, data privacy, information handling, social engineering, phishing, email, password use, virus and malware protection, and other security good practices. Information Security sends notifications to non-compliant employees until course completion.

Logical and Physical Security

Morningstar has established policies and procedures that include standards for logical and physical security, and tools and techniques for restricting access to programs, data, networks, and other information resources. Morningstar uses a combination of manual and automated controls to minimize the risk of information loss, theft, or misuse. We design our policies, standards, and operational procedures to mitigate the potential risks to Morningstar and client data.

Access Management

Morningstar's access control policy establishes a means to control logical access to information systems, and resources. The major components covered in this policy include user account management, privilege user access, password management, review of access rights, and the use of generic accounts. Access control rules incorporate the principle of least privilege, which grants the appropriate level of access required for an individual's specific role.

Employees, contractors, and vendors who require access to Morningstar information systems and network are assigned unique IDs to ensure accountability and traceability. Users who require access to systems and applications must open an access request and obtain approval from system owners before access is granted. In order to ensure that access rights are properly allocated, we review privileged user accounts on a quarterly basis and when a termination, demotion, transfer, or promotion occurs.

Privileged Accounts

Rights to perform system administration to programs, data, and other information resources are restricted to employees with a valid business need. System owners review application and privileged administrative access on a quarterly basis.

Remote Access

Employees who require remote access to Morningstar's network are provided access via a Virtual Private Network (VPN). VPN connections require two-factor authentication. For users who do not require remote access to the network via VPN, Morningstar provides access to an encrypted web-based corporate email system.

Termination Procedures

Morningstar uses Workday to initiate personnel termination processes. Human Resources personnel enter the termination request into Workday. All termination transactions initiate disablement of Active Directory accounts, which disable all access to application servers, email, and virtual private network (VPN). Service desk tickets are generated to the appropriate team to remove physical access and reclaim assets. A log of all activities is available either in Workday and/or our corporate service desk system.

Password Management

Morningstar has implemented password management controls in compliance with corporate standards that include minimum length, expiration, complexity, and account lockout. In addition, default vendor or system passwords must be changed following installation of software. Temporary passwords (resulting from a password reset or initial account creation) must be unique and changed after first login.

Password Policy for Internal Systems (Windows Domain)

- Minimum 8 non-sequential characters
- Expires after 60 days
- Must contain three out of the following—at least one upper case, one lower case, one numeric digit, or one special character (e.g. ! * # $)
- Lock after 5 failed login attempts
- Lock after 15 minutes of inactivity
- Last 8 passwords cannot be used
- Passwords cannot contain any part of username

Encryption

Morningstar uses strong encryption to protect transmission of user authentication and other confidential information passed over public networks (e.g. Internet). We use the industry standard TLS protocol currently used by leading financial service providers and banks to ensure the privacy of data as it moves between the user’s browser and our web servers. Highly sensitive information (credit card numbers, passwords, Social Security numbers, etc.) stored in electronic format requires encryption in transmission and storage, and cannot be held on any non-Morningstar equipment without Information Security authorization.

Network Security

Morningstar maintains a robust perimeter security program using an intrusion detection system (IDS). This system monitors Morningstar's external perimeter and reports security events to dedicated consoles. The data generated by this system is reviewed by Information Security Department members, who provide response capability and analysis on Internet-based threats. Morningstar has firewalls in place to prevent unauthorized access to the network. Morningstar's Information Security team reviews and approves firewall rules and ports. Ports and services are limited to those that are necessary to provide services.

Network Monitoring

Morningstar's security event monitoring process runs 24x7x365 and produces alerts and reports for review and mitigation, if necessary. The Information Security Department reviews various security event logs, including alert data generated by the network intrusion detection sensors and the centralized logging server, on a daily basis. Alerts are configured to identify common potential network-based security attacks to the system.

Virus Prevention

All Windows and Mac-based workstations and servers connected to the Morningstar network are required to have antivirus software installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network. We distribute virus signature definition updates are distributed to servers and desktop workstations as they become available. Alerts triggered by the antivirus clients are sent to a centralized console and the Information Security Department reviews them as needed. If necessary to prevent viral propagation, we disconnect computers infected with viruses, worms, or other forms of malicious code from the network until the infection has been removed.

Web Content Filtering

We use a web proxy and content filtering platform to control outbound Internet traffic from user workstations and to enforce corporate security policies across our network. Our web filter categorizes billions of web pages in more than 50 languages into 85 useful categories that can be blocked or allowed depending on the policies we apply. Morningstar blocks sites categorized as hacking, malicious content, malware, peer-to-peer (P2P), phishing, piracy, proxy avoidance, violence/hate/racism, spam, adult content, nudity, scams, controlled substances, and illegal activity.

Patch Management

Morningstar has established a patch management policy addressing the deployment of security and confidentiality patches to systems. We deploy operating system security and confidentiality patches to desktop and server workstations on a monthly basis. We release patches into test environments to ensure compatibility and stability is maintained before we distribute them to live production environments.

Vulnerability Management

Morningstar's Information Security Department conducts routine vulnerability scans of operating systems, network devices, and web-facing applications. Once a vulnerability assessment is complete, we present results to information and technical owners for remediation and/or risk acceptance. Information Security tracks vulnerabilities from identification to closure.

Application Security Testing

During development and prior to each release of an application, the Information Security team performs an automated static analysis scan on source code to identify common security vulnerabilities. Assessment findings are ranked by severity and entered into our bug-tracking system. The Information Security team reviews vulnerabilities with application development teams and provides a clear set of remediation instructions. We present a summary of the vulnerabilities and their associated risk ratings to management for review on a monthly basis.

System Security Hardening

Server creation and security hardening procedures outline steps for sever creation, standard settings, configurations, and account policies. Security hardening compliance jobs run on critical systems to ensure configurations are in line with Information Security requirements. If a system configuration value affecting the security of the operating system is changed, an alert is sent to the Information Security team for review and remediation. The Information Security team reviews security hardening procedures annually.

Physical Security

Access to Morningstar offices is granted on a least privilege basis. Employee security badges and card readers control access to each office. Visitors must first register with building security and must provide valid government-issued identification prior to being allowed access. Visitors are escorted by Morningstar employees at all times. Temporary security badges are available for pre-authorized visitors and vendors who require extended access.

Access to Morningstar data centers and processing facilities is strictly controlled. Key card readers linked to employee security badges control physical access. Data centers are equipped with on-site security guards and video surveillance at all entrances and exits. Access is granted to employees who require access on a regular basis to perform their job functions, and is reviewed on a quarterly basis. Should a non-authorized individual or visitor require temporary access to a restricted area such as a data center, he or she must first sign in and an authorized Morningstar employee must accompany the visitor at all times. All access attempts are logged and retained for at least 90 days by building security.

Environmental Controls

Morningstar data centers are equipped with the following environmental controls: temperature and humidity detection equipment, leak detection equipment, heating, ventilation and air conditioning ("HVAC"), uninterruptible power supply ("UPS"), redundant power feeds, fire detection systems, handheld fire extinguishers, raised floors to facilitate cooling, and pre-action dry pipe water sprinklers. Morningstar has defined thresholds for monitoring temperature levels, humidity levels, and power/water leak detection. If one of the thresholds is exceeded, it triggers an alert, and facilities and technology personnel respond to assess and resolve the issue. On an annual basis, management contracts third-party vendors to complete fire, humidity, temperature, and leak detection, and fire suppression equipment inspections.

Technology Operations Center

The 24x7 Technology Operations Center is equipped with the tools and resources necessary to closely monitor environmental protections and core infrastructure health, and maintain system uptime. This team's responsibilities include incident management and event management.

Risk Assessments

The purpose of an Information Security risk assessment is to identify, quantify, and prioritize risks against a standardized set of acceptance criteria. Risk assessments highlight areas where security policy gaps or considerable business risk exist. We routinely conduct these assessments on internal information systems (applications, operating systems, etc.), business processes, new business engagements, and external vendors / business partners.

We consider Information Security controls during the specification and design phase of new applications or project engagements. We provide a software architecture and design document to project owners to use as a guide for ensuring information security policies and standards are addressed during project specification. The review and risk assessment of new systems or applications is completed by the Information Security Department prior to implementation.

All risk assessments follow a standardized format, have clearly defined scopes, and use an approved risk analysis method to ensure repeatable results. Morningstar's Information Security team performs a risk assessment, documents findings in a standard risk assessment template, and then presents the results to the business and information system owners. From here, the owners are responsible for outlining priorities based on risk and developing a remediation plan to protect against any identified vulnerabilities. This plan is reviewed, tracked, and managed by the Information Security Department until findings are remediated.

Vendor Risk Management

We assess critical vendors, subcontractors, and other third parties that may process confidential information prior to conducting business with them. Morningstar typically provides the Standardized Information Gathering (SIG) questionnaire to third parties to complete as part of Morningstar's Information Security due diligence process. A full version of this questionnaire is used for medium- to high-risk contracts and a "light" version is used for low- to medium-risk engagements. As part of this assessment, the Information Security team will provide the potential vendor with the questionnaire and ask for security artifacts such as an SSAE 16 SOC report. Upon return, the team will review the questionnaire and all available audit documents. Policy gaps or risks are highlighted and the Morningstar Security Schedule is created for inclusion in the contract with the third-party vendor. The business unit then reviews the risk assessment and defines a risk mitigation or risk acceptance plan for review with Information Security, if needed.

Incident Management

Morningstar's Security and Infrastructure Incident Management Policy serves to minimize the impact and consequences of security- and infrastructure-related incidents; improve our ability to restore operations resulting from an incident; and ensure appropriate parties are promptly notified so that incidents are handled in a consistent and timely manner.

The Security and Infrastructure Incident Management Policy covers information security incidents such as unauthorized access to a system or database, violations by an internal employee of the acceptable use or information security policies, the introduction of viruses or malicious code, denial of service attacks, and/or loss or theft of information. Incidents are ranked according to whether sensitive information is involved, how widespread the incident is, how much the incident impacts customers or business partners, whether the incident affects critical enterprise infrastructure resources or has the potential to raise public attention, involves active threats that could cause severe impact, and/or involves breach of contract or other legal impacts.

The policy creates an Incident Management and Response team to respond to and mitigate all incidents. This team may consist of representatives from management, Infrastructure, Information Security, Corporate Communications, business unit leadership, Client Relationship Management, and Human Resources, depending on the scope and severity of the incident. The policy requires that all suspected policy violations, system intrusions, virus infestations, or other conditions that might jeopardize information or systems must be immediately reported to the Information Security Officer. All incidents that affect the availability or integrity of our networks or computing resources must be reported to our Technology Operations Center.

During an incident, the Incident Management and Response Team will start the analysis and recovery phase to direct triage, response, and recovery; provide technical support and expertise related to impact assessment, incident handling, and technical system management; report incidents to appropriate internal management teams and/or authorities as required; record incident details using Morningstar's standard incident report templates; and prepare external/internal communications and updates. The team will then use Morningstar's standard root cause analysis template to determine what controls or procedures can be put into place to prevent the incidents from reoccurring.

Change Management

Morningstar's applications and IT infrastructure components are subject to formal change management processes and procedures. Change management procedures ensure that changes to systems and applications are performed in a predictable and orderly manner. Changes are logged, scheduled, tested, approved, and communicated to system owners prior to implementation.

Development and QA testing is performed in an environment that is separate from the production environment. The Change Activity Board (CAB) and application owners review and approve change requests before release. Additionally, the Information Security team reviews changes that have the potential to affect the security and/or confidentiality of Morningstar systems. In order to maintain segregation between development, approval, and deployment, Release Managers promote changes to the live production environment. These roles are segregated from other teams, including development.

Privacy and Security Advisory Council

Morningstar's Privacy and Security Advisory Council meets on a quarterly basis to discuss environmental, regulatory, and technological changes and associated risk to security and confidentiality of the organization's information. This meeting is chaired by the Information Security Officer and consists of executive management from the Information Technology, Legal, Audit, and Compliance departments. Council meetings provide a forum for the cross-functional, global identification and resolution of security issues, endorsement of security strategies, and review of significant exceptions to information privacy and security policy. The Privacy and Security Advisory Council also works to identify key corporate security initiatives and standards (for example, virus protection, data classification, security monitoring, intrusion detection, access control to applications and facilities, and remote access policies).

Cyber Security Intelligence

The majority of the Information Security team are Certified Information Systems Security Professionals (CISSP) who provide response capability, analysis, and broad intelligence on cybersecurity threats. They subscribe to many information security websites and industry conferences to keep current with the latest cyber security vulnerabilities and trends. The Morningstar Information Security team is also a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and receives daily critical security alerts, threat notifications, and XML data feeds used in threat analysis.

Cyber intelligence is a continual, iterative process of obtaining, analyzing, and sharing threat information. The Information Security team places a great deal of importance on effectively communicating threats and vulnerabilities internally with its employees and externally with customers and shareholders.

Cybersecurity Insurance

Morningstar carries insurance coverage policy for cybersecurity-related incidents. Morningstar periodically reviews this coverage in association with Morningstar's risk assessment processes to ensure it is sufficient to cover the firm in the event of an incident.

Business Continuity Management

Morningstar recognizes the potential strategic, operational, financial and stakeholder support risks associated with service interruptions and the importance of maintaining the capability to continue critical business processes, with minimum impact, in the event of a business interruption. The enterprise-wide goal after a major emergency or disaster is to restore all critical business activities in a timely manner.

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

Executive Steering Committee

The Executive Steering Committee is responsible for the development and continued oversight of the BCM Program. The Committee is comprised of executive management representatives from across the enterprise. The Steering Committee's primary responsibilities are:

- Setting priorities for BCM Program execution
- Oversight of BCM risk identification and mitigation
- Managing risk mitigation accountability

Business Continuity Policies and Standards

The Business Continuity Policy provides standards for development and maintenance of the Business Continuity Management program at Morningstar. In the event of business interruption, this policy sets out the framework for Morningstar to manage and maintain the continuation of critical, core business functions and services and enable recovery and restoration of those functions and services. Key policy elements are:

- Roles and responsibilities
- Planning requirements
- Plan review and maintenance requirements
- System classification criteria
- Exercise and testing requirements

The IT Disaster recovery portion of the Business Continuity Management program is managed separately and governed by the IT Disaster Recovery Policy.

Business Continuity Strategies

Using the Business Continuity Policy, program strategies are defined. Morningstar formulates methods and strategies that ensure that critical business functions and services are restored in a timely manner. Those strategies are defined to ensure that the RTO and RPO identified in the Business Impact Analysis for every function can be met.

Morningstar’s planning strategies are designed to enable recovery from the short-term loss of staff or facility (up to 7 days), the long-term loss of staff or facility (7 to 31 days), as well as the loss of critical vendors.

Plan Management, Review and Access

To ensure that business continuity plans, procedures and other related documents are always available and accessible, a centralized document repository is maintained outside of Morningstar’s data centers, on a resilient infrastructure that is geographically diverse. This ensures Morningstar will have access to all necessary information in the event of a disaster, even if internal systems are unavailable.

Incident Management

Incident Response Guides are plans for actions to take in response to a disruption of day-to-day operational activities – with the objective of returning to the original state. The management of an incident focuses on determining the impact of the disruption, developing a strategy for response, and recovering impacted systems or processes. Incident Management starts when the ‘disruption’ is reported, and ceases when operations have returned to their original state.

Morningstar's Incident Response Guide establishes the organization, actions and procedures necessary to respond to incidents that may affect our employees, contractors, visitors and physical locations world-wide.

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 utilizes several forms of communications that allow us to distribute notifications in the event of an incident.

Vendor Management

To ensure Morningstar’s compliance with internal standards and regulatory requirements relating to Business Continuity, we have established a risk assessment and due diligence process for our vendors. The purpose of this process is to ensure that our vendors meet or exceed Morningstar’s standards.

Disaster Recovery Program

Morningstar understands that our clients depend on responsiveness and high availability of our products and services. We understand that even a minor outage to one of our products can have a significant impact on our customers. Morningstar's Disaster Recovery program is in place to ensure that we have effective, well designed and tested disaster recovery plans and procedures. With effective plans in place, we can make certain that there is a minimal impact to our customers in the event of a disaster.

Disaster Recovery Policies and Standards

The purpose of Morningstar's disaster recovery policy is to define the scope and overall objectives of the disaster recovery program. This policy is designed to establish a framework that outlines the responsibilities for each business unit and corporate infrastructure as a whole. The key elements of Morningstar's disaster recovery policy include:

- Roles and responsibilities
- Planning requirements
- Plan review and maintenance requirements
- System classification criteria
- Exercise and testing requirements

Disaster Recovery Strategies

Using the Disaster Recovery Policy, program strategies are defined. 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 recovery time objectives (RTO) and recovery point objectives (RPO).

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 infrastructure
- **Business Impact Analysis (BIA)** – based on the identified risks, conduct a business impact analysis
- **Mitigation Strategies** – from the risk assessment and BIA's, mitigation strategies are employed to minimize impacts from assessed risks (e.g. backups, redundancy, data replication, geographic diversity, etc.)

- **Technical Disaster Recovery Plan (TDRP) Development** – plans that meet RTO and RPO are developed based on identified risks while taking the BIA and mitigation strategies in to consideration
- **Plan Testing and Validation** – after development is complete, recovery plans are tested through regular exercises
- **Plan Updates** – plans are updated and improved regularly as result of past exercises, new business requirements, and/or changes in environment

Data Backup and Recovery

All data required for the effective recovery of production systems at Morningstar is backed up in accordance with our Backup and Recovery Policy. This policy dictates backup types, locations, and retention schedule, ensuring regulatory and contractual compliance.

Client Communications and Incident Management

In the unlikely event of a service disruption, Morningstar has a dedicated internal incident manager 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. Morningstar will continue to provide regular status updates to affected clients until such time service is restored to its normal state.