The Risk Management Process in Retail Organization

- The risk management process

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

Radka Bauerová
International Trade Operations
21 March 2023

Content of the presentation

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

1. The role of risk management
2. The risk management process
3. Explanation of the different stages of risk management
4. Explanation of the risk matrix process

Risk Management

Risk management is a **complex systematic process of identifying, eliminating or minimizing uncertain events that may affect an entity and controlling them**. The main objective of risk management is to include the manifestations of risk arising from process ambiguities in human decision making. Risk management also includes anticipating the consequences of these risks and organizing activities so that human, financial and material consequences are as low as possible for the entity. The risk management process is a decision-making process, the critical phase of which is the choice of an optimal solution. It is therefore recommended that, for certain events that may have a significant impact on the business or recur, it is advisable to **consider possible crisis scenarios** and to **determine** their **implementation** using **appropriate methods** to change the external environment or internal development within the organization. (Mulačová et al., 2013)

Risk assessment is a critical component in entrepreneurship by means of **exploiting opportunities**, risk must be assessed as a part of the process. (Miles, 2011)

Importantly, scenarios for situations of a certain type include a relatively detailed plan on **how to proceed in that situation,** because risk management aims **to identify risks and eliminate** them **at an early stage** so that we can prevent unwanted events. Risk management is an important part of strategic management in any organization. (Mulačová et al., 2013)

THE ROLE OF RISK MANAGEMET

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

Risk management is **a discipline for dealing with the organizations´ s risks** (Sadgrove, 2015). Risk management can **enhancing business performance**. The role of risk management in trade operation is following (Reuvid, 2014; Sadgrove, 2015):

- With national economies struggling, stabilizing, and some recovering, risk management has a role to play in **ensuring the health of organizations**; ensuring that whether they be private or public sector, charitable or profit-making, large or small, new or old, they achieve what they have set out to do.
- Risk management must **provide the advice, tools, products and services** that assist an organization with its planning and reporting, feeding into and influencing decisions surrounding resources, priorities and, increasingly, helping to manage expectations.
- Risk management **provides arrangements** through business continuity management **to minimize damage**, **deal with crises** and **recover back to normality**, perhaps even reach a better place.
- Risk management helps a company **avoid cost and disruption.**

The reasons of growing importance of risk management lie, among others, in getting tougher of **legislation** (legislation is more extensive, stringent and the EU now requires companies to carry out risk assessment in health and safety, product liability and finance) and **more expensive insurance** (expensive insurance, audit of insurance company, insurance my not recoup the full amount lost) Sadgrove, 2015.

Five Common Challenges in Risk Management

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS

Risk management has to face five challenges (Reuvid, 2014):

1. **Some key drivers of success are not easily measured**
   - Behaviour or attitudes of people, human aspects such as measure on flexibility, innovation, how knowledge and intellectual property is actually used.
2. **Behaviour is not always in line with strategic objectives**
   - Irrelevant measures go unchallenged, and even if the performance is excellent, if it´s not the required performance then less than optimum outcomes arise, along with resentment and resistance. Through risk based assurance mapping an organization can ensure that the right things are being done, in the right way, by the right people.
3. **Conflict of the performance management system with the culture of the organization**
   - The type of organization is an important consideration when designing and implementing a method of managing performance. Reward and recognition must be aligned for performance management to have motivational impact as well as provide management information for decision making.
4. **The development of measures can be time-consuming or difficult**
   - Creating many measures can take a great deal of time and management attention, the effort itself often being questioned for its efficacy. Effective risk management looks at the interconnectivity of risks and considers the characteristics of possible causes, and the variety of possible consequences of events.
5. **Continual change makes effective planning essential**
   - This requires review and refinement.

The Benefits of Managing Risk

SILESIAN

Risk management can help to company avoid cost, disruption and unhappiness. It can be adapted to meet the needs of each business. It can be used to educate staff, and to give them a deeper understanding of the business risks. This turns managers into business people, and makes the **business more effective**. **Advantages of managing risk** proactively are specified as follows (Sadgrove, 2015):

1. **Marketing risks** – maintain market share
2. **Health and safety risks** – avoid worker litigation; reduce insurance premiums
3. **Environmental risks** – avoid litigation from regulatory authorities; reduced premiums
4. **Fire risks –** avoid loss of goods, avoid going out of business; reduced premiums
5. **Bomb threats –** avoid loss of life or destruction of a building
6. **Computer risks –** prevent inability to invoice, prevent lack of access to information
7. **Theft and fraud –** prevent loss of money, assets or market share
8. **Technical risks –** avoid being left behind with obsolete business operations or technologies
9. **Kidnap and ransom, extortion –** safeguard managers abroad or at home, prevent payment to criminals
10. **Product contamination –** avoid harming customers and prevent litigation

EXPLANATION OF THE RISK MATRIX PROCESS

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

In assessing the likelihood of risk occurrence and its impact on business activities, statistical methods can be used, but in practice most decisions are based on the judgment of the company's experts or employees. A very often used analytical technique for risk assessment is the so-called **risk matrix** designed by Klaus Winterling. It is sometimes referred to as a risk map or an aggregate risk matrix. The matrix allows identification of risks according to two parameters (Mulačová et al., 2013):

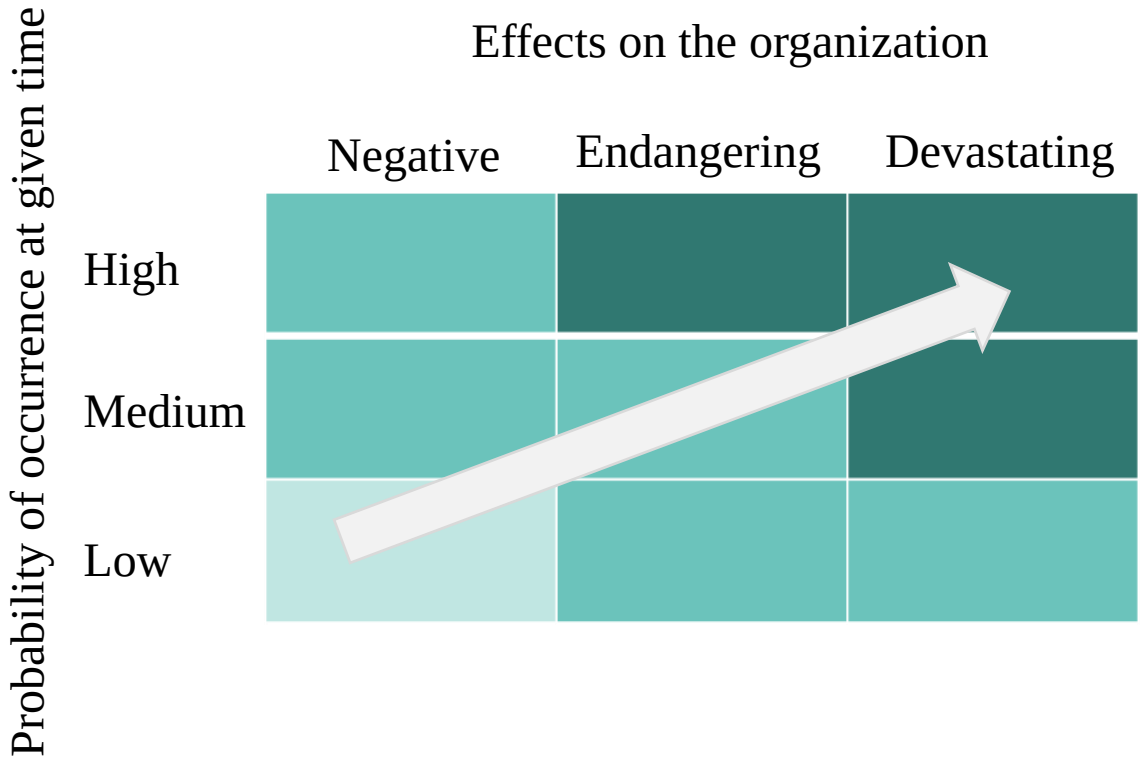
1. **The probability of risk occurring at time** - categorizing how real and probable the risk actually occurs - the matrix defines three levels of probability - low, medium and high (low probability, probability, very probability)
2. **Impact of risk on the organization** - captures what the impact of risk on the organization may be if the risk occurs - the matrix defines three levels of effect - negative, threatening and devastating (low, medium and high impact). Negative effects have little impact on the organization's strategy and operational activities and are characterized by low concerns of stakeholders. The threatening effects have a moderate impact on the organization's strategy and operational activities and there is a slight concern of stakeholders. The devastating effects are characterized by a significant impact on organizations' strategy and operational activities and a high financial impact, which is of considerable concern to stakeholders.

THE RISK MATRIX

The more the risk moves up the diagonal to the right in the risk matrix, the more attention must be paid to this risk in the context of risk and crisis management (Mulačová et al., 2013). The crisis matrix is shown in the Figure 1.

An interval can be specified to determine the probability. For example, 0-20% as a low probability risk, 21-50% as a casual risk and 51-100% probable to very common risk, or a finer breakdown may be used. Likewise, instead of verbal definition, the risk impact interval can be determined as the **monetary value of the loss**. Different colour coding is used to capture individual sectors, which delimits areas according to the sum and highlights the severity of the risks. The risk estimation, expressed in terms of probability of occurrence and possible consequences and effects on the organization, may be quantitative, semi-quantitative or qualitative. It is very often processed into a spreadsheet, as shown in the following example of capturing the **consequences of threats and opportunities**. The result of the risk analysis process can be used to create a risk profile, which allows to classify and organize all identified risks according to their relative importance in a matrix, where we subsequently design and capture measures (risk management plan) and choose appropriate methods or a combination of methods to control them.

Figure 1: The risk matrix



Source: Mulačová et al., 2013

Presenting The Risk Level 4x4 Risk Matrix

It is difficult to quickly grasp the multidimensional nature of risk and the varied threats it might pose to a commercial operation for those outside of the risk field. It is incumbent on assessors to seek to work closely with their business counterparts to demonstrate how risk might affect their success while offering solutions, rather than obstacles, in order to facilitate business. (Blyth, 2008)

The following basic table can be used by managers to represent the risk level (Figure 2). In the following figure the risks is assessing in global nature factors. Companies must assess those factors that may affect it, whether from an external or internal environment, in their assessments.

Figure 2: Representing Risk

		IMPACT			
		Low	Medium	High	Extreme
PROBABILITY	Low	J	I, L	K	
	Medium		G	H	
	High		F	B, C, D, E	
	Extreme				A

Source: adapted of Blyth, 2008 and The Global Risks Landscape 2019

A) Extreme weather events
B) Cyber-attacks
C) Natural disasters
D) Water crises
E) Large-scale involuntary migration
F) Data fraud of theft
G) Failure of national governance
H) Critical information infrastructure breakdown
I) Energy price shock
J) Deflation
K) Failure of financial mechanism or institution
L) State collapse or crisis

INTERNATIONAL TRADE ORGANIZATIONS
-the task

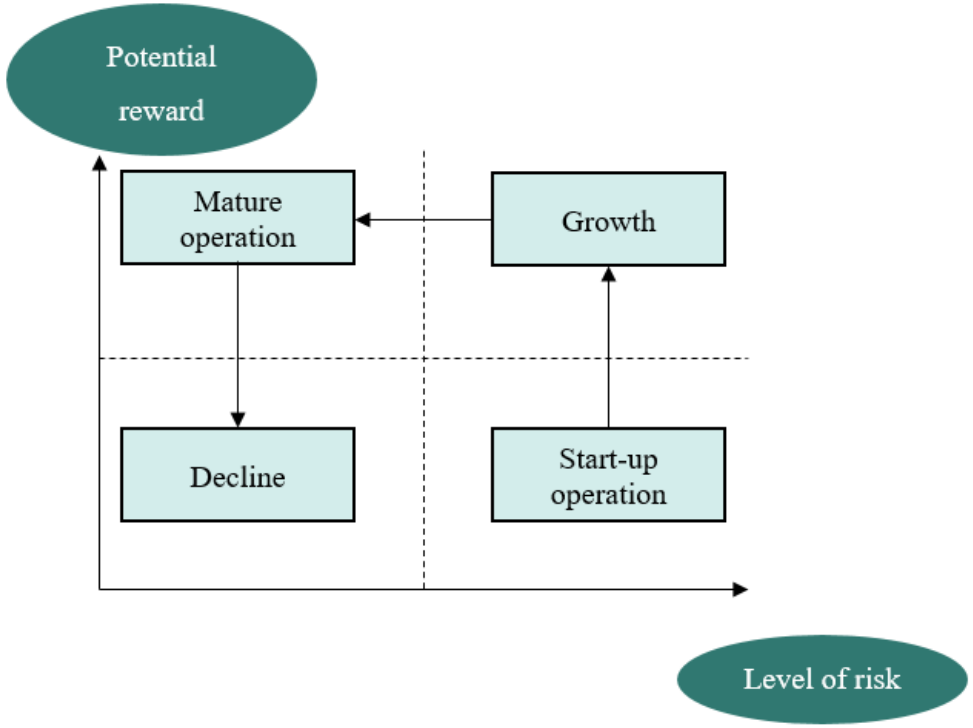
SILESIAN

Risk and Reward

Another feature of risk and risk management is that many risks are taken by organizations in order to achieve a reward. Figure 3 illustrates the **relationship between the level of risk and the anticipated size of reward**. Company will launch a new product because it believes that greater profit is available from the successful marketing of that product. In launching a new product, the organization will put resources at risk because it has decided that a certain amount of risk taking is appropriate. (Hopkin, 2017)

The value at risk represents the risk appetite of the organization with respect to the activity that it is undertaking. When an organization puts value at risk in this way, it should do so with the full knowledge of the risk exposure and it should be satisfied that the risk exposure is within the appetite of the organization. Even more important, it should ensure that it has sufficient resources to cover the risk exposure. Not all business activities will offer the same return for the same level of risk taken. Start-up operations are usually high risk and the initial expected return may be low. Figure 3 demonstrates the **probable risk versus reward development for a new organization or a new product**. At the business develops, it is likely to move to a higher return for the same level of risk. (Hopkin, 2017)

Figure 3: Risk and reward matrix for start-up organizations or new product.



Source: adapted from Hopkin, 2017

Examples of Current Retail Risks Drivers

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

The current retail risks drivers in domestic trade can be include the following (KPMG, 2018):

Cyber Risk

- Retail is one of the most targeted industries when it comes to cyber attacks. This situation is based on the fact that retail disposes the sensitive customer data like personally identifiable information. In fact, over 50% of global retailers were breached in 2018. New and emerging cyber security threats and how they affect the entire organization can be one of risk drivers in this field.

Competition

- Lack of innovation, inability to adapt business model, following vs. leading, imbalance between establishing customer centricity and maintaining brand loyalty

Consumer expectations

- Consumers have more information about the product than the retailer, too many choices eroding brand differentiation, inadequate focus on customer service and ease of interaction, customer experiences that are not meaningful, memorable, shareable, and personalized

Compliance and regulations

- Impact of global controls over GDPR if data on European citizens is held, impact of U.S. tariffs on prices of international products, new revenue recognition and lease accounting rules

Technology disruption

- Being an IT bottleneck, rather than a catalyst for change, spending on applications that company don´t need, continuing to pay for old, out-of-date systems

Data and analytics

- Not aligning a data strategy with overall business strategy, not ensuring organizational data is reliable, spending more time vetting data and reports rather than analysing them

Examples of Current Retail Risks and Risk Drivers -International perspective

SILESIAN

The fast evolving digital technologies, increased regulatory pressure and global economic uncertainty are the key factors in the current global retail risk landscape. **Current retail risk factors** include (KPMG, 2018):

- Challenges in logistics and inventory
- E-commerce creates low-price environments which decrease profit margins for all the retailers
- Risks arising from volatility of price and supply fluctuations of raw materials
- Financial risks relating to credit risk, liquidity and refinancing risks
- Increasing pressure to invest in upcoming technologies, such as Internet of Things, Virtual reality, Driverless vehicles, Robots and Artificial intelligence, to improve efficiency and customer experience
- IT risks relating to disruption in the operation of the systems, or cyber-security breaches
- Macroeconomic uncertainty in key markets from factors such as the UK´s vote to leave the EU, economic recession in Brazil and Russia and slowdown in China resulting in low growth consumer market

Risk drivers

- Disruption caused by changes in international, social, political, legal and economic conditions
- Imposition of barriers on trade and retaliation that could have a cost/inflationary impact
- Currency fluctuations
- Local customs, language and culture
- Unexpected regulatory changes
- Political instability and terrorism
- Changes in diplomatic and trade relationships
- Cargo delays as a result of security considerations or insolvency
- Lack of suitable physical location and price of real estate
- Administration´s tariffs on Chinese goods

Ways to Manage Risk

SILESIAN

There are four ways to manage risks and company adopt one of these solutions for each risk, depending on how likely the threat is, and how severe its impact will be (based on risk level assessment – explained in previous lecture). These ways used to be known as the **4Ts as Terminate, Transfer, Treat and Tolerate.** The risk management standard ISO 31000 uses the phrase **risk treatment** to mean any of all of these four actions. These **four ways to manage risks** are specified as (Sadgrove, 2015):

1. **Avoid them (Terminate)**

-means choosing not to accept the risk. It means decide to stop offering a high-risk service, one that could lead to expensive litigation. Company might choose not to acquire another firm because the risks of its failing are too great or might sell a division that has large peaks and troughs in its profits.

2. **Share them (Transfer)**

-sharing the risk is also known as transferring or spreading risk. Techniques include Joint venture, redundancy, sub-contracting, outsourcing, dual sourcing, offsetting risk to suppliers, diversification or buying insurance.

3. **Accept them (Tolerate)**

-a low-impact, low-probability hazard is quite rare, if only because we don´t really notice them. With no shortage of serious risk to manage, company may decide that a risk is within agreed risk tolerances. This will relation to the small risks that happen rarely. Deciding to accept small risks allows company to concentrate on the major ones, and prevents the risk system from becoming a behemoth.

4. **Control them (Treat)**

-in this area we are talking about the risks that have an impact on trade operations or the probability that they will happen. The standard way of managing these risks is through controls. They can take many forms involving process, practice or policy. The overall aim is to minimize, reduce or control the risk. There are several ways to **classify controls** (specified on the next slide).

The Classification of Risk Management Controls

SILESIAN UNIVERSITY

There are several ways to classify controls. Three common classifications are (Sadgrove, 2015):

A) Preventative, directive or detective controls

1) Preventative controls stop the risk from occurring. This type of controls stop problems before they occur, so they are the best type.
2) Directive controls are usually aimed at getting people to do things. They include policies, procedures and training.
3) Detective controls give feedback, letting staff know whether a system is working properly, or alerting people if a problem has occurred.

Table 4: Examples of preventative, directive and detective controls

Type of risk	Preventative	Directive	Detective
Burglary	Locks	Require staff to close windows when leaving	Intruder alarms, CCTV
Fraud	Numbered order forms, having two people sign cheques	Train people not to give out passwords on the phone	Audit
Hard drive failure	Raid drivers, redundancy, strong password protection	Educate users to watch for data errors occurring	Software to monitor and diagnose drive wear

Sources: adapted from Sadgrove, 2015

B) Physical, management or technical controls

Examples of these controls are:

1) Physical controls: non-slip flooring
2) Management controls: a policy of using protective footwear
3) Technical controls: password-protected access control

C) Manual or automatic controls

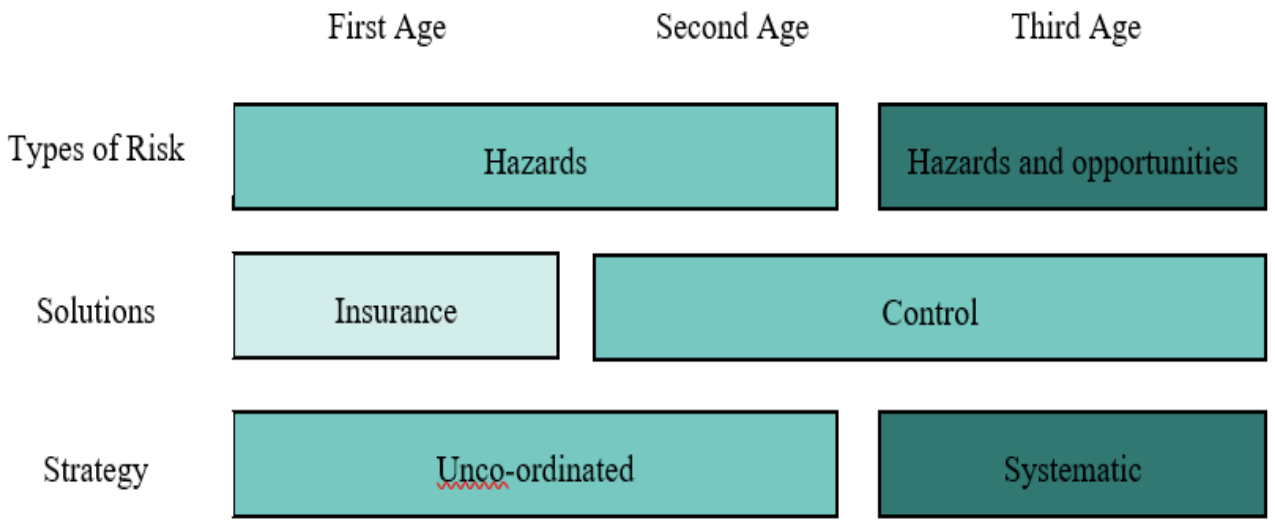
1) Manual controls: Audits required someone to do an inspection.
2) Automatic controls: Automated backups which don´t require human interaction (though getting a staff member to check that the backups are working is just as important, and reminds us that there is often more than one control for any process)

EXPLANATION OF THE DIFFERENT STAGES OF RISK MANAGEMENT

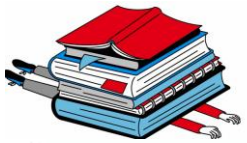
The history of risk management can be split into three ages (see Figure 5). Cargo insurance was introduced nearly 4,000 years ago and until recently insurance was still the main way to managed risk by companies. Therefore, insurance was the **first age of risk management**. In the 1970s and 1980s, business started to introduce quality assurance, to ensure that products conformed to their specifications (ISO 9000). In the **second age of risk management** companies treated risk in a more proactive or preventative way.

Risk awareness was fostered by government legislation (focused on risks to workers and customers). Later companies focused on environmental risks, shareholders risks and chief risk officer. The **third age of risk management** arrived in 1995 with the publishing by Standards Australia of the world´s first risk management standard (AS/NZS 4360). (Sadgrove, 2015)

Figure 5: The three stages of risk management



Source: adapted from Sadgrove, 2015



Risk Management Standards

SILESIAN UNIVERSITY

There are number of established risk management standards and frameworks worldwide. The overall approach of each of these standards is similar (Fraser et al., 2014).

After Australia´s risk management standard, two others in quick succession. In 2001 **Japan** launched a risk management system called **JSI Q 2001**, which introduced continuous improvement. And in 2002 the **UK´s Institute of Risk Management** introduced its own risk management standard. (Sadgrove, 2015)

The standard that had the widest recognition was the **Australian Standard AS 4360**, published in 2004 (Fraser et al., 2014). Later the International Organization for Standardization launched its **ISO 31000 in 2009**, based largely on the Australian standard (Hopkin, 2017).

The **ERM version of the COSO standard** is also widely applied in many organizations. **British Standard BS 31100:2011** Risk Management: Code of Practice and Guidance for the Implementation of BS ISO 31000 was published in 2011. Further guidance to the ISO standard was published in 2013 as **ISO/TR 31004:2013**. (Fraser et al., 2014).

The international Standard **ISO 31000** was published in the latter part of 2009 named as Risk Management: Principles and Guidelines. Although some standards are better recognized than others, organizations should select the approach that is most relevant to their particular circumstances. It is important to distinguish between a risk management standard and a risk management framework. A risk management standard sets out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework that supports that process. In simple terms, a risk management standard is the combination of a description of the risk management process, together with the recommended framework. (Fraser et al., 2014)

THE RISK MANAGEMENT PROCESS

THE RISK MANAGEMENT PROCESS

Risk management is a process of handling risk in a conscious fashion. The following framework present general risk management framework promoted by the Project Management Institute (PMI). There are a number of risk management frameworks that can be pursued beyond the PMI perspective. For example a thoughtful framework has emerged in Australia and is known as the Australia/New Zealand Standard 4360:1999. This framework developed by the Standards Association of Australia, serves as the leading guide to risk management in Australia and New Zealand. Although there are several frameworks, so all pursue the same basic message. They all are predicated on the view that effective risk management requires organizations to plan and deal with risk proactively, identifying risk events, developing strategies to deal with them, then dandling them when they arise. (Frame, 2003)

The risk management framework (continuing on the next slide) (Frame, 2003):

Step 1: **Plan for risk**. Prepare to manage risks consciously. Effective risk management does not occur by accident. It is the result of careful forethought and planning.

Step 2: **Identify risk.** Routinely scan the organization´s internal and external environment to surface risk events that might affect its operations and well-being. Through this process, you develop a good sense of the bad things you might encounter in your projects and operations.

THE RISK MANAGEMENT PROCESS

SILESIAN

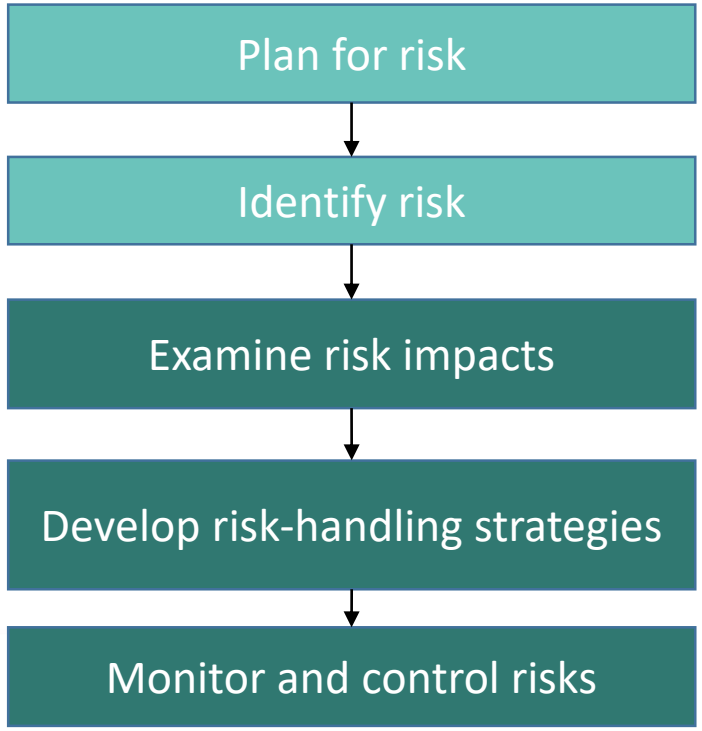
The risk management framework (Frame, 2003):

Step 3: **Examine risk impacts**, both qualitative and quantitative. After you develop a sense of the risk events you might encounter in Step 2, systematically determine the consequences associated with their occurrence. Think through hard-to-measure consequences by means of a qualitative analysis. Model measurable consequences with a quantitative analysis.

Step 4: **Develop risk-handling strategies**. Now that you know what risk events you might encounter (Step2) and the consequences associated with them (Step 3), develop strategies to deal with them.

Step 5: **Monitor and control risks.** As projects and operations are underway, you need to monitor the organization´s risk space to see if untoward events have arisen that need to be handled. If the monitoring effort identifies problems in process, then steps should be taken to control them.

Steps 2 through 4 constitute risk assessment. Together, they comprise an intellectual exercise that allows company to explore its risk space in order to prepare itself to handle the occurrence of untoward events. Step 5 takes company into the realm of action by having a deal with problems that are unfolding. Risk management is the combination of risk assessment and action. (Frame, 2003)



THE RISK MANAGEMENT PROCESS

SILESIAN

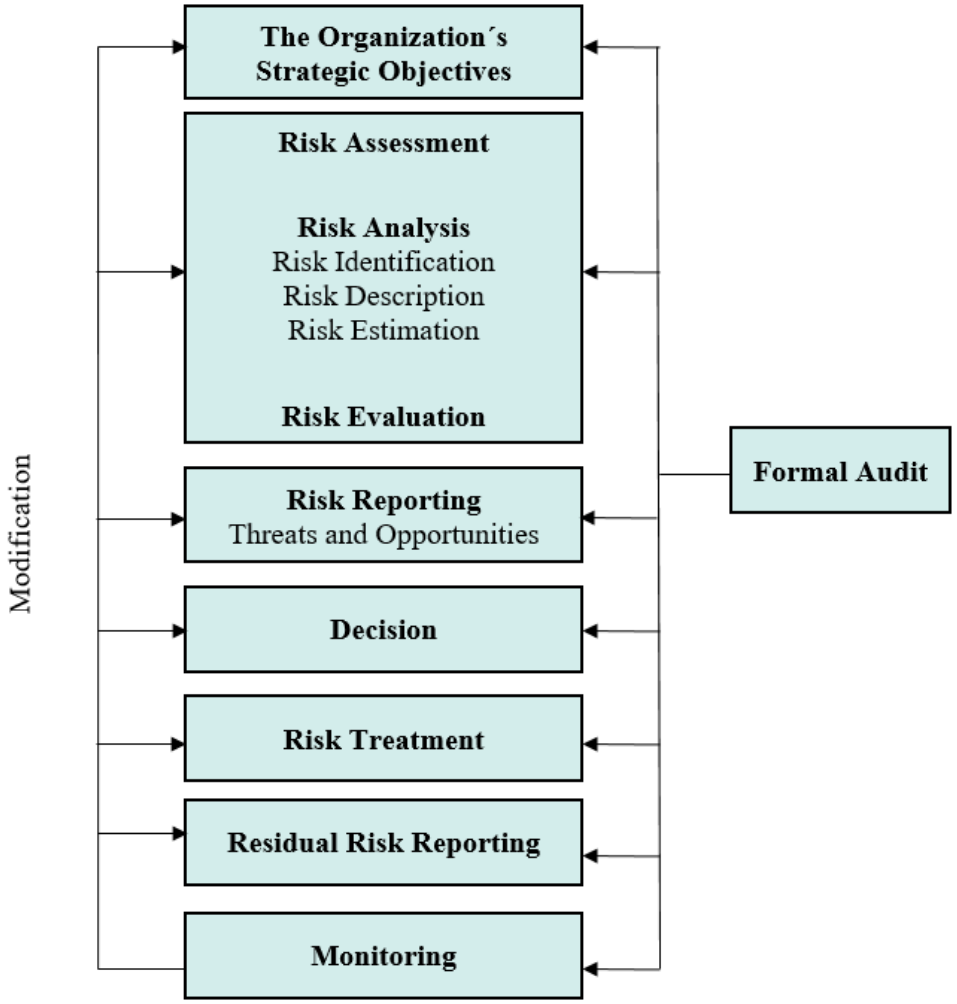
In terms of providing a framework for the risk management process, risk managers should consider these three principal areas when developing the four elements that comprise the risk management plan. These areas are the risk assessment, the contingency planning, crisis management, and the post-incident review, which are deeply specified as follows (Blyth, 2008):

- **Risk Assessment** - warning signs and analysis prior to a crisis event. The value of a risk assessment as a diagnostic tool is measured in terms of accurate intelligence, specialist knowledge, and an achievable and pragmatic set of procedures to reduce the probability of a risk occurring.
- **Contingency Planning** - preparation and prevention phase. Contingency planning refers to measures implemented to prevent recognized or speculated serious events or emergencies. These possible activities should be identified during the risk assessment.
- **Crisis Management** - incident response, damage containment, and recovery period. Crisis management is the response to a problem while it is occurring, or after an incident, utilizing the contingency planning measures, as well as the organization able to respond quickly and effectively to unique requirements.
- **Post-Incident Review** - review and modification of the risk management plan. The documentation of all incident information should be conducted to support adjustments to existing policies and plans, as well as to identify shortfalls within crisis management policies and management teams (mitigating future crisis impact levels).

The Global Risk Management Process

The global risk management process can be presented as **a list of co-ordinated activities**. To help the understanding of an organisation for business continuity purposes in global perspective, a **Business Impact Analysis** (BIA) and **Risk Assessment** (RA) should be applied. The BIA identifies the urgency of each business function undertaken by the organisation through assessing the impact over time of interruption to this activity. This information is used to identify appropriate continuity and resumption strategies for each function. The RA as part of the risk management process (Figure 6) helps in identifying risks which might threaten the achievement of a set of business objectives and the inherent potential severity (before controls are applied) and residual potential severity (after controls are applied) of these being realised. (Graham and Kaye, 2015)

Figure 6: The process of Global Risk Management



Source: adapted from AIRMIC

Foreign Exchange Risk Management Framework

SILESIAN UNIVERSITY

The **exporter will receive the payments for goods shipped after some time**, as the **trade cycle** in international trade **is longer** due to reasons such as transportation time, customs clearance time and credit period. Hence exporter is exposed to **exchange rate fluctuation risks** as the value of currencies keep on changing by the minute in the international market. Therefore an exporter must take necessary **steps to cover his risks** due to exchange rate fluctuations.

The exporter can hedge his risk in various ways. In today´s global environment, **various forward cover facilities are available for authorized dealers** (banks) **for covering exporter risks against currency fluctuations**. For this purpose, the exporter has to enter into a contract with authorized dealer (banks) for covering his exchange rate fluctuations risk. While taking forward cover, the exporter must ensure that the cover is taken for some more number of days rather than just the due date as international payments are subject to same delays due to various reasons.

- Once it is clear that the currency in which the contract has been denominated is exposed to vagaries of fluctuations, the exporter should concentrate his focus on deploying resources, tactics and strategies to manage such risks so as to avoid losses to the firm. A **heuristic approach** along with a diagram to manage this risk effectively is presented below which can be modified (if required to suit the firm´s specific needs).

Foreign Exchange Risk Management Process

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

The following approach shall be used in order to manage foreign exchange risks (Singh, 2009):

1. Forecasts

-having determined the degree of exposure to the currency in which contract is denominated. The first step for an exporter is to develop a forecast on the market trends and also contemplate what can be the main direction and trend of such movements in foreign exchange rates. The period for such forecasts is usually 6 months as the exporter´s concern is to minimize his risks for next month only, during which period he is supposed to bring foreign exchange to country under FEMA (Foreign Exchange Management) Rules. It is important that such forecasts should be based on valid assumptions and contemplations of exporter. The exporter should make a scenario analysis of forecasts in order to determine the probability of trends and direction of currency movements.

2. Risk Estimation

-based on the forecast made by the exporter, he should assess that what can be the actual profit or loss if there is change in downward or upward in the rates according to the forecast. Exporter should also assess that what factors can influence his decisions in controlling such risks such as market-specific problems, poor decisions making system and inadequacies such as reporting gaps and implementation gaps in the firms´ exposure management system.

3. Benchmarking

-having assessed and estimated the risks, the exporter should set his limits for handling foreign exchange exposure risks, if any. The exporter should also decide whether he shall be managing these exposures on a cost centre or profit centre basis as large multinationals in the recent past have also added such activity to their main areas of activities.

Foreign Exchange Risk Management Process

SILESIAN UNIVERSITY

4. Hedging

-on the basis of exposure limits, the exporter should decide an appropriate hedging strategy. There are various financial instruments available today, which the firm can choose from, such as futures, forwards, options and swaps and issue of foreign debt. Hedging strategies are elaborated in the chapter subsequently.

5. Stop Loss

-the ultimate objective of whole risk control exercise is to control the risks and this can be done effectively by exporter risk management decisions, which should be based on forecasts and estimates of reasonably unpredictable directions and trends. It is essential for an exporter to stop losses if the forecasts have been wrong due to errors or omissions. The exporter shall have sustainable and effective monitoring systems in place for detecting such critical levels of ups and down in the foreign exchange rates in order to avoid losses.

6. Reporting and Review

-the exporter should have sound reporting and review system so as to take stock of risk management policies and should have periodic reporting of such risk control exercise. Such exercise should mainly include profit and loss status and variations in actual and benchmarked exchange rate movements. Such a review helps in analysing whether the benchmarks set are valid and effective in controlling the exposures or not and what corrective actions can be taken y the exporter or firm.

RISK MANAGEMENT PLAN

Risk Management Plan

SILESIAN

The risk management plan must be supported at every level in order to be successful. At the corporate level, a risk policy strategy needs to be agreed on and distributed to appropriate individuals and groups, providing a framework for systematically developing risk assessments that corporate and program management can use to guide activities and focuses. At the program level, the plans must be usable and reflective of realistic conditions and responses. Synergies and interfaces between corporate and program-level plans should also be identified and integrated to ensure that corporate and project teams do not work independently of, or in isolation from, each other, but undertake concurrent and complementary activities. Some of these elements should be considered **when developing the risk management plan** (Blyth, 2008):

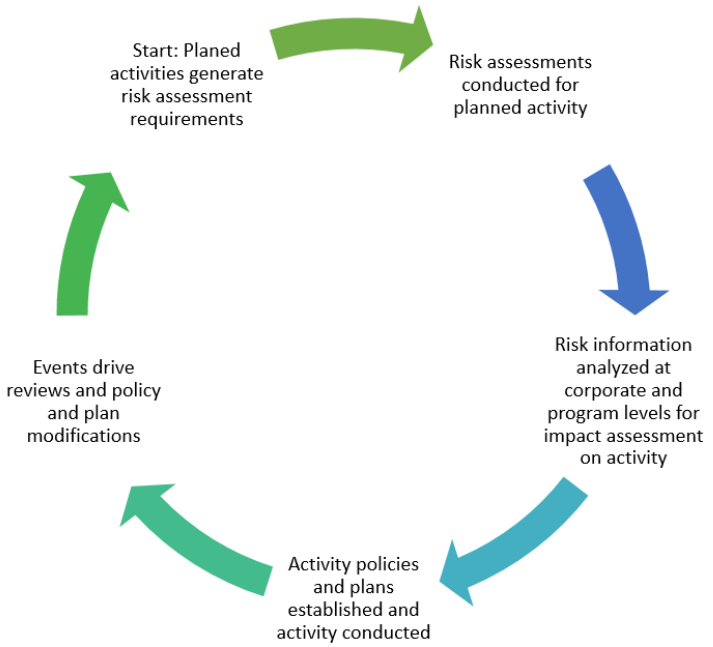
- Establish which elements of the organization need to be brought together – both stakeholders and contributors, prior to any resources being applied, or activities being conducted.
- Provide a convenient framework for developing a quantitative risk assessment that prioritizes both goals and objectives of the company, in the context of the associated risks or threats.
- Provide a systematic and repeatable method for evaluating an organization´s risks using the best available threat information. Seek efficiencies by drawing on existing templates and formats.
- Permit program, project and other key managers the opportunity to identify their departmental and organizational risks.
- Identify information gaps in order to establish a better risk picture.
- Allow risk and security managers to express their expectations about the consequences of successful incidents. Elicit their observations and recommendations on ow to mitigate these risks.
- Allow business leaders and project managers to review the risks and comment on how risk management policies, approaches, and plans might affect program design, objectives, and goals.

Risk Management Plan

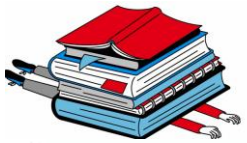
Risk management should be **cyclic in nature**, with continuity between the users (operation and business) and managers (corporate). In addition, the process is cyclic in terms that the business need prompts the requirement for a risk assessment – used to establish which risks the new activity may elicit. These factors then feed business decision making and associated policies and plans, with new or changing events driving modifications to the policies and plans - in turn influencing business needs and decision making (Figure 7).

Risk information needs to be shared with appropriate groups and individuals in order to ensure that a rounded understanding of the risks is gained and that mitigation measures are most effective. Information sharing can be through training, white papers, boardroom briefings, warning posters, leaflets, or daily intelligence briefings that highlight specific risks or risk environments. **The policies and procedures** set to mitigate risk are a **reflection of the requirements identified within the risk management plan**. Depending on the size, nature, and diversity of the organization, the procedures can vary from simple and pragmatic brochures, to volumes of complicated manuals and training exercises covering a multitude of subjects, at varying organizational levels. (Blyth, 2008)

Figure 7: The Risk Management Cycle



Source: adapted from Blyth, 2008



General Risk Management Policies

SILESIAN

General risk management policies apply to the entire company. Policies provide high-level guidelines for managing risks to comply with the general policies is a company-wide requirement. The following are key risk policies (Fraser et al., 2014):

- **Customer satisfaction and retention policy**

-internal and external customer expectations are periodically monitored and communicated in a timely fashion to ensure that service levels are achieved for operational objectives.

- **Ownership policy**

-no information, data, process, report, or asset can exist without having an owner attached to in. Change of ownership can be initiated only upon approval of a designated internal stakeholder. Ownership is assigned according to priority criteria of “most used by”, “first created by” and “most impacted by”.

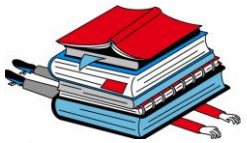
- **Training policy**

-each item in this policy statement must be included in the company´s training program. Corporate culture can be established and maintained only by providing timely and sufficient training to each employee. No employee can be assigned responsibilities without adequate measurement of his o her competencies.

- **Information system policy**

-objectives at all levels (strategic, tactical, and operational) should be mapped down to the infrastructure level.

Context definition should be monitored and reviewed at least yearly and whenever a major event occurs. All risk owners must be cognizant of their dependency on other areas of the business. Integrity, consistency, and accessibility objectives are set by business lines, and information technology hardware architectures are designed to ensure the achievement of such objectives.



General Risk Management Policies

SILESIAN

- **Access rights policy**

-access rights should be provided according to each employee´s responsibility level. Access rights should not be changed without approval of a senior manager. All access rights need to be consistent with the authorization levels. No conflict of interest and segregation of duties issues are permitted to exist.

- **Corporate ethics policy**

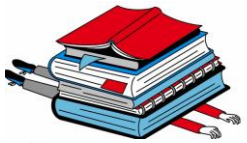
-corporate ethics rules are monitored and maintained by the Audit Committee. Ethics are included in each training seminar and such seminars need to be taken periodically.

- **Human resources policy**

-background screening and training are required for all employees. Compensation is evaluated and performance is monitored by the Compensation Committee. Performance measures with include and reflect a fair amount of collaborative and teamwork performance as well as individual performance to prevent destructive competition. Any contrary action will be considered a failure to comply with the corporate policies and will be treated according to company laws and regulations.

- **Outsourcing and contract management policy**

-outsourcing is used whenever it is beneficial for the organization to do so. A comprehensive risk assessment must be conducted and results must be communicated among internal stakeholders before establishing any outsourcing engagement. Service level agreements are determined according to business needs and set within the tolerance levels of the objectives. Monitoring of Service level agreements is the responsibility of the owner of the business line signing the contract. Dependency on a single outsource agreement must be avoided by establishing alternate sources.



General Risk Management Policies

SILESIAN UNIVERSITY

- **Business continuity policy**

-impact analysis is conducted yearly to assess the impact level of disruption to all business units. Service-level agreements are based on this impact analysis and must be signed by all parties. IT departments use this impact analysis to determine parameters for service levels. Each employee must have a designated backup coordinator.

- **Conflict of interest policy**

-conflicts of interest must be avoided. Special emphasis needs to be given to those areas sensitive to public perceptions.

- Sustainability and environmental protection policy

-maximum effort must be provided to preserving the environment and the resources in each project to enable achievement of business objectives.

- **Insurance policy**

-insurance needs are decided upon after evaluating the current risk profile. Market research must be conducted annually to identify the best total value, which is not necessarily the lowest rate.

- **Market risk policy**

-close monitoring of costs is required throughout the entire business. Exchange rate risks above the limit of accepted amounts in export contracts must be hedged by futures contracts to ensure cost and profit stability. Also, key risk indicators must be accepted and reviewed periodically for effectiveness. Liquidity risks need to be managed by the financial control and accounting departments.

SUMMARY

- Risk management is a **complex systematic process of identifying, eliminating or minimizing uncertain events that may affect an entity and controlling them.**
- The risk management in trade operation **ensuring the health of organizations**, **provide the advice**, **tools, products and services that assist an organization with its planning and reporting**, provides **arrangements through business continuity management to minimize damage**, **deal with crises** and **recover back to normality** and **avoid cost and disruption**.
- In assessing the likelihood of risk occurrence and its impact on business activities, **statistical methods** can be used. A very often is used of **the risk matrix** for risk assessment.
- **The risk matrix assess the effects of risk on organization and probability of occurrence at given time.**
- The current retail risks drivers are **cyber risk, competition, consumer expectations, compliance and regulations, technology disruption, data and analytics.**
- There are four ways to manage risk: **avoid them** (terminate), **share them** (transfer), accept them (tolerate) and **control them** (treat).
- The classifications of risk management controls is divided into **preventative, directive or detective controls; physical, management or technical controls; and manual or automatic controls.**
- The risk management process is set from these stages: **plan for risk, identify risk, examine risk impacts, develop risk-handling strategies, monitor and control risk.**
- The general risk management policies provide high-level guidelines for managing risks, e. g**. customer satisfaction and retention policy, ownership policy, training policy, information system policy, corporate ethics policy, outsourcing and contract management policy, business continuity policy and insurance policy.**

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

THE LITERATURE REVIEW SOURCES

1. BLYTH, M., 2008. *Risk and Security Management: Protecting People and Sites Worldwide*. New Jersey: John Wiley & Sons. ISBN 978-0-470-38727-6.
2. FRAME, J.D., 2003. *Managing Risk in Organizations: A Guide for Managers*. 2nd ed. San Francisco: John Wiley & Sons. ISBN 978-0-7879-7264-6.
3. FRASER, J., B. SIMKINS and K. NARVAEZ, 2014. *Implementing Enterprise Risk Management: Case Studies and Best Practices*. New Jersey: John Wiley & Sons. ISBN 978-1-118-74618-9.
4. GRAHAM, J. and D. KAYE, 2015. *A Risk Management Approach to Business Continuity: Aligning Business Continuity and Corporate Governance.* Brookfield: Rothstein Publishing. ISBN 978-1-931332-88-0.
5. HOPKIN, P., 2017. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. London: Kogan Page Publishers. 978-0-7494-7962-6.
6. MILES, D.A., 2011. *Risk Factors and Business Models: Understanding the Five Forces of Entrepreneurial Risk and the Causes of Business Failure*. Boca Raton: Universal-Publishers. ISBN 978-1-59942-388-3.
7. MULAČOVÁ, V. and P. MULAČ, 2013. *Obchodní podnikání ve 21. století*. Prague: Grada. ISBN 978-80-247-4780-4.
8. REUVID, J., 2014. *Managing Business Risk: A Practical Guide to Protecting Your Business*. 7th ed. New Delhi: Kogan Page Publishers. ISBN 978-0-7494-7044-9.
9. SADGROVE, M.K., 2015. *The Complete Guide to Business Risk Management*. 3rd ed. New York: Gower Publishing, Ltd. ISBN 978-1-4724-4221-5.
10. SINGH, R., 2009. *International Trade Operations*, 2nd ed. New Delhi: Excel Books. ISBN 978-81-7446-735-5.
11. SINGH, R., 2009. *International Trade Operations*, 2nd ed. New Delhi: Excel Books. ISBN 978-81-7446-735-5.
12. Web portal AIRMIC [online] [25.07.2019]. Available at: www.airmic.com.
13. Web portal Bitsight [online] [27.07.2019]. Available at: https://www.bitsight.com/security-ratings-retail.
14. Web portal KPMG - Global Retail Risks 2018 [online] [03.08.2019]. Available at: https://home.kpmg/content/dam/kpmg/za/pdf/2017/12/Retail%202018.pdf.
15. Web portal KPMG [online] [01.08.2019]. Available at: https://assets.kpmg/content/dam/kpmg/us/pdf/2018/05/stay-within-the-guardrails-top-retail-risks-2018.pdf.

THANK YOU FOR YOUR ATTENTION

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA