Current state of risk management and risk governance in practice: evidence from a survey

Prof. Dr. Patrick Ulrich/Julia Barth/Sonja Lehmann
Aalen University
6th Annual Conference on Risk Governance
University of Siegen, October 4th, 2018

Agenda

1. Problem statement
2. Findings from literature
3. Methodology
4. Survey results
5. Conclusion and recommendations

Questions and comments

References

Problem statement

- In times of growing global interdependence and disruption caused by new digital technologies, **risks are becoming increasingly complex** (Romeike 2018).
- Companies are faced with various types of risks, particularly **cyber risks** (Weigel/Hiebel/Wiedemann 2018, Deloitte 2017).
- Interaction and requirements **regarding governance, risk management and compliance** (GRC) are increasing (Rücker/Prigge 2018).

- Thus, the research question of this work is the following:

“What is the current state of risk management in practice?”

Findings from literature

- Risk management shows **ambiguities, gaps and inconsistencies** in today´s dynamically changing business environment (Stein/Wiedemann 2016).
- Literature reviews on risk management suggest the **integrated management of all risks** (Falkner/Hiebl 2015, Bromiley et al. 2015).
- Research on **enterprise risk management** still leaves room for **further development** (Bromiley et al. 2015).
- Risk governance is a new and more comprehensive concept which aims at **proactively managing current and potential risks** (Weigel/Hiebl/Wiedemann 2018).
- The increased level of complexity not only requires an effective operative risk management, but **adequate risk governance** as well (Weigel/Hiebel/Wiedemann 2018).

Methodology

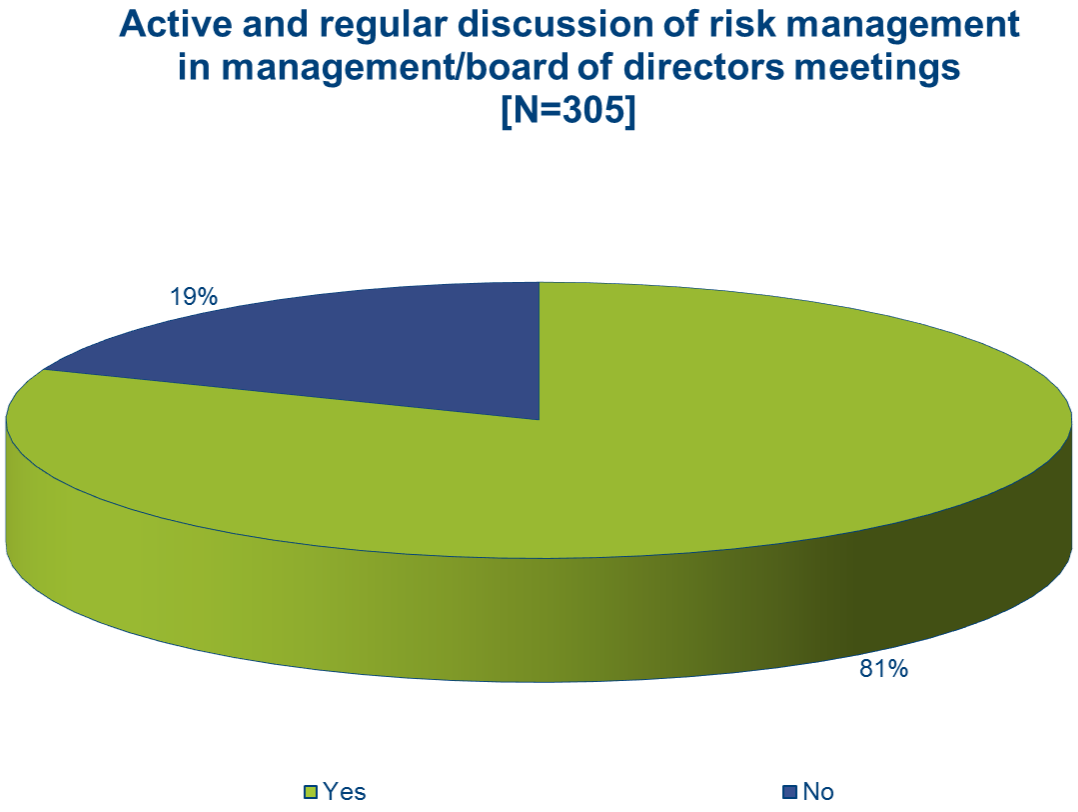
- The study was conducted as an **online survey** and addressed **companies of different sizes and industries**.
- To acquire potential participants, we used the Nexis database und generated a random sample of **19,632 companies** located in Germany.
- The data was collected between **January 16th and February 14th, 2018** using a standardized online questionnaire which contained both open and closed questions.
- Of the 19,632 companies contacted by e-mail, **320** took part in the survey. This corresponds to a **response rate of 1.63 percent**.
- As the questionnaire contained sensitive questions, the **determination of mandatory questions was omitted**, which means that the number of respondents slightly varies from question to question.

Survey results

Characterization of the sample

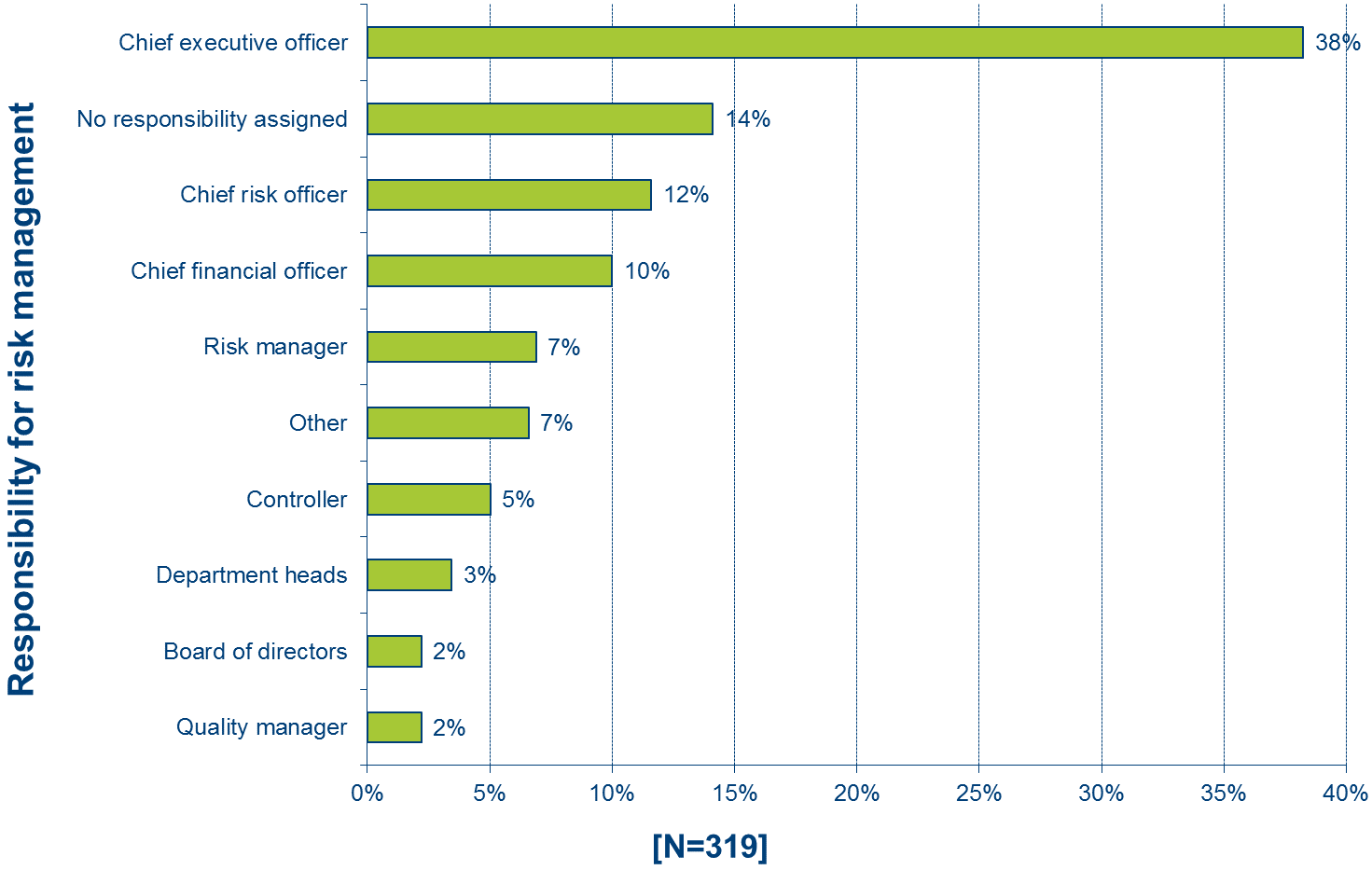
- **Sector**: 55 percent services (whereby 13 percent belong to the financial services sector), 36 percent industrial sector, 9 percent retail
- **Legal form**: 52 percent GmbH, 18 percent GmbH & Co. KG, 8 percent AG, 8 percent eG, 14 percent other categories
- **Median of turnover**: 50 million euros
- **Median number of employees**: 160
- **Capital market oriented company**: 17 percent „yes“, 83 percent „no“
- **Family firm**: 39 percent „yes“, 61 percent „no“
- **Professional function**: 11 percent owner/shareholder, 62 percent employed manager, 27 percent other function

Survey results



Survey results

Survey results

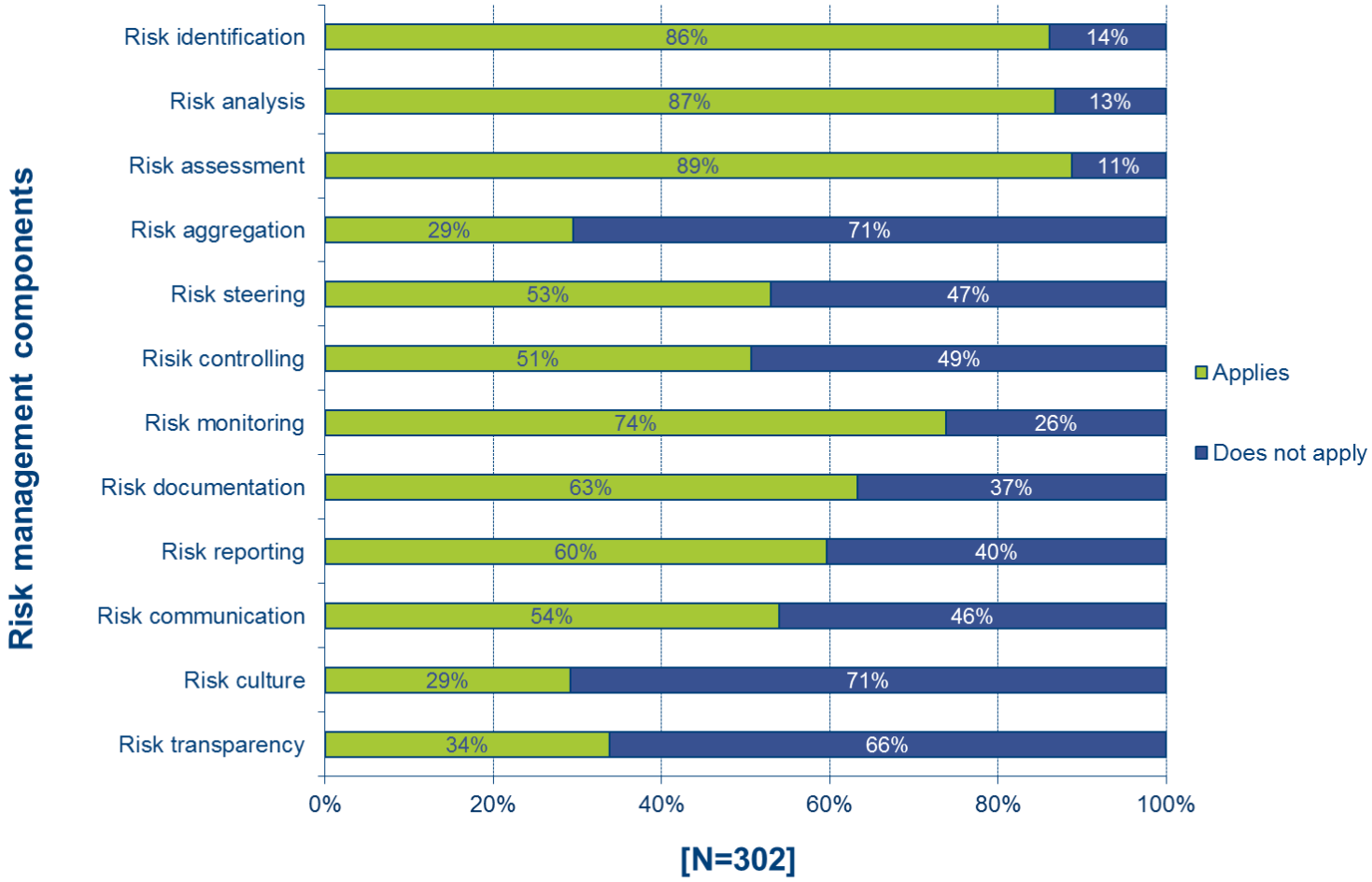


Survey results

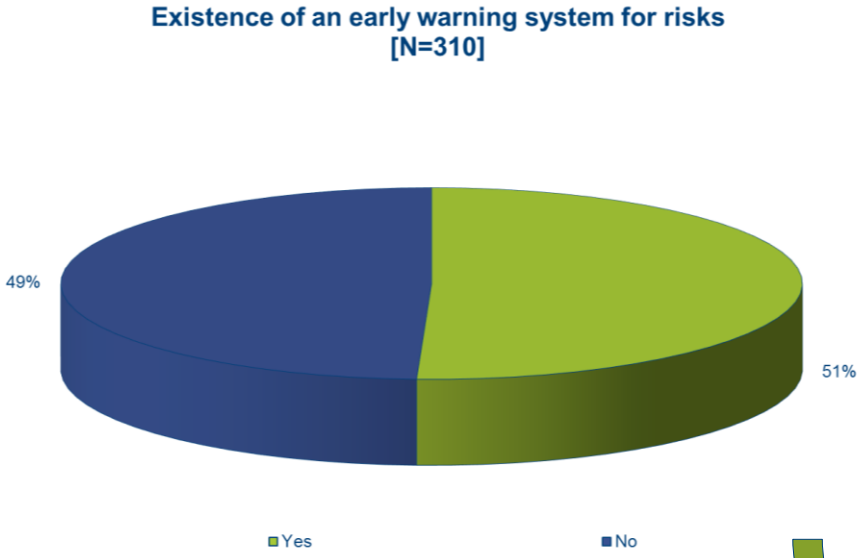
Specification of team/department

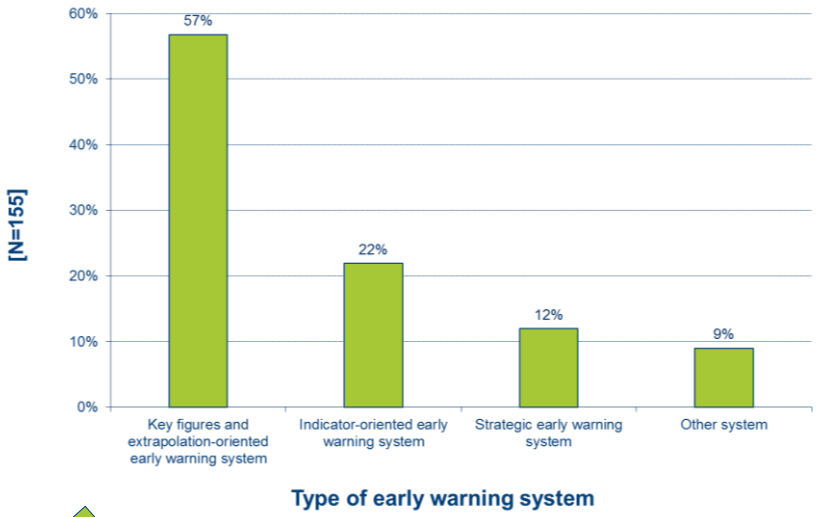
- 35 percent controlling
- 25 percent risk management
- 11 percent quality management

Survey results

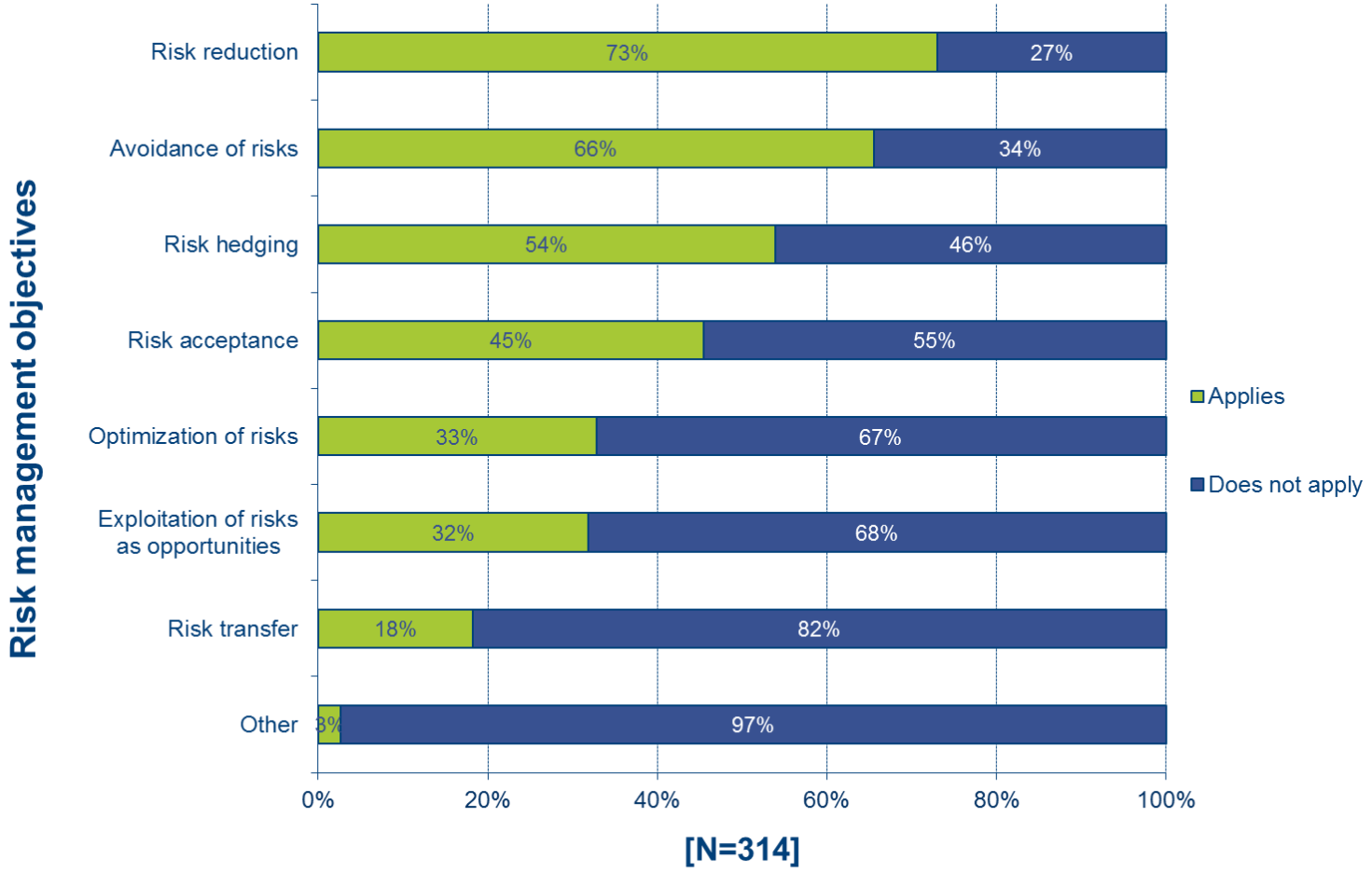


Survey results



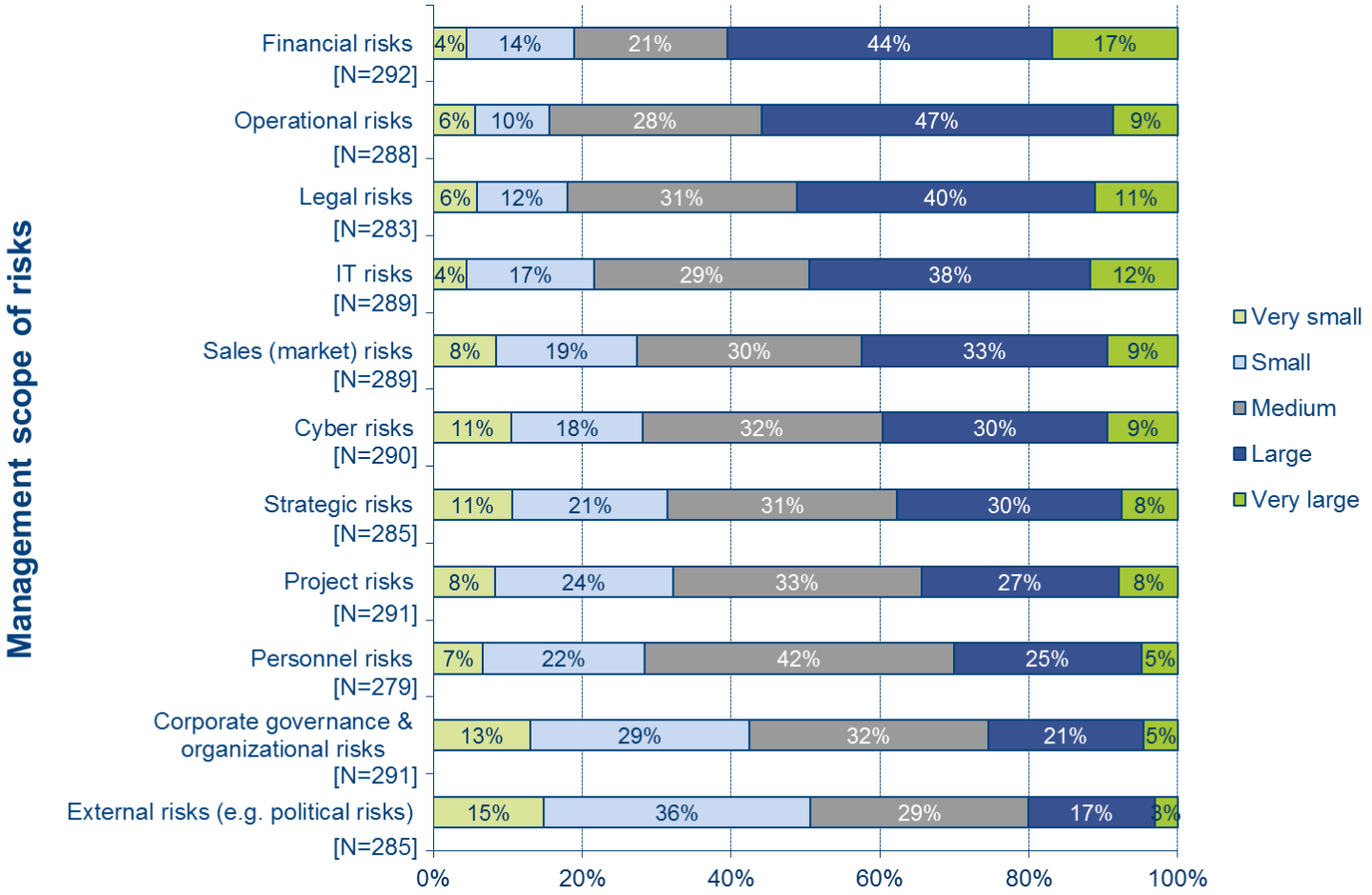


Survey results

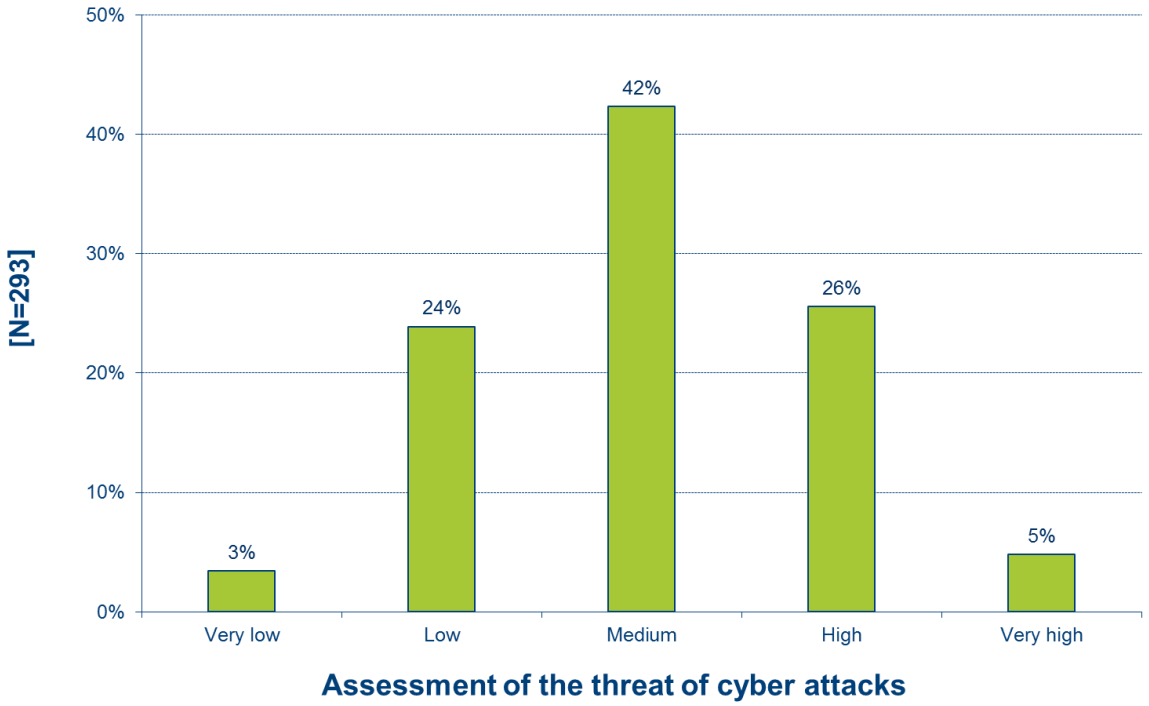


Survey results

Survey results



Survey results

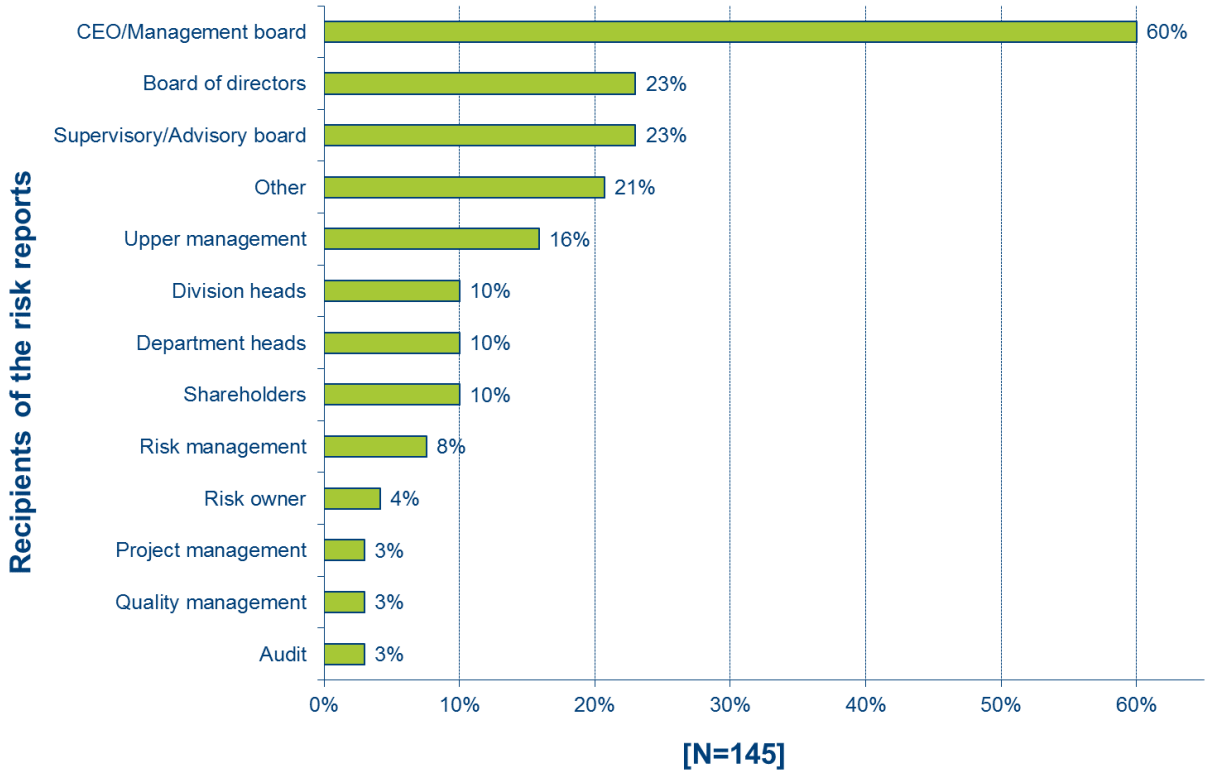


89 percent of the companies protect against cyber risks, using at least one of the following protection measures**:**

- 99 percent technical protection
- 33 percent insurance
- 21 percent legal protection
- 10 percent social protection

Survey results

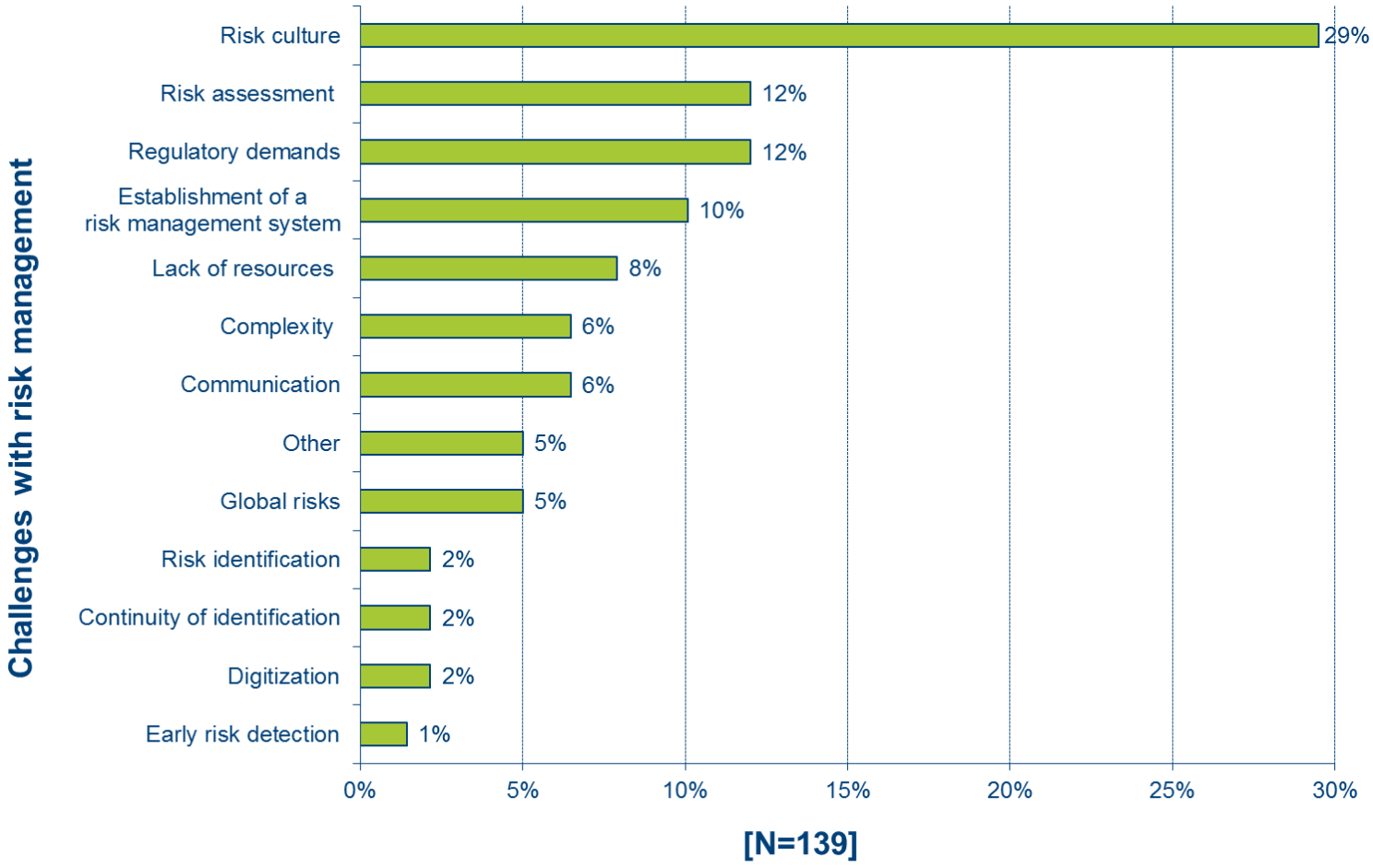
In 54 percent of the companies, regular risk reports are created:



In addition, in 59 percent of the companies an annual overall risk report is created, which is addressed to the following stakeholders:

- 44 percent internal stakeholders
- 28 percent supervisory board
- 10 percent other external stakeholders

Survey results



Survey results

Evaluation

- The **current relevance** of risk management for the company is mostly assessed as **medium** (44 percent), followed by a **high** relevance (30 percent).
- 53 percent of the respondents think that the **relevance will increase in the future**, 46 percent that it **will stay the same**.
- Most respondents (44 percent) **are satisfied with their risk management**, followed by 33 percent who are neither satisfied nor unsatisfied and 15 percent who are unsatisfied.
- 69 percent of the respondents see a **need for improvement in the company's risk management system**, above all regarding the holistic nature of the system (33 percent) and risk culture (23 percent).
- With respect to **value added** that risk management provides **for the company's management decisions**, 44 percent assess it as **medium** and 40 percent as **high**.

Conclusion and recommendations

In many companies, risk management is little formalized and handled as a separated topic.

- → The integration into the overall context of **governance, risk and compliance (GRC)** is necessary.
- → Next to negative target deviations, positive deviations have to be identified and assessed as well in order to ensure comprehensive, holistic and integrated **management of risks and opportunities**.
- → **Early warning systems** ease the identification of potential risks and expand the rooms of action.
- → The establishment of solid **risk governance** helps to structure risk management and provide for transparency and accountability.

Conclusion and recommendations

Risk culture is often seen as a critical aspect and challenge.

- → **Risk culture has to be fostered**, e.g. by creating incentive structures and an appropriate “tone from the top” to **build awareness among employees** and to ensure critical and open communication of risk aspects.
- → **Instruction courses and a code of conduct** may help to ensure a rule-compliant handling of risks.

Companies underestimate the danger of cyber attacks.

- → Next to the defense against external threats from the company environment, companies must as well focus on **finding and closing internal vulnerabilities**.
- → To increase internal cyber security, **prevention measures** have to be established and employees of all hierarchical levels have to be **trained** on potential risks and their proper handling.

Questions and comments

References

- Bromiley, P./McShane, M., Nair, A./Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long Range Planning, Vol. 48, No. 4, pp. 265-276.
- Deloitte (2017). Cyber-Security Report 2017 - Teil 2. Cyber-Risiken in Unternehmen.
- Falkner, E./Hiebl M. (2015). Risk management in SMEs: a systematic review of available evidence. Journal of Risk Finance, Vol. 16, No. 2, pp. 122-144.
- Romeike, F. (2018). Risikomanagement, Wiesbaden
- Stein, V./Wiedemann, A. (2016). Risk governance: conceptualization, tasks, and research agenda. Journal of Business Economics, Vol. 86, No. 8, pp. 813-836.
- Weigel, C./Hiebel, M./Wiedemann, A. (2018). Vom Risk Management zur Risk Governance, in Control Managament review, Vol. 62, No. 1, pp. 34-40.