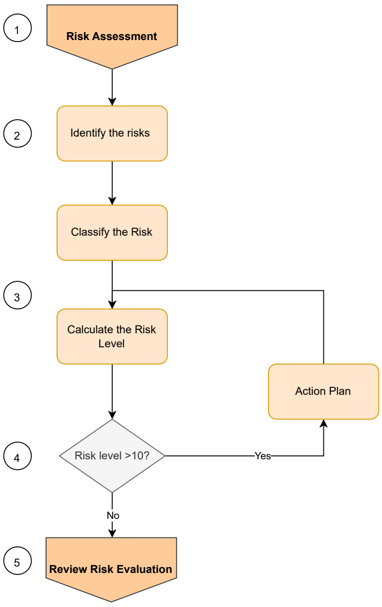
ADDVOLT

Risk Assessment

P 02 4 30



1. Risk Assessment (ISO)

Identify the risk assessment and define the action plans for the assetsclassified as relevant.

2. Identify the risks (ISO)

Risk is the occurrence of an unwanted event, or the non-occurrence of a desired event, which adversely affects the business, it can be:

- The company's assets are not protected against loss.
- The confidentiality, integrity and availability of the information is not reliable.
- There are non-compliances regarding organizational policies and procedures or regarding regulation.

Based on ISO 27001, the risk identification is carried out according to the following sequence:

- **Risk** – Select a risk from the risk inventory or define a new risk.
- **Risk Owner** – Identify the owner of the risk, the function responsible for the action to mitigate the risk or to accept the risk.
- **Impact Assets** – Identification of the assets that will be impacted by the risk.
- **Main concerns** – Identify if the risk impact in Confidentiality, Integrity or Availability, can impact in more than one.
- **Existing Controls** – Describe the controls already defined and put in place.

3. Classify & Calculate the risk level (ISO)

To classify the level of risk we use the methodology defined below, which estimates the level of risk as follows:

Probability of occurrence (likelihood):

- 1 – **Very low** – may occur 2 - 3 times in 5 years or less
- 2 - **Low** – once a year
- 3 - **Average** – once every 6 months
- 4 - **High** – once a month
- 5 – **Very high** – more than once a month

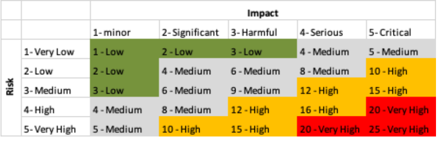
Consequence level:

- **1 - Minor -** some impact, but little or no extra effort needed to repair
- **2 - Significant -** tangible damage, extra effort required to repair
- **3 - Harmful -** significant expenditure of necessary resources and / or damage to reputation and trust
- **4 - Serious –** interruption and / or loss of connectivity and / or compromise of large amounts of data or services
- **5 - Critical -** definitive closure and / or total commitment of the company

Risk level = Probability of Occurrence **x** Consequence level

4. Risk Level > 10? (ISO)

If the risk value is greater than 10, actions must be taken to minimize or control the risks, until the likelihood of their occurrence or the consequence level is reduced. We need to give special attention to the risks with the risk level in “red zone”.



		Impact				
		1- minor	2- Significant	3- Harmful	4- Serious	5- Critical
Risk	1- Very Low	1 - Low	2 - Low	3 - Low	4 - Medium	5 - Medium
	2- Low	2 - Low	4 - Medium	6 - Medium	8 - Medium	10 - High
	3- Medium	3 - Low	6 - Medium	9 - Medium	12 - High	15 - High
	4- High	4 - Medium	8 - Medium	12 - High	16 - High	20 - Very High
	5- Very High	5 - Medium	10 - High	15 - High	20 - Very High	25 - Very High

For each risk we want to mitigate, we will identify the actions that will be implemented, these actions are defined in the Treatment Risk Plan (TRP) table, and for each risk that can be applied the number of TRP is considered necessary.

The defined actions must be monitored in their implementation and review the risk assessment when the implementation is completed.

5. Review Risk Evaluation (ISO)

Until there are no significant changes in the activities and classification of information or assets of ORGANIZATION, the risk assessment should be reviewed at **least once a year**, to validate its suitability and if there are differences, proceed to update it.

Situations that should lead to revision of the Risk Assessment:

- Change of relevant assets in the organization.
- Existence of Security Incidents
- Increase or Change in external service providers
- New digital or physical accesses
- Other situations already identified in the risk assessment

Creation Date: 30/08/2024	**Revision Date:** 30/08/2024	**Macro Process:** Integrated Management System 02 **Process**: 02 4 - Information Security Management System **Procedure**: P 02 4 20 - Risk Assessment	**Creator:** C.Santos	**Approver:** M.Sousa