

# Strategic risk management of ICT related risks in companies

Tihana Mustaf

Faculty of Organization and Informatics  
Student at Organization of business systems  
Pavlinska ulica 2, 42 000 Varaždin  
tmustaf@foi.hr

**Abstract.** Contemporary companies are facing diverse risks in their business activities. Modern strategic approach to risk management perceives risks not only as a threat to achievement of company's goals, but also as an opportunity to benefit (Miloš Sprčić, 2013). The corona virus pandemic and the need to digitally transform companies, raised awareness on ICT related risks. These risks may occur on the strategic and operational level of the company. On the strategic level companies face the risk they will not recognize opportunities arising from technology or risk of mismatching the used technology and company's goals. Also, many companies are using social networks in order to communicate to customers and reach their target groups. In case social networks are used without a clear purpose and strategy, there is a risk that companies will fail to address key customers and their needs, thus risking lower business results. On the operational level, companies are facing cyberthreats and frauds conducted by ICT, data breaches, Internet-of-Things vulnerabilities and failures of ICT systems. All of these ICT related risks may lead to huge financial penalties and reputational damage for the company. The purpose of this poster is to present different types of ICT related risks, but also to propose a framework how companies may strategically manage them.

Strategic risk management of ICT related risks in companies is based on integrated approach. This means that companies are proactive in managing the existing and analysing emerging risks, perceiving risks as an opportunity for growth, adequate risk culture is being built in the company and standardized frameworks, such as COSO (2017) or ISO 31 000 (2018), are used as a guide to risk management (Claypole, 2021).

The proposed framework for strategic risk management of ICT related risks in companies is comprised of four steps: (1) Determination of the situation in the company, (2) Identification and subjective risk analysis/ Making the risk map, (3)

Analysis and objective risk quantification/ Revision of the risk map, (4) Decisions related to risk management (Miloš Sprčić, 2013).

Determination of the situation in the company may be conducted by using SWOT analysis, Porter's five forces model or PESTLE analysis. The results of these analysis are the basis for Identification of risks companies are facing, estimating the probability that risk will occur, the financial impact it may have on the company and visually present these estimates on the risk map. Objective risk quantification includes analysing different stress scenarios in which effects of risks on the company are assessed. Finally, company management reaches certain decisions how they will treat certain risk, based on the conducted risk analysis. These decisions may be to avoid risk, use natural hedging, transfer risks on insurance companies or passively bear risks (Miloš Sprčić et al., 2019). Use of strategic approach to ICT related risks gives the companies a chance to better prepare for emerging situations, respond to them adequately and achieve their strategic aims.

**Keywords.** ICT related risks, strategic risk management

## Acknowledgments

This poster is a result of the research conducted for the purpose of defending the undergraduate thesis *Integrated approach to managing technology induced risks in companies*, under the mentorship of **Ivana Dvorski Lacković, PhD**. The thesis has been defended at the Faculty of Organization and Informatics on 21<sup>st</sup> September 2021.

## References

- Claypole, A. (2021). *Traditional risk management vs enterprise risk management: Which approach is best?* Retrieved from: <https://www.ideagen.com/thought-leadership/blog/traditional-risk-management-vs-enterprise-risk-management-which-approach-is-best>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management Integrating with Strategy and Performance. Executive Summary*. New York: American Institute of Certified Public Accountants.
- ISO - International Organisation of Standardisation (2018). *A Risk Practitioners Guide to ISO 31000:2018*. Retrieved from: <https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>
- Miloš Sprčić, D. (2013). *Upravljanje rizicima - Temeljni koncepti, strategije i instrumenti*. Sinergija nakladništvo, Zagreb
- Miloš Sprčić, D. M., Puškar, J., & Zec, I. (2019). *Primjena modela integriranog upravljanja rizicima - Zbirka poslovnih slučajeva*, Sinergija-nakladništvo d.o.o, Zagreb