KWARTALNIK NAUK O PRZEDSIĘBIORSTWIE

DOI: 10.33119/KNOP.2025.76.2.6 2/2025

Risk management in an organisation based on the example of a manufacturing company

Zarządzanie ryzykiem w organizacji na podstawie przedsiębiorstwa produkcyjnego

PhD Eng. Dorota Wojtyto
Czestochowa University of Technology
Faculty of Management
e-mail: dorota.wojtyto@pcz.pl
ORCID: 0000-003-2493-9808

PhD Eng. Joanna Michalik
Czestochowa University of Technology
Faculty of Management
e-mail: joanna.michalik@pcz.pl
ORCID: 0000-0002-6908-4527

PhD Eng. Szymon Berski
Czestochowa University of Technology
Faculty of Computer Science and Artificial Intelligence
e-mail: szymon.berski@pcz.pl
ORCID: 0000-0001-8367-3152

Keywords:
risk management process, risk matrix, risk identification, risk analysis, risk assessment, risk response, risk management methods

Abstract: Manufacturing companies are increasingly dealing with risk management issues, which makes them more aware of their opportunities and threats in the competitive environment. Due to the diverse nature of enterprises, various risk management methods are also used. The topicality of risk management and testing of available risk management methodology became the inspiration to undertake this work. This article presents a risk management methodology that can be used in any organisation, private and public alike, based on the estimation of probability and effects.tags. Its versatility allows it to be applied to different areas of organisational management, e.g. project management, quality management, strategic management, etc. The aim of this paper was to present the various stages of risk management carried out in a selected production company. The article focuses on determining the context of the organization, risk identification, risk analysis, risk assessment and risk response, including residual risk. On the basis of the case study of a manufacturing company, the risks (along with causes and effects) that occur in the audited organization and the way of evaluating them using a methodology based on estimating two risk parameters: probability and effects, are presented. Then, a risk assessment was carried out using a risk matrix and control mechanisms for these risks were defined in the form of elimination, minimization or mitigation actions. Due to the article length restrictions, as well as time constraints resulting from the possibility of verifying the effectiveness of actions taken within the identified risks by the company, the issues outlined in this paper require continuation and further research in this area.

Słowa kluczowe:
proces zarządzania ryzykiem, matryca ryzyka, identyfikacja ryzyka, analiza ryzyka, ocena ryzyka, reakcja na ryzyko, metody zarządzania ryzykiem

Streszczenie: Przedsiębiorstwa produkcyjne coraz częściej zajmują się problematyką zarządzania ryzykiem, dzięki czemu stają się bardziej świadome swoich szans i zagrożeń w otoczeniu konkurencyjnym. Ze względu na różnorodną specyfikę przedsiębiorstw stosuje się także różnorodne metody zarządzania ryzykiem. Aktualność tematyki zarządzania ryzykiem oraz testowanie dostępnej metodyki zarządzania ryzykiem stała się inspiracją do podjęcia niniejszej pracy. W artykule przedstawiono metodykę zarządzania ryzykiem, która może być wykorzystywana w każdej organizacji, zarówno w przedsiębiorstwie, jak i jednostce publicznej. Ponadto jej uniwersalność umożliwia zastosowanie w różnych dziedzinach zarządzania organizacją, np. w zarządzaniu projektami, zarządzaniu jakością, zarządzaniu strategicznym itd. Celem artykułu było przedstawienie poszczególnych etapów zarządzania ryzykiem realizowanych w wybranym przedsiębiorstwie produkcyjnym. W opracowaniu główną uwagę poświęcono poszczególnym etapom procesu zarządzania, takim jak: ustalenie kontekstu organizacji, identyfikacja ryzyka, analiza ryzyka, ocena ryzyka oraz reakcja na ryzyko wraz z uwzględnieniem ryzyka rezydualnego. Na podstawie studium przypadku firmy produkcyjnej przedstawiono rodzaje ryzyka (wraz z przyczynami i skutkami), które występują w badanej organizacji oraz sposób ich wartościowania za pomocą dwóch parametrów ryzyka: prawdopodobieństwa i skutków. Następnie dokonano oceny ryzyka oraz zdefiniowano mechanizmy kontrolne dla tych rodzajów ryzyka w postaci działań eliminujących, minimalizujących lub łagodzących. Z uwagi na ograniczenia ilościowe i czasowe wynikające z możliwości weryfikacji skuteczności działań podejmowanych w ramach zidentyfikowanych rodzajów ryzyka przez przedsiębiorstwo, przedstawione w niniejszym artykule zagadnienia wymagają kontynuacji i dalszych badań w tym zakresie.

JEL:
L61, L26, L21, D20, G32

Introduction

Risk management is becoming an increasingly popular area of organisational functioning, mainly because it develops managers' awareness and helps strategic management. For example, it is more difficult to avoid mistakes, problems or bad decisions without knowledge of the relevant risks present in an enterprise. Awareness of strengths and weaknesses, as well as of their extent and importance for the organisation, allows good decisions to be made based on calculations, experiences or practices. Modern and expanding businesses are defined by risk management [Boothroyd, 2024]. In a systemic approach to risk management, it is a permanent part of the management system (BCM, information, supply, finance, IT, health and safety, environment, services, management

control, anti-corruption system) [Hopkin, 2018]. Risk management standards and norms undoubtedly help this. These include COSO, Ferma [2003] and ISO 31000 [2018]. They contain guidelines and principles that can be implemented in your organisation and indicate a course of action [Jastrzębska et al., 2014]. A noteworthy comparison of these standards is presented in the article [Czajkowska, 2017]. Further, obtaining a risk management certificate often makes a company more credible to its business partners, provides it with bargaining power and generates more market interest. The essence of risk management in organisations also influences the scientific development of the field and the growing interest of researchers, especially in the area of methodologies that will be effective and that will meet the needs of a given organization.

Each enterprise has its own specificities, so a risk management methodology should be tailored to the organisation in question. While it can be universal, of course, the details of the method will still be closely aligned with the organisation's risks [Kaczmarek, 2020]. It is, therefore, difficult to compare risk management in different companies. What is possible, however, is to compare different areas of an enterprise.

Risk management can be carried out holistically for the entire enterprise. It is also possible to do this for individual departments (e.g. Finance, Quality, Human Resources and IT). Then the risk management methodology will also be specifically tailored. For example, quality management may use FMEA and the RPN indicator [Hubbard, 2020; Jajuga, 2007]. In turn, health and safety management and occupational risk assessment may, for example, apply the Matrix Method, Risk Score, JSA, Five Steps, PHA or Alarp [Romanowska-Słoma, Słomka, 2014]. Information security management may use methods like CRAMM [Anzel, 2011], financial management – the Credit Risk Method, etc. [Orellano, Gourc, 2025]. It is worth noting that project management may focus not only on threats but also on opportunities [Knosala, Deptuła, 2018]. In contrast, crisis management, which accounts for the possibility of external risks, uses a methodology developed by the Government Centre for Security [Skomra, 2015; Wróblewski, 2015]. In the overall approach to risk, a company can adopt its own methodology, which will be the most relevant and represent the true picture of its situation. Unfortunately, one weakness in this respect may be a high degree of subjectivity in selecting risk criteria and parameters or risk valuation, as will be discussed later in the article.

Referring to the risk management methodology, which can apply to different areas of the organisation, it should be mentioned that there are various types of risks. Comparing them with each other using a single methodology may prove challenging and ambiguous. Examples include comparing production risks with information security risks [Liedel, 2005]. Hence, it is vital to develop appropriate criteria. There are many types of risk, and each enterprise may have a different taxonomy. Thus, risks may range from economic, legal, financial, strategic, production [Peng, Jin, 2025; Burduk, 2022], technological, organisational, environmental and information security ones to "force

majeure" [Sienkiewicz, 2006]. A more detailed breakdown is, for example, insurance risk [Jiyeon, 2023], credit risk, operational risk, legal risk, political risk, organisational risk, environmental risk, new technology risk, innovation risk, epidemiological risk, chemical risk, sociological risk, media risk, reputation risk, civilisational risk, natural risk, cultural risk, human risk, social risk, ethical risk, budget risk, market risk, organisational risk, IT risk, etc. [Szczepanik, Sobala, 2021; Monkiewicz, Gąsiorkiewicz, 2020]. On the other hand, the source of risk [Kisielnicki, 2017] can be identified according to the place of occurrence; then, we are dealing with external (macro, meso) and internal (micro) risk. Hence, this taxonomy considers risks dependent on the organisation [Dendera-Gruszka, Kulińska, 2017; Wojtyto, Michalik, 2024] in question (especially resources and the proximate environment), as well as those that are independent (e.g. market conditions, macroeconomic dependencies, the legal and political situation, the international environment, natural hazards, etc.) [Woźniak, Wereda, 2003]. What must be noted here is that if you want to eliminate any risk in your organisation, you have to abandon the task that brings that risk. This often becomes difficult or impossible from a practical standpoint, hence the need to take appropriate action.

Indeed, risk management is not a one-off activity and does not end there. Like other types of management in an organisation, it needs to be implemented continuously so that the company enjoys the expected results and is geared towards continuous development [Peng, Jin, 2025]. Crucial factors in risk management include updating the existing risks, examining the circumstances in which they arise and the changing value of these risks. When an organisation is growing aggressively, more risks may arise, requiring significant investment of its resources. These may be repetitive or fewer in number. New, previously unknown risks will no longer be of such concern if one can capitalise on the previous experience in managing them. Meanwhile, emerging projects can also generate opportunities worth exploring to see if they will add value to the organisation.

Effective risk management [Jiyeon, 2023] also involves allocating powers and responsibilities within the company's organisational structure. It should be adapted to the organisation's nature, size and scope of operations. For example, a risk management team can be established, including roles like manager, risk owner and auditor. These functions should have clearly defined tasks and the key to success is constant communication between them [Wojtyto, Michalik, 2024].

This article outlines the different stages of risk management, such as establishing the organisation's context, risk identification [Wojtyto, Michalik, 2024], risk analysis, risk assessment and risk response. In the planning stage of the risk management process, these phases can be documented in a risk management plan; a database or IT tools can also be utilised. As for communication and control, these stages occur in parallel with the others and are continuous. They provide the opportunity to adjust plans and make additions, etc., on an ongoing basis.

This paper uses a variety of research methods and techniques: literature review, comparative analysis, analysis of collected data, brainstorming and the whole methodology related to risk management. The article presents a case study of a selected manufacturing company.

Stages of the risk management process

The stages of the risk management process are defined in various ways in the literature. For the authors of this paper, the stages that best meet the needs of manufacturing companies mainly concern risk identification, risk analysis, risk assessment and risk response. However, identifying key risks should be preceded by establishing the context in which the company or organisation operates. At the same time, the starting phase may simply be to outline the organisation's main goals and objectives for which the identified risk factors are considered. This works especially well in project management, where one of the activities is precisely risk management – identifying the importance of opportunities and threats while implementing a project or innovation. Moreover, to properly position risks or, indeed, to locate them in the organisation at all, it is also useful to analyse the macro and micro environment, the organisation's immediate and distant surroundings. The data from the analysis will provide knowledge about the areas that generate risks in the company [Raczkowski, Sułkowski, 2014]. The following methods are bound to prove useful in establishing the organisation's context: SPACE, PESTEL, Macro Environment Analysis and Strategic Balance Sheet [Krwawicz, 2020].

Once the first stage is completed, the key stage of identifying risks follows. It is essential because the way we distinguish risks determines how we will deal with them at a later stage. This stage consists in identifying the main risk factors, determining the causes and consequences of the risks, identifying the entities affected and determining the type of risk. Identifying risks in excessive detail will make it difficult to establish the causes and match them with controls [Wojtyto et al., 2019]. If they are identified in an overly general way, there may be too many causes and impacts to consider. At this point, it must be noted that the identified risks must not turn into risk causes themselves, as this will create organisational disorder. It will be difficult to determine the type of risk and its owner. The problem also lies in the fact that if there are too many risks there will be problems in prioritising them, too many risks may be overlooked, and there may be a lack of funds and resources allocated to control mechanisms. Management methods and techniques such as SWOT analysis, brainstorming (the most popular), bow tie analysis, checklist, cause-effect analysis, Ishikawa Diagram and FMEA will be helpful for identification. They are extensively used in organisations to address various issues, not just those related to risk [Kumpiałowska 2015, Krwawicz 2020].

Risk analysis determines how a hazard is dangerous to the organisation. It involves estimating the hazard probability and impact parameters and, additionally, other factors. Methods that guarantee a correct analysis include the decision tree, the RPN indicator, SWIFT and the probability-effect method [Raczkowski, Sułkowski, 2014].

In turn, risk assessment is the determination of the actual level of risk and the willingness and ability of a specific entity to manage the risk. Methods and techniques such as the risk matrix, Pareto, Monte Carlo and HCCP [IEC 31010: 2019] can be used for this purpose. Risk response is about choosing how to deal with risk, whether by taking, avoiding, transferring, mitigating or compensating it, insuring against it or prioritising the application of possible and optimal options for action procedures. Notable methods in this respect include the decision tree and, for example, the Disney creative method.

Two further stages occurring in parallel with the others are effective communication with all stakeholders and, in doing so, the need to build a communication plan (views, opinions, positions of research groups), as well as monitoring, i.e. evaluating the effects of the actions taken – ex-post, and the new formation of the risk management process, including the continued use of methods and tools that have ensured success in risk management.

It should be noted here that the risk management methods mentioned and used in the work, despite their usefulness, also have drawbacks. First of all, they are characterized by high subjectivism in the selection of criteria or the assessment of a given factor. Often, this methodology is based on the personal experience of the evaluator, intuition, or simply limited access to data. This can lead to bias or the omission of significant risks. The second issue is often incomplete identification of risks, which in turn leads to incomplete implementation of the risk management process and failure to notice all potential events, often unexpected and sudden. The disadvantage of risk management methods is also limited resources, knowledge, outdated data, or the changing dynamics of the environment in which the company operates. Other limitations include the problem with statistical data, which often do not reflect reality, as well as the problem with the measurability of immeasurable risks. Limitations in the use of risk management methods also mean costs and time-consuming.

The risk management process in the company under study – a case study

The company under study operates in the automotive industry. It serves the Polish and foreign markets by manufacturing components for the automotive industry. Its total staff number is about 200. The company has an ISO 9001 system in place,

but due to its continuous growth and desire to compete in the sector, it focuses on the issue of risk management.

Establishing the organisation's context

In the manufacturing company under study, the first step to start the risk management process was establishing the organisation's internal and external context, which can be found in Table 1. The context areas cited are derived from the ISO 31000 standard.

Table 1. The organisation's context for the manufacturing company under study

Internal context	
Mission, vision and values	▪ Providing products that meet the highest quality standards ▪ Continuous development and striving for self-improvement ▪ Strengthening market position and winning new customers ▪ Decision-making based on the opinion of qualified staff ▪ Enabling the development of all employees
Management, organisational structure, roles and responsibilities	▪ Clear organisational structure ▪ Clear responsibilities and accountabilities
Strategies, objectives, policies	▪ Financial stability ▪ Delivery of compliant products – zero complaints ▪ On-time delivery – zero delays ▪ Striving for preferred vendor status ▪ Qualified and permanent staff ▪ Introduction of environmentally friendly solutions
Organisation's culture	▪ Clearly defined tasks and work order ▪ Regular briefings on the state of the company ▪ Daily meetings with the team setting the work plan for the day ▪ Team-building meetings and company trips
Standards, guidelines and models adopted by the organisation	▪ ISO 9001 ▪ Documented procedures, instructions ▪ Know-how ▪ Trade Secrets
Capabilities, resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies)	▪ Modern automotive-specific machinery and equipment ▪ Qualified staff of designers and operators ▪ Continuously improving production processes ▪ Financial stability – investment opportunities ▪ Opportunities to take advantage of EU programmes
Data, information systems and information flow	▪ Records of customers and suppliers ▪ Inventory of materials and products – tracking their flow ▪ Structure of employee responsibilities
Relations with internal stakeholders, taking into account their insights and values	▪ Internal training regulations ▪ Meetings with employees ▪ Internal communication with employees (internal management, system documentation, training, regular meetings with staff)

cont. Table 1

Internal context	
Contractual relations and obligations	▪ Contracts with employees ▪ Contracts with suppliers ▪ Contracts with subcontractors ▪ Contracts with employers ▪ Tendering
External context	
Social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, be they international, national, regional or local	▪ Employee qualifications ▪ Labour and energy costs ▪ Subcontracting costs ▪ Material price fluctuations ▪ Material availability
Key factors and trends affecting the organisation's objectives	▪ Staff qualifications and experience ▪ Technological stability ▪ Short lead times ▪ Stable market position ▪ Good customer relations
External stakeholder relationships, perceptions, values, needs and expectations	▪ Delivering quality-compliant products ▪ Delivering products on time
Contractual relations and obligations	▪ Automotive industry

Source: Author's own elaboration.

As shown in Table 1, the risks identified concerned areas of the company's operations related to market stability, quality assurance, continuous improvement, having a qualified workforce, strengthening the competitive position, stability and availability of goods on the supply market and accepted standards. This is where the company looked for the most relevant risks that could significantly affect an organisation and how the way it is shaped.

Risk identification

In the second stage of the risk management process, 30 different risks from several areas of the company's operations were identified using a brainstorming technique, the available company documentation, interviews and information held. The data are shown in Table 2.

As shown in Table 2, a total of 30 risks were identified in the surveyed company, most of which belonged to the human factor-related and market risk categories. As such, these risks are external in nature.

Table 2. Identification of risks for the manufacturing company under study

Risk type	Risk symbol	Risk name	Causes	Impacts
Strategic	R1	Loss of business partners	High competition on the market, quality and logistical problems	Lack of liquidity, loss of good reputation and significant market share
Market	R2	Increased competition from large players	Significant competitive position on the market, diversification of services by competitors	Reduction in demand, loss of some customers and market share
Economic	R3	Exchange rate fluctuations	Macroeconomic changes on the world market, changes in economic policy	Increased prices of services offered, lower demand, reduced profit
Financial	R4	Lack of financial liquidity	Deferred customer payment deadlines together with day-to-day costs incurred for the supply of raw materials and supplies, disruptions to deliveries	Production interruption, loss of some customers, loss of company image, lack of business continuity
Economic	R5	Increased costs	Inflation, increased cost of labour, energy, transport, raw materials and consumables	Increased prices of services offered, lower demand, loss of some customers, reduced profit
Market	R6	Problems at key customers	Internal problems, external circumstances and events	No orders/reduced orders, loss of customers
Related to working conditions	R7	Technical failures, structural collapses	Failure to comply with health and safety regulations, fire	Immediate threats to human life and health, impediments to transport and communication, disruption of the gas, electricity and district heating systems, destruction of company property, material and financial losses, halting/ loss of production
Production	R8	Failure of machinery and equipment, incorrect tooling	Lack of maintenance and inspection, improper operation	Light injury, destruction of or serious damage to equipment, loss of production, reduced product quality, production delays
Resource-related	R9	Theft/loss of physical and financial assets	Crime, burglary, fraud	Financial and material loss, production interruption
Resource-related	R10	Destruction of resources	Crime, burglary, force majeure	Financial loss, production interruption,
Production	R11	Energy supply fluctuations	Power failure	Production interruption, missed or delayed deliveries, financial loss

cont. Table 2

Risk type	Risk symbol	Risk name	Causes	Impacts
Financial	R12	Irregularities in the use of EU funds	Mismanagement of EU funds	Loss of EU funds, costs of unfulfilled contracts
Market	R13	Difficulties in attracting new customers and retaining existing ones	Strong competition	No new business partners, loss of profits and market share
Related to working conditions	R14	Working environment – high temperature	Atmospheric factors – hot summer, insufficient cooling systems	Overheating of machinery, production stoppages, delays, missed deliveries
Human factor-related	R15	Unmotivated staff	No adequate incentive scheme	Poor workmanship quality, unsatisfactory production results,
Human factor-related	R16	Employee mistakes	Haste, disregard for procedures and non-compliance with existing rules	Reduced quality, delayed service delivery, production interruptions, additional costs, financial and material losses
Human factor-related	R17	Insufficient staff competencies	Lack of assessment of employees' competencies, ineffective education and training system, admission of inexperienced staff, labour market problems	High employee turnover, poor workmanship quality, production delays
Human factor-related	R18	Changes in key personnel	External factors, no possibility of continued cooperation	Production delays
Organisational	R19	Inefficient information flow system	Organisational errors	Excessive errors, delayed service delivery, production interruptions, decline in production quality
Human factor-related	R20	Lack of employee commitment	Inadequate employee incentive scheme, team conflicts, low remuneration	Excessive errors, poor workmanship and production quality, delayed service delivery, production interruptions, additional costs, termination of employment contracts
Related to working conditions	R21	Workplace accidents	Failure to comply with health and safety rules, failure to use personal protective equipment, presence of hazardous and harmful factors in the working environment	Employee absences, additional costs, loss of image

Risk type	Risk symbol	Risk name	Causes	Impacts
Human factor-related	R22	Employee resistance, unwillingness to change	Habits, fear of change	Difficulties in introducing new solutions in processes or implementing innovative projects
Strategic	R23	Lack of resources in the market	Changes in the raw materials market, supply problems, international disturbances, international policy changes	Production interruption, inability to make deliveries, loss of some customers, loss of image, loss of profits
Market	R24	Disruption of material deliveries	Non-performance of contracts by suppliers	Production shortages, destruction of materials, financial loss, loss of company image, production interruption, delayed service delivery, loss of sales liquidity
Market	R25	Inability/ difficulties in enforcing liability for the unreliability of suppliers and customers	Lack of leverage over third parties, inability to dispense with monopolistic suppliers, high bargaining power of suppliers	Delivery delays, production interruptions, additional costs, unavailability of production materials, production interruption
Market	R26	Untimely deliveries	Lack of materials on the market, logistical problems	Production interruptions, service delays
Production	R27	Poor quality of raw materials and other materials	Internal problems of suppliers	Production and quality problems, increased production costs, loss of customers
Production	R28	Inability to manufacture a specific product	Non-performance of contracts by suppliers, lack of materials	Production delays, additional investment required for production start-up
IT	R29	Failure of the product's IT system	System component instability, system technical errors, natural disasters, purposeful or accidental human action, security breach, incorrect system configuration, inappropriate user actions	Production interruption, delayed service delivery, business continuity disruption, possible loss of access to data or data confidentiality
IT	R30	Data breach	Cyber attack, human error, insufficient IT systems security	Financial damage, loss of customer trust and company reputation, data loss or disclosure

Source: Author's own elaboration.

Only two of the risks identified are strategic: loss of business partners and lack of resources in the market. These two risks, if at a high level, can make it extremely difficult for the company under study to stay in business. They are, therefore, a priority in the preparation of controls. It is important to note here that there is some difficulty in determining what type of risks are involved. Indeed, risks may be both strategic and market-related at the same time. They can be related to the human factor as well as having an impact on the company's resources (and, after all, employees are company resources). As such, each organisation needs to adopt its own taxonomy of risks. It can be more detailed, (if advisable) or more aggregated, but there must not be too much stratification and, subsequently, confusion.

The most common causes identified in this study are problems related to the supply market and changing economic conditions, as well as technical and human errors in various contexts. The most prevalent consequences of the risks involved are loss of customers and profit, reduced market share and material and financial losses.

By knowing the causes and effects, it is easier to act when determining preventive measures to eliminate the causes or minimise the impacts, as well as to identify those responsible for these risks (risk owners), the resources allocated to the measures and the timing of the measures.

Risk analysis

The next stage of the risk management process in project management is risk analysis (Table 5), which is based on the determination of two risk parameters: probability and impacts [Skomra, 2015]. Risk value is calculated as the product of probability (P) and impacts (I). Nonetheless, good practice indicates that these two quantities do not always need to be used to define risk. Probability should be defined based on statistical or historical data, though this can be difficult in a first-time risk analysis for a company. Hence, probability is often a quantity that risk owners consider intuitively and subjectively based on their knowledge and experience. Instead of probability, one may alternatively specify e.g. relevance to the organisation, resource, project etc. If the scale of risk parameters is the same, the impacts can be broken into material, financial, resource-related, reputational, human, environmental, organisational, business continuity-related, etc. The risk analysis methodology used in Table 5 is based on the criteria in Tables 3 and 4, which define a five-level scale of probability and impacts adapted to the company under study in a generic way (impacts affecting business continuity). A similar risk analysis can optionally be carried out for the opportunities present in the organisation, matching them with actions to capitalise on these opportunities (risk response for opportunities).

Table 3. Probability scale in risk analysis

Probability	Scale	Interpretation
Very high	5	Almost certain: above 75%
High	4	Very likely; 50–75%
Moderate	3	Likely; 25–50%; risk occurrence is realistic but the probability does not exceed 50%.
Low	2	Possible; 10–25%; risk may occur occasionally.
Very low	1	Almost impossible; 0–10%; the risk is unlikely to occur or the possibility of its occurrence is negligible (near zero).

Source: Author's own elaboration.

Table 4. Scale of impacts affecting process execution/business continuity

		Effects on process execution/business continuity
5	Very significant	Failure to execute key processes, failure to meet strategic objectives.
4	Significant	Major delays; inability to implement several processes, resulting in disruption to the continuity of the organisation. Delays in achievement of strategic objectives, resulting in failure to achieve targeted results.
3	Moderate	Major delays in completing an objective/activity; process disruptions, including short-term downtime not affecting business continuity. Delay in achievement of strategic objectives, minor deviations from expected results.
2	Minor	Process/activity disruption slightly impacting the outcome; minor disruption to operations, including task execution. Minor disruptions to strategic activities not affecting their outcomes.
1	Insignificant	No impact or minor disruption not impacting the timeliness/outcome of the process; short-term disruption to operations, including task execution. No impact on the achievement of strategic objectives.

Source: Author's own elaboration.

Table 5. Risk analysis for the manufacturing company under study

Risk symbol	Risk name	Probability – P	Impacts – I	Risk value – R
R1	Loss of business partners	2	5	10
R2	Increased competition from large players	3	5	15
R3	Exchange rate fluctuations	3	3	9
R4	Lack of financial liquidity	3	4	12
R5	Increased costs	5	4	20
R6	Economic problems at key customers	1	3	3
R7	Technical failures, structural collapses	2	4	8
R8	Failure of machinery and equipment	2	4	8
R9	Theft/loss of physical and financial assets	1	3	3
R10	Destruction of resources	1	3	3

cont. Table 5

Risk symbol	Risk name	Probability – P	Impacts – I	Risk value – R
R11	Energy supply fluctuations	3	5	15
R12	Irregularities in the use of EU funds	3	4	12
R13	Difficulties in attracting new customers and retaining existing ones	2	4	8
R14	Environment – machines overheating due to high temperatures	1	3	3
R15	Lack of motivation	2	3	6
R16	Employee mistakes	2	3	6
R17	Insufficient competencies	2	3	6
R18	Changes in key personnel	3	3	9
R19	Inefficient information flow system	2	3	6
R20	Lack of employee commitment	2	3	6
R21	Workplace accidents	1	4	4
R22	Employee resistance, unwillingness to change	2	3	6
R23	Lack of resources in the market	2	5	10
R24	Disruption of material deliveries	3	5	15
R25	Inability/difficulties in enforcing liability for the unreliability of suppliers	2	3	6
R26	Untimely deliveries	3	4	12
R27	Poor quality of raw materials and other materials	3	5	15
R28	Inability to manufacture a specific product	3	3	9
R29	IT system failure	1	4	4
R30	Data breach	1	4	4

Source: Author's own elaboration.

Risk assessment

The risk analysis according to the proposed methodology was followed by an assessment, which indicated the level of identified risks and the further actions required in this respect. This made it possible to move to the next step – risk response. Table 3 data are presented graphically using a risk matrix (Table 6), which takes into account the two parameters used in the analysis: probability and impacts. It indicates three areas of risk: high risk (red box – unacceptable risk level; values between 15 and 25); moderate risk (yellow box – conditionally acceptable risk level; values between 5 and 12); low risk (green box – acceptable risk level; values between 1 and 4). The company under study has adopted the principle that low-level risks should remain unaddressed, without any

changes or additional measures (continuing as usual – the current measures are effective), medium-level risks should be continuously monitored and high-level risks should, as a first step, be reduced to at least a moderate or low level.

Table 6. Risk matrix for the manufacturing company under study

	Details		PROBABILITY				
			Very low	Low	Moderate	High	Very high
			1	2	3	4	5
IMPACTS	Very high	5		R1, R23	R2, R11, R24, R27		
	Significant	4	R21, R29, R30	R7, R8, R13	R4, R12, R26		R5
	Moderate	3	R6, R9, R10, R14	R15, R16, R17, R19, R20, R22, R25	R3, R18, R28		
	Minor	2					
	Insignificant	1					

Source: Author's own elaboration based on: [Wróblewski, 2015; Skomra, 2015].

As shown in Table 6 (risk matrix), the highest level of risk (20) relates to an increase in the company's costs and the lowest (3) concerns the working environment, theft and destruction of assets and customer economic challenges. It follows that the greatest risks originate from the company's economic area, with the smallest ones being related to working conditions, resources and the market. The risks with the highest probability of occurrence (value 5) are an increase in the company's costs and the seven risks with the lowest probability (value 1) are as follows: workplace accident, IT system failure, data breach, economic problems at key customers, hot working environment and theft and destruction of assets. The biggest impacts relate to such risks as (value 5): loss of business partners, strong competition within the sector, energy supply fluctuations, disruptions in the supply of raw materials and other materials, lack of resources in the market, low quality of materials and raw materials supplied. On the other hand, the least significant impacts (value 3) are generated by the following risks: theft/loss of resources, exchange rate fluctuations, economic problems at key customers, inability to produce a specific product, resistance of employees to changes in the company, destruction of assets, difficulties in enforcing liability in cooperation with suppliers, working environment, employee errors, insufficient staff competencies, lack of employee motivation, inefficient information flow system, lack of employee commitment, changes of key employees. The most risks are at the medium level (as many as 19) and the least at the high level (5). A positive aspect of this analysis is that the risks accepted by the company outnumber the unacceptable ones (7). This means that the overall risk for the company

under study oscillates at a medium level. Since this was the first time the company had carried out risk identification, analysis and assessment in such a meticulous and comprehensive manner, it decided to match each risk with appropriate controls as part of its preventive and control measures, as described in the next subsection. In the longer term, once the company has gained experience in risk management, it may take on risks instead of mitigating them, effectively becoming eager to face them. It may also avoid risks, deciding that while they do occur, the company will not be dealing with them because they are not that relevant at the time or there are no resources allocated for that purpose. How an organisation responds to risks is an individual decision of the risk owners. Moreover, with further experience in managing risks, one can expand their activities to include opportunities and analyse and evaluate them accordingly. It is then possible to verify the extent of threats and the level of opportunities in a given company and determine any relevant follow-up actions.

Risk response

The final step in the risk management process presented in this paper was risk response, i.e. a set of actions to minimise or reduce risks. Depending on the level of risk, these actions may have been monitored or recently implemented. The article also describes the controls for low-level risks to demonstrate what has been done to address their occurrence. The measures included in Table 7 are relatively generic. In real organisational practice, each activity is assigned a specific set of tasks to be carried out, along with the necessary work tools.

Table 7. Control mechanisms for the identified risks in the studied company

R1	Loss of business partners	Preventing loss of assets and lack of liquidity and having plans to restore both as soon as possible, diversification of production, alternative sources of supply.
R2	Increased competition from large players	A well-thought-out strategy to improve the organisation's security and stability and to reach out for feedback from external advisors, ensuring the best payment terms and service delivery times.
R3	Exchange rate fluctuations	Considering the possibility of dividing revenue streams or currency payments into small portions, paid at different times, considering the possibility of selling or buying currency in forward transactions.
R4	Lack of financial liquidity	Renegotiating payment terms with creditors. Monitoring payments – analysing the debtor register.
R5	Increased costs	Selecting optimal process parameters, choosing optimal materials, seeking savings in specific areas of the company.
R6	Problems at key customers	Crediting of orders, deferred payments, discounts and price reductions.

R7	Technical failures, structural collapses	Insurance.
R8	Failure of machinery and equipment, incorrect tooling	Inspections, maintenance, using machinery and equipment in line with the instructions, remote troubleshooting.
R9	Theft/loss of physical and financial assets	Technical safeguards, insurance, security service.
R10	Destruction of resources	Insurance, burglary protection, safeguarding of materials.
R11	Energy supply fluctuations	Developing a power outage action plan, considering the installation of an OFF-GRID system.
R12	Irregularities in the use of EU funds	Allocating responsibilities, training and awareness raising, internal control system, fraud risk analysis, culture of ethical conduct.
R13	Difficulties in attracting new customers and retaining existing ones	Building customer relationships, responding quickly to customer needs, appropriate selection of target customer group, taking a personal approach to customers, professional communication.
R14	Working environment – high temperature	Introducing appropriate safety systems, as well as individual and collective protection measures.
R15	Unmotivated staff	Employee interviews, team-building events, establishing an appropriate remuneration system.
R16	Employee mistakes	Training, professional development courses.
R17	Insufficient staff competencies	Proper recruitment and selection of employees, induction training, working with high schools to train students as potential employees.
R18	Changes in key personnel	Proper employee recruitment and screening, induction training for new employees.
R19	Inefficient information flow system	More frequent meetings, sending information electronically to employees.
R20	Lack of employee commitment	Motivating employees, fair remuneration system, penalties and rewards.
R21	Workplace accidents	Health and safety rules, employee training, proper preparation of workstations and designation of hazardous areas, use of personal protective equipment, reduction/elimination of harmful factors, investment in new technology.
R22	Employee resistance, unwillingness to change	Providing up-to-date knowledge and information on the changes being implemented, demonstrating the benefits of the changes, building a sense of non-threat, building good interpersonal relationships, employee participation and motivation, management commitment, change planning.
R23	Lack of resources in the market	Stocking standard or most commonly used materials.
R24	Disruption of material deliveries	Back-up water source for up to 8h of water shortage: 1000 litre IBC pallet container.
R25	Inability/difficulties in enforcing liability for the unreliability of suppliers and customers	Seeking redress through amicable or judicial means.

cont. Table 7

R26	Untimely deliveries	Planning deliveries in advance, confirming delivery dates at the bidding stage, safety stock, contractual penalties for late deliveries, alternative suppliers.
R27	Poor quality of raw materials and other materials	Verifying deliveries, requiring approvals.
R28	Inability to manufacture a specific product	Planning purchases of suitable materials in advance.
R29	Failure of the product's IT system	Auditing the IT system and implementing the necessary changes, system updates (introducing any required extensions, data archiving and backup solutions, anti-virus systems, developing and implementing an information security policy).
R30	Data breach	Anti-virus software, firewalls, authentication (using strong passwords, password-protected routers), developing and implementing a security policy, Intrusion Detection Systems.

Source: Author's own elaboration.

As shown in Table 7, the priority actions address the risks of the highest level. As such, the company will be prioritising the following: choosing the optimal process parameters, optimising material selection, seeking savings in specific areas of the company, developing a power outage plan, considering the installation of an OFF-GRID system, having a well-thought-out strategy to improve the organisation's security and stability and seeking advice from external consultants, ensuring the best payment terms and service delivery times, providing a back-up water source, verifying supplies, requiring approvals. At the risk response stage, it is also vital to identify who owns the risk and who will deal with it, as well as to establish responsibility and then, after a set deadline, verify how the risk owner has performed. Apart from the personal responsibility matters, a timeframe for implementing the activities and an estimated cost should be specified and forwarded to top management for approval. In practice, management may not necessarily agree to the entire risk management plan. It may have objections due to the availability and cost of the planned controls. The role of management at this stage is paramount. The actions must be strictly tailored to the risks, in the optimal and reasonable number (and thus also to the remaining resources – finances, people, time, know-how, etc.). On the other hand, three risks are worth more attention, the value of which is the highest among the other risks: increase in costs, fluctuations in energy supply and lack of possibility or difficulties in enforcing responsibility for the reliability of suppliers and customers. As shown in Table 7, the company has adopted a strategy of dealing with these risks on the basis of their elimination or minimization by implementing control mechanisms that take into account the current spatio-temporal conditions. However, these are key risks and in a situation of high market dynamics, these actions may not be enough in the near future. Therefore, the company, using the benchmarking method, taking into account companies from the industry, has developed solutions that could

be used in a situation where the current ones turn out to be inadequate, insufficient or incomplete. It should be noted, however, that because these are potential activities, they are not fully secured with the available resources. A full timetable and an assessment of the resources for this purpose will be agreeable once the effectiveness of the current control measures has been determined (residual risk calculation). After the analysis of the available solutions, following the example of other companies, potential actions in the case of R5 risk were taken into account – cost increases: long-term contracts with suppliers, outsourcing of expensive services, implementation of lean management in relation to the entire production, helding hedges, or price indexation (price adjustments depending on the cost of raw materials). In the case of another risk of R11 – fluctuations in energy supply – the practice of various companies in the industry indicates the following solutions: energy-intensive processes carried out during off-peak hours, change in the organization of work and production, energy storage, business continuity plans, diversification of energy sources, having several emergency sources. In the case of the R25 risk, the following solutions can be used: contracts with penalty or bonus clauses (bonuses for punctuality and quality), common IT systems integrated.

After the risk response stage, i.e. the preparation of an action plan for a specific period, the principle of residual risk can be applied. It is instrumental in providing feedback to the organisation. This is because it makes it possible to determine which controls were effective and which were not and why. Residual risk is such that remains in place despite the control measures applied. The implication is that the relevant action may have lasted too short, required more funding or perhaps the person responsible for the risk was unqualified, etc. Hence, it is vital to assess the effectiveness of the control measure in question. However, no such assessment can be included in this paper at the present stage as the relevant actions have only just been taken in the company under study. Where several risks occur, action implementation times may be as long as a year. Undoubtedly, an examination of the effectiveness of the control method and measures would be a worthy addition to this article and should form a further part of it.

Conclusion

Risk management is a continuous process and should be constantly monitored in the evolving reality and operating environments of organisations. Informed organisations are paying more and more attention to risk management because this allows them to systematise processes across the company, notice emerging opportunities and threats, make proper use of their resources, correctly define staff roles and responsibilities and check whether employees can handle their tasks. The risk identification, analysis, assessment and response presented in this paper ranks the risks that occur in the

company in a general way, thus answering the questions of what we are dealing with at the moment; how to respond to risks, i.e. what resources and means we have available for risk response; which risks we overlook; which ones we deal with first; what threatens us the most and what to prepare for. The article identifies 30 risks from different areas of the company's business, mainly related to company resources and markets. But there is no denying that, for many risks, the determination of probabilities was characterised by subjectivity. It should be mentioned that risks refer not only to losses but also to opportunities that may arise when implementing certain projects or introducing innovations, among other things. Taking into account the scope of risk management available in the enterprise, the authors of the publication, in the future will continue these topics in terms of mechanisms control for identified threats.

References

Anzel M. [2011], *Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej Ustawy z dn. 5 sierpnia 2010 r. o ochronie informacji niejawnych*, PHU ONE, Poznań.

Boothroyd K. [2024], Fundamentals of risk management: Understanding, evaluating and implementing effective enterprise risk management, Kogan Page.

Burduk A. [2022], *Ryzyko systemów produkcyjnych*, Wydawnictwo Naukowe PWN, Warsaw.

Czajkowska K. [2017], *Metody identyfikacji ryzyka w zarządzaniu ryzykiem w przedsiębiorstwie*, "Journal of Modern Management Process", no. 1(2).

Dendera-Gruszka M., Kulińska E. [2017], *Budowa rejestru ryzyka z wykorzystaniem audytu logi stycznego na przykładzie wybranego przedsiębiorstwa*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie", nr 107.

FERMA [2003], *Standard zarządzania ryzykiem*.

Hopkin P. [2018], *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management,* Kogan Page.

Hubbard D. [2020], *The failure of risk management: Why it's broken and how to fix it*, Wiley.

IEC 31010:2019 Risk management – Risk assessment techniques [2019].

ISO 31000:2018 *Risk management – Guidelines,* Polski Komitet Normalizacyjny, Warsaw.

Jajuga K. [2007], *Zarządzanie ryzykiem*, Wydawnictwo Naukowe PWN, Warsaw.

Jastrzębska M., Janowicz-Lomott M., Łyskawa K. [2014], *Zarządzanie ryzykiem w działalności jednostek samorządu terytorialnego ze szczególnym uwzględnieniem ryzyka katastroficznego*, Wolters Kluwer SA, Warsaw.

Jiyeon Y. [2023], *Effect of enterprise risk management on corporate risk management*, "Finance Research Letters", vol. 55, part B.

Kaczmarek T. [2020], *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warsaw.

Kisielnicki J. [2017], *Zarządzanie projektami*, Wydawnictwo Nieoczywiste, Warsaw.

Knosala R., Deptuła A. [2018], *Ocena ryzyka wdrażania innowacji*, PWE, Warsaw.

Krwawicz M. [2020], *Podstawy organizacji i zarządzania*, Oficyna Wydawnicza Politechniki Warszawskiej, Warsaw.

Kumpiałowska A. [2015], *Praktyczne narzędzia zarządzania ryzykiem w jednostkach sektora publicznego*, C.H. Beck, Warsaw.

Liedel K. [2005], *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo A. Marszałek.

Monkiewicz J., Gąsiorkiewicz L. (eds.) [2020], *Zarządzanie ryzykiem działalności organizacji*, C.H. Beck, Warsaw.

Orellano M., Gourc D. [2025], *What typology of risks and methods for risk management in innovation projects?: A systematic literature review*, „International Journal of Innovation Studies", vol. 9(1).

Peng Y., Jin H. [2025], *Effects of information and technology application in audits and digital economy on enterprise risk management level*, Finance Research Letters.

Raczkowski K., Sułkowski Ł. [2014], *Zarządzanie bezpieczeństwem – metody i techniki*, Difin, Warsaw.

Romanowska-Słoma I., Słomka A. [2014], *Ocena ryzyka zawodowego*, Tarbonus, Kraków–Tranobrzeg.

Skomra W. (ed.) [2015], *Metodyka oceny ryzyka na potrzeby zarządzania kryzysowego*, Wydawnictwo BEL Studio, Warsaw.

Sienkiewicz P. [2006], *Zarządzanie ryzykiem w sytuacjach kryzysowych*, Wydawnictwo AON, Warsaw.

Szczepanik T., Sobala N. [2021], *Zarządzanie ryzykiem w systemach logistycznych*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.

Wojtyto D., Michalik J. [2024], *Metodyka analizy i oceny ryzyka w zarządzaniu projektami*, In: Pachura P., Ociepa-Kubicka A. (eds.), *Zarządzanie projektami w dobie cyfrowej globalizacji*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.

Wojtyto D., Michalik J., Kobuszewska S. [2019], *Risk map for a selected organization*, In: Frączek T. (ed.), *New trends in productio enineering*, Wydawnictwo Sciendo, Warsaw.

Woźniak J., Wereda W. [2023], *Mapa ryzyka w zarządzaniu organizacją*, CeDeWu, Warsaw.

Wróblewski D. [2015], *Zarządzanie ryzykiem – przegląd wybranych metodyk*, CNBOP-PIB, Józefów.