ORACLE

Oracle Risk Management Resiliency Program

April, 2020 | Version 2.0

CONTENTS

RISK MANAGEMENT RESILIENCY PROGRAM (RMRP)

Oracle Risk Management Resiliency Policy

Oracle's Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation and executive approvals for critical business operations.

Risk Management Resiliency Program

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations.

The RMRP approach is comprised of several sub-programs: initial emergency response to unplanned and emergent events, crisis management of serious incidents, Information Technology Disaster Recovery and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.

Each of these sub-programs is a uniquely diverse discipline. However, by consolidating emergency response, crisis management, business continuity, and disaster recovery, they can become a robust collaborative and communicative system.

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

The RMRP is implemented and managed locally, regionally, and globally. The RMRP program management office provides executive scorecard reporting on program activities and status within the lines of business.

Risk Management Resiliency Program Responsibilities

The Risk Management Resiliency Program (RMRP) objective is to establish a business resiliency framework that helps provide an efficient response to business interruption events affecting Oracle. Business Continuity is a key sub-program of Oracle RMRP.

Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance.

This centralized program office is responsible for providing guidance to Risk Managers in the lines of business, to help them fulfill their roles and responsibilities defined in the Oracle Risk Management Resiliency Policy.–As part of this guidance, the RMRP PMO develops planning materials and tools meeting the RMRP Policy requirements as aids to LoB Risk Managers in managing their business continuity plans, testing and training procedures.

Risk Managers in Lines of Business

Functional business continuity planning is managed by the Risk Manager within each Line of Business (LoB). The critical LoBs are required to conduct an annual review of their business continuity plan with the objective of maintaining operational recovery capability, reflecting changes to the risk environment as well as new or revised business processes. The RMRP program requires that identified 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 plan, 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 as needed
- 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 PROGRAM STRUCTURE

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business-interruption events affecting Oracle's operations. The RMRP is implemented and managed locally, regionally, and globally.

Structure of Oracle Risk Management Resiliency Program

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
4. Disaster Recovery, managed by Global Information Technology

At the global level, the RMRP is comprised of senior Oracle executives. This executive focus is designed to ensure that appropriate levels of management are engaged in bringing resources to bear on a situation. Regional Crisis Management Teams (RCMTs) engage with and consult the global executive team.

At the regional level, multiple RCMTs are comprised of executive and senior management at the regional level, 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 key line of business (LOB) at the impacted location. This team collects and disseminates information regarding a local crisis, executes the local Emergency Response Action Plan to assure personnel safety, and activates 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

The Risk Management Resiliency Program (RMRP) objective is to establish a business- resiliency framework that helps provide an efficient response to business-interruption events affecting Oracle. Business Continuity is a key sub-program of Oracle RMRP.

Corporate business continuity policy, standards, and practices are governed by the RMRP Program Management Office (PMO) and are generally aligned with International Standards Organization (ISO) 22301 Business Continuity Management Systems guidance.

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

- Review and update a Risk Assessment
- Write a Business Impact Analysis that includes identification of interdependent resources and internal customers, and the determination of a Recovery Time Objective and Recovery Point Objective
- Define a business continuity strategy
- Review and update a Business Continuity Plan
- Train employees in Business Continuity Plan execution
- Conduct an exercise to test the efficacy of the plan within the LoB, as well as participate in a cross-functional annual exercise assessing the capability of multiple organizations to collaborate effectively in response to events
- Implement lessons learned for plan improvement
- Obtain approval attestation from the LoB's Vice President Approver

Non-critical LoBs are required to:

- Review and update a Business Resiliency Plan identifying contingency business continuity processes to be invoked in the event of a disruptive incident
- Obtain approval attestation from the LoB Vice President Approver

Following the review process, each LoB reports their business continuity status to the RMRP PMO. Using LoB inputs, the PMO constructs the Annual RMRP Scorecard Report and submits it to the program Executive Sponsor.

RISK MANAGEMENT RESILIENCY DISASTER RECOVERY (DR)

The Risk Management Resiliency Program (RMRP) objective is to establish a business- resiliency framework in order to help provide an efficient response to business- interruption events affecting Oracle's internal operations. Disaster recovery is a key sub-program of Oracle RMRP. To understand resilience, business continuity, and disaster recovery practices for Oracle Cloud, please see Oracle Cloud.

Oracle's corporate Disaster Recovery (DR) plan focuses on the resiliency of computing infrastructure supporting Oracle's internal operations. 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. Oracle's DR plan leverages this separation of data centers in conjunction with other recovery strategies to both protect against disruption and enable recovery of services.

Oracle has identified certain critical internal infrastructure systems that are backed up and can be restored. For these systems, Oracle performs the following backups as applicable:

- Database: Full and incremental backups are created on physical and/or electronic media.
- Archive logs: Full and incremental backups are created on physical and/or electronic media

In addition, source code repository backups are performed on recurring bases that vary by environment.

Oracle also implements additional strategies for certain critical internal 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

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

Finally, Oracle's Information Technology organization conducts an annual DR exercise designed to assess our DR plans. Lessons learned from the exercise are implemented as deemed appropriate 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