Business continuity strategies: Understanding your maturity level

An honest self-assessment process is required to understand the maturity level of your disaster recovery practices.

To assess the level of disaster recovery preparedness in a company, group, or application, experts use the concept of "maturity levels." This objective and precise term describes the level of preparedness and the capacity to recover from a service interruption, whether it is the loss of a single file, an application crash, or a complete data center outage. All of these elements can negatively affect a company's operations.

A deeper understanding of this readiness can be gained by evaluating a number of factors that can help reveal your level of disaster recovery maturity.

The following series of questions will allow you to better understand the criteria for assessing the current state of your organization.

Key questions to frame the problem

To begin, consider the impact of inactivity during a disruption and ask yourself:

How severe would the outage be for your business?

At what exact moment would your organization begin to experience the effects of these disruptions?

Consider factors such as:

- Availability of vital systems
- Databases
- Customer data
- Network resources

To assess your organization's maturity level, rate your level of maturity in each category on a scale of 1 to 5, using the following criteria:

1 Very low	**2** Low	**3** Moderate	**4** High	**5** Very high

Let's begin with the evaluation of our independent variables:

1. Recovery time objective

How much downtime can your business withstand? Is it a matter of minutes, hours, or days?

In the event of an incident, **how long do you estimate it would take to recover**? Use the scale above, where 1 is considered unacceptable and 5 is the ideal scenario.

The recovery time objective should be identified for all critical systems, networks, databases, and other I.T. resources. These are key metrics when building disaster recovery plans.

2. Recovery point objective

What is the amount of time the data can "age out" before it is no longer useful to the organization?

And **what do you estimate is the maximum amount of time between when an incident occurs and your last backup?** Evaluate this response using the scale above, where 1 is considered unacceptable and 5 is the ideal scenario.

The shorter the recovery point objective, the more critical the data. The backup process must be robust enough to replicate data in the shortest possible time between the original and the replicated copies.

3. Protection architecture

Does your protection solution offer local recovery, cloud recovery, or both?

Is the solution built from one or multiple products?

Is your network infrastructure resilient enough to support the protection architecture with diverse execution circuits and sufficient bandwidth to handle normal and emergency traffic demands?

Can the protection architecture scale up to accommodate abnormal situations where additional resources are needed beyond what is currently available?

4. Protection scope

What I.T. assets are being protected?

- User files.
- Databases.
- Core applications.
- Server images.
- I.T. infrastructure.

During a disaster:

Will all elements of the I.T. environment be available and operational in a way that allows employees to connect securely and continue working?

5. Documentation

Are all recovery procedures fully documented and up-to-date?

Are multiple copies of the procedures available in paper and electronic format?

Do emergency teams have access to copies of plans in alternate locations, such as in their cars or at home?

Will collaborative resources—intranets and content repositories—be available to securely store copies of plans?

Do emergency teams have copies of disaster recovery plans on their mobile phones?

Are they able to remotely access their plans using their mobile phones?

6. Scope of tests

Evidence can be as simple as an overview of a plan. However, the amount of coverage when testing and validating recovery procedures is significant. For example:

Are files randomly and quickly evaluated?
Are servers taken down or secondary infrastructure checked?

These tests are crucial to ensuring that issues beyond technical problems are not overlooked. They also ensure that necessary financial and supply arrangements are made, such as providing a new workspace if needed.

7. Frequency of tests

How often do you run recovery procedures?

Experience has shown that conducting at least one test per year is a starting point for most I.T. testing systems. However, for systems considered critically important, it is advisable to test more frequently, especially if they have undergone significant changes.

Disaster recovery plans must reflect those changes. Many plans fail because they do not incorporate these changes into their disaster recovery strategy.

8. Organizational sponsorship

Is recovery readiness an I.T.-only project or a company-wide initiative?

Is company leadership involved in driving and supporting the need for disaster recovery or is it solely supported by I.T. management?

Has the administration approved a budget for disaster recovery?

Have I.T. staff received training in disaster recovery procedures from equipment vendors and network service providers?

Ideally, disaster recovery is set up as a dedicated function: with a dedicated and ongoing budget, staff, and activity schedule that includes plan reviews, exercises, and staff training.

Analyzing the results

After internally answering the above questions and assigning a value to each key point, we will obtain a clear result according to the following table, which maps the levels of support and commitment to the five levels of our own maturity model:

LEVEL	SCORE
1 - Ad Hoc	**8**
2 - Reactive	**9 to 15**
3 - Ready	**16 to 22**
4 - Proactive	**23 to 27**
5 - Resilient	**28 to 35**

Achieving level 3 (ready) is an ideal goal for most organizations as it demonstrates an understanding of and commitment to key disaster recovery metrics, including RTO/RPO, documentation, testing, and organizational sponsorship.

Reaching level 4 (proactive) can be accomplished by leveraging the unique services offered by cloud-based providers.

After completing the exercise, how has your organization ranked?

Proper preparation for adverse and unforeseen situations is vital for all organizations. Having the right ally can help elevate your level of preparedness against disasters.

For more information, visit: LIBERTYNET.COM

