Risk-based Planning and Control Systems: Integration of different risk types into strategic, financial and operational management systems

Peter Göstl, Walter S.A. Schwaiger*

Institute of Management Science
Vienna University of Technology / TU Wien

Vienna, August 2016

Abstract

Given that uncertainty is inevitably present as the context for all managerial work and decision-making, the consequences of living in such an uncertain world deserve to be given more attention in our research and literature. In particular, how do control systems function when one essential condition for cybernetic control is the existence of an adequate predictive model? (Otley, 2012, p. 260). To answer this question the risk type categorization of Mikes/Kaplan (2014) as well as the distinction between strategic, financial and operational management systems is taken to identify the adequate risk information and to integrate it into the risk-based predictive models of the three management domains. The proposed risk-based planning and control systems are constructed in line with Bisbe's et al. (2007) conceptual specification process. Accordingly they should provide a solid starting basis for maturity analyses of the enterprise risk management system as well as risk-profile contingent performance analyses.

Keywords: Risk-based planning and control systems, Enterprise risk management, Contingency framework

---

* Corresponding author:

Vienna University of Technology, Institute of Management Science – Accounting, Finance and Management Control Group

A-1040 Vienna, Theresianumgasse 27

Phone: +43.1.58801.33081, Fax: +43.1.58801.33098, http://www.imw.tuwien.ac.at/fc , email: walter.schwaiger@tuwien.ac.at

Table of Contents

Introduction

So what else happened in the last decade? Perhaps the single most important emerging issue has been that of risk management, and the realization by management control researchers that it has been a neglected aspect of study. The topic was first conceptualised for us by Simons (1995) in his idea of boundary systems, although his emphasis remained on strategy implementation. (Otley, 2012, p. 251). … Given that uncertainty is inevitably present as the context for all managerial work and decision-making, the consequences of living in such an uncertain world deserve to be given more attention in our research and literature. In particular, how do control systems function when one essential condition for cybernetic control is the existence of an adequate predictive model? (Otley, 2012, p. 260).

The question concerning adequate predictive models in uncertain business environments highlights the research gap and it constitutes the primary research question of this paper. Otley starts investigating by distinguishing among "uncertainties which cannot be eliminated" in the sense of Taleb's Black Swan concept (Taleb 2008) and "internal uncertainties", which are related to the peculiarities of controlling people that follow their self-interest. A similar categorization is used by Mikes/Kaplan (2014, p. 26-27) who distinguish three types of risk events:

- *Preventable (Category I) risks arise from routine operational breakdowns or from employees' unauthorized, illegal, unethical, incorrect, or inappropriate actions. Companies gain nothing by tolerating such risks; they are inherently undesirable.*
- *In contrast, organizations voluntarily take on strategy execution (Category II) risks in order to generate superior returns... Managers can influence both the likelihood and the impact of their strategy execution risks, but some residual strategy risk will always remain.*
- *External (Category III) risks arise from events that the company cannot influence... Managers are often unaware of these external risks and, even when made aware, are unable to plausibly assess their likelihood. But that should not be the control objective for this category of risk. As external risks are, by definition, unavoidable and impossible to predict, the concern should be with the organization's resilience, should they occur.*

Due to the different nature of the three risk event types Mikes/Kaplan (2014, p. 30) suggest type specific risk management system designs: *We propose that risk management will be most effective when it matches the inherent nature and controllability of the different types of risk the organization faces. Our conclusion is that effective risk management "depends"; it is contingent on the organization's context and circumstances. We can offer preliminary ideas about what risk management likely depends on.*

Mikes/Kaplan's contingent risk management construction gives important insights, but it does not answer the research question, as the predictive models in the cybernetic management systems are not specified. To progress into that direction an additional distinction is introduced. In most enterprises management systems exist at the strategic, financial and operational level.

These three management domains are clearly distinct due to different characteristics of the corresponding risks.

In order to illustrate these differences a 1-person enterprise is chosen. In such an enterprise there are no conflicting interests so that the different risk natures can clearly be seen. In the operational management domain the operational processes are planned and controlled. The risks inherent in the process domain mainly fall into category I, i.e. preventable risks. In the 1-person enterprise the operational manager has to understand the undesirable nature of this risk type (e.g. breakdown of a machinery) and she should try to eliminate these risks as much as possible. In the financial performance management domain the same person – now in its role as financial manager – has to understand the characteristics of the category II, i.e. the strategy execution risks. Such risks have to be taken in order to generate superior returns. Furthermore these risks are – in contrast to the preventable risks – associated with corresponding chances (e.g. the demand for the produced good can decrease or increase). Consequently, the elimination of the strategy execution risks eliminates the corresponding chances as well as potential superior returns. At the strategic management level a long term perspective and a competition orientation are prevailing. In the strategic domain the same person in the 1-person enterprise has to understand the peculiarity of the category III, i.e. the external risks. These risks are connected with chances, like the strategy execution risks are. But in contrast to them the likelihood of external risks normally cannot be influenced by the senior management. Furthermore their likelihood often cannot be plausibly quantified. The management of an external risk does not lie in its elimination. The main focus in the mitigation of external risks lies in the cushioning of their negative as well as the fostering of their positive consequences for the case of their realizations.

This “risk understanding diversity” – demonstrated for simplicity in a 1-person enterprise – is crucial for identifying the relevant risk information needed in the operational, financial and strategic management domains. After having specified the relevant risk information it has to be integrated into the different planning and control systems.

In this paper the different planning and control systems are specified according to the generic structure of the cybernetic control model introduced by Otley/Berry (1980, p. 236). The recursive nature of this generic structure allows refinements in different directions so that it can be used for defining planning and control systems, i.e. “management systems” for the different management domains. An important and often overseen component of such systems is the predictive model for the controlled process. … *having compared actual and desired outcomes and generated a mis-match signal by noting any discrepancy between the two, a control action has to be determined. This requires a predictive model of the process being controlled, that is, a means of forecasting the likely outcomes of various alternatives courses of action. To the extent that such a model is non-existent or defective, than control is impossible and attempted control actions may well be counter-productive. It is noteworthy that many elementary descriptions of control processes completely omit the central position of predictive models…* (Otley/Berry 1980, p. 236).

As mentioned at the beginning the primary research objective of this paper lies in the conceptualization of adequate predictive models for the different management systems in an uncertain business environment. At this point it is important to clarify the meaning of uncertainty. Almost a century ago Frank Knight and John M. Keynes deeply discussed the distinction between risk and uncertainty. In this paper the term "uncertainty" is taken literally in the sense of "not being certain". Consequently predictive models are investigated which do not have a deterministic, but a stochastic nature. In risk-based predictive models the "un-certainty" inherent in the future development of the underlying systems of the different management domains is explicitly taken into account. In the operational management domain mainly (de-)fault events characterize the uncertainty of the underlying operational systems (e.g. breakdown event). Such events are seen as "pure risks" as they do not include chances. In the financial and strategic management domains "speculative risks" are important which include risk events as well as chance events (e.g. changing foreign exchange rates or changing competition). The speculative risks are adequate as they represent the combined risk/chance thinking applied in the financial and strategic management domains to characterize the uncertainty of the underlying business environment.

The risk-based predictive models for the different management domains will be based on pure and speculative risk definitions for adequately characterizing the corresponding environmental uncertainties. Consequently these models internalize the environmental uncertainties into the planning and control activities of the management systems in the operational, financial and strategic management domains and hence establish risk-based management systems. At the strategic level the limited controllability of the external risk type plays an essential role in the specification of the risk-based predictive models. Finally the control strategies implemented in the different models are based upon the risk type specific understandings and desirabilities of the prevailing uncertainties.

The adequate specification of the risk-based management systems answers the primary research question of this paper. In order to demonstrate the usefulness of these specifications also the "risk management (information) system" and the "risk-based corporate governance" are investigated. The integration of the two additional concepts with the risk-based management systems gives the comprehensive perspective over the entire "enterprise risk management system". The usefulness of this comprehensive system definition will be demonstrated by its potential application for ERM (enterprise risk management) maturity analyses as well as risk profile contingent MCS (management control systems) performance analyses.

The paper is organized as follows: Following this introduction the risk-based management systems in the operational, financial and strategic management domains are derived by identifying risk-based predictive models based on pure and speculative risks. In the following section risk management (information) systems are constructed as generator and provider of the risk information. Subsequently the risk-based corporate governance is specified. In the final section the paper is concluded and the usefulness of the enterprise risk management system is demonstrated by addressing its applicability for ERM maturity analyses and risk profile contingent MCS.

Risk-based Management Systems: Integration of Risk Information

Loosely defining, in risk-based management systems the planning and control activities are based on risk considerations. In this sense the statistical quality control model introduced by Shewhart (1980) in the 30-ies of the last century is one of the first examples for such a system. In statistical quality control the actual quality levels of the produced goods are measured, recorded on a scorecard and analyzed against preset quality criteria. As the quality criteria are limit-quantiles of the assumed quality level distribution the quality control model is based on statistics. Furthermore the statistical quality control model is a cybernetic control model, where the planning and control activities constitute the plan and the check and act activities in the PDCA (plan – do – check – act) cycle. The PDCA cycle is the core element of all quality management systems developed since then in the different quality management frameworks.

The control mechanism in the statistical quality control model primarily relates to systemic learning (see Otley/Berry 1980, p. 237) as the mis-match signal in form of significant quality outliers induces as response action the change of the controlled production process (systemic learning). By reflecting the assumptions and comparing them with the empirical evidence also first-order controls (changing inputs), second-order controls (amending objectives) and internal learning (amending the process model) can be initiated. The predictive process model is amended, if all other control adjustments are not able to eliminate the observed mis-match signals. In this case the predictive control model does not work so that it has to be replaced by an improved model that works.

The statistical quality control model shows the pure risk nature of the uncertainty in the operational environment. In operating systems there exist predominantly events with negative impacts on the achievement of the targeted objectives, i.e. risk events. In many constellations chance events are even not possible like in the quality management domain. Delivering a better quality than the targeted one is not the objective of the quality manager.

A drawback of the statistical quality control model is its focus on incurred risk events. Due to this focus it is a reactive management system, which reacts when risk events realize. Furthermore the risk events are not even identified. In the pharmaceutical industry these drawbacks were eliminated when the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH 2005) issued the Q9 Guideline on Quality Risk Management (ICH 2005). This guideline characterizes the transition from the reactive quality management to the proactive quality risk management by requiring the pharmaceutical enterprises to manage potential quality related risk events according to their likelihood and impact. The direct specification of pure risks – which have negative impacts on the achievement of the pharmaceuticals' quality objective – and the assessment of their likelihoods and impacts give the risk information that allows proactive risk mitigation actions. As the pure risks are of a preventable risk type they should be eliminated as much as possible.

The proactive ICH quality risk management system includes important ingredients of a risk-based management system within the operational management domain: Firstly, performance objectives are set in the planning activity, secondly, the uncertainty of the underlying operational system is understood in form of pure risk events with negative impacts onto the objectives, and thirdly, there is a risk strategy that proactively triggers the specified control activities depending on the measured event risk characteristics, i.e. likelihoods and impacts.

Seen from the management control perspective the risk strategy is a risk-based predictive control model that specifies the control rules according to which risk level contingent control actions are selected and executed. Due to the comparison of the actual risk level with the preset risk limit the quality risk management system is a risk limit system with the objective of keeping the risk over time within its limit. Next to the risk limit construction risk-based management systems can be contracted alternatively by using risk measures as indicators in performance management systems. In reliability-based performance management systems, e.g., the reliability, i.e. the probability of the functioning of an operational system serves as key performance indicator. Over time the actual reliability is measured and compared with the targeted reliability level. According to the size of the mis-match signal control actions are taken (e.g. maintenance activities) in order to bring the system's reliability back to the desired level. In the management control perspective the reliability (control) strategy determining the mis-match signal contingent control actions constitutes a risk-based predictive control model.

Bisbe et al. (2007) address the risk of conceptual misspecifications within the conceptual specification processes. Misspecifications are avoided by precisely defining the investigated constructs and by defining the nature and directions of the epistemic relationships in the defined constructs. As a risk-based management system is not directly observable it constitutes a "dimension" which gets concretized by measurable "indicators". According to the properties prevailing in the ICH quality risk and the reliability performance management system three indicators are selected to define of a risk-based management system more precisely, i.e.

1) Objectives and risk (control) strategies (predictive control models),
2) Probabilistic risk understanding
3) Risk management functions, e.g. risk identification, assessment and control.

Risk-based management systems are understood to be manifested through these three indicators. Hence the epistemic relationship between the dimension and its indicators specifies a "reflective model". In future research it is expected that consensus will be reached and a "formative model" will be developed. In this case risk-based management systems will – like e.g. the Balances Scorecard construct (Kaplan/Norton, 1996) – be defined by a set of constitutive, instead of manifesting indicators.

In the operational management domain the uncertainty of the underlying system is mainly related to (technical) failures, i.e. faults and defaults in its operational processes. Furthermore the people involved in the processes might not operate as they should. This can happen by accident or consciously. The second case is connected to Otley's (2012) internal uncertainties which are

related to the difficulties of controlling people with "special" self-interests. In the probabilistic risk perspective such internal uncertainties are seen as fraud risk events which are controlled within compliance (risk) management systems. According to the given definition such a system is risk-based, if 1) compliance objectives (e.g. being compliant with related laws and regulations) and compliance risk strategies (e.g. adequate internal controls are established, if the likelihood of the fraud risk event exceeds a critical level) are set, 2) the compliance risks are seen as probabilistic events and 3) compliance risk management functions (e.g. identification, assessment and elimination of compliance risk events) are established.

Concerning the risk understanding there is a big difference between the operational domain on the one side and the financial and strategic management domains on the other side. As already noticed, in the operational domain the pure risks and in the financial and strategic domains the speculative risks are essential characteristics of the uncertain environment. The speculative risks are combined risk/chance events. This means that "twin" events are considered which have two possible realizations and where the risk events have a negative and the chance events have a positive impact on the targeted objectives. In the financial domain the speculative risks are mainly of a strategy execution risk type so that they are controllable with respect to their likelihoods as well as their impacts. This allows a fine tuning control strategy to achieve the targeted chance/risk profile.

In the financial domain risk-based management systems can be constructed like in the operational system by either setting up risk limit systems or risk-based performance management systems. In risk limit systems risk is usually defined in terms of statistical properties of a random variable that describes the stochastic behavior of the underlying system. E.g., the value at risk (see Hull 2012) of a risky asset is the potential loss that is exceeded with a given loss probability and with the complementary probability the value at risk will not be reached. Consequently the value at risk is a risk limit. This limit is used in the risk limit systems to derive mis-match signals if the actual value at risk is greater than the limit. Depending on the size of the mis-match signal the stock position is reduced in order to bring the risky asset's risk below the preset risk limit. The value at risk measure can also be used as risk indicator in a performance management system. In this situation the value at risk is the targeted objective to be achieved over time. Like in the risk limit system the comparison between actual and targeted value at risk delivers the mis-match signal. But in the performance management system the value at risk control strategy is not restricted to reducing the risk level. In contrast to the risk limit system more risk is taken by additional investments into the risky asset if the actual is lower than the targeted value at risk. Both management systems use risk-based control strategy as the underlying value at risk measure is a probabilistic risk measure.

One of the first risk-based management systems in the financial domain can be traced back to Jaedicke/Robichek (1964) who introduced the probabilistic CVP (cost volume profit) analysis. This analysis is built upon a revenue and cost model which is mainly driven by stochastic sales volumes. The profit inherits the stochastic properties of the sales volumes via the revenue and cost model. Within the CVP framework objectives for the profit as well as control strategies

e.g. with respect to the sales volume can be defined to establish a risk-based management system. The original version of the CVP analysis relates to a single product and a single period. By including the Markowitz (1952) portfolio selection approach the control model can be extended for being applied in a multi-product context. The extension to a multi-period context is possible by including the option pricing theory from Black/Scholes (1973). The resulting risk-based predictive control can be used for constructing either a (dynamic) risk limit system or a risk-based performance management system.

Nowhere is this more apparent than in the processes of evaluating managerial performance, because unexpected events can result in performance that is significantly better or worse than might have been expected in advance. In other words, delivered managerial performance can be a consequence of managerial effort, ability skill and judgement but, in the presence of uncertainty may be primarily attributable to "luck". This effect has always been present in the attempt to distinguish between managerial and unit economic performance, but becomes acute in the presence of significant uncertainty. (Otley 2014, p. 91). Otley's "luck effect" is a severe topic in the financial management domain due to the importance of speculative risks in this domain. It is to be expected that the luck effect can be solved by constructing a risk-based predictive CVP control model that adequately reflects the firm's context including its uncertain business environment. With such a model the causes of the profits are modeled so that significant over- or underperformance should become explainable by tracing it back to its statistical roots.

In the strategic management domain the speculative risks are mainly of an external risk type which can only be controlled with respect to their impacts. Consequently a fine tuning possibility is limited. Due to the mostly huge and often existential impacts of such risk events resilience enhancing control strategies are advised. I.e., adequate operational provisions have to be established which can be executed when the external risk events realize. Furthermore the strategic domain distinguishes from the financial domain by having a broadened perspective onto the uncertain business environment via including a long-term view, market competition considerations and further environmental uncertainties (e.g. disruptive technologies).

In the 60-ies of the last century Ansoff (1965) established a framework for deriving business policies for growth and expansions based on two perspectives, i.e. product and market. Risk and chance considerations were considered at that time via the SWOT (strength, weakness, opportunity, thread) analysis. In the SWOT analysis the firms' internal capabilities are considered in form of strength and weaknesses and they are compared to the external uncertainties in form of opportunities and threads. Porter (1979) integrated an adequately aligned SWOT analysis version in his 5-forces model developed for the analysis of the competition within industries. According to this model the long-run profitability of an industry results from the competition driven by the 5 forces (sources), i.e.

- Industry rivalry
- Threat of substitutes

- Bargaining power of buyers
- Bargaining power of suppliers
- Thread of new entrants.

Knowledge of these underlying sources of competitive pressure provides the groundwork for a strategic agenda of action. They highlight the critical strengths and weaknesses of the company, animate the positioning of the company in its industry, clarify the areas where strategic changes may yield the greatest payoff, and highlight the places where industry trends promise to hold the greatest significance as either opportunities or threats. Understanding these sources also proves to be of help in considering areas for diversification. (Porter, 1979, p. 138).

Based on the 5-forces model Porter investigated predictive control strategies for achieving sustainable competitive advantages by *jockeying for positions among current competitors* (Porter 1979, p. 141). In his book *Competitive Strategy* Porter (1980) refined the control model by distinguishing between cost leadership, differentiation and focus strategies and elaborating on contextual preconditions for their beneficial pursuance.

In the 80-ties and 90-ties of the last century scenario many industries were deregulated (e.g. the Glass Steagal Act separating the commercial and investment banking business and established in 1933 as a consequence of the banking crisis was abolished) so that new market conditions arose. Furthermore the rapid developments information technology and the growing globalization generated new business possibilities. The handling of the increased complexity, the new risks and the insights of limited controllability required new concepts and methodologies.

The scenario planning model methodologically founded by Schoemaker (1993) is a good example of how the limited human knowledge can be extended to handle such complex business environments. *In short, scenario planning attempts to capture the richness and range of possibilities, stimulating decision making to consider changes they would otherwise ignore. At the same time, it organizes those possibilities into narratives that are easier to grasp and use than great volumes of data. Above all, however, scenarios are aimed at challenging the prevailing mind-set. Hence, scenario planning differs from the three aforementioned techniques* (i.e. contingency planning, sensitivity analysis, computer simulations) *in its epistemic level of analysis.* (Schoemaker 1995, p. 27).

Shoemaker's scenario planning methodology consists of 10 steps. By following this iterative procedure among others key uncertainties and multiple scenarios are used to identify strategically relevant topics and to evolve towards decision scenarios which serve to test the proposed strategies and to generate new ideas. The narrative fashion of this methodology makes it more intuitive and accessible to the involved people. As such it allows a coherent discussion in the strategy formulation process in a team consisting of differently minded and educated persons. This diversity is especially helpful for identifying blind spots.

Consequently the scenario planning is able to address the increased complexity, the new risks and the insights of limited controllability in today's business environment. The limited control aspect relates to external risks. By incorporating them into the strategy formulation process one of the essential characteristics of the strategic business environment becomes explicitly considered. In this case a risk-based scenario planning tool emerges which also integrates potential future events that cannot be (fully) controlled into the corporate objectives and control strategies. Although the likelihood of the external risk event per definition cannot be influenced, its qualitative assessment can serve as an early warning indicator in the strategic management domain.

Risk Management (Information) Systems: Generation of Valid Risk Information

For their well-functioning the risk-based management systems presented so far need to have adequate risk information. In such a system a probabilistic risk information is used in the planning and control activities. The risk information depends on the nature of the risks. A pure risk has a likelihood of occurrence and a negative impact. A speculative risk also has a likelihood of occurrence. But the occurrence can be either a risk or a chance event. In the first case the impact is negative and in the second case it is positive. Furthermore the risk control strategy depends on the controllability of the risk types which is management domain specific. In the operational management domain pure risks (e.g. fault, default and fraud risk events) and in the financial and strategic domains speculative risks are predominant. The risk control strategies depend on the type and the controllability of the pure and speculative risks. The control model in the operational domain for the pure risks – which are of the preventable risk type – consists in their elimination. The speculative risks in the financial domain are of a strategy execution type and hence are controllable with respect to their likelihood and their impact. The external risks in the strategic domain are mostly of speculative nature and only controllable with respect their impacts. This advises risk control strategies that enhance the resilience of the enterprise. As the risk information is of a probabilistic nature the domain specific control models are predictive.

The risk information is generated in the risk management system. Such systems are required from capital market oriented enterprises by different laws (e.g. IFRS (international financial reporting standards) requirements and European Community directive on statutory audits (Auditing Directive: AD 2006). In order to fulfill the legal requirements the enterprises have to base their risk management systems on established standards.

An often used standard is the ISO 31000:2009 Risk Management Standard issued by the International Standards Organization (ISO 2009). In this standard risk management is defined via two parts, i.e. the risk management framework and the risk management process. *The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels.*

The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels. (ISO 2009, p. 8f).

The risk management framework consists of the five necessary components (ISO 2009, p. 8f):

- Mandate and commitment (by management and at all levels)
- Design of framework for managing risk
- Implementing risk management (via risk management process)
- Monitoring and review of the framework
- Continual improvement of the framework

The risk management framework is mandated and committed by the management to achieve commitments at all levels. The design, monitoring and improvement components relate to the Plan, Check and Act activities in the PDCA-cycle that conceptually underlies the risk management system. The implemented risk management process consists of the operationally performed Do activities in the PDCA-cycle. The risk management process consists of the five activities (ISO 2009, p. 13f)

- Communication and consultation
- Establishing the context
- Risk assessment: Risk identification, analysis and evaluation
- Risk treatment
- Monitoring and review.

The risk management framework in the ISO risk management constitutes a cybernetic control model with respect to the risk management process. I.e., the risk management process is managed itself according to a closed loop control cycle. The mis-match signal for the process effectiveness results by comparing the actual process performance measured in the monitoring and review component with the performance objective set in the design component. The mis-match contingent control action is executed in the improvement component.

The closed loop control model describes the components and activities in the ISO risk management. These operational elements of the risk management generate the risk information needed in the different management systems. *Risk management is an integral part of all organizational processes: Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes. … Risk management is part of decision making: Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action. … Risk management explicitly*

addresses uncertainty: Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed. (ISO 2009, p. 7).

Although the importance of the risk information generated in the risk management is expressed in the principles just cited the ISO risk management is not precise on the adequacy of the generated risk information. Concerning adequate risk information it is important to notice that the adequacy not only relates to the risk nature, i.e. pure vs. speculative nature. At the same importance is the quality of the delivered risk information, i.e. the risk information's validity.

Due to the probabilistic nature of the risk information its validity is related to the forecasting accuracy. In the statistical sense, the risk information concerning the likelihood – the same holds for a stochastic impact – is accurate if the percentage of the realizations of the random event closely equals its likelihood (probability). This validation concept is based on the statistical law of large number. It underlies e.g. the credit risk provisioning in the banking industry according to the requirements of the Basel Committee of Banking Supervision (BCBS 2011) which has been translated into European law via the Capital Requirements Directive (CAD IV 2013) and the Capital Requirements Regulation (CRR 2013).

The statistical validation concept is adequate for the risks prevailing in the operational and the financial domain. In the strategic domain it does not make sense as the likelihoods of external events are not meaningfully measurable. But this validation problem does not mean that the likelihoods are always meaningless at all. Not precisely determinable and not controllable likelihoods can serve on a qualitative scale as an early warning indicator for changing external risks. In this function the qualitative risk information can signal shifts in the environmental uncertainties in the strategic domain. If, e.g. the likelihood of a disruptive technology event is perceived to increase corresponding control actions should be considered more severely and/or urgently.

The combined view onto the processes and risk information in the risk management system is at the core of the information systems engineering discipline. According to this view this chapter was titled "Risk Management (Information) Systems". The term Information in parentheses indicates the informational aspect in the risk management system. The combined view is important for establishing software applications that adequately support the different activities in the risk management process and framework as well as the management activities in the different risk-based management systems. In this context an adequate support means that the risk nature specific risk information is delivered in a good quality and timely before the planning and control activities have to be set.

The information systems engineering perspective onto a risk management (information) system shows its operational functions and related informational requirements. Consequently the risk management functions and the supporting risk management information system are good indicators for defining the construct of a risk management (information) system. Finally it has to be noted that risk management (information) systems are not brought automatically to live in an enterprise. In order to establish a living system training activities have to be installed. Taking

this aspect the third indicator is identified. Summing up, a reflective model of a risk management (information) system can be defined by the three manifesting indicators, i.e.

1) Risk management functions
2) Supporting risk management information system
3) Risk management training.

Risk-based Corporate Governance: COSO ERM Framework

The principles of the ISO risk management (ISO 2009, p. 7) require that *risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes* and that it is *part of decision making: Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.* This broad anchoring of the ISO risk management into the different management domains can be conceptualized by the risk-based management systems for the strategic, financial and operational management domains.

Mikes (2009, p. 26) investigated similar constructs by searching for ideal types of enterprise risk management. In her study Mikes distinguished among the four ideal ERM types, i.e.

- Risk silo management driven by bank capital adequacy
- Integrated risk management driven by rating agency expectations on capital adequacy
- Risk-based management driven by shareholder value imperative
- Holistic risk management driven by risk-based (internal) control systems.

The holistic risk management is according to Mikes connected to the Anglo-Saxon and German corporate governance. It includes also non-quantifiable risk, provides the senior management with strategic view of risks and it uses among others scenario analysis and sensitivity analyses. These characteristics and the connection to the corporate governance pave the way for considering the risk-based management systems and the supporting management (information) system in the light of a risk-based corporate governance.

A well-known framework for a risk-based corporate governance is the ERM model of the Committee of Sponsoring Organizations of the Treadway Commission (COSO 2004). The COSO ERM model (COSO 2004, p. 2) is defined at a high abstraction level as follows: *Enterprise risk management is:*

- *A process, ongoing and flowing through an entity*
- *Effected by people at every level of an organization*
- *Applied in strategy setting*

- *Applied across the enterprise, at every level and unit, and includes taking an entitylevel portfolio view of risk*
- *Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite*
- *Able to provide reasonable assurance to an entity's management and board of directors*
- *Geared to achievement of objectives in one or more separate but overlapping categories*

According to this generic definition the risk management is completely integrated into all operational and managerial processes in the different management domains. Risk information is generated and used in the different domains to achieve the set objectives. For the objectives four types are considered, i.e. strategic, operational, reporting and compliance. Via the reporting objectives the legal requirements for adequate internal control systems for ensuring a reliable reporting are integrable. The compliance objective allows the integration of compliance considerations in all management domains. So Otley's internal uncertainties relate not only to the operational and financial but also strategic management domain. The distinction between strategic and operational objectives is important for incorporating the strategic aspect into the financial and operational domains. E.g., the Balanced Scorecard (Kaplan/Norton 1996) can be used for connecting the strategies formulated at the strategic level with the financial and the operational process as well as the customer and the learning and growth perspectives.

The integration of the adequate risk information into the different management systems is achieved by the objective based definition of risks and chances. Risks are potential events that have a negative impact on the objectives, whereas the potential chance events have a positive impact. With this understanding pure and speculative risks can defined. This risk and change understanding and the corresponding common language give the COSO ERM the flexibility for incorporating the characteristic risk understanding diversity within an enterprise context. The pure risks arising in the operational domain are risk events. The speculative and (only partially) controllable speculative risks in the financial and strategic domains are combinations of risk and change events. Upon this generic understand and language domain specific risk models can be formulated so that everybody in the enterprise can live within his own risk understanding.

Due to the generic nature of the COSO ERM model it allows refinements in different directions. One important refinement is the organizational structure of the enterprise risk management. This aspect is at the core of the 3-LoD (3-Lines of Defense) model that was developed by The Institute of Internal Auditors in order to provide a clear responsibility structure within the enterprise risk management. *Although risk management frameworks can effectively identify the types of risks that modern businesses must control, these frameworks are largely silent about how specific duties should be assigned and coordinated within the organization.* (IIA 2013, p. 1). The 3-LoD model provides a clear organizational structure based on best practices by distinguishing (IIA 2013, p. 3) *among three groups (or lines) involved in effective risk management:*

- *Functions that own and manage risks.*

- *Functions that overseas risks.*
- *Functions that provide independent assurance.*

In the 1st line of defense the risk owners can be the process owners as well as the managers at the strategic, financial and operational level who eliminate the preventable risks, control the strategy execution risks and promote the resilience for the external risks. At this point is has to be mentioned that the resilience aspect is not explicitly mentioned in the COSO ERM. The framework concentrates on potential risk events, whereas in the resilience management the incurred (realized) risk events are considered. In the COSO ERM language the resilience management relates to the mitigation of the impacts of the external events.

In the 2nd line of defense it is the enterprise risk manager function that oversees the risks from an enterprise-wide and a corporate perspective. The enterprise-wide perspective helps establishing consistent risk-based management systems in all domains. The corporate perspective is important for considering all risk within a portfolio view. At the 3rd line of defense the internal audit responsible provide the independent assurance to the audit committee by checking the effectiveness of the implemented enterprise risk management.

The previous considerations are helpful for distilling manifesting indicator for a risk-based corporate governance. Firstly, there have to corporate objectives and corporate (risk) control strategies from with objectives and strategies for the different management domains can be derived in a consistent manner. Secondly, for a consistent integration of the risk understanding diversity in the enterprise context there has to be a common risk communication language. Thirdly, responsibilities for the different functions in the enterprise risk management have to be defined, consistently organized and assigned, e.g. according to the 3-LoD model. Taking these three manifesting indicators the construct of a risk-based corporate management can be defined as a reflective model by

1) Corporate objectives and corporate risk control strategies
2) Risk understanding diversity covered by a common risk communication language
3) Aligned risk management organization.

Having defined the constructs of risk-based management systems, risk management (information) systems and risk-based corporate governance they can be used in the next step to define the construct of an “Enterprise Risk Management System” (ERMS) by taking the three dimensions for the definition of a latent ERMS model. In the ERMS model the comprehensive alignment of the enterprise risk management system can be seen from the top down approach, i.e. from the risk-based governance, over the risk management (information) system to the risk-based management systems.

Conclusion and Further Research

The question concerning adequate models in uncertain business environments was the primary research question of this paper. This question was answered by showing how the diversity of the risk nature, i.e. pure vs. speculative risks as well as the desirability and controllability of the preventable, strategy execution and external risk types have to be integrated into the planning and control activities of risk-based management systems in the strategic, financial and operational domains. The predictive nature of the control models relates to the probabilistic definition of risks and chances in form of potential events that have a negative and a positive impact on the achievement of the set objectives. Depending on the management domain context different risk-based predictive control models were proposed. In the operational and the financial domain risk can be fine tuned either by risk limit systems or by risk-based performance management systems. At the strategic level the fine tuning is not possible according to the uncontrollability of the likelihoods of external risks. Instead of controlling the likelihoods the impacts are mitigated. In the case of negative impacts caused by external risk events the objective of impact mitigation is an increase of the firm's resilience. Due to the conceptual orientation of this research paper empirical evidence was not provided.

The proposed risk-based management systems should be beneficial for top managers, financial and operational managers who have to establish in their domains management systems that adequately integrate the specifics of the risks within their uncertain business environments.

The risk-based management systems elaborated in this paper can be seen as the part of an enterprise risk management system that uses risk information in their planning and control activities. Another part of the enterprise risk management system can be defined as the generator and the provider of risk information. In simple cases the two parts are performed together in a management domain. This constellation corresponds to a silo risk management organization. In more advanced cases different functions of the risk management systems are outsourced and assigned to a special organizational unit, e.g. the risk management unit. In this case competences and skills can be bundled and an enterprise-wide coordination can ensure conceptual and procedural consistencies. In order to align the risk information provider and risk information user functions they have to be integrated within a risk-based corporate governance. The triple of the three parts can be used for defining an enterprise risk management system.

This approach was followed to define the enterprise risk management system (ERMS) as a 3-dimensional construct consisting of three dimensions, i.e. risk-based governance, risk management (information) systems and risk-based management systems. To avoid misspecifications for each dimension three manifesting indicators were specified that build up a latent model for the enterprise risk management system. Hence the resulting ERMS is precisely defined so that it can be operationalized by specifying operational variables that are observable. Such an operationalization could be beneficial for empirical research in two different directions, i.e. in the direction of ERM maturity analyses and the direction of MCS performance analyses.

The maturity analysis literature starts with Humphrey (1988) who investigated the software development process, characterized different process performance attributes and built a process maturity framework thereon. Adequately adjusted maturity analyses can also be established for the enterprise risk management. That adjustments are needed can be seen from the ERMS definition. The ERMS not only consists of processes. The risk management process is just one element in the risk management (information) system dimension. The ERMS definition suggests a 3-dimensional construct to be measured in an ERM maturity analysis. For the risk-based corporate governance dimension and the risk-based management systems dimension process execution related maturity levels are not adequate. Instead different configurations of the two dimensions have to be defined for the different maturity levels. For this purpose the indicators in the two dimensions show beneficial. They can be used to define the different configuration levels from basic over intermediate to advanced. This profile approach for operationalizing the indicators is preferable compared to the aggregate approach due to the complexity of the ERM construct. *A profile approach assumes it is meaningless to algebraically combine the constitutive dimensions of a construct. Instead, it operationalizes constructs as particular combinations of levels of the operational variables that measure its dimensions. In this type of operationalization, each operational variable that measures a dimension is dichotomized or artificially partitioned into discrete levels. Different combinations of these dichotomized operational variables are then used to form various theoretically meaningful profiles of the multidimensional construct.* (Bisbe et al. 2007, p. 816).

Based on Otley's (1980) contingency theory of management accounting many different contingency studies were performed to categorize MCS configurations, specify the fit of the individually observed to the proposed configurations and test the impact of the fit with respect to the MCS performance. An interesting idea would be a contingency analysis of Simons' MCS construction (Simons 1995) based on contingency variables in form of Mikes/Kaplan's risk types. Conceptually this would be an extension of Widener's MCS contingency analysis by using additional contingency variables for the preventable, the strategy execution and the external risk types. For such a risk profile contingent MCS performance analysis the proposed ERMS definition should be beneficial as its indicators could give a solid guideline for specifying the contingency variables and the corresponding survey questions for their operationalizations. A more elaborated extension could be needed if the results of the first extension indicate an inadequacy of Simons' MCS conceptualization and operationalization used by Widener. In this case it seems worthwhile to investigate not a single MCS conceptualization but instead of using a differentiated conceptualization in form of risk-based MCS constructs for the strategic, financial and operational domains.

References

Auditing Directive (AD 2006): Directive 2006/43/EC of the European Parliament and of the Council, Directive on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC

Ansoff I. (1965): Corporate Strategy – An Analytic Approach to Business Policy for Growth and Expansion, McGraw-Hill, 1965

Basel Committee on Banking Supervision (BCBS 2011): Basel III: A global regulatory framework for more resilient banks and banking systems, Bank for International Settlements, Basel

Bisbe J., Batista-Foguet J.-M., Chenhall R. (2007): Defining management accounting constructs: A methodological note on the risks of conceptual misspecification, Accounting, Organizations and Society, Vol. 32, 789-820

Black F./Scholes M. (1973): The Pricing of Options and Corporate Liabilities, The Journal of Political Economy, 81(3), 637-654

Capital Requirements Directive (CRD IV 2013): Directive 2013/36/EU of the European Parliament and of the Council, Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, June 26, 2013

Capital Requirements Regulation (EU) (CRR 2013): Regulation (EU) No. 575/2014 of the European Parliament and of the Council, Regulation on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012, June 26, 2013

Committee of Sponsoring Organizations of the Treadway Commission (COSO 2004): Enterprise risk management framework, American Institute of Certified Public Accountants, New York, NY

Hull, J. (2012): Options, Futures and Other Derivatives, 9th Edition, Boston et al., Prentice Hall

Humphrey W. (1988): Characterizing the Software Process: A Maturity Framework, Software, IEEE, Vol. 5, Issue 2, pp. 73-79

International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH 2005): Quality Risk Management Q9, ICH Harmonised Tripartite Guideline, Current Step 4 version, November 9, 2005

Institute of Internal Auditors (IIA 2013): The three lines of defense in effective risk management and control, IIA Position Paper, Altamonte Springs, Florida, January 2013

International Standards Organization (ISO 2009): Risk Management Principles and Guidelines, International Standards Organization, Geneva

Jaedicke R., Robichek A. (1964): Cost-Volume-Profit Analysis under Conditions of Uncertainty, The Accounting Review, Vol. 39(4), 917-926

Kaplan R./Norton D. (1996): The balanced scorecard – Translating strategy into action, Harvard Business School Press, Boston, Massachusetts

Mikes A. (2009): Risk management and calculative cultures, Management Accounting Research, 20, 18–40

Markowitz H. (1952): Portfolio Selection, Journal of Finance, Vol. 7, 77-91

Mikes A./Kaplan R. (2014): Towards a Contingency Theory of Enterprise Risk Management, Harvard Working Paper, 13-063, January 13, 2014

Otley D. (2014): Management Control under Uncertainty: Thinking about Uncertainty, in: **Otley D./Soin K.**: Management Control and Uncertainty, Palrave Macmillan, London/New York

Otley D. (2012): Performance management under conditions of uncertainty: some valedictory reflections, Pacific Accounting Review, Vol. 24(3), 247-261

Otley D. (1980): The contingency theory of management accounting: Achievement and prognosis, Accounting, Organizations and Society, Vol. 5(4), 413-428

Otley D./Berry A. (1980): Control, Organisation and Accounting, Accounting, Organizations and Society, Vol. 5(2), 231-244

Porter M. (1980): Competitive Strategy – Techniques for Analyzing Industries and Competitors, Free Press, New York

Porter M. (1979): How Competitive Forces Shape Strategy – Awareness of these forces can help a company stake out a position in its industry that is less vulnerable to attack, Harvard Business Review, 1979, 137-145

Shewhart W. (1980): Economic Control of Quality of Manufactured Product, 50th Anniversary Commemorative Reissue, American Society for Quality Control, Milwaukee

Schoemaker P. (1995): Scenario Planning – A Tool for Strategic Thinking, Sloan Management Review, Winter 1995, 25-40

Simons R. (1995): Levers of Control, Harvard Business School Press, Boston

Widener, S. (2007): An empirical analysis of the levers of control framework, Accounting, Organizations and Society 32, 171-185

Taleb N. (2008): The Black Swan, Penguin, New York, NY