ORACLE

Risk Management Resiliency Program

Business as usual…during unusual times.

May, 2023 | Version 4.0

RISK MANAGEMENT RESILIENCY PROGRAM (RMRP)

Oracle Risk Management Resiliency Policy

Oracle's Risk Management Resiliency Policy defines requirements for all Oracle Lines of Business (LOBs) to plan for and respond to potential business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability across LOBs and geographies. It authorizes a centralized Program Management Office (PMO) to manage a global Risk Management Resiliency Program (RMRP) which oversees LOB plans and preparedness, in alignment with ISO 22301 international standard for business continuity management.

Risk Management Resiliency Program

The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework to help facilitate efficient responses to business interruption events affecting operations.

The RMRP approach is comprised of several sub-programs: emergency response to unplanned and emergent events, crisis management, technology disaster recovery and business continuity management. Each of these sub-programs is a uniquely diverse discipline. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.

Oracle's RMRP is designed to engage multiple aspects of emergency management and business continuity from the onset of an event and to leverage various teams, technology and personnel based on the needs of the situation.

The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive reporting on program activities and status across the Lines of Business.

RISK MANAGEMENT RESILIENCY STRUCTURE

The RMRP program is comprised of four Risk Management functions:

1. Emergency Response, managed by Real Estate Facilities Environment, Health and Safety Program
2. Crisis Management, managed by Global Physical Security
3. Business Continuity Management, managed by the corporate RMRP Program Management Office and operated by LOBs
4. Disaster Recovery, managed by LOBs, Information Technology teams and cloud Operations teams

At the global level, the RMRP is sponsored by senior executives. This executive focus is designed to engage appropriate levels of management in bringing resources to bear on a situation. Regional Crisis Management Teams (RCMTs) advise and consult the executive team.

At the regional level, multiple RCMTs are comprised of senior management who can make decisions and authorize the Crisis Commander to act on escalated matters.

At the local level, the RMRP is implemented via a Local Crisis Management Team (LCMT). The LCMT is comprised of a Crisis Commander and representatives from each relevant LOB for the impacted location. This team collects and disseminates information about a local crisis and executes an Emergency Response Action Plan to address personnel safety. When necessary, an LOB activates their own local business-resiliency plans to maintain critical business functions. The Crisis Commander funnels this information and escalates any issues to the Regional Crisis Management Team (RCMT) RISK MANAGEMENT RESILIENCY Business continuity

RISK MANAGEMENT RESILIENCY PROGRAM RESPONSIBILITIES

Business Continuity is a key sub-program of Oracle's Risk Management Resiliency Program. Corporate business continuity policy, standards, and Line of Business (LOB) practices are overseen by the RMRP Program Management Office (PMO).

This centralized program office guides LOB Risk Managers to help them fulfill their responsibilities defined in the Oracle Risk Management Resiliency Policy. As part of this guidance, the RMRP PMO develops planning materials and tools as aids to LOB Risk Managers in defining and maintaining their business continuity plans, performing plan testing and for training.

Risk Managers in Lines of Business

Business continuity planning is managed by the Risk Manager in each Line of Business (LOB). Critical LOBs are required to conduct an annual review of their business continuity plans with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes and technology. The RMRP program requires that critical LOBs:

- Identify relevant business interruption scenarios, considering essential people, resources, facilities and technology
- Conduct a Business Impact Analysis that specifies a Recovery Time Objective and Recovery Point Objective (if appropriate to the function) and identifies the organization's business continuity contingencies strategy
- Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information
- Revise business continuity plans based on changes to operations, business requirements, and risks
- Educate personnel about their contingency planning controls and procedures
- Conduct an exercise to test the efficacy of the plans, as well as participate in a cross-functional annual exercise assessing the capability of multiple organizations to collaborate effectively in response to events
- Implement their business continuity plans
- Analyze lessons learned for continual improvement of plans and procedures
- Obtain approval from the LOB's executive

In addition, all LOBs are required to:

- Identify relevant business interruption scenarios, including essential people, resources, facilities and technology
- Define a business continuity plan and procedures to effectively manage and respond to these risk scenarios, including emergency contact information.
- Obtain approval from the LOB's executive

RISK MANAGEMENT RESILIENCY DISASTER RECOVERY (DR)

Disaster recovery is a key sub-program of Oracle Risk Management Resiliency Program (RMRP). To understand resilience, business continuity, and disaster recovery practices for cloud services, please see Oracle Cloud Hosting and Delivery Policies.

Oracle Lines of Business (LOBs) are required to maintain and test their Disaster Recovery (DR) plans, including backup and recovery strategies, as part of their business continuity efforts.

Disaster Recovery (DR) plans focus on the resiliency of computing infrastructure supporting Oracle's internal operations and cloud services. Oracle's production data centers are geographically separated and have component and power redundancy, with backup generators in place for availability of data center resources in case of an impacting event. LOB recovery strategies are designed to both protect against disruption and enable recovery of services including backups for identified critical systems. For these systems, Oracle performs the following backups as applicable:

- Database: Full and incremental backups
- Archive logs: Full and incremental backups

Oracle LOBs also implement additional DR strategies for certain critical systems, such as:

- Application failover
- Current copy of the production database at a secondary site using solutions such as Oracle Data Guard, which manages the two databases. Oracle Data Guard provides remote archiving, managed recovery, switchover, and failover features.
- Redundant middle or application server tiers consisting of a set of servers to distribute application functionality across multiple host machines.
- Physical backup media such as tape is periodically relocated to a secure offsite location

Further, Oracle also maintains a redundant network infrastructure, including DNS servers to route between primary and secondary sites, network devices, and load balancers.

Finally, Oracle information technology organizations conduct an annual DR exercise for internal infrastructure designed to assess their DR plans. Lessons learned from the exercise are implemented into standard operations and DR procedures as appropriate.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle