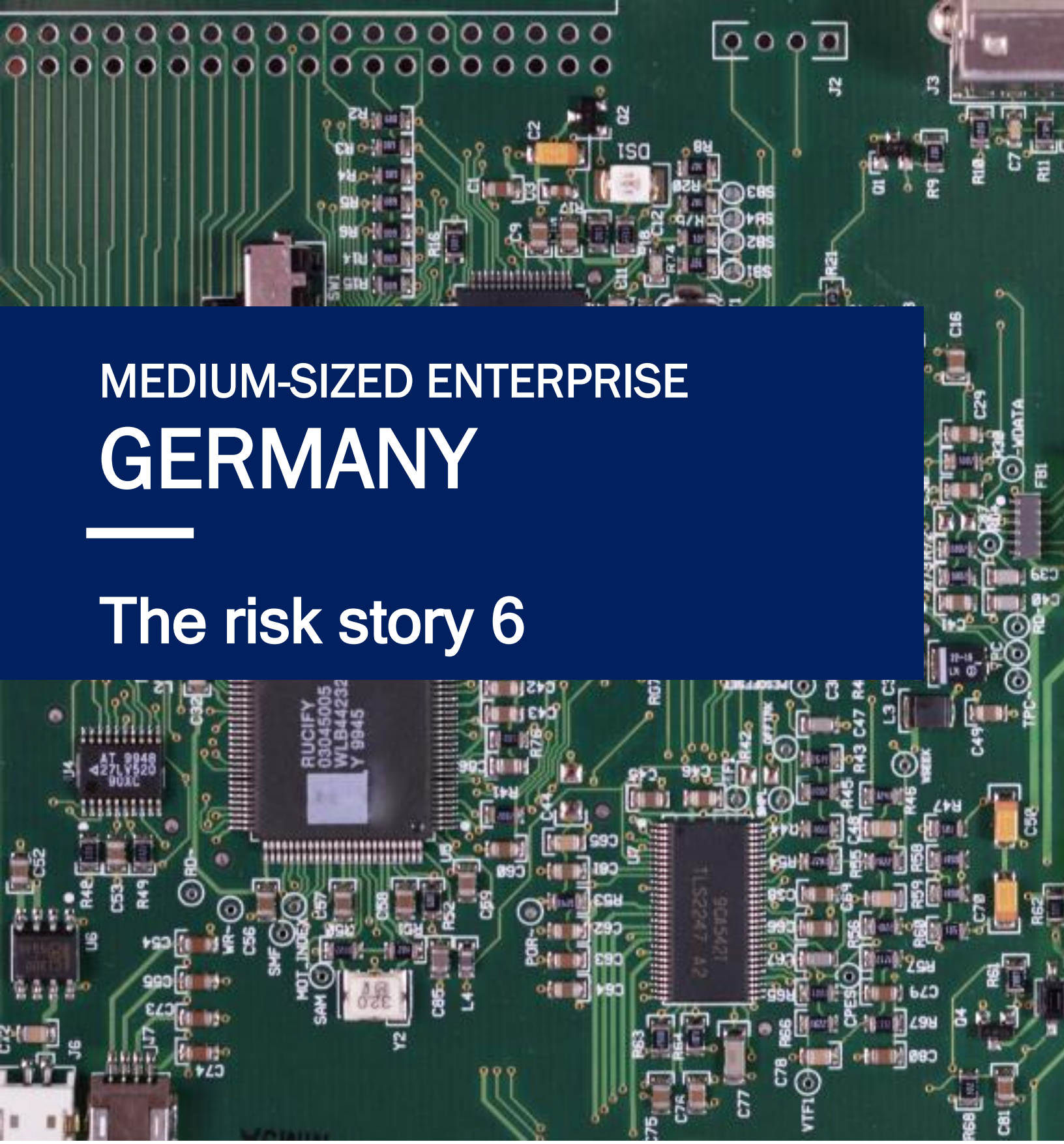

MEDIUM-SIZED ENTERPRISE

GERMANY

The risk story 6

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

BEPREPARED

Medium-sized enterprise from Germany

Context of the Company and the Supply Chain

The company has around 200 employees, sales turnover round between 10-15 million Euros per year and produces sensor technologies for special transportation and other industrial sensor demand. The company produces sensors as system components as a contract manufacturer as well as produces proprietary products using delivered components and commodity goods of suppliers. Supply chain partners are mainly located in the EU. The company has an export rate of around 40% to customers amongst others in Asia and Russia. The enterprise was founded in the era of German post-war recovery in the fifties and has today a deep and specialized production know-how and capital to run its own production facilities. The final installation of the sensors is done directly by customers or their assembly manufacturers, which mostly are market dominating purchasers.

Digitalization of SC

The SME is using a modern ERP-System for their own inhouse value chain and is piloting an additional cloud instance for sales and distribution as well as introducing a barcode application into its production flow. The company uses different other tools to direct production and capture data like CAD (Computer Aided Design), databases for knowledge management and excel sheets for risk management decisions.
Receiving and sending orders mostly happens via email, only in one case the bidding for leads of a bigger customer happens directly out of the ERP-System. The experiences with this kind of data exchange are so far neutral, but more automation might reduce time, costs and errors compared to now.
The own R&D product data is collected digitally and, due to contract reasons, often has to be exchanged with customers. As a contract manufacturer it is relevant to deliver the product as demanded, thus auditors from customers or their associations are often inspecting the production locally to prove quality & quantity. But nevertheless, the unique internal data is, wherever applicable, not shared with

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

the outside world. The company does not request production data from its suppliers so far and is not transferring any vendor data to its clients.

Risk Management

The SME has – unusual for a small company - a dedicated risk management carried-out as part time tasks by management or employees, who meet once a year to consolidate their insights and enact actions. Addressed risk management aspects are:

1. safety at work & plant protection addressing the overall production risks and change risks within
2. quality risks for products and the processes
3. financial risks covered from C-Level
4. environmental risks against pollution
5. miscellaneous risks for all other dangers resulting from data protection and cyber security risks, export risks and the like.

Practice of Risk Management*:*

Operational risk

One major risk of the company is delivering parts which are defective. Accordingly, risks in product quality are covered through dedicated quality management, test and proofs while sampling. But there are always big quality differences of components to be installed into the sensors.

Market risks

In the past, the company experienced the risk of being dependent from single customers, which could lead to higher unexpected ups and downs of sales. The market, partner and contract risks are covered over the long time from C-Level by diversification and reduction of former very high dependence on some customer. Now no customer accounts for more than 15% of sales.

Cyber risks

The firm is aware about cyber risks and has a modern and sophisticated fire wall. The major risks feared are the losses of know-how and/or personal. But even if these major risks are very present, to some extent there is no alternative to collaboration in the SCM: The owner and the management team decided to add a new cloud aspect to its ERP-System, which will as a first step be implemented in the sales area. Security is of highest importance and some digital possible data exchange is not taken because of knowledge risk exposure.

Overall, the company trusts in the data security and protection capabilities of the ERP software provider and the own IT team and its established risk management, which has been proven to be effective in the past. However, the IT department and the CEO are sure that there are and have been unknown trials of attack and breaches.

The COVID-19 related risks

As the company is ranked as system relevant, it would have been possible to receive rare commodities, special help in security or selected permissions. But this so far could not hinder big total losses during lockdown. Especially in situations of the pandemic, partners drew back their logistic problems to the company: The shutdown of big customer enterprises provoked extreme stock levels of not delivered goods and not assembled components from the SMEs own suppliers. During shutdown the company itself and several other SMEs out of their communities not only “did not make money”, but also had higher costs for stocks especially in case of voluminous product dimensions, challenging some of the SMEs in the traffic sector heavily. COVID-19 showed new unforeseen risks and displayed the dependency of customers and missing flexibility in the production, paired with a small warehouse which can cause extra costs if full.

Legal Risks

The German “fair global SC law” is feared and rejected from the interviewed owner. He argues that enterprises would be accountable to mitigate, that there is no child labour, environmental pollution, “unallowed” work conditions or danger for employees and the like in their own SC. The main reason for this fear is that the knowledge is missing, how to gather and handle SC information in a feasible and cost-efficient way. Currently for the owner, it is totally unthinkable to drop partner contracts with respect to some incidents which might appear.

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

Furthermore, it is risky to be in charge of toxic commodities from suppliers, and it might get very expensive in the near future to exchange poisonous components due to legal regulations.

Knowledge Risks

Exclusiveness of innovation is fading as imitation is always possible. The company sees a high risk of products being copied by suppliers and competitors. Regarding production of sensors as components: If something is purchased from a customer, drawings and technical specifications for the components are exchanged in digital form. Even if the products or its parts are patented, certain information should not spill-over
to competitors, especially process knowledge which is difficult to patent. All possible agreements (e.g. Non-Disclosure Agreements, NDAs) are made with the respective suppliers to prevent unwanted spillovers or leakage.

Other contract risks including compliance and warranty are handled via external supervisors like their advocate and tax accountant.

Benefits of risk management: Due to a good risk management, the company could decrease the risk of knowledge exposures and an increased diversification and reduction of the dependency on certain customers reduced the market risks. Further, the introduction of a high-developed security system decreased the risks of cyber-attacks tremendously and increased the trust of partners that their shared data is safe.

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