# Availability and Recovery Worksheet

## Concepts and Definitions

**Availability:** The overall measure of a systems' up time over a given period of time represents its overall availability. Commonly represented in terms of 'Nines' – or total percentage of up-time throughout an entire period of time (commonly a calendar year) – such as 99% up time, 99.9% up time, 99.99% etc.

**High Availability:** The use of redundant systems (such as redundant NICs, power supplies, or even 'teamed' servers and entire systems) to increase overall uptime and availability. Typically, to be highly available, redundant systems must be able to 'failover' almost immediate and virtually automatically when problems are detected. To this end, systems that are 'fault tolerant' are described as being High(ly) Available systems and this term (High Availability or HA), in turn, ends up being used to describe entire deployments that can handle minor outages in terms of single points of failure within redundant systems.

**Disaster Recovery:** Simultaneously used to define the set of routines or processes that SysAdmins follow to resolve major disasters (not covered or addressed by typical redundancy) as well as to define the precautions taken to help ensure that backups, instructions, skills, and other resources are available as needed in the case of true emergencies.

**Recovery Time Objective (RTO):** Used to describe the ideal amount of TOLERATED down-time – or the objective for the point at which recovery is finalized or achieved. (i.e., an RPO of 5 minutes would state that systems should be operational within 5 minutes of a disaster).

**Recovery Point Objective (RPO):** Defines the ideal amount of TOLERATED data-loss during a disaster. For example, an RTO of 1 minute would mean that during a disaster, only up to 1 minute's worth of data would have been lost BEFORE the disaster. (RPO time would then be 'added' to this to help indicate/define TOTAL down-time and loss of continuity.) See this post for more details.

## Disaster and Down-Time Definitions

**Maintenance.** While maintenance isn't a disaster, it can and will commonly result in down-time. Highly-available systems therefore either need to schedule this for 'off-peak' execution and/or address redundancy to minimize downtime when patching, etc.

**Single Points of Failure / Minor Failures and Outages.** 'Simple' component and system failures restricted, typically, to just a single (redundant) system and therefore 'covered' or addressed by highly-available systems. Examples include things like failed memory controllers, lost back-planes, system and OS hangs or crashes, NIC failures, etc.

**Logical Corruption Problems**. Many Highly Available systems do not address the problem of data being logically corrupted by end-users or applications. If a software bug or admin accidentally 'messes up' data, that data is now incorrect or wrong – but highly available (redundant). In many instances, operations will continue AFTER data is logically corrupted – making it harder to remove or address. Likewise, other aspects of overall functionality may work 'fine' – while a single table or set of tables may be 'corrupt' or busted. Consequently, these outages are a 'special' type of disaster and are best addressed with the use of 3rd Party Log Reader Agents.

**Major Disasters / Systemic Failures.** Physical corruption, major network /power outages, significant SAN outages, long-term active directory issues; Fires, Earthquakes, and other natural disasters.

## Matrix

Fill out the following targets or objectives – in either minutes or hours (e.g., 1 minute, 5 minutes, 3 hours, etc.).

| | **RPOs**<br>*Target for Tolerated Amount of Data Loss* | **RTOs**<br>*Target for Tolerated Amount of Down Time* |
|---|---|---|
| **Maintenance Outages**<br>Planned outages – executed during off-peak hours* | | |
| **Single Points of Failure (HA)**<br>Single Point of Failure / Loss of Single System | | |
| **Logical Corruption**<br>Software Bugs and 'Ooops' problems by SysAdmins | | |
| **Systemic Failures (Disaster Recovery)**<br>Loss of Data Center or Significant Data Corruption** | | |

* When and where possible/available.

** Physical data corruption (as opposed to logical corruption).

## Sample Matrix and Translations

The following, sample, matrix outlines an example of what could be used to define an outage – and then provides 'translations' of what the RPOs and RTOs signify:

| | **RPOs**<br>*Target for Tolerated Amount of Data Loss* | **RTOs**<br>*Target for Tolerated Amount of Down Time* |
|---|---|---|
| **Maintenance Outages**<br>Planned outages – executed during off-peak hours* | 0 minutes | Up to 20 minutes. |
| **Single Points of Failure (HA)**<br>Single Point of Failure / Loss of Single System | 1 minute | 2 minutes |
| **Logical Corruption**<br>Software Bugs and 'Ooops' problems by SysAdmins | 1 minute | 4 hours |
| **Systemic Failures (Disaster Recovery)**<br>Loss of Data Center or Significant Data Corruption** | 10 minutes | 3 hours |

**Translations**

For Maintenance, the expectation is that data should NOT be lost (other than in-flight transactions that should be rolled back), and that 20 minutes of total down-time IS tolerable. (Anything greater than this would, then, require management approval.)

For simple failures (or HA-covered scenarios), up to 1 minute of data loss could be tolerated, and 'failover' could take up to 2 minutes.

For logical corruption problems, the idea is that data loss is NOT desirable – so things should be able to be corrected to within 1 minutes' worth of time. However, given how hard these issues can be to recover from (especially since they sometimes go undetected for a significant period of time), up to 4 hours is tolerated for these issues to be addressed.

For wide-spread systemic failures, up to 10 minutes of data can be lost (meaning that SQL Server Transaction Logs should be getting regularly backed up at least every 10 minutes and being copied OFF SITE to ensure a 'smoke and rubble' contingency). Recovery time, however, is listed at 3 hours – which (depending upon infrastructure and needs) might be enough time to simply restore all backups from disk (manually), or might require another DR solution like Log Shipping, Mirroring, or AlwaysOn (AGs of 'stretch' FCIs).