

MassMutual Business Continuity Disclosure Statement

Overview

Resiliency is a high priority at Massachusetts Mutual Life Insurance Company (“MassMutual” or the “Company”). To that end, significant focus has been made to enhance technology, workspace and remote working capability to mitigate the potential risk of disasters. The primary Data Center is located in Virginia and equipped with redundant utility feeds, uninterruptible power supply (UPS), generators, and a state-of-the-art fire monitoring system. Systems are backed up to MassMutual-owned hardware in Colorado (1,700 miles away) and Virginia (400 miles away), with a third copy of system data available in the cloud.

MassMutual's home office location in Springfield has also been backed up with generators, capable of powering around 3,700 workstations, more than we believe would be needed for the first 30 days of a recovery event. If workspace becomes unavailable in the MassMutual home office in Springfield, 95% of employees have remote work capability. MassMutual also has established critical operations and workspace outside of its home office region in Boston, New York, and a population of permanent remote workers throughout the United States.

Despite these steps to further harden systems and facilities, MassMutual still maintains a continuity planning program that is intended to address, among other things, facility/systems failure, loss of workforce and 3rd party supplier outages. This document is intended as a summary of how MassMutual's Business Continuity Program (“Program”) is structured, tested and maintained.

Program Management

The MassMutual Continuity Officer reports results directly to Executive Leadership and administratively to the Head of ETX Strategy & Governance. In the first quarter of each year, the MassMutual Continuity Officer (or delegate) composes the Annual State of Preparedness, which documents the status of projects designed to enhance resiliency and any known or reasonably foreseeable risks or concerns.

Under the MassMutual Continuity Officer is a core continuity team responsible for providing program oversight and governance of the company policy, as well as testing and consulting services. This team also manages the tools that enable situational awareness monitoring, continuity plan development and maintenance, emergency

notification and testing, and exercises of the company crisis management plan, High Severity Incident plan.

Divisional Coordinators are responsible for working with the core continuity team, and individual plan leaders within their business unit, to monitor compliance with the Company policy, develop and maintain appropriate recovery time objectives, analyze risks, and develop mitigating strategies, and oversee plan maintenance and testing requirements.

During emergencies, key representation from areas such as Communications, Human Resources, Law, Enterprise Technology, Enterprise Risk Management and impacted Lines of Business assemble to form a High Severity Incident Team, which has authority to declare a disaster and direct recovery efforts.

Risk Evaluation and Control

Risk assessments are completed annually for each MassMutual operating location. The risk assessment process is intended to consider reasonably foreseeable external risks (natural and man-made disasters) and the potential for internal vulnerabilities. As new items are discovered through the risk assessment process, the core continuity team is responsible for developing and executing the appropriate mitigating proposals, which are included in the Annual State of Preparedness. The core continuity team partners with Enterprise Risk Management for ongoing risk monitoring across the company.

Overall Resiliency Strategy

As noted earlier, MassMutual's recovery strategy is focused on diversification. Data Center recovery utilizes capabilities in other states, currently a combination of Colorado, Virginia, Texas and the cloud, intended to protect against the impact from regional disasters, and multiple replication/backup technologies are used to protect against hardware failure. Workspace recovery is available within multiple MassMutual-owned buildings in Massachusetts, with our primary site having generator backup and diverse paths for network and utilities. Broader or diverse regional protection is provided through offices in Boston and New York.

Finally, the ability for Company employees to work remotely has greatly expanded and is designed to leverage multiple solutions including remote desktop capabilities, laptops and virtual desktops, which enable 95% of the employees to work remotely. A diverse set of solutions are utilized with the purpose of ensuring that critical processes can continue, regardless of the potential disruption.

Emergency Preparedness and Response

Emergency Response Plans (“ERPs”) for each operating location document the Company’s response to business interruption and include building characteristics, emergency procedures for evacuation, shelter-in-place, damage assessment, disaster declaration, restoration management and internal/external communications. ERPs are modeled after FEMA’s Incident Command System and enable the activation of the High-Severity Incident Management Team and appropriate Response Teams, to accomplish recovery objectives and ensure timely communications both internally and externally. The Company utilizes a vendor-hosted emergency notification system for global employee communication. This system is backed up by paper-based call trees.

Business Continuity Planning

MassMutual’s business continuity program utilizes a Business Impact Analysis (“BIA”) as the foundation for continuity planning efforts. The BIA allows a functional area to assess their dependencies, along with potential Reputational, Financial, Regulatory/Legal and Customer impacts, based on varying degrees of disruption. This data is then used to calculate the appropriate Recovery Time Objective for each respective business function. The program requires that the BIA and recovery plan information be reviewed at least annually and as changes occur within the business unit.

MassMutual’s business continuity template is intended to address four general scenarios: workspace outage: short and long-term, technology outage (infrastructure or business application, voice, e-mail, etc.), workforce outage (large absenteeism) and failure of key internal or external business partner(s). Within each scenario, Plan Leaders provide specific information about their function and contingency plans, based on the outage scenario. Company policy requires all business functions to be covered by a continuity plan that is maintained in a web-based planning tool.

IT Disaster Recovery Planning

MassMutual maintains two types of technical continuity plans: Application and Infrastructure. Recovery Time Objectives (time to restore service in a disaster) and Recovery Point Objectives (acceptable data loss in a disaster) are guided by business continuity plan priorities. Objectives are compared to actual recovery time capabilities, and gaps are assessed to determine if technology is properly aligned with the needs of customers and the business. Critical applications are generally replicated using near-real-time replication from the production data center to the recovery data center, while non-critical applications are backed up using virtual backup to the recovery data center or long-term storage. Critical applications are generally restored within 24-48 hours, while non-critical applications may be restored several days after declaration. By

policy, all applicable technology in the Data Center must be covered by the appropriate technical continuity plan in the Company's web-based planning tool.

Strategic Supplier Oversight

The Company's philosophy around strategic suppliers is that continuity plans for these parties must be given the same level of oversight and scrutiny that would be applied to internal continuity planning. To accomplish this objective, contract language specific to resiliency, planning and testing is included in the Company's Master Services and Hosted Service templates. The core continuity planning team is engaged during the negotiation of new strategic supplier engagements to conduct a resiliency risk assessment to identify any concerns. Identified risks are reviewed with senior management prior to contract completion.

Once an agreement is in place, a Supplier Relationship Manager is assigned to the engagement and is tasked with overseeing the strategic supplier's continuity program. The Supplier Relationship Manager acts as the primary point of contact and notification for suppliers in case of an incident. As requested, suppliers are required to respond to questionnaires that address resiliency-related topics.

Awareness and Training

Often considered the cornerstone of a solid business continuity program, awareness and training occurs on an ongoing basis at MassMutual. Prepared employees are the foundation of a successful continuity program. To that end, employees are exposed to continuity planning during new hire orientation and continue to be provided with information on a periodic basis. Continuity plan leaders have the responsibility to educate employees about their department plan(s) and each employee's role in that plan.

If employees wish to learn more, there is reference material on the Company's intranet site, dedicated to continuity planning and preparedness. This includes topics such as program roles, governance activities and FEMA's Incident Command System. Finally, to ensure employees receive firsthand exposure, an annual Preparedness Fair is held in September, in partnership with the American Red Cross, state and federal emergency management agencies and a host of internal planning teams, to demonstrate proper preparedness and to distribute educational materials.

Members of the continuity planning team are encouraged to pursue FEMA Incident Command System certification, CBCP (Certified Business Continuity Professional) and MBCP (Master Business Continuity Professional) certification through DRI International and participate in industry events (LOMA, NEDRIX, ACP). To date, three members of the planning team are MBCP certified and two members are CBCP certified.

Exercising and Maintenance

Exercising: Efforts to keep plans accurate and actionable take on many forms. Emergency response testing is done throughout the year and includes High Severity Incident Team simulations, evacuation drills and exercising of specialized plans, such as Pandemic Response, Customer Disaster Response, Aviation and others. Enterprise Technology disaster recovery testing is conducted on an annual basis and includes critical applications and their dependencies, and a rotation of non-critical applications. Finally, business continuity and emergency response plans participate in testing throughout the year, which may include an annual electronic exercise, division-level simulations, plan walkthroughs and tabletop exercises. All plans must participate in at least one testing exercise each year.

Maintenance: Plan maintenance is handled through regularly scheduled reviews. Continuity plans are validated annually. Finally, ongoing reviews are conducted throughout the year to ensure all processes and technology items are covered by appropriate continuity plans and meet the Company policy.

Coordination with External Agencies

MassMutual is continuing to expand public/private partnerships. Members of the core continuity team participate in Local Emergency Planning Committees (LEPC). This has opened the door to joint testing, where MassMutual participates in emergency responder exercises with the city, and city officials participate in crisis management exercises at the company's home office. The team has engaged at the state and federal level, including the Massachusetts Emergency Management Agency and the Department of Homeland Security through federal training programs.