

# Transforming risk management

---

In an increasingly volatile and uncertain world, organizational risk management is critical. However, it tends to be perceived as a rather bureaucratic activity with a one-sided focus on known risks. Against this backdrop, we analyze the status quo of corporate risk management and develop a four-step approach to make risk management more effective.

*Utz Schäffer, Florian Storek*

In many large companies, risk management practices have grown organically and reflect the perceived risks and regulatory requirements of the organization's different functions, regions, and businesses. At the same time, sufficient top management attention and a comprehensive top-down approach to risk governance are frequently missing (cf. Gius et al. 2018). As a consequence, risk management tends to be characterized by multiple players, processes, and interfaces. Since the roles and responsibilities of these players are often not sufficiently clarified and aligned, risk identification and assessment activities tend to exist in parallel or are even duplicated, interfaces

are often not clearly defined, and an integrative perspective, the “big picture” of risk management, may be lacking. Controllers often assess the risks and opportunities of a business throughout the internal planning process. In contrast, risk managers evaluate the same risks for external risk reporting – likely with different results. Such a lack of alignment is neither efficient nor effective. It provides a breeding ground for internal politics and a situation where risk-related knowledge is not shared and organizational learning is hampered. To be clear: we are not advocating that risk management should necessarily be centralized or performed by one corporate actor alone. However, we are saying that risk management activities ought to be aligned and comprehensively governed across functions, regions, and businesses.

## Summary

- Within corporate risk management, strategic business risks and external, uncontrollable risks are frequently given insufficient attention.
- To counteract this, the authors have developed a four-step approach to make risk management more effective.
- The authors' approach encompasses mapping risk management activities, establishing clear governance principles, rethinking the role of risk managers, and fostering an appropriate risk culture.

## Risk management often neglects strategic and uncontrollable risks

Preventable risks arising from within the company such as quality, supply chain, and compliance risks are manifold. They can cause substantial damage, offer no strategic benefit, and are often subject to regulatory requirements. Companies, therefore, tend to employ boundaries and formalized processes around standard operating procedures and internal control systems to eliminate or avoid these risks (cf. Kaplan/Mikes

2012). Risk managers, in turn, focus on this type of risk and the respective formalized procedures (cf. Gius et al. 2018; Taleb/Goldstein/Spitznagel 2009). Other risks which require a different approach tend to be neglected, as a recent study of the WHU Controller Panel shows: strategic business risks which companies incur to obtain higher returns and the risk of external shocks such as 9/11 or COVID-19 both receive less management attention than operational and compliance risks (cf. Schäffer/Brückner 2021). In a context of intense competition and volatile, uncertain, complex, and ambiguous environments, such neglect of strategic business risks and external, uncontrollable risks seems far from optimal.

### Managers oftentimes do not act as first line of defense

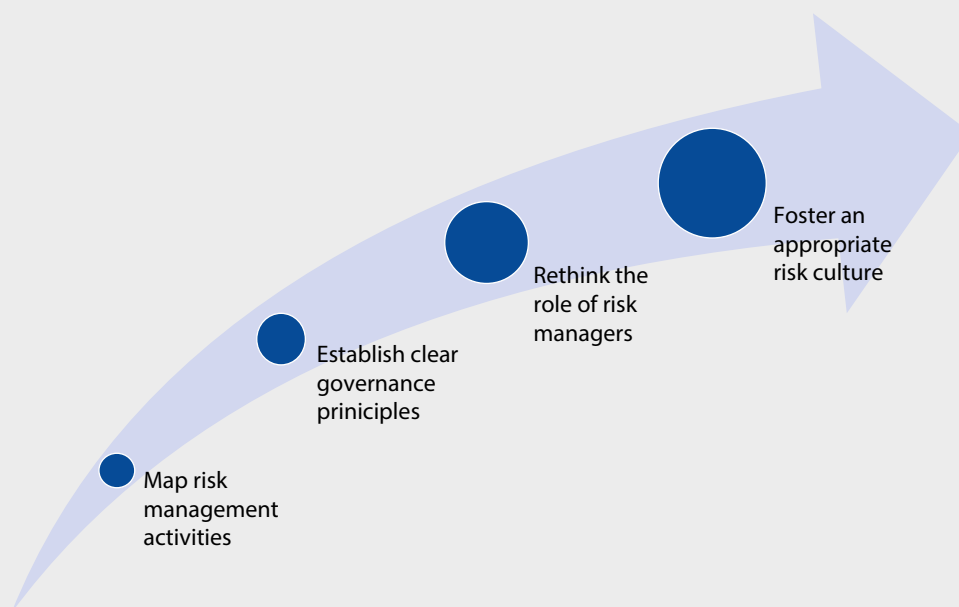
According to the Three Lines of Defense model (Institute of Internal Auditors 2020), managers should be fully accountable for reaching organizational objectives and act as the first line of defense in risk management. However, most managers tend to focus on business opportunities rather than risk. They have learned that ignoring or even denying risks can help to get investment proposals accepted (Levy et al. 2015). In addition,

they may simply lack the resources for effective risk management or have become used to risk managers and other service providers (such as compliance officers, quality officers or controllers) taking care of the identification, assessment, and mitigation of risks. Consequently, risk management is mostly perceived as a downstream activity that reactively deals with the risks created by previous decisions. Managers are often frustrated with the “paperwork” and the formalized nature of risk procedures rather than seeing the benefits of integrating risk management considerations into strategic decision-making.

### A four-step approach to effective risk management

Most of the challenges mentioned above are difficult to address since organizational routines that deal with risk are often taken for granted and deeply embedded in the corporate DNA. Vested interests and internal politics form additional barriers to change. Against that backdrop, we propose a four-step approach (see **figure 1**) to increase the effectiveness of corporate risk management and leave it to the discretion of individual companies to what extent they approach the steps sequentially or in parallel.

**Fig. 1** Four-step approach to effective risk management



Source: Authors' illustration

### Step 1: Map risk management activities

As a first step, it is helpful to map the status quo by creating an overview of existing activities across organizational units, hierarchy levels, and risk types. Managers should make sure that they do not limit this exercise to known risks that risk managers or other internal service providers are already dealing with. On the contrary, they need to make sure that preventable risks, strategic business risks, and external, uncontrollable risks are all covered in the mapping of risk-related management activities, and that overlaps, parallel work, relevant interfaces, and white spots are identified. Finally, the proclaimed relevance of different risk types should be compared with the actual management attention given to the respective risks: is the management team walking the (risk) talk? One way of doing this is to measure the time allocated to different risk types during board and annual business review meetings and to compare it with the statements of senior board members about the importance of operational and strategic, internal and external, and known and unknown risks.

### Step 2: Establish clear governance principles

In the second step, managers should leverage the transparency created by the mapping exercise to ensure proper distribution of management attention and to develop or fine-tune a shared risk management language as well as a set of risk oversight and governance principles. While this might sound straightforward, we firmly believe that any set of governance principles will only be implemented successfully if top management understands the importance of effective and coordinated risk management and develops a shared understanding of the company's risk profile across all the risk types mentioned above. In addition, the principles need to

- emphasize the role of management as the owner of all risks and define risk ownership for all relevant risk categories in the “first line of defense” accordingly,
- provide a clear definition of the role of supporting staff groups (i. e., risk managers, controllers, strategists, etc.) and clearly outline the type of support these staff groups should provide,
- provide suitable incentives to ensure that all relevant business decisions are based on an analysis of both risks and opportunities (cf. Gleißner/Romeike 2020),
- define interfaces and encourage coordination between the staff groups mentioned above. Aligning key parameters for planning and risk management, for example, can be a prag-

matic first step to improving the collaboration of risk managers, controllers, and strategists (cf. Angermüller/Gleissner 2011),

- take account of the fact that requirements might differ across the company's regions, business models, and business units,
- and, finally, be communicated, enforced, and continuously improved under the oversight of top management, e. g., via a risk committee chaired by the CEO or the CFO (cf. Tonello 2012).

### Step 3: Rethink the role of risk managers

With a shared understanding of the company's risk management activities and clear governance principles in place, corporate risk managers and other staff groups can embark on their journey to change their focus from running the process of managing operational and compliance risks to supporting the management of strategic business risks and external, uncontrollable risks.

As a first step, we recommend freeing up support resources for the management of strategic business risks and external, uncontrollable risks by combining two levers. Firstly, CEOs and CFOs need to make sure that risk managers and controllers do not “run” the whole process of managing preventable risks but rather support managers as risk owners and the first line of defense in the process of identifying, assessing, and mitigating risks. Secondly, top management should foster the use of big data and analytics and the automation of risk-related reporting, monitoring, and, if possible, mitigation activities. Both levers should free up resources that can then be used to shift the role of risk managers and controllers from operating the management of operational and compliance risks to becoming full-fledged business partners with a stronger focus on strategic risks.

To succeed in this endeavor, staff groups need to complement the support for existing risk management processes with a new role that focuses on enabling the first line of defense and facilitating the corporate risk dialogue by

- facilitating discussions on strategic business risks, utilizing methodologies such as scenario analyses, war games, and similar formats,
- providing relevant frameworks, techniques, and risk management expertise,
- raising awareness of cognitive biases in the risk management process and employing debiasing techniques,
- ensuring adequate monitoring of strategic business risks as well as risk signposts and early warning indicators,

- being involved in business continuity management activities and making sure that these activities are sufficiently aligned with other risk management activities,
- challenging and assessing the appropriateness of given risk assessment and mitigation strategies,
- and, last but not least, ensuring that the dialogue results in risk-related decisions and initiatives (cf. Schäffer/Brückner 2021; Gleißner 2020).

Making the outlined changes in the risk-related role profile of managers and staff groups work requires additional competencies among risk managers and controllers. For example, staff group members might need to develop business acumen, strategic thinking, competencies in digital technologies and analytics, as well as communication and collaboration skills. However, changing the competency profile of risk managers and controllers is not enough.

#### Step 4: Foster an appropriate risk culture

Guidelines and changes in the profile of staff groups alone will not be enough to make management accept its role as the first line of defense across risk types. Therefore, top management needs to complement the first three steps with a cultural change effort and make sure that the sum of mindsets and behavioral norms that determine how an organization identifies and manages risks (cf. Higgins et al. 2020) are adequate. This process can be kicked off after completing step three or can be carried out simultaneously. To get started, managers and staff groups must analyze the existing risk culture and answer the following questions:

- Is there a sufficient degree of risk-related transparency?
- What is considered to be the adequate level of risk appetite, and for what type of risk? Is this appetite clearly defined, communicated, and monitored?
- Is the organization characterized by an open exchange of risk-related information across functions and hierarchy levels? Is the corporate risk dialogue open and candid or rather political, especially when it comes to strategic business decisions?
- To what extent does the organization derive sufficient learnings from failures?
- To what extent are insights from the risk management process translated into managerial action?
- To what degree does management feel accountable for all relevant risk types? To what extent does management accept its role as the first line of defense?
- Is the risk culture in place sufficiently aligned with the overall management culture and incentive schemes?



S. Schöning, V. Mendel  
**Kompetenzentwicklung  
 im Controlling**  
 Mit systematischer  
 Personalentwicklung in  
 der Digitalisierung und  
 Globalisierung zum Erfolg

2021. XI, 364 S. 86 Abb., 1 Abb. in Farbe. Brosch.

€ (D) 54,99 | € (A) 56,53 | CHF 61.00

ISBN 978-3-658-29658-2

€ (D) 42,99 | CHF 48.50

ISBN 978-3-658-29659-9 (eBook)

- Dient als Leitfaden einer systemischen Personalentwicklung im Controlling
- Berücksichtigt digitale und interkulturelle Kompetenzen in der Kompetenzentwicklung
- Veranschaulicht Fach-, Methoden-, Sozial-, Selbst- und Handlungskompetenzen

€ (D): gebundener Ladenpreis in Deutschland, € (A): Preis in Österreich. CHF: unverbindliche Preisempfehlung. Alle Preise inkl. gesetzl. MwSt. Für Endkunden ist die Standard-Lieferung kostenfrei. Für weitere Informationen kontaktieren Sie bitte unseren Kundenservice per E-Mail: [customerservice@springernature.com](mailto:customerservice@springernature.com)

Part of **SPRINGER NATURE**

[springer.com/empfehlung](https://springer.com/empfehlung)

Based on an honest discussion of these questions, top management needs to analyze where the status quo is counterproductive to the intended changes in risk management and then initiate cultural change. This process may contain the usual elements of change processes such as intensive communication, training, and workshops at all hierarchy levels, but also changes in compensation schemes and staffing. Role modeling from the top and a long-term approach are paramount. Let us be clear: cultural change is a marathon, not a sprint.

## Conclusion

Many companies suffer from formalized, bureaucratic risk management processes that are mainly delegated to functional experts and do not focus enough on strategic risk management. This frequently leads to frustrations and cynicism. To help corporate risk management realize its full potential and to add value, we recommend a comprehensive approach that starts out with mapping risk management activities across organizational units, hierarchy levels, and risk types and implements clear risk oversight and governance principles. Once this is done, companies can embark on a journey to transform their risk management practices. They need to make sure that managers themselves are in the driver's seat and act as the first line of defense across different risk types – internal and external, operational and strategic. Risk managers and other involved staff groups should be enabled to add value as business partners and centers of expertise in supporting risk-aware strategic business decisions. Finally, companies must put effort into fostering and developing an appropriate risk culture.

## Literature

Angermüller, N. O./Gleißner, W. (2011): Verbindung von Controlling und Risikomanagement: Eine empirische Studie der Gegebenheiten bei H-DAX Unternehmen, in: *Controlling*, 23 (6), pp. 308-316.

Gius, D./Mieszala, J.-C./Panayiotou, E./Poppensieker, T. (2018): Value and resilience through better risk management, <https://go.sn.pub/2Z5RHi> (latest view: 11.09.2021).

Gleißner, W. (2020): Risikomanagement: Gegenwart und Zukunft, in: *Rethinking Finance*, 2020 (4), pp. 24-28.

Gleißner, W./Romeike, F. (2020): Entscheidungsorientiertes Risikomanagement nach DIIR RS Nr.2, in: *Der Aufsichtsrat*, 2020 (4), pp. 55-57.

Higgins, R./Liou, G./Maurenbrecher, S./Poppensieker, T./White, O. (2020): Strengthening institutional risk and integrity culture, <https://go.sn.pub/xGLU5f> (latest view: 11.09.2021).

Institute of Internal Auditors (2020): The IIAs three lines model – an update of the three lines of defense, <https://go.sn.pub/P9jLYl> (latest view: 11.09.2021).

Kaplan, R. S./Mikes, A. (2012): Managing risks: a new framework, <https://hbr.org/2012/06/managing-risks-a-new-framework> (latest view: 11.09.2021).

Levy, C./Krivkovich, A./El Ouali, M./Graf, J. (2015): Managing the people side of risk – risk culture transformation, <https://go.sn.pub/IV1bIU> (latest view: 11.09.2021).

Schäffer, U./Brückner, L. (2021): Fünf Herausforderungen für das Risiko-Management, in: *Controlling & Management Review*, 65 (4), pp. 52-59. <https://go.sn.pub/w7chSW>

Taleb, N./Goldstein, D./Spitznagel, M. (2009): The six mistakes executives make in risk management, in: *Harvard Business Review*, 87(10), pp. 81-85.

Tonello, M. (2012): Should your board have a separate risk committee?, <https://go.sn.pub/u3mkGu> (latest view: 11.09.2021).

## Angaben zu den Autoren



### Utz Schäffer

is a Director of the Institute of Management Accounting and Control (IMC) of WHU – Otto Beisheim School of Management, Vallendar, and Co-Editor of the *Controlling & Management Review*.  
E-Mail: [utz.schaeffer@whu.edu](mailto:utz.schaeffer@whu.edu)



### Florian Storek

is Head of Operational Excellence & Governance Germany at Janssen Europe, Middle East & Africa, Neuss.  
E-Mail: [florianstorek@freenet.de](mailto:florianstorek@freenet.de)



## Risiko-Management



Heß, G./Kleinen, A.-C. (2021): Resilienz im Einkauf. Konzept und Praxisleitfaden zum Management unerwarteter Risiken in der Lieferkette, Wiesbaden. <https://go.sn.pub/zPLbsb>

Romeike, F./Hager, P. (2020): Erfolgsfaktor Risiko-Management 4.0. Methoden, Beispiele, Checklisten, Praxishandbuch für Industrie und Handel, 4. Auflage, Wiesbaden. <https://go.sn.pub/zlBv9u>

Brauweiler, H.-C. (2019): Risiko-Management in Unternehmen. Ein grundlegender Überblick für die Management-Praxis, 2. Auflage, Wiesbaden. <https://go.sn.pub/HFD2lD>

# rəturn

Magazin für Transformation und Turnaround

## Schutz gegen den freien Fall



© iStockphoto.com/jeffbergen

Beim Bewältigen von **Unternehmenskrisen** oder noch besser beim Verhindern eines möglichen freien Falls halten Vorstände und Geschäftsführer besonders viel Verantwortung und Risiko in ihren Händen. **Clevere Unternehmer und Manager sorgen vor:** Gegen Krisen sind sie gewappnet – mit klugen Lösungen für erfolgreiches Handeln für Transformation und Turnaround.

**return – das Magazin für Manager, die Krisen besser meistern.**



Jetzt kostenlos testen:  
[meinfachwissen.de/return](https://meinfachwissen.de/return)

 Springer Gabler