Business Continuity (BC) and Disaster Recovery (DR)

Business continuity management is a planning and holistic management through which institutions create and implement measures, strategies and plans which are effective to manage crises, respond to/ and recover from a disaster.

Business continuity is more than just a plan to recover from a disaster but a survival strategy for enterprises that enhances systems resilience, ensures high availability and continuous operations of solutions. All institutions shall therefore have Disaster Recovery plans as a measure and guide to use for Business Continuity in case disasters befall.

Disaster recovery consists of developing step-by-step procedures for ensuring a full recovery, however, when many think about DR, they usually think about Backup, while it is only one piece in BC-DR. Therefore, the following are recommended to be followed for best practices:

A. Based on the data and systems inventory and classification:

- All institutions shall have a backup mechanism for all data that is performed regularly and most importantly kept offsite; this means having taken your backups, stored them in a safe and accessible way. Local Backup on Recovery Devices shall be stored in house and then replicated
- to an offsite location where applicable. It is the local site that shall serve a master role and then the offsite backup.
- For important data and systems, all institutions shall have a Hot-standby DR solution based on both the Business Continuity and Disaster Recovery plans.
- For critical data and systems having a DR solution shall no longer be an option but an active-active DR solution by which both primary and secondary sites shall be active and processing requests in parallel. This solution shall not help in recovery and continuity of the business after the disaster but shall avoid a disaster altogether by minimizing the risk of losing data, systems and information The Recovery time objective and Recovery point objective (RPO and RPO shall be near to zero).
- For further clarifications and understanding about Disaster recovery and Business continuity refer to the current Business Continuity Management guidelines issued by RISA.
- For critical IT systems and applications hosted in the National Data Centre, the institution shall ensure that they subscribe to a minimum hosting plan that includes daily backups and disaster recovery services.
- For critical IT systems and applications hosted on premises, the government entity shall immediately consult RISA to devise a strategic road map for migration to the National Data Center.
- Pending full migration of critical IT systems and applications, to the National Data Centre and other IT systems and applications deemed non-critical and kept on premises, Government institutions shall be required to comply with the institution’s detailed data

backup schedule.

- For government data that resides on personal computers (Laptops & Desktops), government institutions shall set up a local file server that automatically synchronizes with users’ personal computers to keep copies of any data files as created/updated by users.
- Personal computers shall also be installed with an up-to-date Antivirus/Antimalware and no user shall be allowed to keep government data on a non-protected personal computer.
- Personal computers and servers shall have the latest Operating Systems installed or upgraded to the latest operating system.

Revision #3
Created 11 July 2025 14:56:59 by RISA
Updated 14 July 2025 07:31:36 by RISA