MERCER

Mercer's Business Resiliency Plan (BRP)

With the current outbreak of the coronavirus (COVID-19), we want to inform you about how Mercer is protecting the health and safety of our employees while continuing to meet our clients' needs.

Mercer's Business Resiliency Plan (BRP) is a critical component of our client offering and includes solutions that allow our business to maintain full operational capability during disasters and large-scale infectious disease events such as COVID-19. We leverage the Business Resiliency Management Group (BRMG) of our parent company, Marsh & McLennan Companies. We expect to maintain full operational capability as the COVID-19 outbreak continues and will execute the necessary component of our BRP as events continue to unfold.

The BRMG is an enterprise-wide team of Marsh & McLennan Companies Business Resiliency managers who coordinate the business resiliency and emergency planning for Marsh & McLennan Companies and its various operating companies. The BRMG defines and develops corporate resiliency strategies, standards and programs. Additionally, the BRMG provides post-incident assistance to affected locations and proactive guidance and procurement of assistance and services in response to potential emergencies.

Mercer's business maintains business resiliency/disaster recovery plans with specific provisions for staff mobilization, alternate workspaces, remote access to network and client trading systems, restoration of data and communication with clients. These plans were created based on a business impact analysis that identifies every location's recovery requirements and priorities. The plan follows the guidance as outlined by Marsh & McLennan Companies Business Resiliency Management Group (BRMG), which provides continued program management to all of our operating companies (Marsh, Mercer, Guy Carpenter and Oliver Wyman). A copy of our Business Resiliency Management Statement of Recoverability is attached for your reference.

To the extent our solutions rely upon third parties, those third parties also have appropriate business resiliency programs and Mercer is actively working with such third parties to ensure continuity of services.

Our primary goal is ensuring the safety and well-being of our personnel and local communities, while sustaining business operations. While we address this current situation, we are working diligently to mitigate any potential impact to service delivery. We will keep you apprised of relevant developments and, as always, please do not hesitate to contact us directly if you have any questions.

Important Notices

References to Mercer shall be construed to include Mercer LLC and/or its associated companies.

This contains confidential and proprietary information of Mercer and is intended for the exclusive use of the parties to whom it was provided by Mercer. Its content may not be modified, sold or otherwise provided, in whole or in part, to any other person or entity without Mercer's prior written permission.

Investment management and advisory services for U.S. clients are provided by Mercer Investments LLC (Mercer Investments). Mercer Investments is a federally registered investment adviser under the Investment Advisers Act of 1940, as amended. Registration as an investment adviser does not imply a certain level of skill or training. The oral and written communications of an adviser provide you with information about which you determine to hire or retain an adviser. Mercer Investments' Form ADV Part 2A & 2B can be obtained by written request directed to: Compliance Department, Mercer Investments, 99 High Street, Boston, MA 02110.

MARSH & McLENNAN COMPANIES

Statement of Recoverability

JANUARY 2020

OUR COMMITMENT TO PREPAREDNESS

The leadership of Marsh & McLennan Companies (MMC) has committed to protect, preserve and recover enterprise resources (for example, personnel, facilities, equipment, IT systems and information assets) if a disruptive event occurs.

As an integral part of our operations, we plan for the continuity of business and service to our clients. We are committed to ensuring that our Business Resiliency, Disaster Recovery, Crisis Management and Incident Response plans are reviewed, updated and tested regularly.

STATEMENT OF RECOVERABILITY

Protection of information and continuation of services, even in the event of a disaster, is a cornerstone of MMC’s commitment to its clients. To support that commitment, we maintain a robust business resiliency program which includes:

- Conducting Business Impact Analyses (BIAs).
- Establishing and maintaining business resiliency, disaster recovery, crisis management, and incident response plans.
- Performing periodic assessments of key third-party dependencies.
- Periodic testing of recovery capabilities and exercising of response plans to validate our ability to serve and support our clients in the event of a business disruption.

BUSINESS RESILIENCY MANAGEMENT (BRM) GROUP

The Business Resiliency Management (BRM) group provides business continuity guidance and overall program management, including compliance monitoring, to all of our operating companies and corporate functions:

- Marsh
- Guy Carpenter
- Mercer
- Oliver Wyman
- MMC Corporate

The BRM group coordinates communications and other shared resources, including emergency communication systems, business resiliency planning systems and external vendor capabilities such as work area recovery.

BUSINESS RESILIENCY PLANNING

Our critical business and corporate functions maintain Business Resiliency plans with specific provisions for colleague mobilization, alternate work spaces, and communication with clients and critical third parties. These plans are created based on a Business Impact Analysis that identifies business recovery requirements and priorities.

The Business Resiliency plans address loss of:

- Office facilities and personnel.
- Critical applications.
- Mission-critical functions and processes.
- Key third-party providers.

Critical MMC operations and functions are required to maintain copies of their current Business Resiliency plans on the Business Resiliency Management plan digital repository and, as they deem necessary, in hard copy.

Business Resiliency plans include:

- Key stakeholders and contacts for every critical operation and function.
- Detailed step-by-step business operation recovery playbook.
- Incident impact assessment, timetables and action plans, including recovery time objectives (RTOs).
- Plans for implementing long- and short-term alternate operations.
- Contingency plans to use other corporate or operating company offices, service centers and resources in the event of facility loss.
- Contracts with external parties for work-area equipment and facilities.

DISASTER RECOVERY PLANNING

Our technology organization develops and maintains Disaster Recovery plans with procedures and capabilities for recovery of network and telecommunications systems, recovery of critical business applications, and restoration of data. These plans are created based on a BIA and an application risk analysis that, combined, identify requirements for technology recovery.

The Disaster Recovery plans address loss of:

- Network services
- Databases
- Operating systems
- Critical applications

Disaster Recovery plans are kept and maintained by the operating company technology organizations; copies are also maintained by the technology infrastructure organization, centrally.

Disaster Recovery plans include:

- Strategies to restore IT applications and services within a specific time frame.
- Key stakeholders and contacts for every system and application.
- Detailed step-by-step technology recovery runbook.
- Strategies to foster the restoration of data within a specific time period following a disaster.
- Ongoing cross-site replication of critical or high-volume data.
- Technology team notification procedures and details.
- Disaster impact assessment, timetables, and action plans – recovery point objectives (RPOs).
- Contingency plans to replace computing equipment.

- Contingency plans to use other corporate data centers and resources in the event of disruption.

ALTERNATE WORK SITES

MMC uses a multi-layered approach to providing alternate work sites in the event that an office suffers a service interruption. This approach is aligned closely with each of our businesses and functions, and it recognizes important support requirements and interdependencies of all phases of our operations. In this matrix approach, our colleagues may work from one of the places below when a business resiliency plan has been activated:

- Home, using high-speed Internet connections and Virtual Private Networking (VPN) to access company network and resources.
- An alternate work space, where prior arrangements for recovery support have been made.
- Commercial recovery service centers and mobile work sites.
- Other corporate or operating company offices (with or without the transfer of colleagues from the affected locations).

Should there be a complete facility outage, critical operations of an affected office will be deployed to the alternate location(s) and processes resumed. Additional equipment and facilities will be made available as required for the scale the processes require.

TECHNOLOGY RESILIENCE

Local Office

Networks in all MMC offices use a fault-tolerant approach to system designs. In other words, we have implemented technologies that limit our vulnerabilities in case of a systems failure, office location failure or natural disaster. Each office's computing environment is established using global standards that facilitate remote support.

Data centers and server rooms are protected against unauthorized access, environmental hazards using dedicated fire response protection, moisture detection and cooling systems, as well as backup and uninterruptible power supply (UPS) systems.

MMC uses a range of commercial and custom bespoke software applications. The Company’s subsidiaries maintain dedicated technology or solutions delivery teams that are responsible for application development and maintenance.

Data Centers

MMC operates data center facilities throughout the world with primary and secondary data centers housed in each of three key regions - the US, UK and Australia.

Data centers are configured with redundant power feeds, telecommunications circuits, back-up generator power and UPS systems. Server rooms are configured with UPS systems and depending on the facility’s size, there may be on-site back-up power, such as a generator. Such systems are tested on a periodic basis (e.g., quarterly, semi-annually) depending on system and location.

Critical applications are designed for high availability, using clustering or load-balancing technology. Disaster recovery strategies are implemented based on business-defined requirements, including near-time replication to meet business recovery time objectives.

MMC also has dedicated business resiliency and disaster recovery teams that coordinate the Company's capability to recover systems and provide work areas using internal or external resources. Solutions are designed to meet requirements defined by impact analyses of system or facility outages. Where appropriate, human or computer workload is distributed among multiple locations to reduce or eliminate downtime due to local outages.

Disaster recovery tests are coordinated by the Company's technology infrastructure organization working with internal business IT teams and application owners. Test objectives are defined and agreed to by the business lead, business IT support lead, and technology infrastructure leads.

Data Backup

We back up critical data nightly (differential backup) and weekly (full backup). Backups are stored both at offsite storage facilities and in secured onsite data-storage facilities. We also perform cross-site replication of critical or high-volume data. The standardization of backup systems and storage procedures across our offices enables recovery efforts at alternate sites.

Cyber Security

MMC has established internal controls for the protection of its information assets, and to comply with business and regulatory requirements. These controls, which include related planning, development and implementation of appropriate policies and procedures, are reviewed regularly and updated where applicable to ensure the integrity, availability and confidentiality of corporate and client information.

We maintain an incident response plan with designated incident response leaders who assemble the necessary personnel to promptly respond to computer security incidents. The plan focuses on preparation, detection, analysis, containment, eradication, recovery and post-incident improvements. This response capability addresses events such as cyber-attacks, data loss, malware/virus infections, denial of service (DoS) attacks, critical system outages, violations of security policy, imminent threats and suspected breaches.

CRISIS MANAGEMENT

Structure

MMC uses a tiered crisis management and response structure that emphasizes activation of teams tailored to the situation and its potential impacts. The overarching goal is to minimize adverse impact on the Company, its colleagues, assets, business operations, clients, and reputation.

- Responses are managed as close to the incident as possible.
- Coordination is facilitated within and across MMC operating companies via local, country and corporate crisis response teams.
- Key response teams are exercised on a regular basis via scenarios for role and response capability.
- Leadership is kept appraised of incidents, and possible impacts, through regular updates.

Response

The crisis management and response structure recognizes and aligns all aspects of response from immediate, tactical emergency response to executive strategic decision-making on critical business, financial and policy issues. This streamlined approach:

- Provides an overall response structure, with clarity in “division of labor” among teams and levels.
- Supports a common, comprehensive and predictable management response process, while providing flexibility to adapt to each situation.
- Crosses operational/business lines and promotes consistent, cross-functional support.
- Provides immediate, proximate assistance and resources where/when able.

PANDEMIC PREPAREDNESS

MMC’s Business Resiliency Management Group, in concert with our Health and Life Safety Committee, identifies and assesses issues relating to communicable diseases and develops and helps implement protocols to mitigate the effect they may have on our operations, our colleagues, and our ability to serve clients.

The Business Resiliency Management Group and Health and Life Safety Committee also monitor and develop responses to communicable disease issues, including actual and potential threats, supported by third-party advisors and by risk and pandemic preparedness experts at our operating companies, including Marsh and Mercer.

SUCCESSFUL PLAN EXECUTION

MMC has successfully supported critical business activities during disruptions of normal business processes resulting from both natural and man-made disasters. On each occasion that plans have been invoked, they have been executed successfully. Some examples include:

- Potential Mass Transit Outages: USA.
- Acts of Terrorism: United States, Belgium, UK, India, Norway, France, Turkey, Sweden, and Spain.
- Hurricanes: Bermuda, Cayman Islands, USA, the Dominican Republic and Ireland.
- Typhoons: Japan, China, Taiwan, Hong Kong, India, Fiji and the Philippines.
- Pacific Tsunamis.
- Flooding: Thailand, Indonesia, India, the Philippines, UK and Australia.
- Wildfires: USA, Australia, and India.
- Communicable Disease/Pandemics: Sudden Acute Respiratory Syndrome (SARS), Influenza (Swine & Avian Flu), MERS-CoV and Ebola.
- World Trade Organization (WTO) and G8/G20 Global Summit Meetings: USA, and Canada.
- Earthquakes and Volcanic Eruptions: Chile, New Zealand, the Philippines, Japan, Iceland and Mexico.
- Superstorm Sandy.
- Political unrest and demonstrations: Egypt, Indonesia, Brazil, Thailand, Israel, Ukraine, Hong Kong (Occupy Central), Turkey, Spain, South Korea, India and Jakarta.

FREQUENTLY ASKED QUESTIONS

1. Does your organization have a dedicated team focused on Business Continuity and/or Disaster Recovery?

   MMC has dedicated business resiliency and disaster recovery teams that coordinate the Company's capability to recover systems and provide work areas using internal or external resources.

2. What criteria are used for the creation of recovery strategies in Business Continuity and/or Disaster Recovery?

   Solutions are designed to meet requirements defined by impact analyses of system or facility outages. Where appropriate, human or computer workload is distributed among multiple locations to reduce or eliminate downtime due to local outages.

3. I would like to review a copy of your Business Continuity ("BC") or Disaster Recovery ("DR") Plan. Do you allow this?

   In order to protect our intellectual property, client confidentiality and colleague personal identity information, we do not release our documented BC or DR plans.

4. How often do you test / exercise your Business Continuity and/or Disaster Recovery plans?

   Our plans are tested / exercised on a regular and representative basis. Using a risk-based approach, we do not test / exercise all plans on the same schedule.

5. What methods of testing / exercising do you undertake?

   We employ a range of test / exercise methods, as appropriate. Representative examples include:
   - *Remote access (e.g. work from home, work from a different office)*
   - *Commercial work area recovery exercises*
   - *System fail-over testing, including external vendors where appropriate*
   - *Evacuation drills, notification system tests and periodic generator tests*

6. Can I participate in, or observe, the performance of a Business Continuity or Disaster Recovery exercise/test?

   In order to protect our intellectual property and client confidentiality, we do not permit third-party observation of, or participation in, our exercise or test activity.

7. What is the expected recovery time objective for critical business functions?

   Recovery time objectives vary based on requirements defined through the Business Impact and Application Risk Analyses.