GORM: Goal Oriented Risk Management

Author: DI. Andreas Nehfort

Abstract

Risk management has become an integral part of (IT) project management- and software process models. Nevertheless risk management in practice mostly is not that effective.

With GORM - Goal Oriented Risk Management – I tried to eliminate typical weak points of risk management regarding the participation of the relevant stakeholders.

GORM is a systematic approach to derive project risks from project goals and involve the stakeholder which represents the goals into risk management.

This paper describes the ideas behind GORM, its base practices and first experiences applying this goal oriented risk approach.

Keywords

- Project management
- Risk management

Classification:

- Industrial experience report: project management

1 Motivation

In the last 15 years risk management has become an integral part of (IT) project management- and software process theory:

- In the PMI – Project Management Body of Knowledge [1] and the PM baselines [2] (PMA/IPMA) risk management is a “method” for project management
- In the leading process reference models CMMI [4] and SPICE [5] risk management is a (supporting) management process
- Risk management is one of the “ten essentials of RUP” [7] - the “Rational Unified Process” [6].
- In the MSF – Microsoft Solution Framework [8] risk management is called a “core discipline” [9]
- And Tom DeMarco [3] simply says: “Risk management is project management for grown-up’s”.

The newer the model the more risk management becomes an important role → the project team and the project's stakeholders shall not take project success as a matter of course - that's the good news.

During my consulting work I can see that despite to this increasing attention to risk management the practical effect to real world projects is limited - that's the bad news:

- In many projects risk management is not performed at all!
- In most projects, which perform risk management, it is not effective. Risks are identified – but no risk action plan is derived and identified risks are not tracked.
- Only a few projects identify their relevant risks and attack them actively.

Often risk management works as follows:

- Risk management is part of the standard project management process; a risk assessment report and/or risk list is input for the mile-stone-review to start implementation.
- The risk list is produced just for this "quality gate", and then it is part of the project folder; the risk list typically is written once – used never!
- In some way the dealing with risk management reminds me to the dealing with ISO 9001 conformant process descriptions in some companies: produced for the audit ...

In many companies risk management is seen just as a project manager's task. But many risks do not affect the project manager – and so is the result of risk management.

Due to this finding I tried to offer a risk management approach, which is able to affect the people – and to generate value for the project. The first experiences with GORM - the goal oriented risk management approach - are positive!

2 Why do project risks hardly affect the people?

From my point of view there are two reasons why risk management can hardly affect the people:

Reason 1: Risk management is dealing with some unexpected and unwanted consequences of the project – with problems!

"Danger of Avalanches" can trigger the message: "Skiing outside the slopes is dangerous". But for a good skier skiing outside the slopes is fun! This can initiate some conflicts, which we don't want to have … and consequently don't want to deal with.

Reason 2: Risk management is applied probability theory – and man has no sense organ for probability! A risk is a potential problem – and at no time we have the problem "potentially":

- As long as the risk is a potential problem, we do not have the problem at all.
- And when the risk becomes a problem, we have the problem entirely.

And so mostly the motivation is low to deal with project risks! And due to the low motivation most project managers do not develop the skills to apply the risk management techniques to their project in a way that can help them to prevent potential problems.

And sometimes the line management makes risk management difficult when it does not act consistently:

- On the one hand they call their project managers to apply risk management
- On the other hand they do not want to be affected by the problems …

I will illustrate that with a true example of one of my customers:

- Mr. Meyer: Project Manager; he has prepared his top-three risk-list for the milestone-review meeting
- Mr. Smith: Line Manager; member of the steering committee

Mr. Smith:
Well, Mr. Meyer what's about risks in you project?

Mr. Meyer:
My number one risk is, that you could shift my key-resources to another project. Then I would get seriously problems with the quality of the results and with the schedule.

Mr. Smith:
Ah … You can forget that! That's no risk – that's **my** management decision!

The result: Mr. Mayer was unhappy – no he was angry and frustrated! Nobody was interested in his number one risk!

His reaction: If they don't care about my number one risk, I don't care about risk management any more!

All the risk management techniques mentioned in the introduction and in the bibliography do not address these motivation problems. And they typically do not address the balance of rights and duties of the project manager and his/her contractors (stakeholders).

3 GORM – the basic idea

For assessing the influence of standard risks (like estimation errors, function growth and so on) Tom DeMarco's RISKOLOGY-Tool [3] shows a reasonable way that has proofed in praxis. So I focused on the analysis of project individual risks and the project specific valuation of risks.

The story of Mr. Mayer and Mr. Smith told me that the view to a risk is stakeholder specific and may differ substantially. And that was the initial impulse to GORM – the **G**oal **O**riented **R**isk **M**anagement approach.

The basic idea:

- To link risks to their stakeholders!
- To involve stakeholders in risk analysis and deriving risk consequences:

In project context the project is defined by goals (and this goals may be substantiated as requirements)

- The goals are coming from stakeholders which are interested in (some of) the project results.
- So in the project context a “risk” can be defined as the possibility to fail a goal.
- So we can allocate each risk to (at least one) stakeholder (see the figure below).
- So each stakeholder can valuate his/her risks and bring in his/her interest in risk mitigation.
- So the project manager can negotiate about risk mitigation with those stakeholders, who are affected by the potential problem.

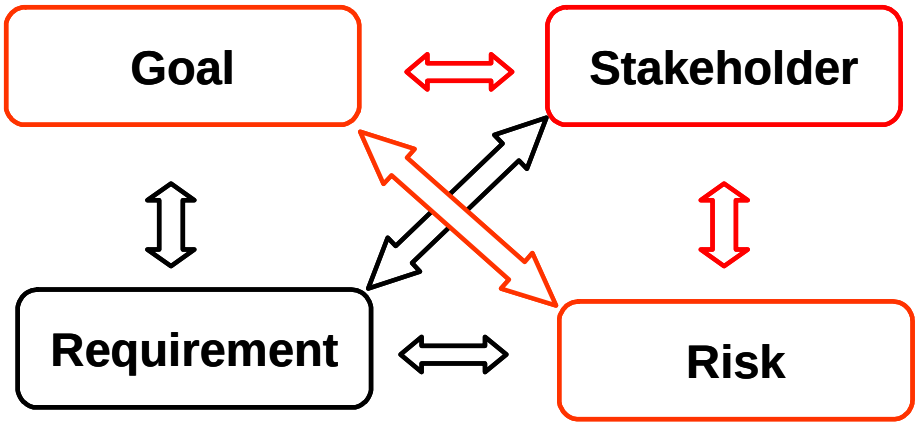

Fig. 1: Stakeholder ⇔ Goal ⇔ Risk Relationship

Using this approach we can shift risk management from an academic routine for project managers to a steering instrument for project stakeholders.

Note: When the risk becomes a problem, it is always the stakeholder who has the problem. For most problems this stakeholder is outside the project team. The team typically provides but does not need the project results, does not bear additional costs, …

This kind of stakeholder involvement follows Kent Becks [10] principle: “The customer makes business decisions and the development team makes technical decisions”. Stating business goals and acting on the corresponding risks is a business decision.

This goal oriented view to risks means on the other side: “No goal - No risk!” When there is no goal – there is no risk to fail the goal!

An example:

- "When do you want to arrive?"
- "Well, I start in the morning and go – and I will see how long it takes – and when I an there - I am arrived."

Fine thing: No risk to come late! - It is the same with projects:
Without clearly stated goals there is no basis for clearly risk statements!

4 GORM – how it works

Following the typical steps of risk management I will figure out the specific points of goal oriented risk management – the stakeholder involvement:

- Identify the stakeholders
- Goal oriented risk identification
- Goal oriented risk analysis
- Goal oriented risk action planning
- Goal oriented risk tracking

The goal oriented risk identification starts with identifying the project's stakeholders and their goals. If the project manager realizes, that the stakeholders and/or their goals are not clearly stated he/she has identified a fundamental project risk:

- An ambiguous project order!

4.1 Identify the stakeholders

Typical classes of stakeholders are:

- The stakeholder(s) for the utilization of the application → business benefit
- The stakeholder(s) for the use of the application → usability & efficiency
- The stakeholder(s) which fund the investment → ROI - return of investment
- The stakeholder(s) for legal and application specific regulations → compliance
- The stakeholder(s) which operates the application → IT services
- The stakeholder(s) for implementing the application → feasibility, schedule and budget

Some of these stakeholders (but typically not all of them) may be represented in the "steering committee", but some of them are typically not represented in the early definition phase of a project. This may but need not to be a source of risks.

Some of them are used to act in their stakeholder role, some of them are not, some of them are in close contact to the project, some of them may be far away when the course is set …That all depends on the project setting.

I can not recommend to identify and involve all these stakeholders – this would unnecessarily obstruct the project in a critical phase regarding its progress – but you

should not overlook (ignore) stakeholders which are associated with risky project goals, features or characteristics.

4.2 Goal oriented risk identification

Typical steps of goal oriented risk identification are:

- Go to the stakeholders (or bring them together)
- Ask them for their goals → If necessary: help them to formulate their goals.
- Search for causes which can lead in failing the goal → the risks.

4.3 Goal oriented risk analysis

Analyze the risks together with the stakeholders:

- Go to the stakeholders (or bring them together)
- Ask them for the importance of their goals.
- Ask them for the consequences of failing the goal → the problem
- Discuss with the stakeholder the cause and impact of the risk / problem
- Estimate together risk probability and potential losses.
- Formulate the risk statement (e.g. as described in the MSF risk management papers see [9]).

4.4 Goal oriented risk action planning

Negotiation with each stakeholder or the affected group of stakeholders:

- Discus the relevance of the problem
- Discus potential means to reduce the risk
  - Preventive actions to reduce risk probability
  - Preventive actions to reduce potential losses.
  - Emergency actions to reduce the losses when the problem has occurred.
- Discus the effort & costs of potential means to reduce the risk and whether it would count for.
- Define agreed risk mitigation actions including responsibility for acting and further risk tracking (each stakeholder can have his/her own risk portfolio to care for …)

4.5 Goal oriented risk tracking

Involve the stakeholder in tracking their risks regarding

- the re-assessment of the meaning of the potential problem
- the assessment of the effect of performed risk actions
- and the re-adjustment of the risk action plan.

5 GORM – first experiences

The first experiences applying the goal oriented risk approach are positive regarding it's use and benefit for the projects; but they are a little bit surprising regarding the results:

- A project manager had problems to identify his stakeholders: he could list the most important, but he had problems to list them all – to decide who is stakeholder and who is not.
- Some stakeholders (members of the steering committee) were not used to state goals (they typically approve a project request and authorize the budget)
- We had problems to elicit the (business) goals behind the system requirements. Our goal oriented risk approach was the first attempt to ask why shall the system fulfill all these requirements.

In all these cases the goal oriented risk approach did us in the first attempt not lead to better risk statements, but it lead us to deficiencies in the goal formulation and helped us to a better understanding of the stakeholder needs. It also helped to evolve the understanding what the stakeholders role is regarding the project.

The acceptance for the goal oriented risk approach is high – the feedback is, that it makes risk management less abstract and more tangible.

Another side effect was, that the goal oriented risk approach lead us to discuss chances, e.g.:

- What would be the losses, if we start operation three months later than scheduled? … no clear answer …
- What would be the wins, if we start operation three months earlier than scheduled? … thinking …
- I stated: If it does not matter whether we are three months late or early, why do you invest in that system? … thinking …
- And then the stakeholders started an inspired discussion about the expected benefits of the new system, and what we should do, to assure them.
- At the end we discussed, how much the system may cost more, if we manage the start of operation three months earlier.

Bibliography

[1] **PMBOK® guide Ed. 2004**:
A guide to Project Management - Body Of Knowledge;
PMI Project Management Institute Inc. © 2004

[2] **pm baseline Version 2.3** - January 2005
pma - Project Management Austria → www.p-m-a.at
(the Austrian Chapter of the IPMA)

[3] **Waltzing with Bears**: Managing Risks on Software projects
Tom DeMarco & Timothy Lister

2003, Dorset House Publishing Co., Inc.
German Edition:
Bärentango - Mit Risikomanagement Projekte zum Erfolg führen
Tom DeMarco & Timothy Lister (german translation: Dr. Doris Märtin)
2003, Hanser Verlag, Wien, München
ISBN 3-446-22333-9

[4] **CMMI for Development V1.2**; 2006 - **C**apability **M**aturity **M**odel **I**ntegration
Carnegy Mellon University – Software Engineering Institute
→ http://www.sei.cmu.edu/cmmi/

[5] **ISO 15504-5:2006** - Information Technology – Process Assessment
An exemplar process assessment model → www.iso.ch

[6] **RUP® – Rational Unified Process**; Process Guidance by IBM Rational

[7] **The Ten Essentials of RUP**: The Essence of an Effective Development Process;
Rational Software White Paper; © 2000 - Leslee Probasco

[8] **MSF – Microsoft Solution Framework**; Process Guidance by Microsoft
→ www.microsoft.com/msf

[9] Microsoft Solutions Framework Core Whitepapers
MSF Risk Management Discipline v.1.1 Whitepaper;
2002 - Microsoft Corporation

[10] **Extreme Programming Explained**; Kent Beck
Addison Wesley © 2000, ISBN: 0-201-61641-6

Authors biography: DI. Andreas Nehfort

- Consultant for IT & Software Process Improvement (SPI);
  Nehfort IT-Consulting → www.nehfort.at
- Focus: Software Process Models and Software Process Improvement – Agile Processes, Assessment Based Process Improvement → CMMI / SPiCE, Project Management & IT Quality Management.
- Intacs Certified ISO 15504 Assessor
- since 1988 Trainer for IT Project Management, Software Engineering & SW Quality Assurance and reference Models (CMMI & SPICE)
- since1986 self-employed → Nehfort IT-Consulting → www.nehfort.at.
- since 1982 Project Manager, Requirements Analyst & Consultant for Software Engineering & Software Processes
- 1978: start of my professional career as Software-Developer;
- 1975 – 1979: Study of Technical Mathematics at the Technical University of Vienna – certificate Dipl.Ing. (DI.)