Systems Administration ASIST

Topic 2

Business Continuity Management

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

Business Continuity Management

- The use of computer resources is a reality[1]
- Even at a particular level, the use of computer resources 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, 17/8/2020: 99.2% of companies with 10 or more workers (Portugal)

[2] Pordata, 17/8/2020: 3,641,758 Internet access subscribers (Portugal)

Business Continuity Management

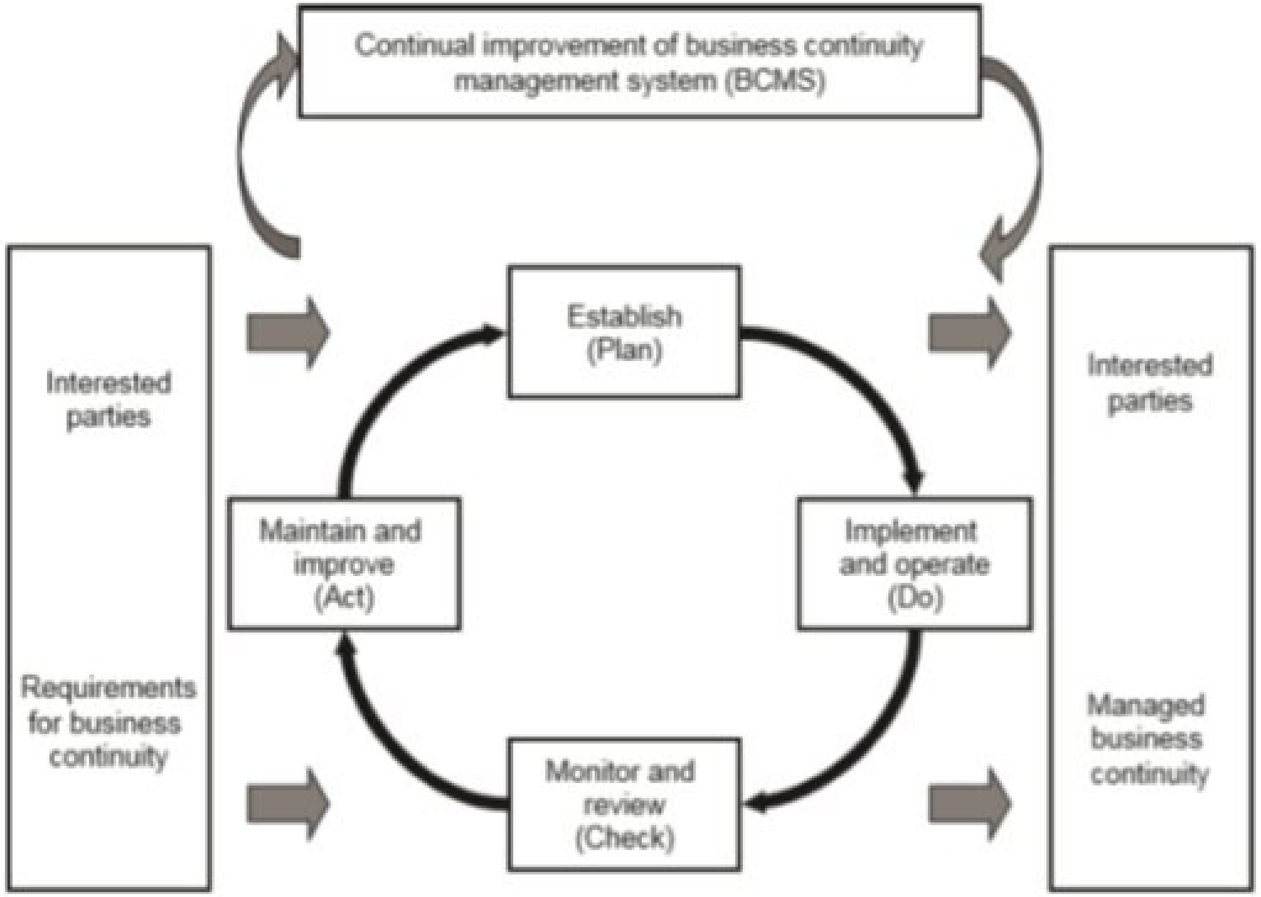
- No!
- What changes is the expectation and speed required for its use
- The desires and needs are the same, what changes is the ability (or desire) to maintain the desired level of functioning
- Therefore, it became urgent to create a methodology to measure the level of functioning of computer systems, 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 Tolerable Downtime*** **(MTD)**

- These two criteria have an approximate meaning and define:
  - MTPD: maximum time below the performance requirements of the IT infrastructure
  - MTD: the 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 (ie *the business*) are 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 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 (which we will see later) in terms of security, integrity and availability (ie, 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
Criteria I

- *Business Impact Analysis* (BIA)
  - Identifies the critical activities of the organization and its dependencies; this way allows prioritizing recovery operations after a disruption

- *Risk Assessment* (RA)
  - Constituted by scenarios that can affect business continuity, the probability of occurring and their impact

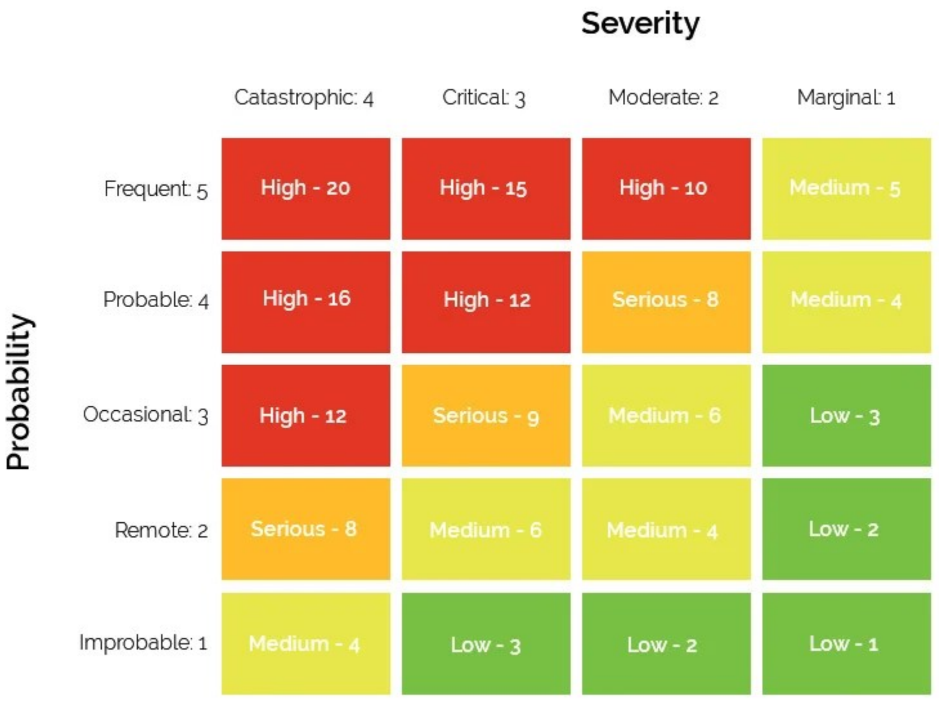
- *Business Continuity Plan* (BCP)
  - BCP is an integral part of BCM and documents the procedures to be performed to respond, recover, resume and restore to a pre-defined level of operation after the interruption

Business Continuity Management
Criteria II

- ***Risk Assessment*** **(RA)** is usually represented by a risk matrix
- Each item has an associated probability and estimated impact (severity); the product of these factors gives a measure for the risk

Risk = Impact x Probability

- Considering probabilities on a scale of 1 (least possible) to 5 (most possible) and impact on a scale of 1 (marginal) to 4 (catastrophic), we have



Probability

	Severity			
	Catastrophic: 4	Critical: 3	Moderate: 2	Marginal: 1
Frequent: 5	High - 20	High - 15	High - 10	Medium - 5
Probable: 4	High - 16	High - 12	Serious - 8	Medium - 4
Occasional: 3	High - 12	Serious - 9	Medium - 6	Low - 3
Remote: 2	Serious - 8	Medium - 6	Medium - 4	Low - 2
Improbable: 1	Medium - 4	Low - 3	Low - 2	Low - 1

Source: Industry Safe

Business Continuity Management
Criteria III

- *Risk assessment* must be defined for all risks identified
- There may be no need to build the risk matrix, but having it helps to determine the most worrying risks and reduce (mitigate) them
- But it is important that in BCM the threats considered and their risk classification are defined

Business Continuity Management
Criteria IV

- ***Disaster Recovery Plan*** **(DRP)**

- DRP is also part of the BCM
- In normal situation, the infrastructure works within the parameters defined in the SLA and BCM takes care of the observation (monitoring), planning, implementation of corrective actions and other acts deemed necessary
- However, problems may occur that imply a violation of the SLA
- But do they also violate the MBCO or the MTD?
  - If the MBCO or the MTD are not affected, the BCM must contain the necessary procedures to recover the SLA from disrupting services
  - If affected, the DRP takes control until the desired situation is recovered

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

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

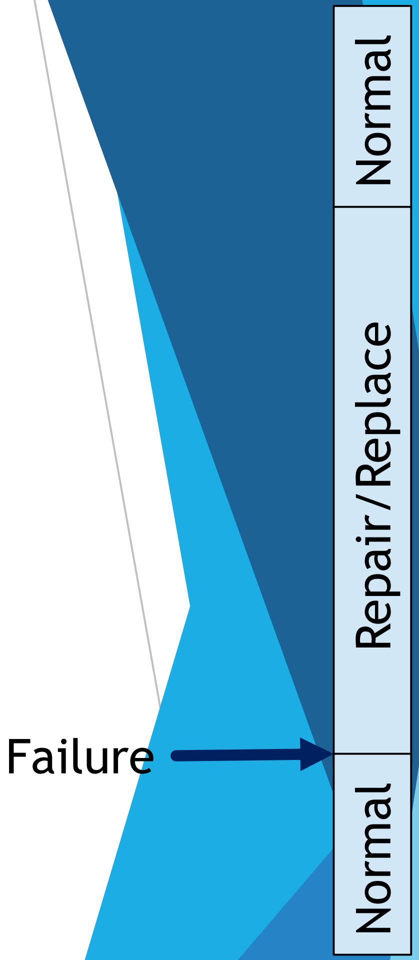
Business Continuity Management

- 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

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



Normal

Repair/Replace

Failure

Normal

Business Continuity Management

- The inverse of MTBF is the **failure rate per hour**, represented by λ, or, if calculated for one million hours, the failure rate per million hours (**FIT**)
- The MTBF calculation for a system or service that depends on several subcomponents in series can be calculated as the inverse of the sum of failure rates per hour (or per million hours) of each subcomponent
- Assume a system consisting of three (3) non-redundant components
  - Component 1: MTBF1 = 20000 → FIT1 = 1000000/MTBF1 = 50
  - Component 2: MTBF2 = 10000 → FIT2 = 1000000/MTBF2 = 100
  - Component 3: MTBF3 = 15000 → FIT3 = 1000000/MTBF3 = 66,67
- The calculation of FIT of the complete system is **FIT1 + FIT2 + FIT3 = 216,67** so

$$\mathbf{MTBF_{total} = 1000000 \,/\, FIT \approx 4615{,}3}$$

Business Continuity Management

- To obtain a better availability it is essential to increase the MTTF and decrease the MTTR
- The increase in MTTF can be obtained through a quality control of products / services
- The decrease in MTTR is not always achieved with the same quality control of products/services - in addition to being dependent on the type of product/service in question
- The repair of a service that interrupts its operation is not comparable to the replacement of a system!
- **High availability** means obtaining an availability of 100% or close to that value

Business Continuity Management

- Among the principles that can be activated to increase availability, there is **redundancy**
- However, one aspect to take into account is the total independence and autonomy of the redundant components
- The calculation of the MTBF of a redundant system uses the failure rate per hour, λ, of its components
- Assume a system consisting of three (3) redundant but non-redundant between themselves
  - Component 1: MTBF1 = 20000 → $\lambda 1 = 1/\text{MTBF1} = 0{,}00005$
  - Component 2: MTBF2 = 10000 → $\lambda 2 = 1/\text{MTBF2} = 0{,}001$
  - Component 3: MTBF3 = 15000 → $\lambda 3 = 1/\text{MTBF3} \approx 0{,}000067$
- The calculation of F for the complete system is $\boldsymbol{\lambda 1 \times \lambda 2 \times \lambda 3 \approx 0{,}0000000000003}$ so

$$\mathbf{MTBF_{total} = 1 / \lambda \approx 3 \times 10^{12}}$$

Business Continuity Management

- Through **fault prevention** (*Fault Avoidance*) the avoidance of failures occurrence that jeopardizes business continuity is seek
- Various mechanisms can be used, of which monitoring and alarmism stand out (checking the use of resources such as disk, CPU, temperature control, humidity, etc.)

- The **Fault Tolerance** level classifies the system or service according to its behavior in the event of a failure of any origin
  - Is it keeps working: ***Full Fault Tolerant***
  - If a temporary degradation occurs: ***Gracefull Degradation***
  - If degradation is significant or prolonged: ***Fail Soft***
  - If the system/service becomes unavailable but maintains integrity: ***Fail Safe***

Business Continuity Management

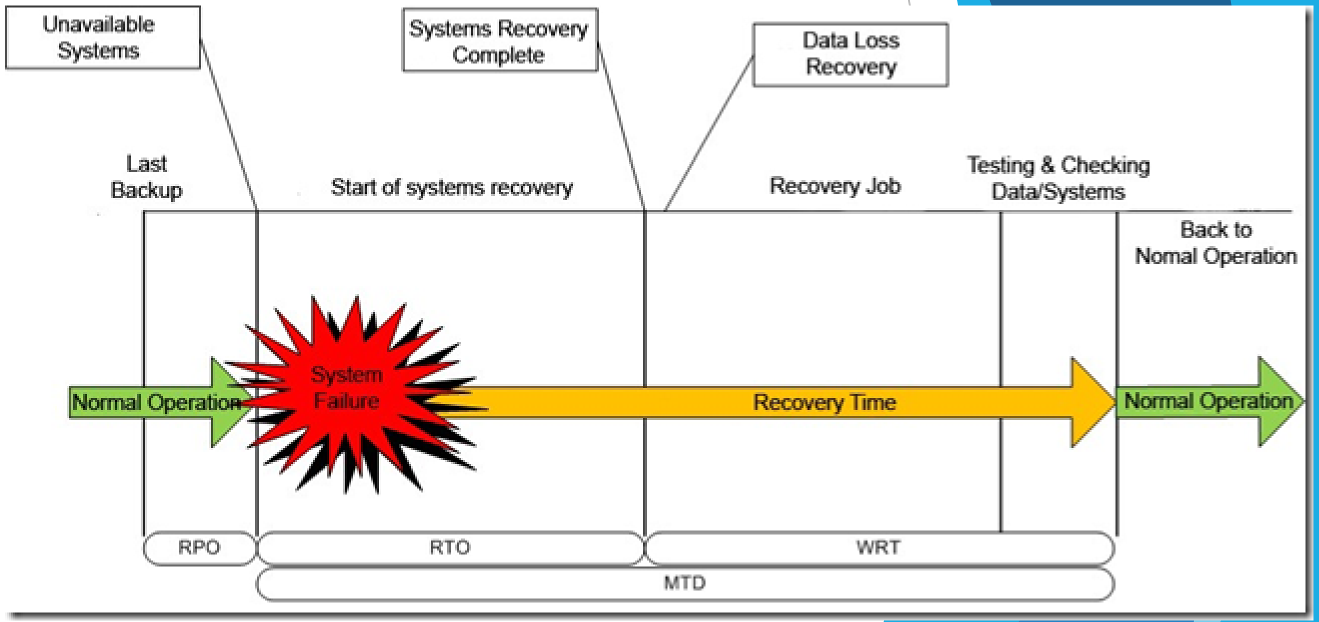
- Even with redundancy, note that there may be components common to the redundant system
  - Example: power supply, redundancy control system
- These common components are called **SPOF** (*Single Point Of Failure*) and should be avoided
- There may also be faults connected or not to physical components 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

- Let's look at the MTTR components in more detail so that it meets the desired MTD
- Failure can be minor and easily resolved or more complex
- Therefore, it is important to ensure aspects such as backup copies or equivalent, thus allowing the situation immediately before the failure to resume.
- However, it should be noted that the MTTR only ends when the operation is fully recovered
  - In other words, the time to restore backup copies is still an integral part of MTTR

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

$$\mathbf{SLE = AV \times EF}$$

- 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)

$$\mathbf{ALE = SLE \times ARO = AV \times EF \times ARO}$$

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

Business Continuity Management

Case 1

- Imagine the following factors
  - AV = 500€
  - EF = 20%
  - ARO = 3
  - SLE = 500 x 20% = 100€
  - ALE = SLE x ARO = 100 x 3 = 300€
  - The action must be considered if its cost is <= 300€

Case 2

- Imagine the following factors
  - AV = 1000€
  - EF = 30%
  - ARO = 2
  - SLE = 1000 x 30% = 300€
  - ALE = SLE x ARO = 300 x 2 = 600€
  - The action must be considered if its cost is <= 600€

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), several strategies can be used, for example
  - *Mirroring* to remote location or premises
  - Backup copies
- Both strategies have benefits and drawbacks
- Note that the RTO is or can be independent of the strategy adopted
  - But the WRT is influenced by the strategy

Business Continuity Management

- *Mirroring* for remote location/premises
  - Can be synchronous or asynchronous
  - 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

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

Business Continuity Management

- Backup has three possible strategies (ii)
  - Differential
    - Always needs a prior integral/full copy
    - Copies all data that has been changed since the previous full copy
- What is the best strategy with RPO, RTO and WRT in mind?
  - It depends…
    - Of the execution environment…
    - Of the possibility or not to keep the system running during the copy run…

Business Continuity Management

- If the possible strategy is backup, whatever your methodology,
  - Must always be done in duplicate
  - One of the media containing the copy must be kept in a remote location
  - …
  - And do not forget that the copy and the ability to restore data should be randomly checked!