Student: Alessandro Riboni
Course: Risk Management
Assignment 3 – Applicability of Risk Management

Risk Management in a Software Development Project

1. Introduction

In the first assignment was presented an application of Risk management in an IT company. The case study was based on a fictional Software Company called *Software House Inc*., while, in the second one was evaluated three alternative risk analytical methods (PESTLE, SWOT and Bow-tie) in order to choose the best risk management strategy for the case study presented.
The purpose of this paper is to make a critical reflection on the applicability of risk management processes analysis by contrasting the theoretical approaches presented by Hopkin with Cox's point of view.
In the following section are presented the key points of two articles written by Cox (*"What's Wrong with Hazard-Ranking Systems? An Expository Note*" and "*Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small*?").
Finally, is reported a discussion on the validity of the results, the applicability of the methods evaluated and their impact on the solutions in assignment 1 and 2.

2. Literature review of Cox's articles

2.1. "What's Wrong with Hazard-Ranking Systems? An Expository Note", Cox (2009)

In this article, the author criticizes the use of priority scoring and rating system to manage and mitigate hazard risks. He claims that these methodologies have intrinsic limitations when the events are dependent on each other, which means that they are not appropriate for correlation risks.
In particular, Cox (2009) argues that "when risk-reducing opportunities have correlated consequences, due to uncertainties about common elements (such as potencies of chemicals, effectiveness of countermeasures, etc.), then methods for optimizing selection of a portfolio (subset) of risk-reducing opportunities can often achieve significantly greater risk reductions for resources spent than can priority-scoring rules."
Before presenting several real-world examples where rating systems are not efficient, Cox explains a general framework called the priority-setting process. This is composed of three elements:

- A set of items to be ranked or scored;
- An ordered set of priority scores (it may be sorted categorically, such as "low", "medium" and "high";
- A priority-scoring rule that may be a mathematical function, a procedure, or an algorithm that determinates to each hazard a single priority score.

Through this framework, it is possible to create priority lists. These don't produce effective risk management decision in multiple risky systems. Always according to Cox (2009) "applying investment portfolio optimization principles (such as optimal diversification,

consideration of risk aversion, and exploitation of correlations among risk reductions from different activities) can create better portfolios of risk-reducing activities in these situations than any that can be expressed by priority scores."
The author concludes the article by saying that the use of risk priority scores often produces wrong answers and that it is necessary to use optimization techniques that take into account the correlation among risk-reducing interventions for multiple targets.

2.2. "Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?", Cox (2011)

In this article, the author comments on a work by Professor Aven in which he underlines the importance of clarifying the meaning of "scientific uncertainty" for use in risk management. Cox discusses the efforts made to define "accurate" models and "small" input uncertainties. Through the analysis of three examples, the author seeks to demonstrate that the increase in input uncertainty can reduce uncertainty in model outputs, that even correct models with small uncertainties can produce inaccurate or useless predictions in risk management, and finally, that accurate predictive models do not necessarily have to be accurate causal models.
According to Cox (2011), there is no point in making comparisons between scientific uncertainties, defining them as larger or smaller than others. He also argues that "we may have to accept that the models and uncertainties that matter in risk analysis are often (perhaps usually) too complex to permit useful (or unambiguous) classifications in terms of concepts such as large or small, or accurate and inaccurate."
Cox also focuses on the concept of the accuracy of a predictive model. He argues that the application of a model influences the results and therefore it is only possible to evaluate it in the situation in which it is applied.

3. Critical reflection and discussion

In these two articles, Cox criticizes some methods commonly used for risk management. In the first article, he proposes several examples to support his thesis, and his point of view is easy to understand. I believe that the results he proposes are valid and that in some situations, they are realistic and applicable. The author highlights several issues related to the use of a rating system but does not present in detail the use and application of portfolio optimization techniques.
In my opinion, these techniques can be very useful but at the same time expensive due to the high complexity. It is necessary to make a careful assessment, because in some cases, the use of priority lists combined with qualitative assessment methods may be sufficient to ensure optimal risk management.
However, dependencies between risky events are an issue that an organization needs to assess carefully. A division of tasks after the first phase of qualitative assessment and a lack of communication within the team of specialists can, if there is a correlation between the risks, lead to disruptive consequences for the company.

In the second article, instead, the author comments on Professor Aven's thought, this thought is reported superficially, and it is difficult to understand Cox's analysis without having first read the professor's paper. I agree with Cox that in many situations we have to accept that the models and uncertainties that count in the risk analysis are often too complex to allow useful classifications in terms of size (large or small) or accuracy (accurate and inaccurate). Regarding this article, I think that the proposed results are valid, but I think they are more difficult to apply to real cases being much more general and abstract than those presented in the first article.

4. What does it mean for the solutions in Assignment 1 and 2?

In the first assignment, the case study was presented, and the risk matrix was used to assess the likelihood and magnitude (or impact) of possible events to which the company is subjected. In the second, three qualitative risk assessment methods were presented. As already mentioned, a qualitative approach in the planning phase of software development cannot be sufficient to manage risks. Working with an AGILE methodology and keeping a risk register updated through the company intranet, it is possible to minimize the consequences due to dependencies between the risks.

Some of the risks presented in the two previous assignments have dependencies, and assessing them individually could be dangerous for the company. For example, a virus infection after the first official release can have consequences on other risks, including compliance and sociological risks. First of all, it would reduce the cohesion of the development team. Also, according to the GDPR (General Data Protection Regulation), it would be necessary to notify the cyber-attack if the scale of the attack is considerable. If the organization does not have an adequate level of security, it may receive administrative fines for non-compliance by supervisory authorities.

For these reasons, the use of a risk matrix may not be appropriate. The assignment of the "low", "medium" and "high" likelihood and magnitude values of the individual risks would not take into account the correlation. It is possible to evaluate the use of portfolio optimization techniques. These take into account the dependencies between the risks to avoid negative consequences for the organization.

In conclusion, I think that Cox's ideas are right and that every company should take them into account when evaluating risks. I cannot entirely agree with Cox that rating systems and priority lists should be completely replaced by optimization techniques due to their high cost and complexity.

Considering also the methodologies and standards presented by Hopkin, I believe that each company should, based on the theory and experience of others, study an ad-hoc risk assessment plan, deciding which techniques to use according to the type of risks to which it is exposed.

5. References

- *Paul Hopkin, 2018; Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management. 5th edition.*
- *Cox Jr., L. (2009). What's wrong with hazard-ranking stems? An expository note: Perspectives. Risk Analysis, 29(7), 940-948.*
- *Cox Jr., L. (2011). "Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?", Risk Analysis: An International Journal, 31(10), 1530-1533.*