A Maturity Model for Risk Management

Diogo Proença¹, ², João Estevens², Ricardo Vieira¹, ², José Borbinha¹, ²

¹INESC-ID, 1000-029, Lisbon, Portugal
²Instituto Superior Técnico, 1049-001, Lisbon, Portugal

Risk is the effect of uncertainty on the achievement of objectives. Therefore, all organizations are subject to risk and uncertainty, and the need to manage risk in a structured way is increasingly recognized. Risk management consists of "coordinated activities to direct and control an organization with respect to risk". Often, organizations use different risk management practices and do not always do so in a systematic way. In order to help organizations manage risk more efficiently, a number of risk management structures have been created. One of them, ISO 31000 is recognized as a consensual reference, which has influenced some organizations that develop risk management structures to review their work in order to be in line with ISO 31000. ISO 31000 is comprehensive and can be used in all industries and for all types of risk, regardless of their nature. Consequently, this reference does not prescribe a risk management system, merely supporting and integrating risk management into the overall management system of an organization. The implementation of the risk management process is not always easy and some organizations give up without achieving the desired outcomes. This may be due to the fact that they are unable to carry out the risk management process in a consistent and predictable way over time.

Maturity models are tools that represents a path towards an increasingly organized and systematic way of doing business which usually involve people, organizations, and processes. There has been a great popularization of these tools in the last years through the use of maturity models in several domains, for example: data management, information security, and project management. In maturity models, the evolutionary path is described through discrete stages, to reach the next level it is necessary to achieve the objectives of the desired level and all previous levels.

This communication presents a maturity model for the risk management process. For the implementation of the model to be possible, it is necessary to assess the risk management process of organizations. Considering risk management is a process, ISO15504 will be used, which establishes how the assessment of a process should be carried out. This maturity model allows organizations to assess a risk management process according to best practice defined in risk management references. The maturity model can also be used as a reference for improving this process since it sets a clear path of how a risk management process should be performed. This work was supported by national funds through Fundação para a Ciência e e Tecnologia (FCT) with reference UID/CEC/50021/2013.

Keywords: Maturity Model, Risk Management, ISO31000, ISO15504

Presentation type: Oral Communication
**Topic:** T01 - New methods, new tools, new data in risk and resilience research