Risk Management

Overview

This article provides an overview of Risk Management.

Let's start with the basic concepts.

Learn more

Risk-Based Testing (RBT) is built on top of Risk Management and thus the same concepts and principles apply. To learn more about it check Risk-Based Testing.

If you want to learn how to perform RBT whenever using Xray, please have a look at Performing Risk-Based Testing (RBT) with Xray

Concepts and Terminology

Risk

In general, we can define **Risk as the "effect of uncertainty on objectives" (ISO 31000:2018) that can be positive (opportunity) or negative (threat)**.

We can also look at it as an uncertain event with a positive or negative effect on the measurable success-criteria of a project.

Therefore, and as a way to overcome a common misconception, risks are not always negative; however, many times we may be more focused on these ones.

Examples:

- *dependency on unsupported open-source library*
- *dependency on a closed, proprietary library without access to source-code*
- *replacement of relational database with a NoSQL one*
- *lack of sample data*
- *inability to thoroughly verify/discuss requirements with customer*
- *new technology, never used before*
- *lack of skills within the team*

Level of Risk

The level of risk, sometimes just simply called "risk value" or "risk," can be defined as a combination of the probability/likelihood and the impact /consequence of an event on the objectives.

Risk = Probability (of event) * Impact			
Also know as:	(Level of Risk / Risk Score / Risk Exposure)	(Likelihood/Frequency)	(Consequence/Damage/Revenue/Business Criticality)

Probability / Likelihood

Probability of an event occurring.

It can be defined as a percentage, a number interval (e.g. 0-4) or as a ordered list of values (e.g. "low", "medium", "high", "very high.")

Probability can be evaluated using multiple weighted criteria/factors (e.g. software maturity, software complexity, type of change, number of changed components, related defect rate, etc).

Impact / Consequence

The outcome of an event affecting objectives. In other words, it can also be defined as the overall loss or revenue that could occur IF the risk occurs.

An impact...

- Can be positive (i.e. an "opportunity") or negative (i.e. ”threat”)
- Can be evaluated using multiple weighted criteria
    - frequency of use, number of affected users, category/significance of affected users, type of impact, etc

Thus, if the probability of an event is 0, that risk won't happen. Likewise, a risk with no impact also leads to a risk score of 0.

Having a high-impact risk by itself is not something to worry much about unless the probability of the associated event is "high" enough.

Impact may be defined as a number interval (e.g. [0-4]) or as a ordered list of values (e.g. ["low", "medium", "high", "very high"]).

Source

The risk source is the *"element which alone or in combination has the intrinsic potential to give rise to risk"* (ISO 31000).

Examples:

- *unclear requirements*
- *external library*
- *external stakeholder*
- *regulatory constraints*
- *adoption of new process*
- *...*

Criteria

Risk criteria correspond to the *"terms of reference against which the significance of a risk is evaluated"* (ISO 31000).

"Criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes."

This risk criteria includes the definition of multiple levels for the probability and impact variables.

Categories

Risk categories are a way of classifying and grouping risks together.

Examples:

- *business*
- *technical*

- *operational*
- *project management*
- *external*
- *compliance*
- ...

"Types" of Risks

Inherent Risk

Existing risk, and implicit risk level, before any *treatment* actions are taken.

Residual Risk

Remaining risk, and implicitly residual risk level, after risk *treatment* actions have been taken.

Exposures

Exposure

Although not part of ISO 31000, "exposure" is commonly used to refer the categorization (e.g. "low", "medium", "high", "severe") of the risk based on its level. Sometimes it's also used as a synonym for the calculated risk level value, so please be aware of it.

Residual Exposure

Residual exposure corresponds to the exposure after *treatment*, based on the remaining residual risk. Sometimes it's also used as a synonym for the calculated residual risk level value, so please be aware of it.

Risk Register

The Risk Register is used to store and document risks along with the risk treatment responses. It is an essential tool for assisting with the risk management activities that can give visibility of current risks, and help in the process of documenting and reviewing them.

Risk Management

Risk Management corresponds to the "coordinated activities to direct and control an organization with regard to risk."

All organizations and projects are subject to risks of many different categories that may or not happen and if so, may impact the defined objectives.

The purpose of Risk Management is to have a systematic approach to address risks effectively by having the defined objectives in mind, taking advantage of them in case there are opportunities that benefit our objectives, or by minimizing threats that may impact negatively on what we foresee to achieve.

Risk Management Process

There are a set of activities that are part of the Risk Management Process: Establishing the Context, Risk Assessment, Risk Treatment, Monitoring & Reviewing. Risk Assessment is in turn composed of Identification, Analysis and Treatment.

The overall process starts by establishing the context, so users have a common understanding of the objectives, the internal/external "constraints" and agree on the definition of risk criteria.

After that, users will identify and describe the risks, analyze them as a means to obtain their characteristics (e.g. risk level), and decide what actions (i.e. *tre atments*), if any, to take depending on the latter.

Monitoring and reviewing of risks is an ongoing activity that provides a feedback loop to the whole Risk Management Process, to depict changes in context, risk criteria, risks themselves and related treatments.

0. Establishing the Context

The foundation of the Risk Management Process is establishing the context.

Context provides information about the objectives that need to be pursued and also the internal and external environments or contexts that are involved.

Part of setting the context is the definition of *risk criteria* itself, based on the internal and external contexts and on the objectives to be pursued.

1. Risk Assessment

Risk assessment corresponds to the overall process of performing risk identification, analysis and evaluation (ISO 31000).

1.1. Risk Identification

Risk identification is the process of finding, recognizing and describing risks (ISO 31000).

1.2. Risk Analysis

Per ISO 31000, it corresponds to the: *"Process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation."*

In other words, and oversimplifying it a bit, the purpose of this activity is to assess the event probability/likelihood and impact for the identified risks. This may involve answering a set of well-defined weighted questions to find out their value.

Probability and Impact can be defined as integers with a limited range (e.g. 0-4). By having a very limited range for the values, it makes the process more manageable and easier to perform.

After having agreed on the risk's probability and impact, the same principle can be applied to the calculated risk level which we may categorize by truncating it to something similar to, for example:

- 0: none
- 1-4: low
- 5-8: medium
- 9-12: high
- 13-15: very high
- 16: severe

If you segment the calculated value or not, and how you do that, is more or less up to you.

This is an example of a risk matrix with the calculated risk levels. You may also use colours to quickly depict the higher risks.

Probability (likelihood)	**4 (very high)**	0	4	8	12	**16**
	3 (high)	0	3	6	9	12
	2 (medium)	0	2	4	6	8
	1 (low)	0	1	2	3	4
	0 (none)	0	0	0	0	0
		0 (none)	**1 (low)**	**2 (medium)**	**3 (high)**	**4 (very high)**
		Impact (consequence)				

1.3. Risk Evaluation

Per ISO 31000, it corresponds to the *"process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment".*

Having the inputs from Risk Analysis, risks need to be evaluated and compared against certain criteria (i.e. risk criteria). This will lead to some sort of relative risk ranking that can be used to decide what decisions to take, which risks need treatments to apply and their priorities.

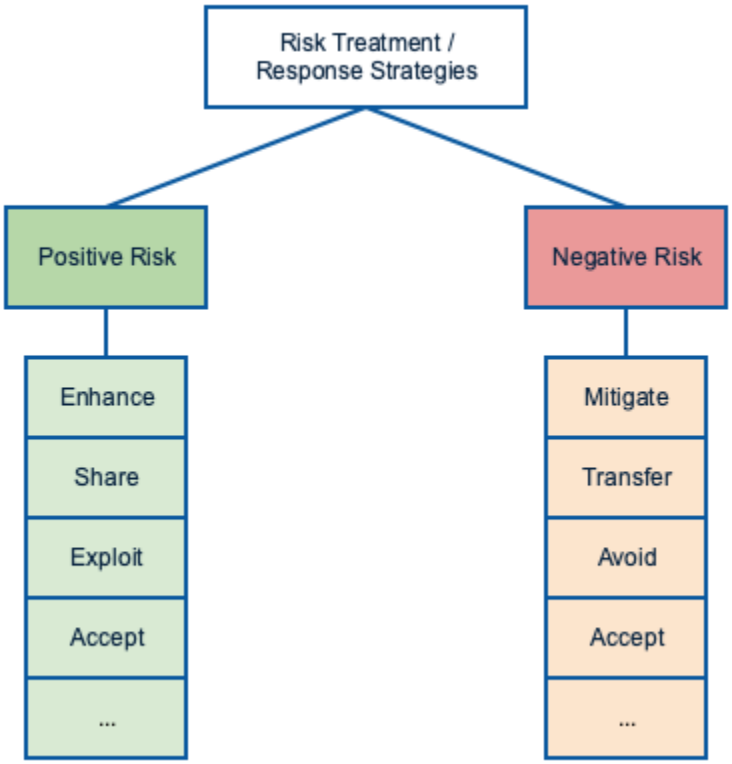
In the end, users need to decide whether risks are acceptable or tolerable, or if they want to modify them instead by treatment measures. As an example, you may decide to apply treatments only on risks categorized as "high," "very high" or "severe."

2. Risk Treatment

Risk Treatment comes as a natural consequence of Risk Evaluation and it corresponds to the "process to modify risk" (ISO 31000).

A risk can be "modified" either by removing its source or because the probability or the impact changed.

Whenever acting on a risk, users can apply one or more of the several possible response strategies (i.e. *treatments,*) depending on the nature /consequence of the risk (i.e. positive or negative risk.)



Briefly, some possible "treatments" are:

- Positive Risk (i.e. "opportunity")
  - Enhance (increase the probability of happening)
  - Share (allocate some/all ownership to a third party)
  - Exploit (ensure opportunity is realized)
  - Accept (leave it as-is and simply take advantage of it, if and when it happens)
- Negative Risk (i.e. "threat")
  - Mitigate (reduce probability of happening)
  - Transfer (transfer it to a third party entity, which may leave some residual risk)
  - Avoid (remove/eliminate risk source)
  - Accept (acknowledge it; don't do anything about it)

3. Parallel, ongoing activities

3.1. Communication and consultation

"Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process."

Communication should happen continuously in order to leverage other activities.

First of all, internal and external stakeholders should be consulted, as a means to establish the context (or reviewing it later on.) However, all of them are invited to provide feedback on the remaining activities as projects/systems and risks evolve in dynamic.

3.2. Risk Monitoring and Reviewing

These are some of the questions we need to answer.

- Can a risk be closed?
- Did the impact or likelihood change?
- Have new risks arisen?
- Did any of the contexts change?
- What have we learned from past events? Are we actively analyzing them?

"Risk monitoring and reviewing" try to answer the previous questions; it can be seen as active surveillance over the whole process as means to ensure that we're effectively on control.

Risk Management in Jira

There are several apps for Risk Management in Jira.

However, they follow different approaches to handling risk.

Some of them perform Risk Management...

- at the issue level with some custom fields
- or at the project level, using a specific issue type

References

- Risk management - Principles and guidelines: ISO 31000:2009(E)
- ISO/IEC 25010:2011 and old ISO 9126:1999 (brief, non-official overview)