

# **METLIFE BUSINESS CONTINUITY MANAGEMENT PROGRAM**

## **Table of Contents**

Mission .....	3
Overview .....	3
MetLife Global Resiliency Staff Qualifications .....	3
Business Continuity Management and Cyber Security .....	4
Infrastructure .....	4
Continuity Management System .....	5
xMatters Notification Tool .....	6
Customer Notification Overview .....	7
Business Continuity Management Recovery Time Objective/Recovery Point Objective (RTO/RPO) Overview .....	7
Exercise and Testing Overview .....	8
MetLife Global Framework .....	9

**Mission**

Drive the global MetLife organization to a resiliency model by providing a framework for the Lines of Business (LOBs) to implement and holistically execute.

1. Proactive preparedness for times of organizational stress
2. Ensure the availability of MetLife
3. Identify potential threats to business process operations
4. Enable an effective response to disruption of people, process, and/or technology
5. Foster a culture of resiliency and preparedness throughout the enterprise
6. Monitor resiliency industry best practices and coordination of integration into the corporate program

**Overview**

Business Continuity Management is the holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. *Source: ISO 22301:2012 –Societal Security– Business Continuity Management Systems – Requirements*

Business Continuity Overview: Understanding business resiliency and preparedness needs, as well as the necessity for establishing business resiliency management policy and objectives; implementing and operating controls and measures for managing an organization's overall continuity risks; monitoring and reviewing the performance and effectiveness of the business continuity management system; and continual improvement based on objective measurements.

Disaster Recovery Overview: Enables the recovery or continuation of vital technology infrastructure and systems following a natural or man-made disaster to support critical business functions in Americas ,EMEA, LATAM and Asia Regions providing analysis of disaster resiliency data to ensure proper Disaster Recovery plan development processes are followed.

**MetLife Global Resiliency Staff Qualifications**

The MetLife Global Resiliency Program strives to support its customers and be on top of the latest business continuity management trends. The head of Global Resiliency has been actively involved in the business continuity field since 1994 and has worked for financial services companies in Boston, Massachusetts and Dublin, Ireland and an eCommerce company in

California prior to moving to North Carolina in 2014. She has held board level positions with business continuity organizations, written publications and spoken at business continuity management conferences in North America, Europe, Asia and the Middle East.

In 2011, she was awarded a Master of Science in Business Continuity from Norwich University in Northfield, Vermont with honors. She has been certified as a Member of the Business Continuity Institute (MBCI) and a Master Business Continuity Professional (MBCP).

The Global Resiliency team has approximately 30 industry certifications for business continuity management, information security, international standards, and information technology with the knowledge and experience appropriate for a world class organization.

### **Business Continuity Management and Cyber Security**

IT systems, applications and databases can be vulnerable to a variety of threats, particularly as invasive technology becomes more sophisticated and available. Global Resiliency reviews and updates its policies, standards, and procedures on a regular basis in light of emerging threats and new and changing technologies. An internal committee of Business Information Security Officers (BISOs) with representation from Technology, Law, Internal Audit, Human Resources, the MCPO and other Lines of Business areas helps oversee our information technology security policies, emerging risks and compliance requirements.

MetLife's IT Risk & Security Department works with IT and business management to institute controls for IT systems, applications and databases, and for vendor and application service provider arrangements. MetLife's internal systems use electronic firewalls and other security measures designed to prevent unauthorized access to our electronic records.

IT Risk & Security employs security scans to monitor for policy noncompliance and vulnerabilities. This is performed at various levels of the technology infrastructure as well as on various applications. Performance measures for key security processes critical to the security of the IT environment (such as anti-virus reports, spam totals, etc.) have been defined. IT Risk & Security has oversight responsibilities over these processes through IT internal risk reporting.

Additionally, MetLife has a formal Computer Security Incident Response Team (CSIRT) that is charged with responding to internal and external threats and taking appropriate action. The process includes emergency response, evaluation of security fixes and the implementation of required fixes.

### **Infrastructure**

eBRP Business Continuity Management System

The eBRP suite provides MetLife a standardized global approach to calculation and rank of Recovery Time Objectives (RTO) for the business and is comprised of three modules which are the eBIA – Business Impact Analysis, Toolkit – Business Continuity & Disaster Recovery Plans, and Command Center – Plan activation.

The eBIA module is leveraged during the Business Impact Analysis and provides the capability for automatic calculation of Recovery Time Objectives (RTO)/Recovery Point Objective (RPO) and Criticality values for Business Processes based on survey responses. Resulting RTO/RPO and Criticality values are fed into the Toolkit Process records.

The Toolkit functions as the data repository for the suite and utilizes five key assets for loss that are leveraged throughout Plan development and the Global Resiliency Framework lifecycle. These key assets are people, processes, facilities, technology, and third parties.

Plan development in Toolkit for Business Continuity and Disaster Recovery is procedure based so that plans are easy to use, easy to maintain, flexible, scalable, and secure.

User access and permissions are determined by team membership. Teams are assigned to processes (Group Functions), plans (Group Strategies), and other assets.

Process & Plan Owners are responsible for the development and maintenance of their records and submission of completed records for approval to Approver teams. Process & Plan Approvers are accountable for sign off and certification that records are accurate. Process and Plan records are certified annually or after significant changes have been realized for the records.

Command Center provides a holistic view of Plan activation and execution during major business disruptions and facilitates: testing & exercising; communication and collaboration; real-time impact analysis and monitoring; and issue escalation and decision support.

In summary, eBRP provides the capability to store all Global Resiliency Plans with enterprise secured availability; provides an optimized user experience with enhanced secured functionality and business resiliency function; enhances productivity, supportability, and accessibility offerings; facilitates an enterprise-wide view of MetLife Global Resiliency capabilities and operational status and is a standardized tool to support comprehensive metrics for decision making for our global enterprise business continuity management environment.

### **Continuity Management System**

The eBRP suite supports the complete Business Continuity Management Lifecycle by providing an integrated, single vendor solution to support all phases of a Business Continuity/Disaster Recovery program which includes risk assessment, business impact analysis (Surveys, Rule

Engine, Approval Workflow), plan development/Approval/Maintenance, exercise scheduling & tracking, alternate work area planning, exercise simulation, testing & incident management, reporting & dashboards, and Geographic Information System (GIS) mapping & “What if?” analyses.

The eBRP Suite is a web-based vendor-hosted solution that is designed for unlimited concurrent users. There are no restrictions on content volumes (Plans, Locations, etc.), and the suite complies with all information security controls as best business practices to include a high-availability design from the datacenters and infrastructure. eBRP is SSAE-16 certified.

eBRP Suite incorporates Risk-Assessments which follow the recommendations of the NIST 800-030 framework. The following elements are part of the risk assessment utility (all are user-definable):

- Threats
- Vulnerabilities
- Likelihood
- Impact
- Mitigation strategy
- Prioritization
- Current State of Mitigation

### **xMatters Notification Tool**

Global Resiliency uses xMatters as a global Exercise/Testing Notification Tool. xMatters provides Global Resiliency key support in the form of Communications, Data Resources and Redundancy Support. xMatters also provide security in the form of Data Privacy, Data Security and Privileged User access.

The communications plans we use are SMS, Voice, Mobile Push, Pager and Email to notify our employees if there is an incident. The messages can be tailored to the situation and in different languages for our global environment.

All employee and contractor contact information is held in a single place with no limit to the number of roles that can be created and the messages can be saved for quick access in a library to reduce reaction time in case of an incident.

The redundancy support includes 24x7 – Forum, Online, and Phone support; an uptime guarantee of 99.99%; no Single Point of Failure; multiple Data Centers globally; and every tier of service within the data centers are redundant (application, database, and network).

Data Security includes website access encrypted using Hyper Text Transmission Protocol Secured (HTTPS) and Transport Layer Security (TLS) v1.2. The xMatters database is protected by defense in depth strategy that includes physical, technical and administrative controls.

**Customer Notification Overview**

Metlife customer notification is the responsibility of the business account executive within Corporate Affairs. Any information pertaining to an issue will be disseminated through those channels and not through Global Resiliency.

**Business Continuity Management Recovery Time Objective/Recovery Point Objective (RTO/RPO) Overview**

The prioritization of business processes and supporting technology are divided into four key categories: Critical, High, Medium and Low. The definition of each prioritization follows.

Critical is defined as mission-critical real-time business, customer impacting processes with direct impact to primary revenue streams labeled Severe includes processes that could negatively affect company reputation, customer facing, critical to operations, pose an external business exposure, impact revenue streams and systems required for legal compliance. The technology parameters for severe are Active/Active or Active/Passive; geographically diverse; real-time data replication; and no single points of failure. The Exercising/Testing is specified as Live/ Functional Exercise/Test with all participants, a post-mortem report and mitigation tracked.

Exercising/Testing occurs every 2 years with a simulation between years with all participants. The RTO: < 24 hours and RPO: < 1 hour.

The identified High business processes required to conduct business transactions are Significant and includes processes that could negatively affect company reputation, customer facing, operations, and impact revenue streams. These are geographically diverse and best efforts to complete the processes are required and only slightly lower than critical processes. The technology parameter for significant is Active/Passive, real-time data replication and no single points of failure. The Exercising/Testing is Live/ Functional Exercise with key participants, post-mortem report and mitigation tracked with a simulation annually. The RTO: 25 - 48 hours and RPO: < 4 hours.

Medium business processes are considered non-mission critical processes and are rated Adverse which includes internal and customer facing processes that can be offline for an extended period of time. These are systems which are low revenue generating or support low revenue generating processes. The strategy is to assign the processes to a non-impacted area or build out the processes in a non-impacted area. Failover may require manual reconfiguration or deployment of cold servers which could be rebuilt on-site or repurpose existing hardware. The exercising and testing standard would be to conduct a tabletop Exercise or simulation every 2 years with an exercise findings report. The RTO: 49 – 72 hours and RPO: < 4 hours.

Identified Low business processes are non- mission critical processes and are rated Minor to Moderate. These processes are non-critical functions, non-customer facing, not revenue

generating, and no significant business impact. They should have a manual work around and the lowest priority. Processes could be skipped if necessary. Only current platform, systems and storage are used. Recovery would include procuring new hardware and tape backup. The exercising and testing consists of having a plan developed, reviewed and revised annually. The RTO: 73 + hours and RPO: 72 hours.

### **Exercise and Testing Overview**

The Business Continuity/Disaster Recovery function helps ensure that all of MetLife's business continuity/disaster recovery plans are exercised/tested, respectively, and reviewed on a criticality basis to analyze incorrect assumptions, oversights or changes to equipment, and employees and to identify any changes in business requirements not reflected in specific plans. Any undocumented requirements discovered are documented through this function. In addition, appropriate information owners and users are informed of updates to plans. Risk monitoring and exercising/testing helps ensure that MetLife's business continuity/disaster recovery program is attainable to support the business.

MetLife exercises its business continuity plans to help ensure that they are consistent with the business objectives. For business sites which contain:

1. Processes identified as Critical by the Business Impact Analysis (BIA), a business relocation exercise (recovery at an alternate geographical site) is to be conducted every 2 calendar years and a table top exercise or simulation exercise conducted on alternating years.
2. Processes identified as High by the Business Impact Analysis (BIA), a simulation exercise is to be conducted annually.
3. Processes identified as Medium by the Business Impact Analysis (BIA), a table top exercise is to be conducted every other year.
4. Processes identified as Low by the Business Impact Analysis (BIA), a process walk through is to be conducted every other year

MetLife Inc. tests its disaster recovery plans to help ensure that they are consistent with the technology objectives. For application/information resources with a:

1. Recovery Timeframe Objective (RTO) of 24 hours or less, a documentation review and a technical recovery test is required annually and confirmation of the documented plan is valid.
2. For application/infrastructure resources with a RTO greater than 24 hours, a documentation review and technical recovery test is required to be completed every 2 years and confirmation of the documented plan is valid.
3. Disaster recovery servers must be able to take the full load of the production servers during peak operating times.
4. Use MetLife Global Resiliency framework and methodology.



For new applications with an active/passive failover recovery strategy:

1. A Disaster Recovery test will be conducted within 14 calendar days before the Production deployment date.
2. If the Disaster Recovery test is performed before the Production deployment date and additional change(s) take place prior to the Production date, the Disaster Recovery test should be repeated before going live.

For existing applications with an active/passive recovery strategy:

1. If any significant changes take place, a Disaster Recovery test will be conducted within 14 calendar days before the Production deployment date.
2. If the Disaster Recovery test is performed before the Production deployment date and additional change(s) take place prior to the Production date, the Disaster Recovery test should be repeated before going live.

### MetLife Global Framework



Submission Number: 1205532  
Material Title: Global Resiliency  
Certification Due Date: 01/01/2018  
Approver Name: Steven Jackson

This submission has been approved and is in a Certification Required status. Please complete the certification process by the due date noted.