SMALL ENTERPRISE

PORTUGAL

The risk story 2

Co-funded by the
Erasmus+ Programme
of the European Union

BEPREPARED

Small enterprise from Portugal

Context of the Company and the Supply Chain

Founded in the 1980s, the company operates in the plastic injection molding industry. Its core business relies on manufacturing the most innovative and efficient fully electric add-on systems by developing several technologies that deliver more sustainable and flexible solutions to its customers.

It is an engineering company: it transforms ideas into end products. These are designed in-house in partnership with its clients. The company takes care of the research and development process, but subcontractors do all the manufacturing-related activities. Each subcontractor gets a part of the equipment, like a Lego piece, without knowing the puzzle where such a part fits in. That part, together with many others, will be incorporated into the final product.

Digitalization of SC

The company works with different IT systems available through an intranet with varying access levels, depending on the function and responsibilities of the employees. They can also remotely access them through a VPN.

Neither customers nor suppliers have access to the company's intranet. Interaction with customers occurs mainly through email, while an FTP server may also be used for file transfer – e.g., when sharing bigger files.

The company uses a COTS ERP system that integrates with the system to manage production.

Co-funded by the
Erasmus+ Programme
of the European Union

Risk Management

There is, in fact, a risk management strategy in company 2. However, cyber risk is not considered, despite an awareness as to the importance of this risk.

Practice of Risk Management

From the internal and external analysis carried out, it is possible to identify the SWOT and verify the consequence and impact on the company's business. This risk identification and assessment is carried out in a matrix. Considering the Quality and Innovation policy, objectives are defined, and actions are taken to achieve the goals, as well as the steps needed to address the risks identified in the matrix.

Risks

Operational risk

The company makes use of non-disclosure agreements to safeguard the interests of both the organization and its customers. Such agreements may be extended to integrate other entities into the process, like universities or – rarely, but possible –, when complex systems are at stake, suppliers.

Regarding customers, the only information exchanged is the product requirements, while only technical drawings are exchanged with suppliers. The company feels secure about its suppliers: first, they operate in a different business area from their suppliers; second, each supplier only produces one equipment component, so they do not have access to its entire technical design.

The company uses software to analyze risks from a mechanical and electrical standpoint in developing a product.

Financial Risk

The company has 75% financial autonomy and does not make use of bank loans for its operation.

Co-funded by the
Erasmus+ Programme
of the European Union

Market Risk

When the company develops something innovative, the company applies for a patent before going to the market.

Cyber Risk

Cyber risks are not considered. Therefore, the company cannot quantify this type of risk, although some awareness of their potential gravity is perceived.
The only risk identified at the cyber level was hacking. But, considering the company's perspective, it would not be so catastrophic since security copies are made daily, located outside the company. Moreover, it isn't easy to replicate a product patented by the company.

The company just relies on a person to manage IT systems. Regarding the company's information security policy, the following preventive measures are considered: at the contract with employees, unlawful use of company data is covered (even though nothing prevents someone from downloading important data); backups are done daily to a location outside the company; firewall and antivirus are used for threat protection.

There is, in fact, a general lack of knowledge, which also results in a devaluation of such risks. However, it is essential to point out that, despite this type of risk not being formally considered so far, the company's top management has demonstrated an openness to adopting information risk management.

Covid-19 related risks

Even though some employees had to work remotely in the company, it was felt that, regarding information security risks, no extra awareness was needed. In this sense, no additional measures were applied too.

Co-funded by the
Erasmus+ Programme
of the European Union