ENTERPRISE RISK MANAGEMENT

THE DARK SIDE OF PERFORMANCE MANAGEMENT

DRAFT 2020

7 Enterprise Risk Management

Table of Content

7.1 Introduction and Learning Objectives

The chapter shall give the student an overview of the magnitude and functionality of Enterprise Risk Management (ERM). After introducing the significance of this management activity, the student shall gain a proper insight into the concepts of Enterprise Risk Management by understanding the term itself, the instruments used, and the methods of applying a risk map. Additionally, risk assessment will be extended by discussing the importance of internal controls. This section highlights the methods of internal auditing and bank reconciliation in order to frame the theoretical approach to risk assessment management. Applying theory to practice, the case study of BASF SE, based on the Annual reports of 2011 and 2012, shall demonstrate the implementation of Enterprise Risk Management.

The Austrian-American economist Peter Drucker once stated that all economic activities bind current resources to an uncertain future Uncertainty in terms of risks is, thus, the only definite characteristic of the future and considering insecurities is a crucial part of profitable business performance. A reason why the BASF Group enhances risk management because it actively encourages identification and evaluation of “risks and opportunities as early as possible and to take appropriate measures in order to seize opportunities and limit business losses” (BASF Group, 2012: 107). But this is not the only major corporation that emphasizes the importance of enterprise risk management. Examples like BER Berlin-Brandenburg Airport in 2012, BP Deepwater Horizon in 2010 or the Tepco-Fukushima disaster starting in 2011 are just some of the recent illustrations underscoring the significance of this topic. The adoption of enterprise risk management finds its rationale in volatile economic environments, instable/ unpredictable political conflict-situations and changing market situation through mergers and acquisitions as well as progressive technologies. Moreover, major incidents like the case of Enron, the fall of Lehman Brothers and the financial crisis of 2007 demonstrate that the former approach and perception of ERM did not meet the aims of sustainably increasing growth and wealth. Management and executive performance was accused of being biased, self-serving and greedy; they were not seen as being successful in adjusting risk potentials with responsive strategies to pursue corporate values. Those incidents instilled a lack of confidence

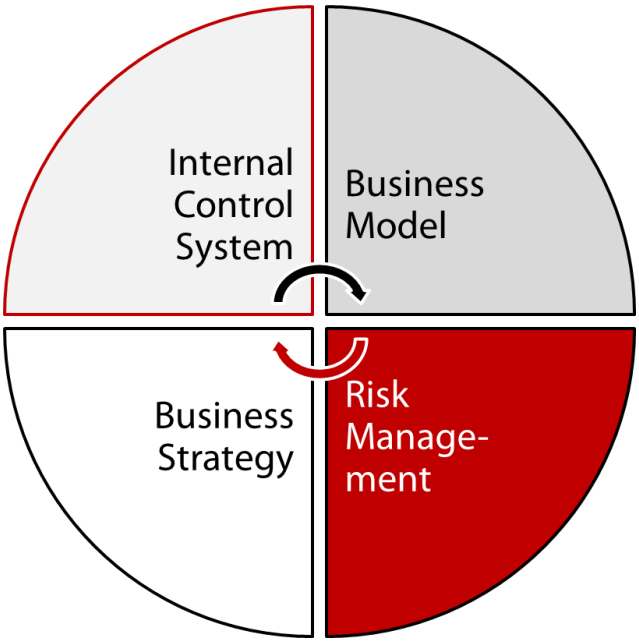


Figure 1: Risk Management Everywhere

and trust in the current risk assessment engagements. Aspects of financial reporting, corporate governance, external auditing and regulatory compliance were vehemently alleged to have failed or to have been misjudged. As a reaction legal measures implemented by governments, like the American Sarbanes-Oxley Act 2002, the German legislation named KonTraG (Gesetz zur Kontrolle und Transparenz) or the EU-Basel Accords for the banking industry, restricted previously permissible actions and emphasized the importance of strict risk assessment and corporate responsibility.

Enterprise risk management (ERM) may be defined as the instrument for any organization, whether profit or non-profit, to identify, understand and counteract potential uncertainties – which can be understood as a threat (risk) that is imperative to avoid, or alternatively as a value-increasing opportunity, either arising from outside or within the organization – with the purpose of creating and protecting the value of stakeholders including owners, shareholders, employees, customers and society in general (Monahan, 2008: 8ff.). If directed well, ERM contributes to a company's competitive advantage in forms of growth, consistency and value, by delivering an informative foundation for sustainable, effective managerial activities and decision-making. Implementing an effective ERM has been an important challenge for many companies since then. Changing behavioral decision-making patterns and operational processes within a corporation is essential to creating a proper understanding of risk management amongst executives and managers who receive a more accountable and responsible role in the perception of ERM. It highlights the necessity to gain an oversight of potential risk factors, deal with the multitudes of risks and coordinate them on a company-wide level so that the decision-making process is based upon taking considerable risks, which will help to achieve company-specified goals and missions. Taking such a holistic approach nowadays improves the understanding of not only the individual risks for the company, but also the further risks that are incurred by other

subjects in the global market and their interactions. In this context, amongst Internal Control Systems (ICS), ERM is perceived as part of the corporate governance framework. As illustrated in the graphic, ERM strongly relates to the strategy aspect of an organization, whereas ICS reflects the business model. Still the ICS and ERM components interconnect. The ERM tries to find the threats of what could go wrong and the best ways to react. The ICS rather assesses operational risk, especially regarding internal weaknesses appearing in form of fraud or false compliance.

Before exploring the matter of ERM in detail, the terminology concerning risk and enterprise risk management is discussed in order to establish a common understanding for the further discussion. Business organizations face risks on an everyday-basis. Any transaction, decision-making or organizational activity will generate various outcomes with unpredictable likelihoods of occurrence. Events with a negative impact represent risks, which can prevent value creation or erode existing value. Consequently, “risk is the threat that an event, action, or non-action will adversely affect an organization’s ability to achieve its business objectives and execute its strategies successfully”. (COSO, 2004)

In the words of the BASF Group, opportunities exceed potential success while risk negatively impacts short-term operational and long-term strategic objectives. Generally speaking risk is quantified in terms of impact and likelihood, truly involving a great portion of uncertainty. Thus, risk will always be an uncertainty; only in a quantized manner does if fulfil the ideal purpose of changing the uncertain future into certainty. In this context it is essential for organizations to adopt management functions which solely focus on risk assessment, questioning which risks cause further threats and the amount of risk-taking a company can bear. Knowing the influential factors - risk drivers and risk controls – helps to identify the likelihood of potential event outcomes as well as to increase one’s ability to judge them (Monahan, 2008: 5ff.). This management function deals with the dynamic, continuously changing risk environment at an organizational level to achieve business objectives and successfully execute strategies. Amongst similar definitions by various organizations, the Committee of Sponsoring Organisations of the Treadway Comission (COSO) outlines the present topic as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk

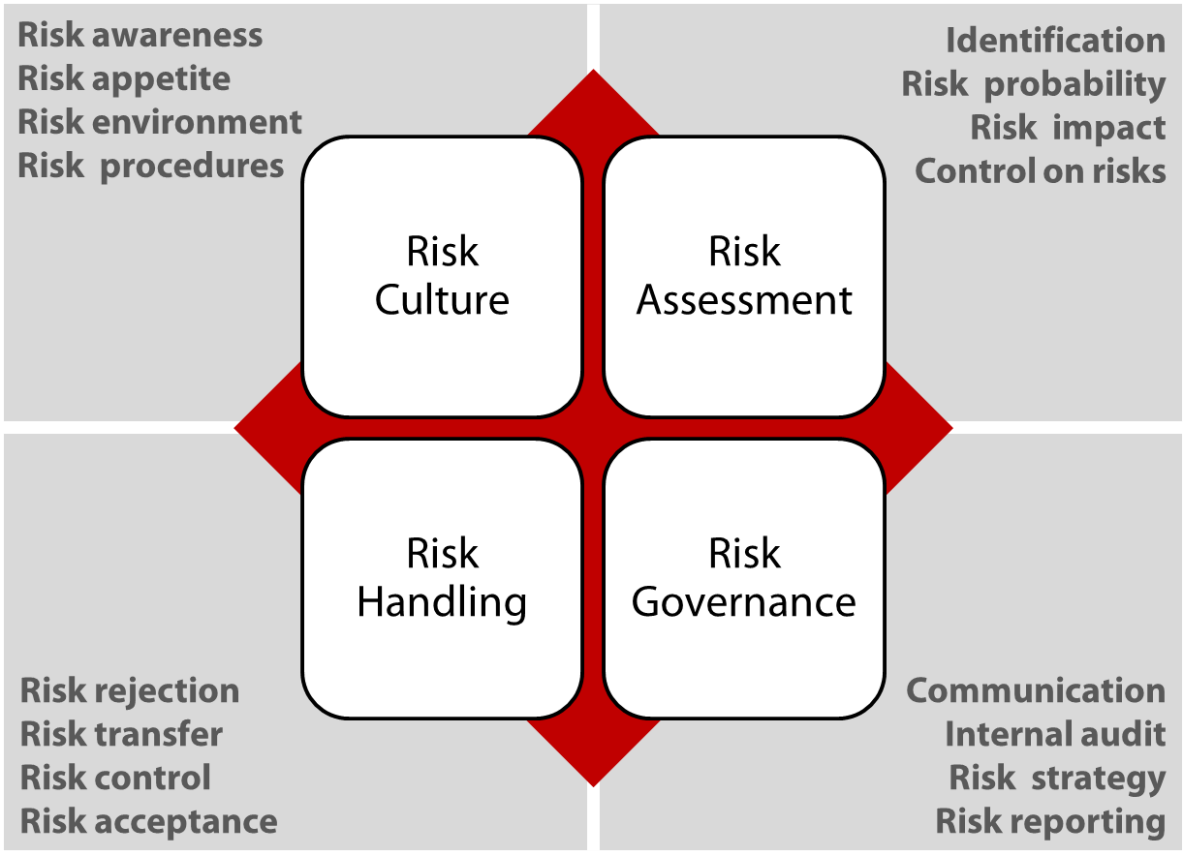
appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004: 2).

For the sake of simplicity, I have added another definition, which goes like this:

"**Risk management is a systematic process of identifying, assessing, monitoring and consciously dealing with uncertain events and situations which might harm an organization and have the potential to prevent it from achieving its objectives.**"

7.2 An Integrated Risk Management Framework

In the following, an integrated risk management framework is presented which depicts risk management along four main categories: risk culture, risk assessment, risk handling and risk governance.



7.3 Risk Culture

The risk culture describes the soft and structural bases of risk management within an organization. Or company. The risk culture is the mirror of awareness that risk is an important factor of any company and that it needs to be addressed properly. This risk awareness might be interpreted as a kind of organizational maturity. Start-ups may

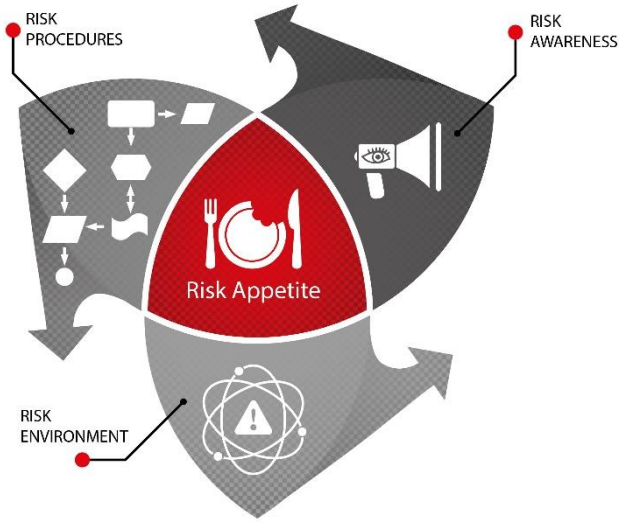


Figure 7-2: Elements of the Risk Culture

ignore risks and focus instead on opportunities. For young entrepreneurs with nothing to lose, risk management might even be an unnecessary bureaucratic hurdle in the way of value creation. But with the growing wealth and value generation of a company, the awareness that this wealth could be at risk usually grows. Family-owned businesses see family values imposed on their company and with growing children and grand-children, the risk awareness grows. Publicly traded companies are subject to special risk awareness, since they belong to the shareholders with - in most cases- no direct influence on operative business decisions. Dealing with the money of other people creates the need for accountability towards the risks taken to increase the shareholders' value. The risk appetite of a company is correlated to the risk awareness and the expected opportunities. The more profitable a business the more risk the shareholders are willing to take. Risk appetite also has a time dimension. Investment into long-term projects might have a strategic value, but fickle shareholders with an investment horizon of less than three years have difficulties to invest into long-term opportunities. Family-owned businesses are said to be less myopic, but it is clear that the risk aversion or the risk appetite of the shareholders will dominate the business behavior of a company.

The risk environment is the manifestation of the risk awareness. We see the structural responsibilities, Chief Risk Officers and risk managers along the hierarchy. In order to perform a successful ERM all processes, roles and responsibilities have to be properly defined and executed as shown in the BASF Group's reporting and risk management structure below.

BASF Group's Risk Management Organisation

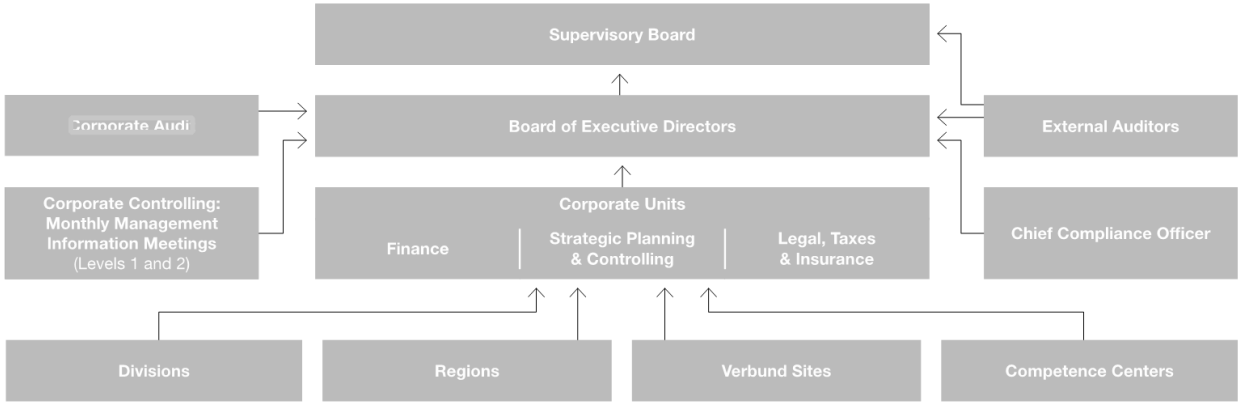


Figure 7-3: Risk structures and responsibilities (BASF Group, 2012: 108)

The Board of Executive Directors carries full responsibility for risk management, granting approvals for investments, acquisitions and divestitures. Supporting the Board of Executive Directors, the process of risk and opportunity management is well embedded in the strategy, planning and budgeting process of the following divisions: Finance, Strategic Planning & Controlling, Legal, Taxes & Insurance, Corporate Controlling and Chief Compliance Officer (CCO). The CCO directly reports to the Board of Executive Directors and the Supervisory Board's Audit Committee and offers guidance in compliance and codes of conduct. The risk management is largely conducted at a local level within the business units, which have to consolidate on a group-wide level to approve counteractions.

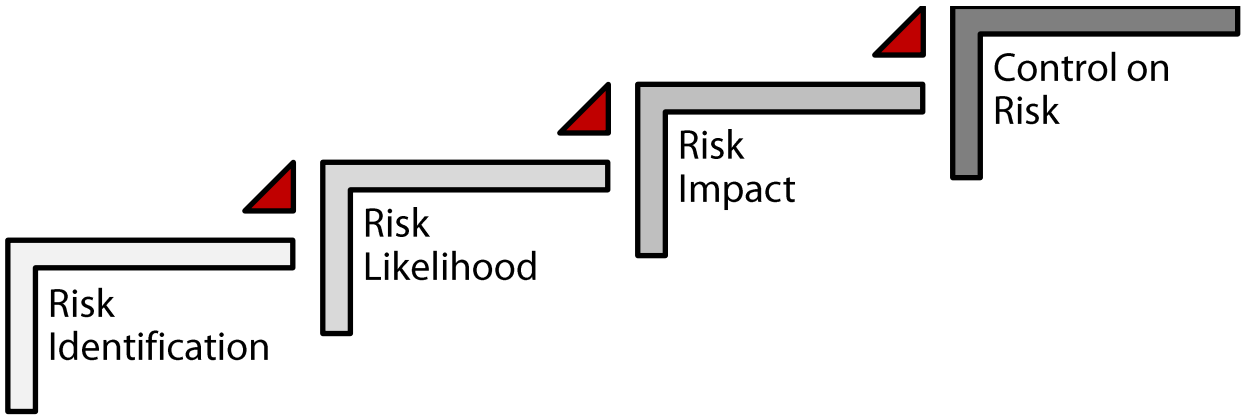
The risk environment incorporates the attitude towards risk management: Is risk management regarded as an unnecessary evil or a value-creating activity? The set-up of responsibilities and organizational charts might be just a masquerade to cover up an inner skepticism against dealing with risk management. If risk management becomes a corporate ritual for ignoring risks and systematically covering up the risk environment it is not effective. Last but not least the risk culture is determined by the risk procedures and processes.

Critical Questions for assessing the effectiveness of a risk environment

- Is risk a topic that is shunned and never talked of?
- Are employees who talk about risks marginalized?
- Does the company have a Chief Risk Officer or a designated risk manager with direct access to top management?
- Does the company engage in business which might put the existence of the company at risk?
- Does the company have written risk procedures?

7.4 Risk Assessment

A systematic assessment of risks is the prerequisite for managing them consciously. The assessment includes the identification of potential risks, their probability and potential impact as well as the assessment of the control the company might wield over the risk.



7.4.1 Risk Identification

Risks are part of everyday life: The areas of risks for companies from which events might occur which threaten the achievement of company objectives is long. They can be classified into three essential areas: operational, strategic and environmental risks.

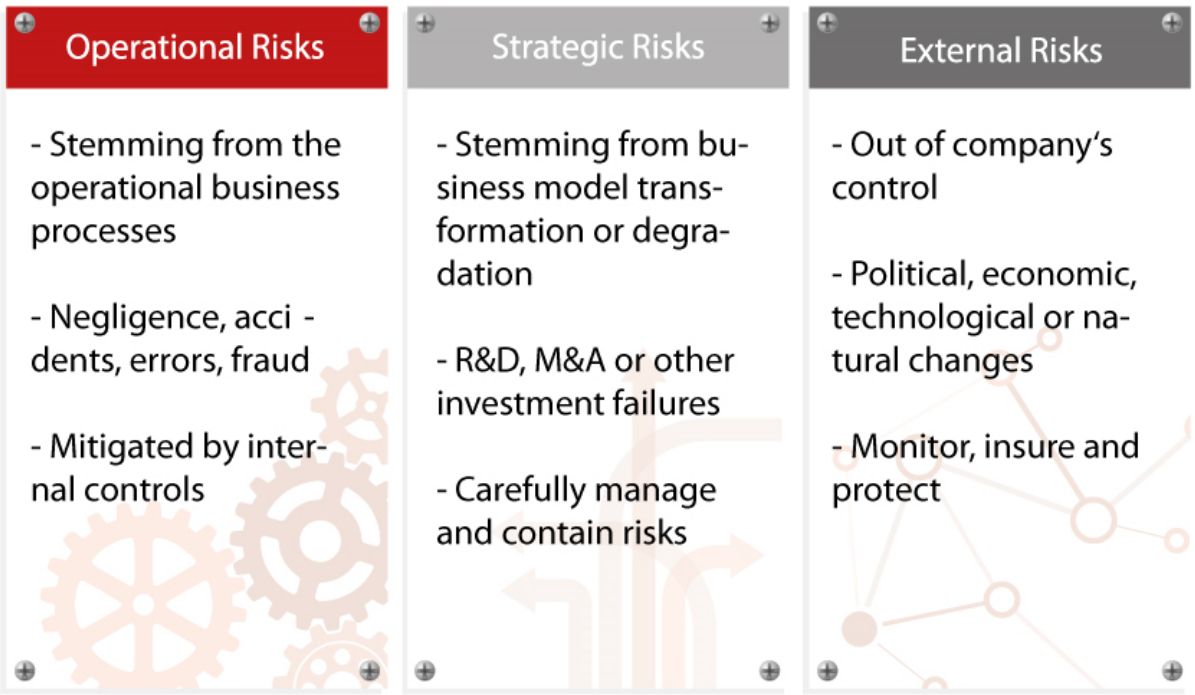


Figure 4: Risk Areas

Operational Risks

The operational risks stem from the operational performance cycle of the company, which means they are an intrinsic part of the business model. Just like in the saying "You can't make an omelet without breaking eggs," most activities come with a risk: negligence, accidents, errors and fraud happen in the office, on the shop floor, in the interaction with customers and banks. Not everything goes according to plan, employees are not robots and even the technology has its downside potential. In the following a few examples of operational risks are listed:

- IT failure leads to interruptions in the production or wrong inventory data.
- IT espionage / hacking leads to reputational damage or competitive disadvantages.
- The cash clerk steals several thousand Euros to pay for his gambling debts.
- Several key employees leave the company: They take their customer contacts to the competition.
- On the shop floor injuries incur with employees left maimed or dead.
- A complete department falls ill with a flue which leads to late delivery of products and liquidated damages.
- A key customer goes bankrupt and the trade receivables will not be paid back. In the aftermath our credit rating suffers and we have to pay higher interests for our refinancing.

- A lorry which was transporting goods to our customer had a traffic accident and the goods were damaged.
- A machine breaks down and leads to delay in the production schedule.
- The new product X had problems and had to be called back and replaced. Apart from the huge financial damage the reputation as a high quality supplier suffers.
- Customers do not like the design of product Y and buy instead the products from the competition.

The operational risks occur but they can be mitigated by internal controls which will be treated in the next section on risk handling.

Strategic Risks

Strategic risks are long-term risks that arise from the degradation or the transformation of the existing business model. The long-term degradations of the business model are natural processes and can provoke a scheduled loss in patent rights and the deprivation of the capital asset base, e.g. machines, infrastructure. It might also include a deterioration of the corporate culture or the competitive situation due to new competitors or technological developments. This can be summed up as the negligence price to be paid for not regularly transforming the existing business model. The status quo is always at risk.

The transformation of the business model also implies risks. If the strategy is driven to achieve a long-term profitable growth strategy, the envisaged projects for growth or increased profitability might not deliver the promised results. The risks for the organic growth strategy pivot around research & development and investments into new long-term assets like new plants. The R&D pipeline might not provide the envisioned products at the right time, the right quality or the right costs. Even if it does, the new products might not hit the nerve of the customers and thus do not fulfil the sales and profit expectations. Technology problems with new products might even put the reputation of the company as a high quality supplier into question. The competition does not sleep and might have, by the time the product launches, already developed an even better, cheaper product more in line with customer expectations. Large growth-investment projects such as the set-up of a new plant in an emerging economy like India are at risk of not meeting the time-schedule, costing more than initially planned or even creating reputational damage. An example would be the new BER Berlin Airport in Schönefeld, where all of the mentioned risks have become striking.

Another form of transformational projects might be organizational changes, restructuring (reduction in headcount) or the implementation of a new Enterprise Resource Planning (ERP)-system. These projects usually can have, apart from cost-overruns and delays, unintended side-effects like low employee morale, the loss/ departure of key personnel or a decline of the employer branding.

Strategic Risks

- Products cannot be developed at the right time, quality and cost level.
- The newly developed products do not meet changing customer expectations.
- The competition has already developed a better, cheaper product more in line with customer expectations.
- The new product shows traits which endanger the reputation of the company.
- Growth-investment projects do not meet cost budgets, time schedules or are even putting the reputation of the company at risk.
- Transformational projects (e.g. re-organization, restructuring, ERP implementation) cost more than initially planned and do not result in the budgeted savings or synergies.
- M&A transactions are not realized due to cartel-office objections, excessive market prices or lack of suitable targets.
- Realized M&A transactions do not achieve the planned objectives due to a lack of integration efforts.

The last area of strategic risks stems from mergers & acquisitions transactions. Here we have the risks of not finding and realizing budgeted M&A projects and at the same time the realization of M&A projects entails a myriad of other risks. First, acquisitions form a part of the strategic plans of corporations, especially in markets that do not provide an inherent growth trajectory. Not being able to realize the planned transactions because of a lack of opportunity, prices that are too high, regulatory issues or cartel-office objections will probably endanger the fulfilment of the planned growth. On the other hand, companies that pay too high a price, are unable to realize anticipated synergies due to a lack of will or knowledge of post-merger integration, might even face higher risks on the monetary and reputational scale. Not acting is risky, but acting might imply even greater risks. Strategic risks cannot be avoided in a market economy and are at the heart of the entrepreneurial decision and management processes.

External Risks

The external risks of a company are out of its direct sphere of influence. Although they might be of substantial impact, the company has to accept them, monitor closely and eventually share the risks or insure against them. Any classification of external risks is arbitrary and generic, including the following which concentrates on economic, ecological, political, social, competitive and technological risks.

Ecological risks include volatility in national or global GDP growth, currency exchange rates, or interest rates. Financial shocks derived from a financial crisis or exaggerations in the stock markets also have a tremendous negative impact on companies. Ecological risks include natural disasters like thunderstorms, earthquakes or tsunamis. Here, the effect on the business model could be tremendous. Since the locations of some sites are prone to ecological disasters, a careful weighing of the risks has to be performed. Building a nuclear power plant close to a Japanese coastline which has a history of earthquakes and tsunamis, like in Fukushima, appears in hindsight to be dangerously careless.

Political risks depend on the regulatory bodies of state governments. These might be democratic or authoritarian. Both use their regulatory powers which might lead to the end of the business model as known. German utility companies were confronted with the so called “Energiewende”, the energy reversal under chancellor Merkel, marking the sudden end to nuclear power stations in response to the Tepco-Fukushima power plant disaster. European sanctions against Russia in 2014 have impeded free trade between the European Union and Russia at the great disadvantage of companies exporting to Russia. Other regulations like quotas for women on supervisory boards also come at a cost.

Figure 5: External Risks

Social risks involve demographic trends. The growth in the diapers market for children depends on the fertility rates of societies. Social problems might arise from growing social perceptions of a company which are not in line with social expectations. The case of the Nike sweatshops and the poor working conditions under which Apple's suppliers in Asia operate have shown that a disconnect with social expectations might hurt the reputation of a company, even one with a with a halo-effect for its brand such as Apple.

Competitive risks come from unexpected or expected market reactions of competitors or new market entrants. The lowering of prices and a subsequent price war might have negative consequences. New entrants usually pursue aggressive entry strategies. This might include legal battles over intellectual property infringements (Apple vs. Samsung) or fighting over limited resources or supplier capacities.

Technological risks come as disruptive changes like the internet, allowing online traders like Amazon to provide competitive alternatives to mortar-and-brick shops, rendering old business models obsolete. A breakthrough in electric cars might endanger the profits of the petrol industry or efficient LEDs might make traditional light bulb producers look outdated. Electronic media and the internet have eaten away the market for the makers of newspaper grade paper machines. Overall the external risks can have a substantial impact on companies.

7.4.2 Risk Likelihood

The realm of the uncertainty of future events cannot be turned into manageable probabilities without compromising on the truth. Talking about the likelihood of risks falls short of the somewhat presumptuous approach of determining a clear probability between zero and one for a particular event based on substantial empirical or

theoretical footing. Although a company might have substantial historical data on bad debt or injury statistics, which might allow for the calculation of probabilities in the past, they may not be adequate for forecasting future events, since management measures might have an effect on debt management and injuries. Future events might also not have antecedents in the past. Unique projects or one-off events have no credible probability tag. The term likelihood therefore is an exercise in humility. The attributes of low, moderate, high or very high likelihoods are the product of subjective assessments. Nevertheless, the following table gives an overview of the different levels of risk likelihood, offering a guiding propensity in percentages and examples.

Risk Likelihood	Explanation	Example
Low	The event happens rarely (in less than 0.1 % of the cases) and depends on various circumstances.	Unpredicted natural disaster destroys production.
Moderate	The event may occur from time to time (between 0.1% and 1% of the cases) depending on repeating circumstances.	Sudden death of a key employee.
High	The event is likely to occur on a regular basis (between 1% and 10% of the cases).	Accounts receivables are not collectible.
Very high	The event has a very high probability (>10% of the cases) to occur up to a point of almost certainty.	Misappropriation of company assets by employees.

It might be useful to define the risk propensities of certain risks in a different way. However, it is important to define what is meant by different likelihood levels and create consistency over the whole risk spectrum.

7.4.3 Risk Impact

Measuring the impact of potential events opens the second dimensions of risk assessments. And the impact can have various dimensions, too. Obviously, the bottom-line effect in terms of losses has a great importance. However, reputational risks are catching up fast as a result of social media platforms like Facebook, Xing and Twitter spreading rumors quickly. The following table offers a rubric for minor, modest, severe and disastrous impacts of identified risks. Other definitions are possible. All classifications are artificial and based on subjective estimations, but defining risk

impact dimensions can help develop a common language for talking about risks within the company and for communicating about risks to stakeholders.

Risk Impact	Explanation	Example
Minor	▪ The event has a negative financial impact of in less than 1 % of equity. ▪ The event has local impact on the company's reputation	Accident in the production with few casualties.
Modest	▪ The event has a negative financial impact of 1 to 5 % of equity. ▪ The event has regional impact on the company's reputation	An accident leads to the leakage of toxic matters into the river.
Severe	▪ The event has a negative financial impact of 5 to 20 % of equity. ▪ The event has national impact on the company's reputation	National recall of product.
Disastrous	▪ The event has a negative financial impact of more than 20 % of equity. ▪ The event has international impact on the company's reputation	Big oil spill with international media coverage.

Merging the two dimensions of risk likelihood and impact opens a two dimensional risks map. Multiplying risk likelihood and risk impact creates quantified risk levels. In the example of a 4X4 risk matrix, the risk coefficients from 1 to 4 show small risks. Risk coefficients from 5 to 10 show medium risks, whereas a risk coefficient above 10 is substantial and above 15 indicates existential risks.

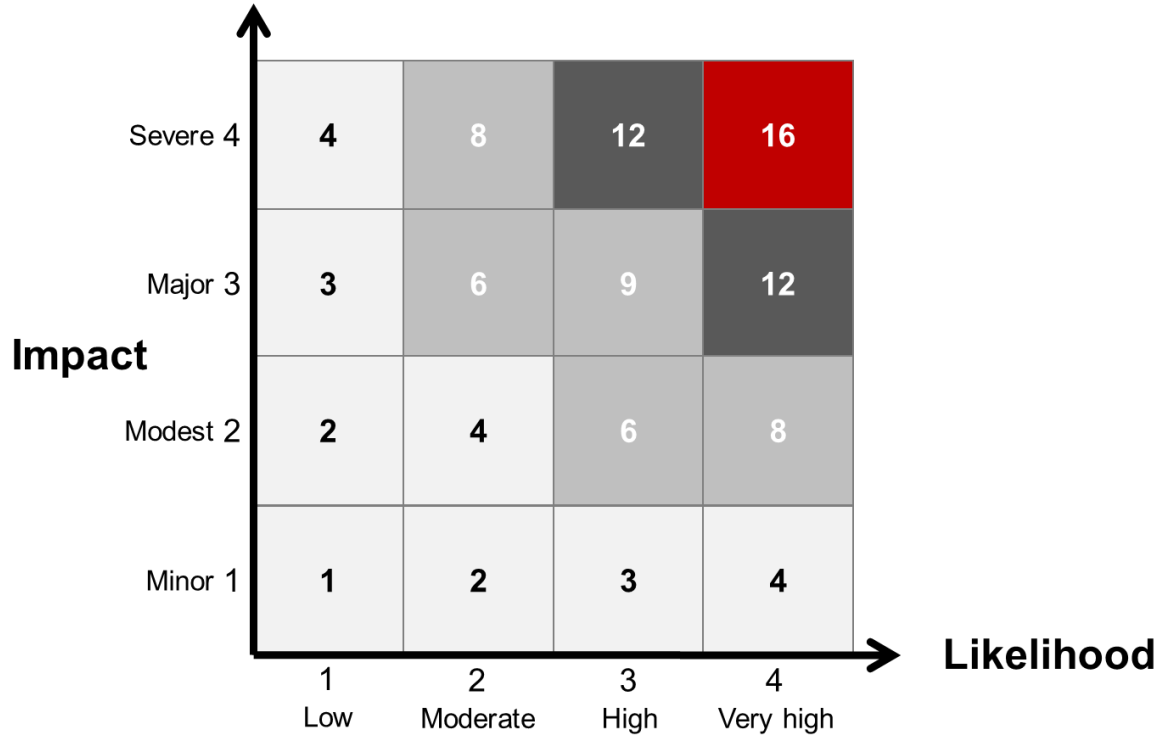


Figure 6: Risk Matrix

The risk levels can also serve as a basis for deciding how to handle the assessed risks.

7.4.4 Control on Risk

Having identified potential risks events and assessing them in terms of likelihood and impact allows the company to draw a risk map. For the next step of managing or handling risks, the entity has to understand the nature of the specific risks in terms of how to influence and control the risk.

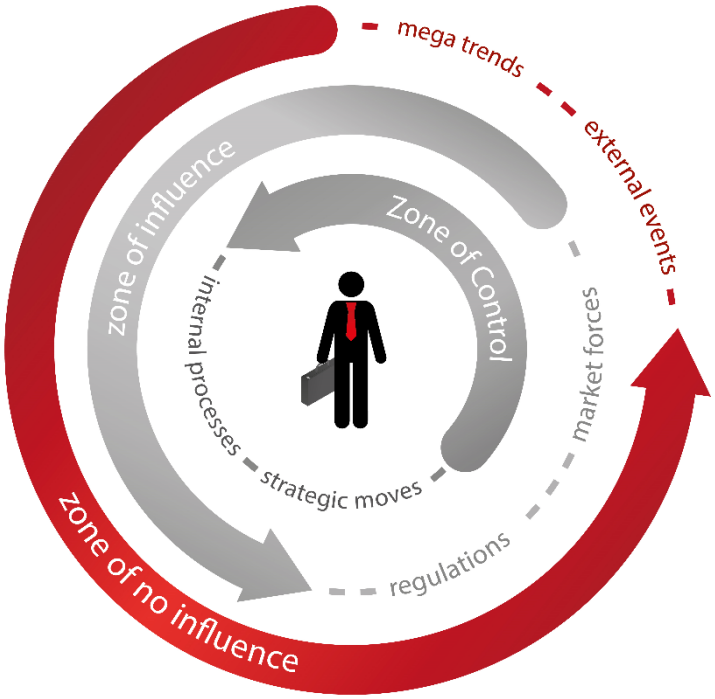


Figure 7: Control on Risk

It might come as a surprise or an exercise in humility, but the **zone of control** is relatively small for most entities. It is restricted to the areas where the outcome of events depends heavily on our decisions and actions. In the world of the enterprise this includes well defined and controlled business processes and strategic moves. The potential exercise of power and control does not lead to full predictability of the outcome, however. Even within the realm of our enterprise processes we depend on more or less empowered human beings to perform as planned. However, we can actively increase the internal control environment and achieve reasonable assurance that the business processes within our zone of control are performed as planned. The same is true for strategic moves: The decisions to invest or divest, to engage in research or internationalize our market reach remains with us. Even if we cannot foresee the outcomes of these decisions, we are in entrepreneurial control of making them.

The **zone of influence** marks the field of the business environment on which you as an entity have only indirect influence. This includes for example the reactions of competitors and politically set market regulations. In most areas this influence is indirect through lobby groups or advertising. The rules of robust capitalism imply in many states that prices cannot be fixed among competitors and laws cannot be dictated by enterprises. However, asserting a soft power approach may prove helpful in shaping the image of a company and in positively influencing relevant legislative processes.

The biggest portion of the business environment is to be accepted as a **zone of no influence**. This includes the megatrends like urbanization or mobility, natural disasters, foreign exchange rate fluctuations or political instability. Companies have to accept the given realities and to adapt to them as necessary. Zone of no influence,

however, does not mean that one cannot prepare or take action against potential threats and risks.

The level of influence or control might be integrated into risk maps by adding a symbolic bubble size for each risk: The higher the influence, the bigger the bubble. One might use five different sizes: Small for no influence, medium for influence and big for control.

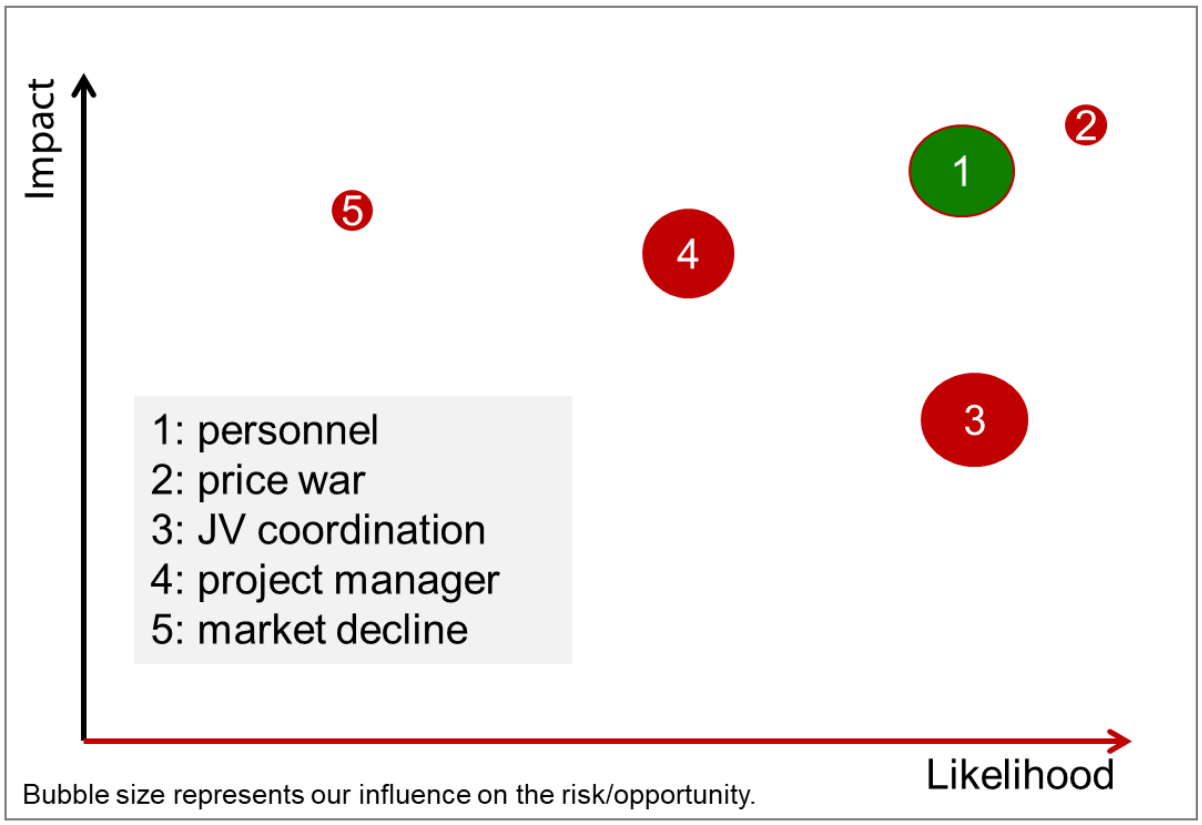
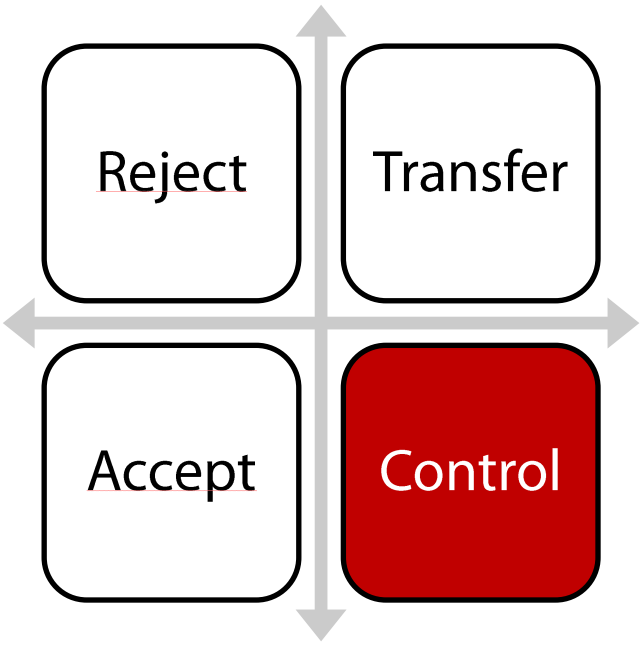


Figure 8: Three-dimensional Risk Map

7.5 Risk Handling

7.5.1 Risk Handling Options

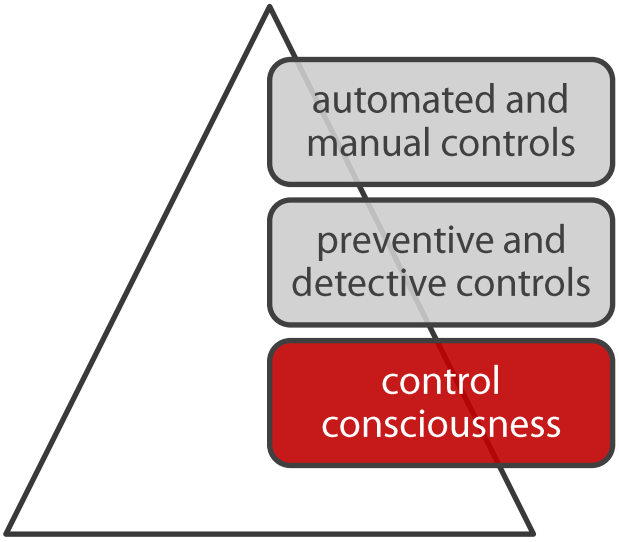
Once the risks are identified and assessed, they have to be dealt with or handled. Basically, companies have four different options to deal with an assessed risk. Rejection, transfer, control or acceptance. They can **reject** it. This means, all activities which imply a certain risk will be avoided. These could be drilling for oil in the Artic Sea, illegal or dubious financial transactions as well as abstaining from doing business with politically unstable countries or financially unstable business partners. The rejection of substantial business risks comes at the price of losing risky and potentially profitable business opportunities. However, the maturity and effectiveness of an enterprise risk management system can best be assessed by understanding which risks a company is not willing to take. The **transfer of risks** means to accept the business opportunity and engage in risky behavior. However, the potential exposure to the striking risk is partly or fully transferred. The most common example is insurance of certain risks, like the fire insurance. The insurance comes at a certain cost, but the risk for a fire in the production will at least financially be mitigated. The insurance company takes on the risk of a fire incident of running a production facility against an insurance premium. The transfer of a risk could also come in the form of a joint risk and opportunity venture (**joint venture**). This could be a cooperation of two or more different companies who jointly share the risk (and opportunities) of researching a new technology. The overall development and potential failure costs might be too big for one company to bear. Joint ventures are also a (partly forced) cooperation for the market entry of foreign companies like China. Taking **control** over risks means to put measures in place to mitigate the risks. This topic will be treated under internal controls in the subsequent section. And finally, some risks in the strategy setting or the operational business are closely monitored but accepted. This can be the case for regulations and law or the economic development.



7.5.2 Internal controls

Internal controls are the manifestation of a control consciousness in all business activities and can be divided into preventive controls and detective controls. Preventive controls are built into the business process to actively prevent inefficiencies, errors, accidents or fraud. A lock at the server room might for example keep out unauthorized personnel which might switch it off. Separation of duties makes sure that no one single person can manage the whole booking and ordering cycle.

Detective controls are built to check on past business transactions and assesses their adequacy. The bank reconciliation at the end of each month should detect money outflows without legitimation. With the progress in IT the ERP system plays a crucial part in the internal control system. Therefore one distinguishes between automated and manual controls (both preventive and detective). Automated controls include the check whether purchase order and related invoice have the same amount and otherwise give a warning. The change-log of the ERP system records all transactions including the time and logged-in individual. False bookings can thus easily be tied to an individual with a password. In the following some internal controls are presented and categorized.



- Daily cash counts of petty cash by a person supervising the cash clerk. (**manual-detective**)
- The creditworthiness of customers and their responding credit limit is defined by accounting/finance and cannot be changed by sales managers. (**automated-preventive**)
- Effective planning/budgeting processes create transparencies about efficiencies and provide a basis for control. (**manual-preventive**)
- Purchasing limits for different employees and written approvals by their supervisors prevent inefficient and illegitimate purchases. (**automated/manual–preventive**)

- Specific policies for business process descriptions (including control activities) provide guidance and security for all employees. (**manual-preventive**)
- Comparison of reported results with plans and budgets. (**manual-detective**)
- Reconciliation of cycle inventory counts with perpetual records. **(manual-detective)**

However, there are limits to internal controls. On the one hand, most controls can be circumvented or overcome with some criminal energy. This is especially the case, if several individuals collude to circumvent controls. On the other hand, control activities require time and management attention and ultimately come at a cost which is only partly compensated by growing efficiencies and reduced errors and fraud.

7.6 Risk Governance

Risk governance as part of corporate governance is a comprehensive approach for decision making processes associated with strategic, operational and environmental risks in line with stakeholders' expectations.

Governance refers to the actions, procedures, and structures by which power is exercised and decisions are taken and executed. Risk governance applies the codes of good and reflected governance to the risk strategy, the management and communication of risks and the assurance of the effectiveness of the risk management through internal audits.

Since risk taking forms part of the entrepreneurial core of enterprise decision making, stakeholders claim the right to be involved and effectively informed about the risks a company is taking. Relevant stakeholders might be shareholder, bondholders, suppliers, customers and employees, as well as the direct neighborhood and communities in which the enterprise operates.

Good corporate governance strives to ensure that a company's strategy is in line with the risk appetite of its stakeholders. The strategy of a company is developed by management against a backdrop of risks and opportunities. Any strategic choice implies strategic risks. The stakeholders and their representatives on the board of directors or supervisory board can only assess the impact of strategic decisions if they have a fair view on the risk exposure entailed. Aligning management with stakeholders' risk perception and building an informed decision and learning process concerning corporate risks builds mutual trust. The risk strategy is to be defined by the board of

directors and depicts the paths for ensuring effective risk management is part of leadership and decision making on all levels.

Effective risk communication is a cultural challenge for many companies. It starts with informal communication about risks on an operational and strategic level. The awareness and open discussion of risks and opportunities needs to become a daily routine. Formal risk workshops can help identify operational and strategic risks. A special type of risk arises from project businesses (e.g. large tool machines, power plants, etc.): They are subject to commercial and technical risks which need to be assessed for each project. Before a big project is accepted, the individual risks need to be formally assessed by a standardized risk list. This risk assessment might serve as an attention director for project management throughout the project execution phase.

The effectiveness of risk communication might depend on circumstances. On an operational level, a risk scorecard might be useful with a traffic light system. Key risk indicators (KRIs) could be developed to match the KPIs of a Balanced Scorecard or other management control system. Operational performance dashboards might be enriched by selective risk indicators.

An aggregated risk (and opportunity) list could be a good communication tool for intercompany communication like subsidiary-headquarter communication. External **risk reporting** as part of the annual report or sustainability report offers stakeholders access to the company's risk profile.

Internal auditing plays a crucial role in the risk governance by testing and reporting on the effectiveness of the enterprise risk management system on all company levels. It should, however, not manage the enterprise risk management system, but rather test its effectiveness. The risk management should be performed on the operational level. The internal auditing function should concentrate on monitoring the existing risk management.

In many companies, the head of internal auditing is at the same time the Chief Risk Officer or Chief Compliance Officer. There is an apparent conflict of interest here, since the internal auditing department has the role to prove the effectiveness of the risk and compliance management system.

7.7 Conclusion

Enterprise Risk Management acknowledges the fact that business is performed against a backdrop of uncertainty and is becoming more and more important in current business practice. The management accountant can play an active part in risk management in the strategic or operational performance loops. The biggest challenge and opportunity for risk management beyond the adoption of the presented techniques is the implied cultural change to put risk management at the heart of performance management.

Further readings:

Classics:

Banks, Erik (2012): *Risk Culture*

Blyth, Michael (2008): *Risk and security management* (ISBN: 978-0-470-37305-7)

Borgehsi / Gaudenzi (2013): *Risk management- how to assess, transfer and communicate critical risks* (ISBN: 978-88-470-2531-8)

Frigo & Anderson (2009). *A Strategic Framework for Governance, Risk, and Compliance.* Strategic Finance, 90(8), 20-61.

Mikes/ Kaplan (2012): *Managing Risks: A New Framework* (published in HBR) https://hbr.org/2012/06/managing-risks-a-new-framework

OECD (2014): *Risk Management and Corporate Governance* http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf

Rothschild, M., & Stiglitz, J. E. (1970). *Increasing Risk: I. A Definition*. Journal of Economic Theory, 2(3), 225.

Scandizzo, S. (2005). *Risk Mapping and Key Risk Indicators in Operational Risk Management*. Economic Notes, 34(2), 231-256

Current research:

Lundqvist, S. A. (2014). *An Exploratory Study of Enterprise Risk Management: Pillars of ERM*. Journal Of Accounting, Auditing & Finance, 29(3), 393-429

Maguire, S., & Hardy, C. (2013): *Organizing Processes and the construction of Risk: A Discursive Approach*. Academy of Management Journal, 56 (1), 231-255

Shad, M. K., & Fong-Woon, L. (2015). *A Conceptual Framework for Enterprise Risk Management performance measure through Economic Value Added*. Global Business & Management Research, 7(2), 1-11.

Tadewald, J. (2014). *GRC Integration: A Conceptual Foundation Model for Success.* Management Accounting Quarterly, 15(3), 10-18.

Current Business Application:

Accenture: BASEL III Handbook
http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Basel-III-Handbook.pdf

Harvard Business Review (2015): How to Live with Risks (published in HBR)
https://hbr.org/2015/07/how-to-live-with-risks

McKinsey & Company: Risk Management
http://www.mckinsey.com/insights/risk_management

Taleb/ Goldstein/ Spitznagel (2009): The Six Mistakes Executives Make in Risk Management (published in HBR)
https://hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management

Videos:

ASQ: *Enterprise Risk Management at LEGO*
https://www.youtube.com/watch?v=PWKLjxuinG4

Multiple Choice questions (please mark all applicable)**:**

1. The rationale for adopting enterprise risk management is based on an uncertain future and ever-changing market conditions
   a) Yes
   b) No

2. Enterprise risk management can have an influence on:
   a) The value creation of a company
   b) Manage uncertainties
   c) Protecting managers from claims of shareholders
   d) All of the above

3. Risk culture includes the following within an entity
   a) The awareness of risk on all organisational levels
   b) The willingness of management to participate in risky activities
   c) The delegation of responsibility for risk away from Board of Executives

4. Risks are part of everyday activities of business
   a) Incorrect
   b) Correct

5. Strategic Risks can be abolished by making use of Internal Control Systems
   a) Correct
   b) Incorrect

6. What could be an example of an Operational Risk?
   a) The Head of Controlling leaves the company without instructing his successor on procedures and deadlines
   b) The Innovation introduced to the market is said to harm the environment
   c) The target cost decided upon for Product G cannot be met by Production due to its location in a high-cost country

7. Companies can actively influence all three areas of risk (Operational, Strategic, External)?
   a) Correct
   b) Incorrect

8. Increasing social media activities also increase the needs for companies to take care of Risk Management
   a) Correct
   b) Incorrect

9. Companies can lower their exposure to risks by means of the following:
   a) Hedging of Exchange Rates
   b) Factoring of receivables
   c) Entering International Market because this will lower the dependence of the Home market
   d) None of the above

10. Internal Control activities belongs to Accepting risks and making sure they are monitored:
    a) Yes
    b) No

11. Risk Management is a part of the GRC (Governance, Risk and Compliance) Framework:
    a) Incorrect
    b) Correct

12. Internal Auditing is about identifying meaningful KRI:
    a) Yes
    b) No

13. Leakage of Information is an example for a:
    a) Operational Risk

b) Strategic Risk
c) External Risk

14. What is a useful tool for managing external risks?
    a) Guidelines
    b) Consultancy services
    c) Insurances

Answer sheet:

Question	Correct Answer
1	B
2	D
3	A&B
4	B
5	B
6	A
7	A
8	A (As they offer direct contact methods for affected people →Shitstorms
9	A&B
10	A
11	B
12	B
13	A
14	C

Additional Assignment:

- Please prepare a risk map for Albert's Nursery and state how he can actively manage these
- Go to an Annual Report of a DAX30 member of your choice and analyse how they address the area of Risk Management
- Please Draw a Risk Map of you finishing your study program and also come up with a list of countermeasures
- Please comment on the following: Risk Management is becoming more and more important due to more globalisation, higher information transparency and information networks.