Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security SEGSI

TP01

Business Continuity

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Business Continuity

- Computer resources usage is a reality[1]
- Even at a particular level, its use is an increasingly pressing reality[2]
- This reality made the (good) functioning of computer resources essential
- But what is the impact depending on the type of user?
  - It does not matter whether it is an individual or a company?

[1] Pordata, 2019: 99.0% of companies with 10-49 or more workers, 100% with 50 and higher (Portugal)
[2] Pordata, 2022: 4,057,223 Internet access subscribers (Portugal)

Business Continuity

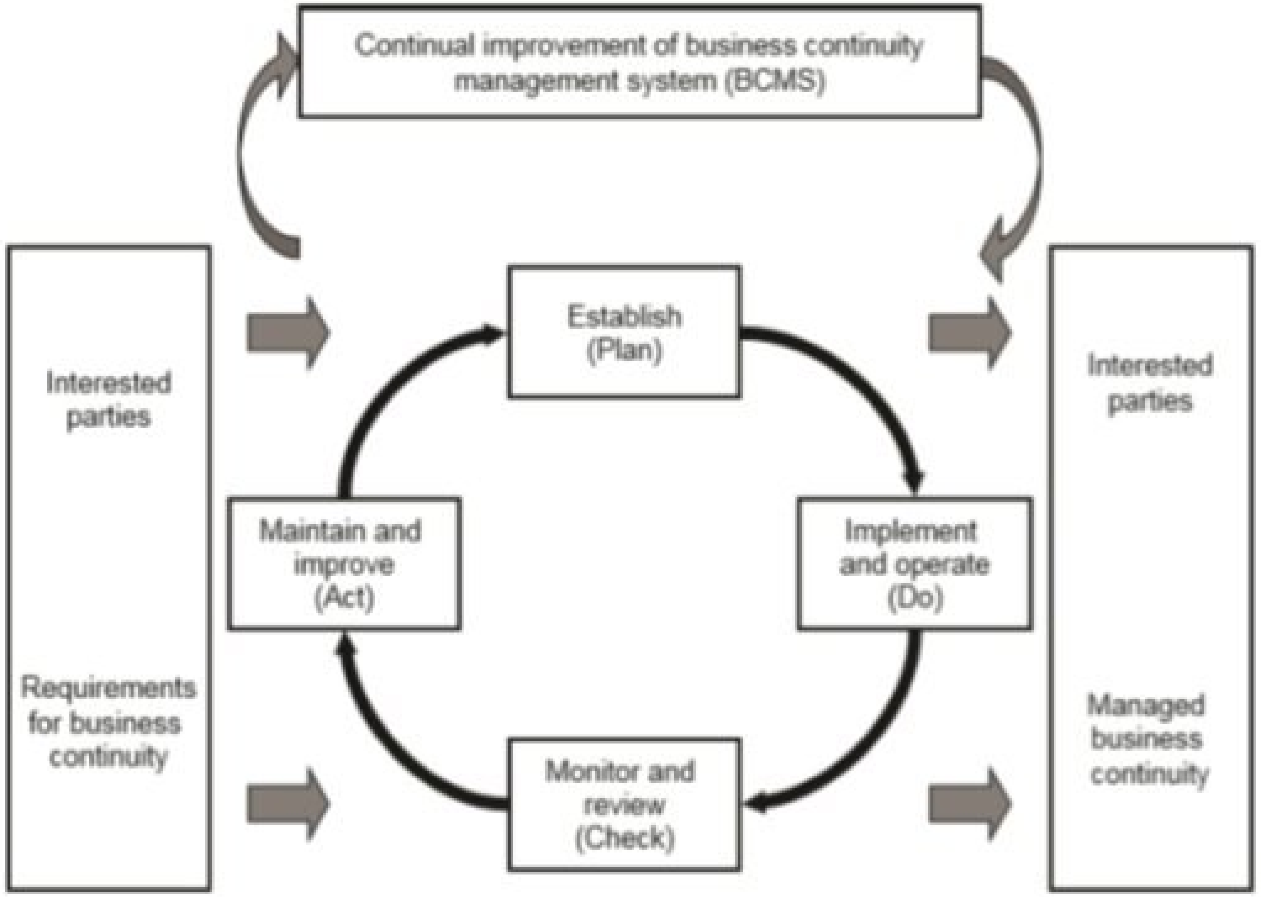
- No!
- What changes is the expectation and speed required for its use
- The desires and needs are the same, what changes is the ability (or desire) to maintain the desired level of functioning
- Therefore, it became urgent to create a methodology to measure the level of functioning of computer systems, and the definition of criteria that measure and / or define them
- In this way, standards emerged, of which we highlight the ISO 27000

Business Continuity Management

- ISO 27000 standards, supported by other standards including ISO 22301 and 22313, define criteria to maintain business continuity
  - Note that *business* should be understood in the broad sense
- They define rules with organizations in mind, but adaptable to their size (which may even be a particular)
- The objective is to standardize methodologies and thus enable common criteria
- As a common feature, the need to be a *top-down* methodology, that is, it does not make sense to be an individual decision of a single individual without the support of decision makers (in an organization, top management)
- These standards define *Business Continuity Management* (BCM)

Business Continuity Management

- The model recommended in the standards is the *Plan-Do-Check-Act* (PDCA)
    - That is, it is a model of continuous observation, planning and action
- As an essential part for the application of the model, it integrates a set of criteria that must be met


Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Implement and operate (Do)
Monitor and review (Check)
Maintain and improve (Act)
Interested parties
Managed business continuity

Source: ISO 22301:2012

Business Continuity Management
Criteria I

- ***Maximum Tolerable Period of Disruption*** **(MTPD)**
  - Maximum time below the performance requirements of the IT infrastructure
- ***Maximum Tolerable Downtime*** **(MTD)**
  - Maximum downtime of the IT infrastructure

- The objective is that, in a period shorter than defined by these criteria, the activity and performance requirements of the organization (i.e. *the business*) is resumed
- These values may not be fixed, static
  - For example, there may be a time period more demanding than another - for example in seasonal businesses
  - There may also be a more pressing service than another
  - In that case, BCM must specify all applicable

Business Continuity Management

Criteria II

- *Minimum Business Continuity Objective* (MBCO)

- Specifies the minimum level of operability that must be maintained during an infrastructure disruption
- For example, the S1 service may not be operational but the S2 service must remain at an acceptable level of operation
- MTD/MTPD will certainly be more restricted for the services associated with this objective

Business Continuity Management

- One question that can be raised here is what is the acceptable level of functioning
- This is the level of functioning in terms of security, integrity and availability (i.e., in terms of response time) that is intended and accepted by the organization
- This set of qualitative and quantitative parameters is called ***Service Level Agreement*** (SLA)

Business Continuity Management

- If business continuity is intended, BCM design must analyze and mitigate potential constraints
- All threats and failures that may occur must be assessed and possibly eliminated - or at least mitigated
- Let's start by looking at the SLA criteria; it must contemplate not only the service levels (confidentiality, integrity and availability) intended but also how to measure and validate them
- A system that complies with the combined SLA is called a **secure system**

Business Continuity Management

- But for a system to be secure, it is necessary to analyze and mitigate failures that may occur
- What is the probability of failure (**P**) of a service?
  - The service depends on components, which in turn can depend on other components, etc. (see as an example a service that runs on a system, but that system depends on memory, disk, power supply, etc.)
- The probability of failure of a service dependent on several factors is given by the sum of the probabilities of failure of all factors involved

$$\mathbf{P = P_1 + P_2 + \ldots + P_N}$$

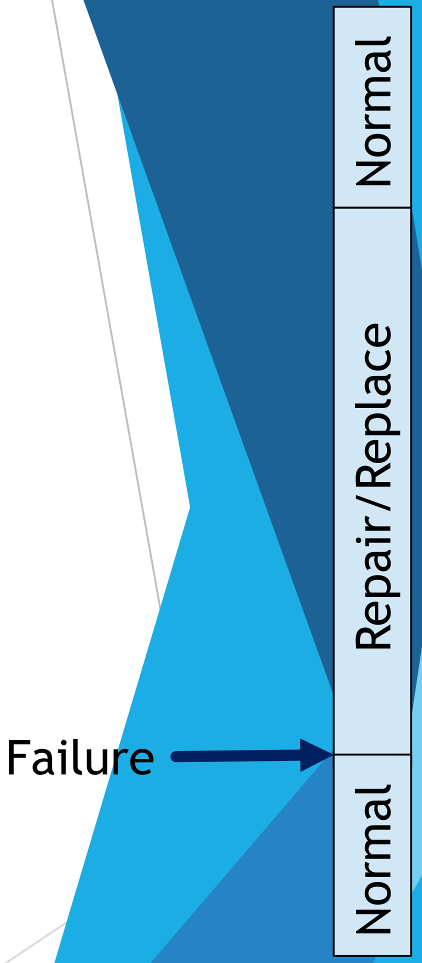
Business Continuity Management

- However, it is more common to use the average time between failures (***Mean Time Between Failures*** **MTBF**)
- For its calculation, not only the average time to fail (***Mean Time To Fail*** **MTTF**) is taken into account but also the time needed to repair or replace (***Mean Time To Repair/Replace*** **MTTR**)

MTBF = MTTF + MTTR

- Based on this value, we can calculate the availability of a system or service

$$\boldsymbol{Availability = \frac{operating\ time\ without\ failure}{total\ operating\ tme} = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF}}$$

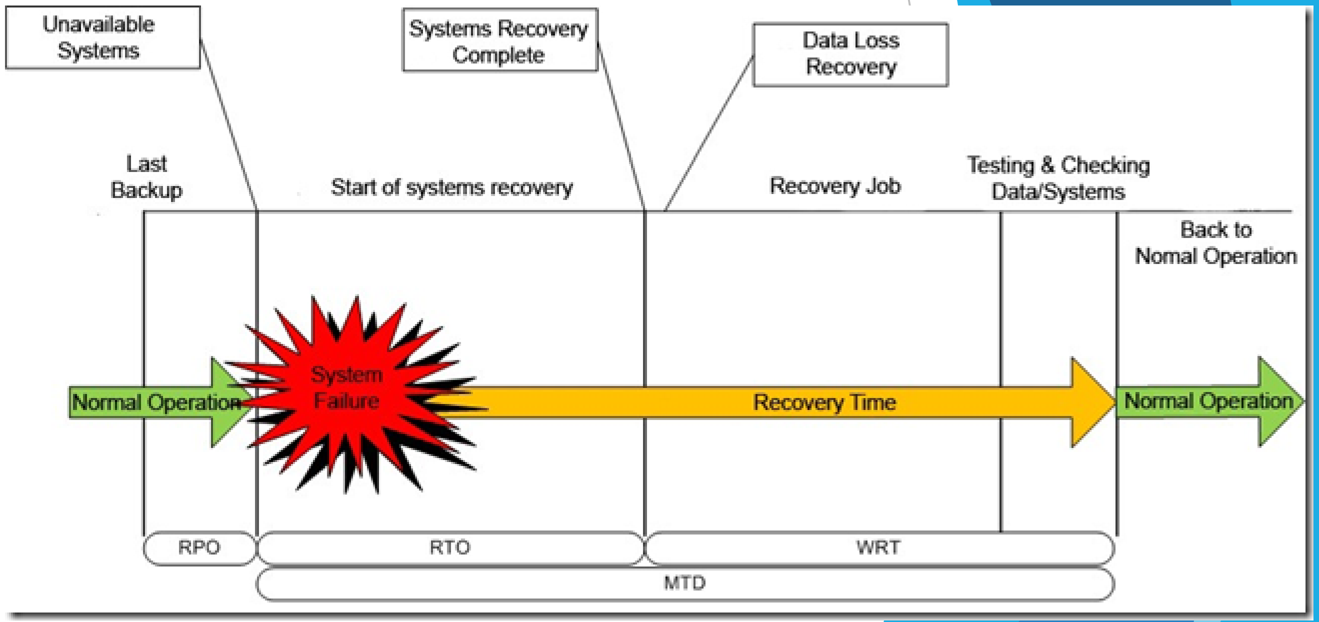


Business Continuity Management

- Even with redundancy, note that there may be components common to the redundant system
  - Example: power supply, redundancy control system
- These common components are called **SPOF** (*Single Point Of Failure*) and should be avoided
- There may also be faults connected or not to physical components that imply system unavailability
  - Example: operating system vulnerability
- A **CMF** (*Common-Mode Fault*) is a failure that causes the unavailability of more than one component of the redundant system
  - A SPOF is always a CMF but the reverse is not true

Business Continuity Management

- It is more appropriate and useful to set goals for both the average recovery time of the functionality and the volume of data loss that is accepted
  - ***Recovery Time Objective*** (**RTO**) is the average recovery time for systems and infrastructures
  - ***Recovery Point Objective*** (**RPO**) is the maximum accepted data loss time
  - ***Work Recovery Time*** (**WRT**) is the time required to restore data and applications and test them



Source: CISSWhat? - A CISSP Review

Business Continuity Management

- In theory, it is always possible to find a strategy to ensure business continuity
- However, some of these strategies (and whose risk according to the identified risk matrix is considerable) may imply an inappropriate cost to the benefit obtained

- It is therefore necessary to analyze and calculate the cost of mitigating risk in view of the benefit obtained

Business Continuity Management

- Let's define an ***Asset Value*** (AV) that represents the value of the item in question
- The risk exposure of this item is represented by the ***Exposure Factor*** (EF)
- ***Single Loss Expenditure*** (SLE) is obtained by multiplying these two factors

$$SLE = AV \times EF$$

- It can also be obtained or calculated the probability of the occurrence of damage in the item over the course of a year, that is, the ***Annualized Rate of Occurrence*** (ARO), which allows the calculation of the ***Annualized Loss Expectancy*** (ALE)

$$ALE = SLE \times ARO = AV \times EF \times ARO$$

- The amount obtained must be compared with the cost of the necessary to mitigate the risk

Business Continuity Management

- With the BCM in mind, what is the ALE if
  - Asset value = 4.000€
  - Exposure factor = 30%
  - Annualized rate of occurrence = 6

  - ALE = 4.000€ x 30% x 6 = 7.200€

Business Continuity Management

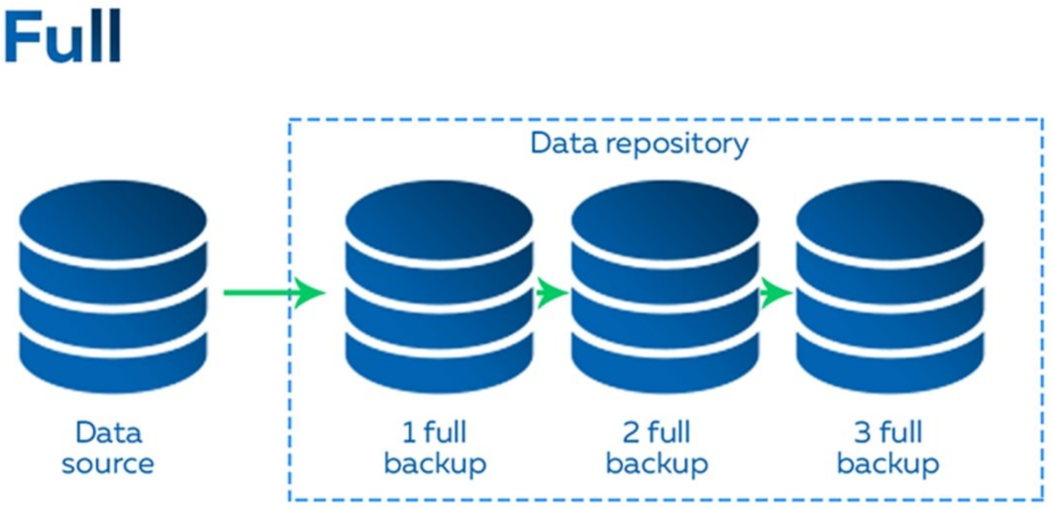
- What about the opposite way?
- If the organization does not accept and annualized loss expenditure (ALE) greater than 4.000€ and considering the following values, what can be the maximum exposure factor (EF)?
  - Asset value = 10.000€
  - Exposure factor = ?
  - Annualized rate of occurrence = 8
  - EF <= 4.000€ / 10.000 / 8 = 5%

Business Continuity Management

- Calculation of AV might not be always so simple
  - What is the value of data?
- To predict data loss (which influences the RPO calculation), some strategies can be used, for example
  - Backup copies
  - *Mirroring* to remote location or premises
- Both strategies have benefits and drawbacks
- Note that the RTO is independent of the strategy adopted
  - But the WRT is influenced by the strategy

Business Continuity Management

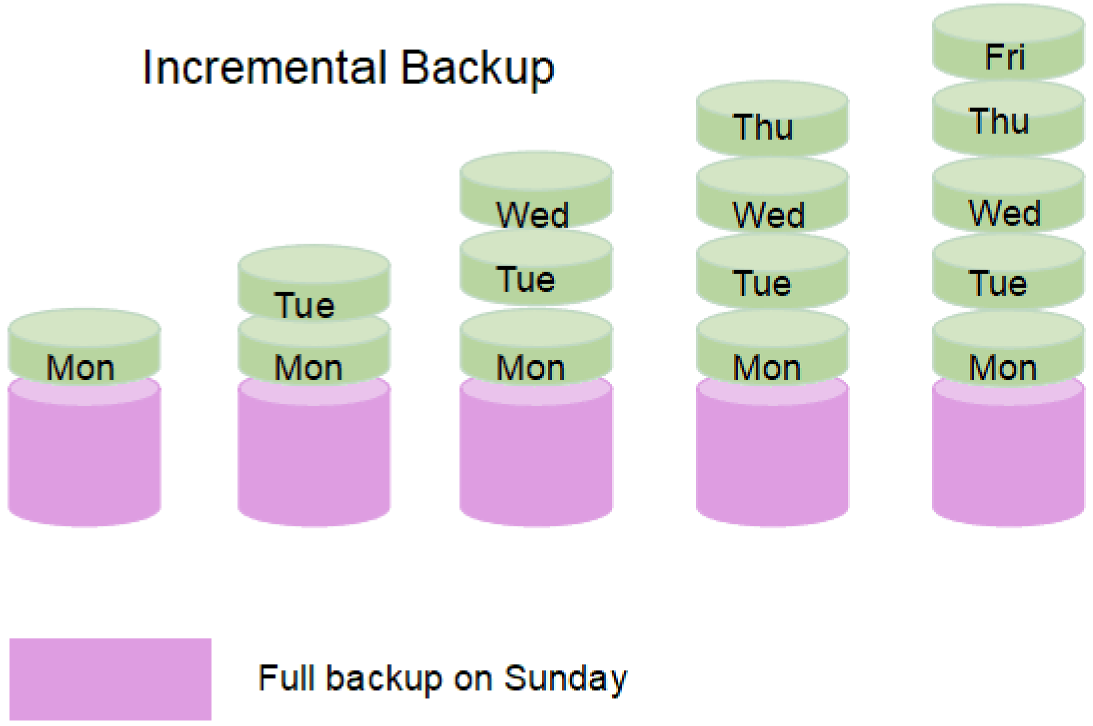
- Backup has three possible strategies
  - Integral/Full
    - Copies all data; implies longer copy time (which affects RPO); implies less replacement time (which benefits the WRT)



Source: 123host

Business Continuity Management

- Backup has three possible strategies
  - Incremental
    - Always needs a prior integral/full copy; copies all data that has changed since the previous incremental copy (or the integral if it is the first incremental)

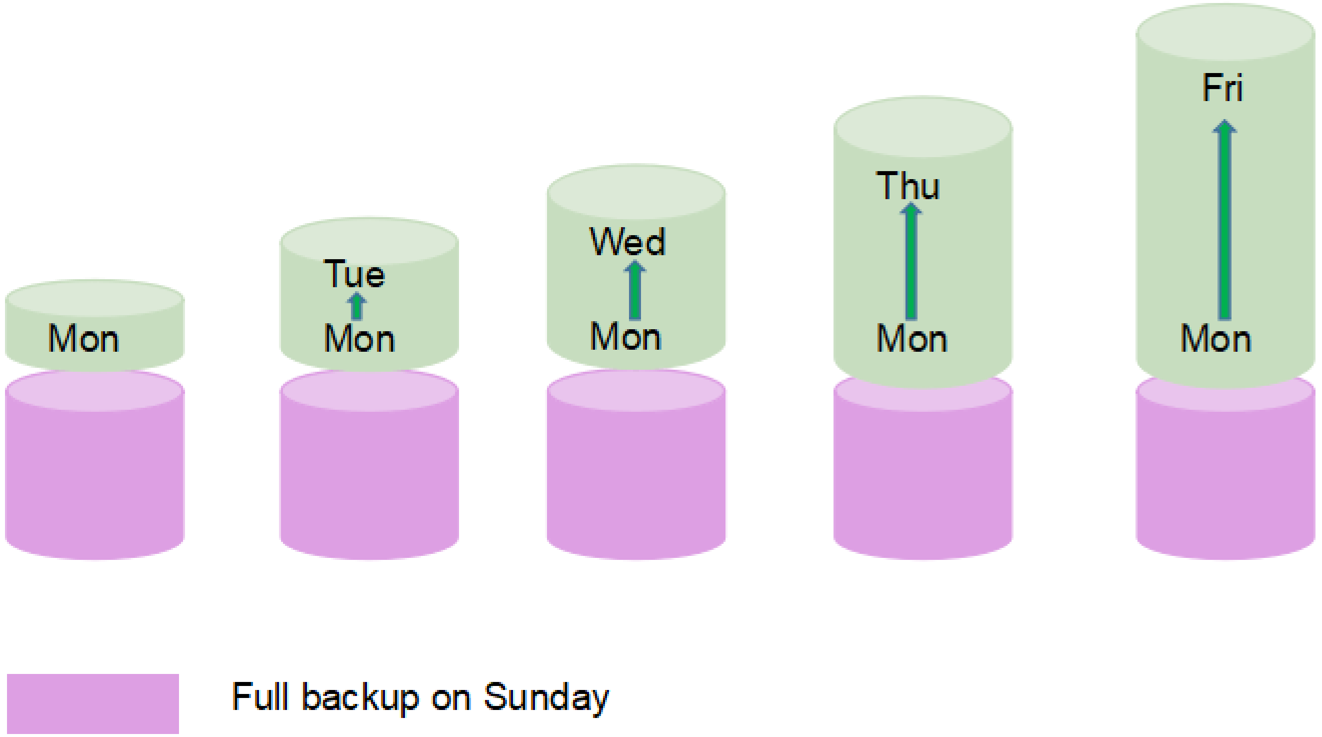


Source: digitalphabet

Business Continuity Management

- Backup has three possible strategies
  - Differential
    - Always needs a prior integral/full copy; Copies all data that has been changed since the previous full copy

Differential Backup



Source: digitalphabet

Business Continuity Management

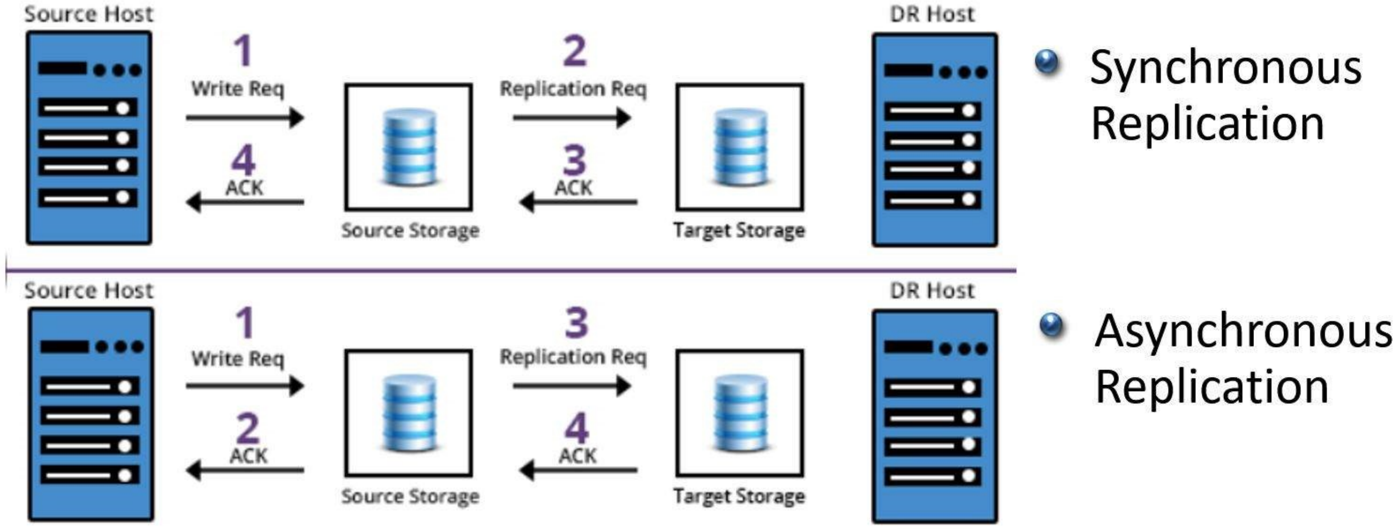
- What is the best strategy with RPO and WRT in mind?
  - It depends…
    - Of the execution environment…
    - Of the possibility or not to keep the system running during the copy run…
  - What is more important: the downtime of operation due to the execution of a backup, or the amount of time needed to restore it in case of trouble?

Business Continuity Management

- *Mirroring* for remote location/premises
  - Can be with synchronous or asynchronous replication
  - Facilitates disaster recovery
  - The RPO and WRT are null (if it is synchronous) or very close to it (if it is asynchronous)
  - It implies the need to guarantee the confidentiality and integrity of the data, which will in turn cause greater latency in the network with a possible impact on the availability of operation (and inherently in the SLA)

Business Continuity Management

- Mirroring
  - Synchronous
    - Application only continues after the data is stored in both locations
  - Asynchronous
    - Application continues after the data is stored on the main premises



Source: Flackbox

Business Continuity Management

- What is the best option?
- What are the constraints one should consider on data resilience?
- Backups
  - They must always be done, whatever option for BCM is taken
- Mirroring
  - If it is a strategy, what principles and/or cares must / should be planned?

Business Continuity Management

- But the risk always remains…
- … and directives and regulations exists to enforce business continuity
  - NIS Directive Art.º 7 n.º 2/i (that will be looked later at the lecture class)
  - GDPR Art.º 32 n.º 1/b (however by a different perspective)
- What can one proceed about risks?
  - Avoid
  - Transfer
  - Mitigate
  - Accept

Business Continuity Management

- **Avoid**
  - Eliminate the cause of the risk by eliminating the process that generates it
- **Transfer**
  - Direct the responsibility for the consequences to third parties
- **Mitigate**
  - Reduce risk exposure by drawing up action plans and applying specific controls, in order to mitigate the risk or reduce it to fit the risk acceptance criteria defined by the organization
- **Accept**
  - Becoming aware of the risk without adopting controls

Business Continuity Management

- Which action to choose?
- That depends of several factors, like the cost of the action among others
- Whatever the action will be implemented, it must / should be consistent with a risk acceptance criterion to be adopted by the entity
- Whichever action is decided, it must / should be sustained with the calculation of the ALE

Business Continuity Management

- Let us focus on the BCM components
  - One part of it is the *Business Continuity Plan* (**BCP**) that addresses the usual operation of the infrastructure
    - Meaning that it should state the MTD, MBCO, RTO, RPO, WRT, MTPD, risks, backup strategy, rules – and penalties - that must be observed by all, and the procedures when something fails, among other parts
  - Another part is the *Disaster Recovery Plan* (**DRP**) that addresses the procedures to apply if the planned criteria (MTD, MTPD, MBCO, …) are surpassed
  - When at least one of the mandatory criteria is exceeded, DRP assumes the operation while the responsible team (that is also defined on the BCP) solves the problem(s)
    - Its operation ends when the *normal* infrastructure is again operational

Business Continuity Management

- What threats occurs or can occur
  - Malfunction
    - System error, damaged keyboard, etc.
  - Accident
    - Drink spilled over the system, human involuntary error, etc.
  - Natural
    - Earthquake, floods, etc.
  - Application error or incorrect behavior
    - Some result was expected yet a different one is obtained
  - Attack
    - Malware, ransomware, etc.
  - Human origin
    - Credentials captured, etc.

Business Continuity Management

- For all of them a plan can be previously defined and implemented in advance
  - Did anyone imagine that the lockdown due to Covid-19 could happen?
- And might not jeopardize the usual operation of the company
- Those threads can / should be addressed by the BCP