MassMutual

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 in Massachusetts has been outfitted with an uninterruptible power supply (UPS), N+1 generation capacity and a state-of-the-art fire monitoring system. Should there be a larger issue, systems are backed up to MassMutual-owned hardware in Colorado (1,700 miles away), and a third copy of system data is also sent to Connecticut.

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, or the office in Enfield, Connecticut, employees may be relocated to the office not impacted or may work remotely. MassMutual also has established critical operations and workspace outside of its home office region in Boston, New York, and Phoenix.

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, pandemics and 3rd party 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 Technology, Service and Resiliency. In February, the MassMutual Continuity Officer (or delegate) presents 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 against 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 exercise High Severity Incident Management.

Divisional Coordinators are responsible for working with the core continuity team, and individual plan leaders, to monitor compliance with the Company policy, develop and maintain appropriate recovery time objectives, analyze risks and develop mitigating strategies, and maintain and test all components of their program.

During emergencies, representation from Communications, Human Resources, Law, Enterprise Technology, Enterprise Risk Management and all Lines of Business assemble to form a High Severity Incident Management 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 take into account 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 project proposals. Risk and mitigation proposals are then rolled up into the Annual State of Preparedness and presented annually to leadership. The core continuity team partners with Enterprise Risk Management for ongoing 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 Colorado and Connecticut, 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 and Connecticut, many of which have generator backup and diverse paths for network and utilities. Broader or diverse regional protection is provided through offices in Boston, New York, and Phoenix.

Finally, the ability for Company employees to work remotely has greatly expanded and is designed to leverage multiple solutions ranging from remote desktop capabilities, to laptops, to virtual desktops. A diverse set of solutions are utilized with the purpose of ensuring that critical processes can continue regardless of the scenario. The Company's remote strategy has been a focus since 2005, when the threat of global pandemic made headlines. Additionally, cross-training, spread prevention protocol and social distancing also play a role in ensuring the Company can continue operating during a 6-

8 week stretch with 40% absenteeism rates, which is consistent with the Centers for Disease Control (CDC) standard.

Emergency Preparedness and Response

Emergency Response Plans ("ERPs") for each operating location document the Company's response to business interruption and include 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 release timely communications 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 the 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. The program requires that the BIA and recovery plan information be reviewed at least semi-annually and as changes occur within the business unit.

MassMutual's business continuity template is intended to address six general scenarios: short-term workspace outage, long-term workspace outage, systems outage (processor, infrastructure or business application), communications outage (data, voice, e-mail, inter / intranet, paper mail), workforce outage (an event resulting in large absenteeism rates) and failure of key internal and external business partners. Within each scenario, Plan Leaders provide specific information about their function and response and recovery strategies. Company policy requires business functions be covered by a continuity plan that is maintained in a web-based planning tool.

IT Disaster Recovery Planning

MassMutual maintains three types of technical continuity plans: Application, Infrastructure and Processor. Recovery Time Objectives (time to restore service in a disaster) and Recovery Point Objectives (acceptable data loss in a disaster) are governed by business continuity plan priorities. Objectives are compared to actual recovery time capabilities, and gaps are dealt with on a case-by-case basis until all technology is properly aligned with the needs of customers and the business. Essential applications are generally replicated using near-real-time replication to Colorado and Connecticut, while non-essential applications are backed up using virtual tape backup to Colorado and Connecticut. Essential applications are generally restored within 2–8 hours, while non-essential applications can take up to three days for complete restoration. By policy, all 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 risk assessment to identify any resiliency concerns. Identified risks are reviewed with senior management prior to contract completion. Site visits to strategic supplier locations are also considered during this process, when reasonable and appropriate, based on the results of the risk assessment.

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 and keeping current copies of their continuity plans and post-test reports on file. The Supplier Relationship Manager acts as the primary point of contact and notification for suppliers in case of an event. Suppliers are also required to respond to the Company's Controls Self-Assessment process, which includes a series of detailed resiliency questions that are updated at reasonable intervals.

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 training and reference material on the Company's intranet site dedicated to continuity planning and preparedness. This includes topics such as program roles, workplace violence prevention 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 and wallet cards.

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

Exercising, Auditing 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 monthly simulations, evacuation drills and exercising of specialized plans, such as Pandemic Response, Customer Disaster Response, Aircraft Incident and others. Enterprise Technology disaster recovery testing is conducted on an annual basis and includes essential applications and a rotation of non-essential applications. Finally, business continuity testing is conducted throughout the year and includes annual testing through an online simulator, division-level simulations and tabletop walkthroughs.

Auditing: In addition to planned testing, auditors have an active role in auditing continuity plans and test results across the Company.   When potential issues are identified, such issues are documented, assigned an owner and tracked through to completion. Overdue issue resolution is reported to the Chairman, President and CEO. A full continuity program assessment was conducted in 2017 by internal audit, and the program was found to be reliable and compliant with British Standard BS-25999, NFPA 1600, and the FFIEC IT Examination Handbook.

Maintenance: Plan maintenance is handled through regularly scheduled reviews. Emergency Response Plans and contact information are validated quarterly. Continuity plans, both business and technical, are validated semi-annually. Finally, ongoing reviews are conducted throughout the year to ensure all processes and technology items are covered by continuity plans and to ensure they meet the Company's Guiding Principles framework within the company policy for recovery prioritization.

Coordination with External Agencies

MassMutual is continuing to expand public/private partnerships. Members of the core continuity team sit on the 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 is also active at the state and federal level and was recognized publicly for ongoing partnership by the Massachusetts Emergency Management Agency and Environmental Agency in 2011. Finally, the team has become more active with the Department of Homeland Security.