How to set up an effective DRP?

DRP solution architecture · https://nuabee.com/documents/establish-effective-disaster-recovery-plan/

The proper use of Nuabee protection tiers

A Disaster Recovery Plan (DRP) is similar to an insurance policy: as long as no disaster occurs, its usefulness may seem abstract. As with any insurance, the challenge is to optimize the cost-benefit ratio in order to obtain adequate protection without oversizing the investment.

It is precisely this logic that underpins the protection tiers system proposed by the Nuabee solution, which enables a graduated and economically rational approach. :

- **Critical applications:** Essential to the functioning of key business processes. Their unavailability leads to an immediate halt in activity..
- Important applications: Required at a later stage if the interruption lasts longer than a few days. Their absence becomes critical after this period.
- **Other applications:** Only desirable in the event of a prolonged interruption. Their restoration can be deferred without any major impact on business.

Methodology for selecting applications to protect

Simplified approach without BIA

If you want to avoid a Business Impact Analysis (**BIA**) approach, which requires experienced resources (CISO, external consultant) and can be particularly structuring, a lighter approach is still possible to define the scope of protection.

This simplified methodology consists of two steps:

Step 1: Identification and classification of business applications

- Prioritize critical and important business applications according to their operational impact.
- Deduce the exhaustive list of business servers to be included in the DRP.

Step 2: Dependency analysis

- Examine interdependencies with cross-functional and technical applications.
- Assess their level of criticality specifically in the context of the DRP.

Risk scenarios to be covered by the DRP

Defining risk scenarios is a key factor in establishing the scope of the DRP. Deployment can be phased according to the different types of threats to be covered.

Scenario family	Origin(s)	Type of impact	To be covered within Nuabee DRP
DC(s) Destruction	• Natural disaster • Industrial hazards • DC fire(s) • Malicious acts • ...	Total and prolonged unavailability of the information system	Deployment of the DRP perimeter can be phased according to the risk scenarios to be covered.
Cyber attack	• Targeted cyber attack • Hypervisor attack • Ransomware (filer)	Unavailability of part of the IS. WAN/security components not impacted	
Human crisis	• Social movements • Health crisis, • Pandemic	Lack of personnel to manage IS	
Complex IT incident	• Complex infra-technical failure	More or less short unavailability of the IS on a few components	

Definition of RTOs and RPOs: economic impact

Understanding the financial implications

The choices made for **RTO** (Recovery Time Objective) and **RPO** (Recovery Point Objective) directly influence the recurring costs of the solution:

I**mpact of short RTOs:** The more ambitious the recovery time objectives, the more powerful the components involved in the restart (virtual machines, storage systems, network interfaces) must be, resulting in proportionally higher costs.

Impact of short RPOs: Minimized data loss objectives require increased backup frequency, leading to an increase in the amount of storage required and bandwidth consumption to perform backups.

Customization by server

The Nuabee DRP solution generally offers global RTO and RPO settings, while providing the option to customize these values for particularly sensitive servers:

RTO customization: Example: hotline support application that must be restarted within 4 hours

RPO customization: Example: critical database requiring hourly backups to limit potential data loss

This modular approach optimizes investment by focusing resources on elements that are truly critical to business continuity.