Student: Alessandro Riboni
Course: Risk Management
Assignment 1 – Application and Overview

Risk Management in a Software Development Project

1. Background

The purpose of this paper is to present an application of Risk management in an IT organization. This overview is based on a fictional Software Company called *Software House Inc.* The aim is to analyze and manage the different types of risk that an IT company encounters during the development of new software, according to the risk management process presented by Hopkin (2018).

1.1. Risk definition

There are several definitions of risk, and some of them indicate that taking risks will only have negative outcomes. However, it is possible that risks can have positive results, and for this reason, companies want to take risks.

It is essential that the organization chooses how to define risks in the most suitable way for its purposes. *Software House Inc.* adopts the definition proposed by Hopkin (2018): "An event with the ability to impact (inhibit, enhance or cause doubt about) the effectiveness and efficiency of the core processes of an organization."

1.2. Risk Management definition

As for the word Risk, there are different definitions of Risk Management, and it is crucial for an organization to choose only one in order to develop a clear strategy to identify potential risks and be able to manage them. Also, in this case, the company embraces the definition proposed by Hopkin (2018): "Risk management is the set of activities within an organization undertaken to deliver the most favorable outcome and reduce the volatility or variability of that outcome."

1.3. Principle of Risk Management

Among the available risk management standards, one of the most important is the international standard, ISO 31000. This standard includes a detailed list of suggested principles of Risk Management. An example is the acronym PACED. It provides an optimal set of principles that are the basis of a successful approach to control risks within an organization.

"It is suggested that a successful risk management initiative (and framework) will be:

- proportionate to the level of risk within the organization;
- aligned with other business activities;
- comprehensive, systematic and structured;
- embedded within business procedures and protocols;
- dynamic, iterative, and responsive to change" (Hopkin, 2018).

2. Risk assessment

Carrying out a careful risk assessment is essential to achieve corporate objectives, minimize costs, and maintain a good reputation. Firstly, *Software House Inc* needs to identify and classify risks so that it can manage them in the best possible way.

Hopkin (2018) classifies risks in four different categories: compliance (or mandatory) risks, hazard risks, control (or uncertainty) risks, and opportunity risks.

2.1. Risk description

Risk description is a section of the Risk Management process that is necessary for a common understanding of the risk within the organization.

During the first step of a System Development life cycle (SDLC), called *planning, Software House* categorizes risks in order to minimize their likelihood.

The organization must make a careful evaluation of compliance (or mandatory) risks.

In particular, an IT company must be careful to comply with GDPR and new Data Protection Laws. These regulations force companies into a higher level of security, and if *Software House Inc* fails to comply with them could have adverse consequences for the economy and the reputation.

The company should consider using external experts to minimize the possibility of such events occurring. Another critical risk that could result in unplanned disruption for the organization is a virus infection after the first official release. This is a hazard risk because it can only have negative outcomes and, as Hopkin (2018) argues, it must be mitigated.

Furthermore, when developing projects, an organization has to accept a level of uncertainty. Control (or uncertainty) risks are an unavoidable part of an IT project undertaking process. *Software House Inc.* must make an optimal estimation of working time, cost, and resources. Hopkin (2018) claims that the deviation from a project anticipated benefits represents uncertainties that can only be accepted within a certain range. The company has to estimate this range through the experience of the specialist and using analytical models based on its historical data.

Finally, every company wants to embrace opportunity risks, because these are the type of risk with the potential to enhance the achievement of the mission of the organization. *Software House Inc* wants to develop new software with new features to embrace business opportunities and increase customer satisfaction.

2.2. Risk classification

An important aspect of Risk Management is Risk classification. Once the risks have been identified, it is essential to classify them according to the nature of their impact, and then it is possible to estimate the consequences and assess a strategy that reduces the inherent level of risks.

The following table presents the risks described above, including the category, classifications, and possible consequences.

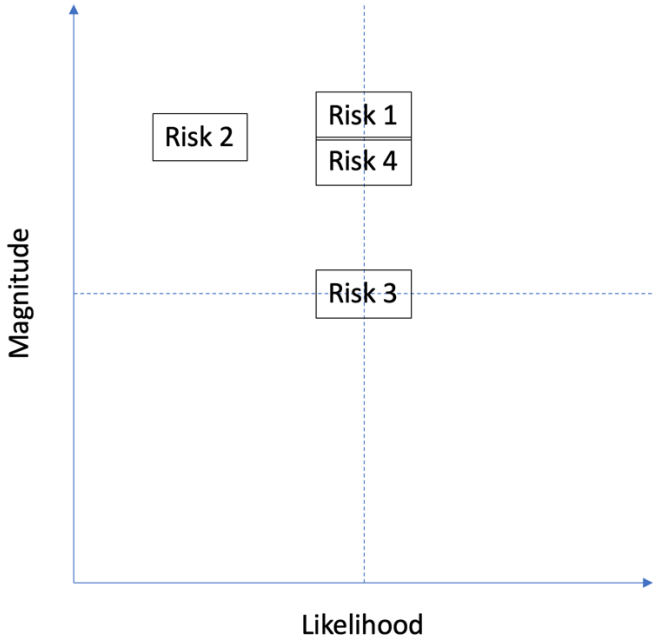
Risk index	Risk Description	Category	Classification	Consequences
1	Violate GDPR/ Data Protection Compliance	Compliance	Legislation/ Compliance/ Financial	Economic: Authorities will have the ability to impose fines up to 20 millions euros of 4% of company's total global annual turnover.
				Reputational: failing to comply with GDPR could subject to public scrutiny.
				Commercial: The company could lose customers
2	Bugs and/or Virus infection after the first official release	Hazard	Financial	Commercial: The company could lose customers. It is necessarily to intervene promptly to limite the damage.
3	Bad estimation of time, cost and/or resources	Control	Financial/Human	Unable to deliver the software to customers on time. Decrease of customer satisfaction.
				Too much effort is required of developers
4	High level software with new features	Opportunity	Financial	If the quality of the new software is high, the company could increase sales and customer satisfaction.

2.3. Risk analysis and evaluation

There are different techniques of risk evaluation that a company could use to achieve optimal results in each situation. *Software House Inc* decides to use a simple risk matrix, where the vertical axis is used to indicate the magnitude, and the horizontal axis indicates the likelihood, presented by Hopkin (2018). This is a commonly used method of illustrating risk likelihood and the magnitude (or severity) of the event should the risk materialize.

Risk index	Risk Description	Likelihood	Magnitude
1	Violate GDPR/ DataProtection Compliance	Medium	High
2	Bugs or Virus infection after the first release	Low	High
3	Bad estimation of time, cost and/or resources	Medium	Medium
4	High level software with new features	Medium	High

2.3.1. Risk matrix



3. Risk strategy

After careful analysis and evaluation of the risks associated with the development of software, it is necessary to design a strategy that allows the company to minimize the probability of events that can lead to negative and to decrease these events' impact.

A possible strategy to control risks periodically is to use an AGILE methodology, rather than a traditional Waterfall model.

The waterfall model is a breakdown of project activities into linear sequential phases, where each phase depends on the deliverables of the previous one and corresponds to a specialization of tasks.

Instead, an AGILE methodology is a practice that helps continuous iteration of development and testing in the software development process. In this model, development and testing activities are concurrent, unlike the Waterfall model. This process allows more communication between developers, managers, testers, and customers. This model allows to:

- limit the range of uncertainty of control risks
- increase customer satisfaction through better communication with the customer
- AGILE method assures that quality of the development is maintained, less likelihood of bugs
- the process is completely based on incremental progress. Therefore, the client and team know exactly what is complete and what is not. This reduces risk in the development process.

3.1. Risk control and monitoring

One of the possible methods for monitoring and controlling risks is the use of a risk register. The ISO Guide 73 defines a risk register as the 'document used for recording risk management process for identified risks.'

Hopkin argues that a well-constructed and dynamic risk register is at the heart of a successful risk management initiative and, using an AGILE methodology, could be possible take full advantage from the use of it.

Furthermore, *Software House Inc.* may make the register available on its intranet in a manner that facilitates use, consultation, and possible updating for developers.

Information can be provided on the intranet about the generic risk assessments, that have been undertaken, and the control measures, that have been identified. The intranet can also be used to communicate urgent risk information, as well as providing updates on risk assessments, control measures, and the current level of any particular risk. (Hopkin, 2018).

4. Conclusion

Through the use of a fictitious company, it has been possible to carry out a risk management process on pseudo-real problems, highlighting some of the risks that need to be considered during the development of software. As Hopkin has reported several times, there are different techniques that can be used to evaluate, identify, categorize, and control possible risks. Each company, depending on the kind of risk and depending on the environment in which it operates, has to choose definitions and standards that will help the company in its purpose.

The main aims must always be to mitigate hazard risks, which can only lead to negative results, to minimize compliance risk, to estimate a range for uncertainty risks and to embrace opportunity risks, because this is the type of risk with the potential to enhance the achievement of the mission of the organization.

5. References

- *Paul Hopkin, 2018; Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management. 5th edition.*
- *Hughey, Douglas (2009). "Comparing Traditional Systems Analysis and Design with Agile Methodologies." University of Missouri – St. Louis. Retrieved 11 August 2014.*