



## 12 REASONS FOR RISK MANAGEMENT FAILURE

# RISK

*The latest economic instability gives risk management an increased attention and importance. Successful organizations continuously attempt to identify and treat potential risks. They are willing to efficiently integrate risk management at all levels of management process. While, very few project managers or organizations recognize and admit their risks, which lead to risk management failure. Risk Management failures prohibit organizations from meeting their goals, thus determining repetitive and sometimes of exponential magnitude, business and project failures. These failures can cause consequences for the organization in both time and cost. Therefore, understanding the strategy of how the organization is making profits and the risks inherent in the business model is essential in order to avoid such failures.*

*This article is focused on how inappropriate Risk Management implementation leads to failure of projects, and also discusses the major reasons and possible solutions that are associated with risk management failure. Such a solution involves adopting an internationally recognized standard such as ISO 31000, which is built on the most relevant best-practice scenarios from organizations worldwide and it is general enough to reduce or eliminate bias.*

Risk management has gained an increased attention and interest in recent years, both from industry professionals and academics. The main focus of sound risk management is the continuous identification and treatment of the potential risks. Its objective is to add maximum continual value to all the activities within the organization. In addition, in developed and emergent countries, capital markets have become more significant and as a result nonfinancial corporations and banks recognized that the number, type, and extent of their threat landscape and inherent risk have increased significantly. Finally, a wave of unpredictable financial payment related enhancements can be considered both a source of risk and a method to mitigate.

Risk management has also gained attention considering the ongoing and widely publicized failures having roots in its erroneous implementation. Risk Management failures prohibit organizations from meeting their goals, thus determining repetitive and sometimes of exponential magnitude, business and project failures. Although the risk management approach varies among firms, enterprise risks management is an organizational pivot point in achieving corporate goals. Risk and performance are inevitably connected. By establishing a reliable and controlled process for managing risks, organizations can develop the predictability of their outcome. Enterprise risk management enables enhanced decision making, consequently enabling significant cost savings. Additionally, if properly implemented, Risk Management connects risks across various levels in the organization and leveraging other processes such as Program Management enables threat to opportunity conversion.

While considering the valuable role of risk management, it is also essential to understand the many circumstances in which risk management failures may occur.

Enterprise Risk Management can adjust with the business hypothesis and intensively help in overcoming potential business failures. Matei et al. (2012) emphasize that organizations fail because of unexpected losses created by three main factors:

1. Insufficient capital,
2. Model errors, and
3. Risk ignorance.



Consequently, management system and risk mitigation may be unsuccessful for more delicate and indirect reasons. At this point, there are three other well-known reasons why risk management fails:

4. Agency risk,
5. Shift or changes threat landscape and inherently in the form of risk,
6. Incremental failure.

Agency risk refers to the risk that a manager or employee, unintentionally or decisively, does not succeed to pursue procedures intended to manage and moderate risks. Next, there is often an affinity for risk to shift or change form. Although an organization may moderate its risk by acquiring insurance, these proceedings do not decrease systematic risk in the economy. Furthermore, there is tendency for risk management process to fail incrementally across a long period of time. The incremental failure is frequently caused by an extensive incubator duration coming from an evenly degradation of the risk management processes, which gather over a long period of time.

Once risks are identified and quantified, they must be inferred at the organizational upper management level. Inability to properly communicate risks to the top management may cause overall risk management failure. These failures are an indicator of unnecessary risk acceptance and or exposure. Stulz (2008) showed that failures on risk management can be divided into six classes:

7. Mismeasurement of known risks,
8. Failure to take risks into account,
9. Failure in communicating the risks to top management,
10. Failure in monitoring risks,
11. Failure in managing risks,
12. Failure to use appropriate risk metrics or measurement system.

Risk management failure can be caused by the use of improper risk metrics which induces inaccurate measurements. A practical example is weather forecasting. The most common risk metrics in modern risk management is "Value at Risk" (VaR). Despite the fact that VaR has been proven to be quintessential risk measure, meaningfulness is directly dependent on the quality of the associated answer and inherent question.

Taking into account factors which may be accountable for risk management failure it is consequently appropriate to affirm that operators and operational failure are the two main groups in which risk management failures may fall into.

## HOW TO AVOID OR OVERCOME THESE FAILURES?

As discussed above, risk management failures can cause consequences for the organization in both time and cost. Therefore, understanding the strategy of how the organization is making profits and the risks inherent in the business model is essential in order to avoid such failures. Subsequently, top management must recognize empower and manage positions of trust; the employees whose activities can subject the organization to considerable or significant risk events must be carefully selected, trained and continuously evaluated. Establishing responsibility for outcomes and building a procedure for timely escalation in addition to building a common risk language, shared definitions, a common culture of risk awareness and comprehensible procedures for measuring, monitoring, communicating and dealing with risks are some of the main things an organization should consider when targeting a mature Risk Management approach.



Communication is another key process within any organization. Communicate regularly on risks that are more complex to measure and for which results cannot be forecasted with minimal confidence. Available, defined and detailed risk appetite is vital when defining unacceptable risk exposures.

Taking into consideration risk management failures, organizations should consistently manage risks by identifying, assessing, evaluating, prioritizing and monitoring them, continuously looking for opportunities to improve their risk stance. Concrete plans to support these processes should be enforced top-down.

**These plans should include, balancing:**

- a) Risk and benefit
- b) Risk and cost.

With all above in place, a useful and proven scheme for effectively managing many risks may be applied to streamline Risk Management and align it to best practices. Such a solution involves adopting an internationally recognized standard such as ISO 31000, which is built on the most relevant best-practice scenarios from organizations worldwide and it is general enough to reduce or eliminate bias.

ISO 31000 explains the mechanism of risk management implementation. It provides a framework for implementing a risk management suite, rather than merely a framework for supporting the risk management process. Moreover, with due cognizance of its own internal and external contexts, an organization must recognize the applicable and relevant laws and should put into practice a system of controls to attain compliance. Additionally, ISO 31000 distinguishes the significance of feedback by means of two mechanisms: communicating and consulting and the monitoring and reviewing of performance. Communicating and consulting ensures the engagement of relevant internal and external stakeholders while monitoring and reviewing guarantee that the organization observes risk performance, thereby gaining knowledge from experience and practices.

PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO 31000 courses.

For further information, please visit: <https://pecb.com/iso-31000-training-courses>

## ABOUT THE AUTHOR

**Alba Keqa** is an Account Manager for Risk & Management at PECB. She is in charge of conducting market research while developing and providing information related to Risk and Management standards. If you have any questions, please do not hesitate to contact: [marketing.rm@pecb.com](mailto:marketing.rm@pecb.com).

## ABOUT THE CONTRIBUTOR

**Bogdan Dragomir** is a COO at Vernance LLC. He is an expert in the area of Risk Management, Integrated Compliance, Secure Architecture Design and Analysis, Incident Management, Security Assessment and Auditing. If you have any questions, please do not hesitate to contact: [bdragomir@gmail.com](mailto:bdragomir@gmail.com).

