3. RISKS 

Recurring question: Is the following statement more of a threat or an opportunity?

RISK 01 The most important thing is that the company's strategy was established in the past

Threat § 4.1 ★★★

Every three years on average, it's advisable to verify the strategy's adequacy with the company's context and the expectations and needs of stakeholders. It's a threat because the date when the strategy was developed isn't specified

RISK 02 The company's context is an element that can be considered (even if the boss forgot to mention it)

Threat § 4.1 ☆☆

This is a requirement of the standard and is unavoidable. It's one of the first tasks to carry out since the validation of the company's strategy depends on it

RISK 03 Trying to anticipate the evolution of customer expectations is a waste of time (if the boss says so)

Threat § 4.2 ★

Since the company's goal is to sustainably satisfy its customers, knowing the evolution of expectations is a key success factor for the future

4. MCT (multiple choice test) 

MCT 01 Which of the following statements is correct?

1. A product can be certified ISO 27001
2. A service can be certified ISO 27001
3. The management system of an organization can be certified ISO 27001
4. Any organization with more than 100 people shall be ISO 27001 certified

§ 0.1 ★

A product is certified from a technical point of view according to a reference system, such as CE 023 for a medical device, for example. Only the management system of an organization can be certified ISO 27001. Certification is voluntary for any organization, whatever the size

MCT 02 The first edition of ISO 27001 was published in:

1. 1995
2. 1996
3. 2005

Foreword ★

1995 saw the first version of BS 7799. 1996 saw the first version of ISO 13335

MCT 03 Confidentiality is the property of information to be: (even if the boss has no opinion):

1. Accessible to authorized persons only
2. Usable at the right time
3. Unaltered
4. For internal use only

§ 3.10 ☆☆

Definition of ISO 27000 version 2018. 2. Availability. 3. It's integrity. 4. It is a classification of information, see Appendix A.5

PRACTICES PRACTICES PRACTICES PRACTICES PRACTICES

5. PRACTICES 

Recurring question: Is the following statement more a good or a bad practice?

PRACTICE 01 The diagnosis of the organization context includes the main external and internal issues (even if the boss doesn't know about it)
Good practice § 4.1 ★
To understand the context of the organization, top management must prioritize internal and external issues

PRACTICE 02 To determine the issues of the context, the analysis of the competitive environment is a priority
Bad practice § 4.1 ★
Top management must first determine internal and external issues

PRACTICE 03 The analysis of the needs and expectations of stakeholders is independent of the products and services of the organization
Bad practice § 4.2 ☆☆
The organization's products and services must take into account the needs and expectations of stakeholders

CASE 01 CONTEXT

Situation: external and internal issues influence the strategic direction and the overall performance of the organization

Challenge: how can we understand the influence of external and internal issues?

Solution 1: regularly monitor and review issues

Solution 2: determine the positive or negative influence of each issue

Solution 3: use SWOT and PEST tools

§ 4.1 ★★★

All these activities are very useful for analyzing the context

CASE 02 CUSTOMERS AND NEEDS

Situation: for some months the organization has had stagnating sales. Nonconformities have begun to fill the prison

Challenge: what solution should be chosen to reverse the situation?

Solution 1: stand out from the competition with very low prices

Solution 2: recruit a marketing agent out of a top college

Solution 3: contact the customer and identify the problem

§ 4.2 ★

Setting very low prices is daring but it is not a guarantee of success and can have disastrous financial consequences

A new marketing agent can bring profits but it is time consuming and requires a significant investment

Find the causes of the intolerable amount of nonconformities and quickly set up a plan of action. Then, openly discuss it with customers, as understanding their needs and expectations is a prerequisite for the recovery of the organization

CASE 03 SCOPE OF THE ISMS

Situation: we need to maintain the scope of the ISMS in the form of documented information

Challenge: what must we do to determine the scope of the ISMS?

Solution 1: justify each non-applicable requirement in a documented information

Solution 2: maintain the scope of the ISMS (sites, processes, products and services) as documented information

Solution 3: base the scope of the ISMS on the business context, the requirements of stakeholders and the products and services provided

§ 4.3 ★

All these activities are useful for determining the scope of the ISMS