Risk-First

Software Development De-Risked

Volume 1: The Menagerie

Rob Moffat

Risk First: The Menagerie

By Rob Moffat

ISBN: tbd.

Credits

tbd

Cover Images: Biodiversity Heritage Library. Biologia Centrali-Americana. Insecta. Rhynchota. Hemiptera-Homoptera. Volume 1 (1881-1905)

Cover Design By P. Moffat (`peter@petermoffat.com`)

Thanks to:

Books In The Series

- **Risk First: The Menagerie:** Book one of the **Risk-First** series argues the case for viewing *all* of the activities on a software project through the lens of *managing risk*. It introduces the menagerie of different risks you’re likely to meet on a software project, naming and classifying them so that we can try to understand them better.
- **Risk First: Tools and Practices:** Book two of the **Risk First** series explores the relationship between software project risks and the tools and practices we use to mitigate them. Due for publication in 2020.

Online

Material for the books is freely available to read, drawn from `risk-first.org`.

Published By

Kite9 Ltd.
14 Manor Close
Colchester
CO6 4AR

Contents

Preface

Welcome to Risk-First!

Let's cover some of the big questions up-front: The why, what, who, how and where of *The Menagerie*.

Why

> "Scrum, Waterfall, Lean, Prince2: what do they all have in common?"

I've started this because, on my career journey, I've noticed that the way I do things doesn't seem to match up with the way the books *say* it should be done. And, I found this odd and wanted to explore it further. Hopefully, you, the reader, will find something of use in this.

I started with this observation: *Development Teams* put a lot of faith in methodology. Sometimes, this faith is often so strong it borders on religion. (Which in itself is a concern.) For some, this is Prince2. For others, it might be Lean or Agile.

Developers put a lot of faith in *particular tools* too. Some developers are pro-or-anti-Java, others are pro-or-anti-XML. All of them have their views coloured by their *experiences* (or lack of) with these tools. Was this because their past projects *succeeded* or *failed* because of them?

As time went by, I came to see that the choice of methodology, process or tool was contingent on the problem being solved, and the person solving the problem. We don't face a shortage of tools in IT, or a shortage of methodologies, or a shortage of practices. Essentially, that all the tools and methodologies that the industry had supplied were there to help *minimize the risk of my project failing*.

This book considers that perspective: that building software is all about *managing risk*, and that these methodologies are acknowledgements of this fact, and they differ because they have *different ideas* about which are the most important *risks to manage*.

What This Is

Hopefully, after reading this, you'll come away with:

- An appreciation of how risk underpins everything we do as developers, whether we want it to or not.
- A framework for evaluating methodologies, tools and practices and choosing the right one for the task-at-hand.
- A recontextualization of the software process as being an exercise in mitigating different kinds of risk.
- The tools to help you decide when a methodology or tool is *letting you down*, and the vocabulary to argue for when it's a good idea to deviate from it.

This is not intended to be a rigorously scientific work: I don't believe it's possible to objectively analyze a field like software development in any meaningful, statistically significant way. (For one, things just change too fast.)

> "I have this Pattern"

Does that diminish it? If you have visited the TVTropes website, you'll know that it's a set of web-pages describing *common patterns* of narrative, production, character design etc. to do with fiction. For example:

> tbd.

Is it scientific? No. Is it correct? Almost certainly. TVTropes is a set of *empirical patterns* for how stories on TV and other media work. It's really useful, and a lot of fun. (Warning: it's also incredibly addictive).

In the same way, tbd, the tbd published a book called "Design Patterns: tbd". Which shows you patterns of *structure* within Object-Oriented programming:

> tbd.

Patterns For Practitioners

This book aimed to be a set of *useful* patterns which practitioners could use in their software to achieve certain goals. "I have this pattern" was a phrase used to describe how they had seen a certain set of constraints before, and how they had solved it in software.

This book was a set of experts handing down their battle-tested practices for other developers to use, and, whether you like patterns or not, knowing them is an important part of being a software developer, as you will see them used everywhere you go and probably use them yourself.

In the same way, this book aims to be a set of *Patterns for Software Risk*. Hopefully after reading this book, you will see where risk hides in software projects, and have a name for it when you see it.

Towards a "Periodic Table"

In the latter chapters of "The Menagerie" we try to assemble these risk patterns into a cohesive whole. Projects fail because of risks, and risks arise from predictable sources.

What This is Not

This is not intended to be a rigorously scientific work: I don't believe it's possible to objectively analyze a field like software development in any meaningful, statistically significant way. (For one, things just change too fast.)

Neither is this site isn't going to be an exhaustive guide of every possible software development practice and methodology. That would just be too long and tedious.

Neither is this really a practitioner's guide to using any particular methodology: If you've come here to learn the best way to do Retrospectives, then you're in the wrong place. There are plenty of places you can find that information already. Where possible, this site will link to or reference concepts on Wikipedia or the wider internet for further reading on each subject.

Who

This work is intended to be read by people who work on software projects, and especially those who are involved in managing software projects.

If you work collaboratively with other people in a software process, you should find Risk-First a useful lexicon of terms to help describe the risks you face.

But here's a warning: This is going to be a depressing book to read. It is book one of a two-book series, but in **Book One** you only get to meet the bad guy.

While **Book Two** is all about *how to succeed*, This book is all about how projects *fail*. In it, we're going to try and put together a framework for understanding the risk of failure, in order that we can reconstruct our understanding of our activities on a project based on avoiding it.

So, if you are interested in *avoiding your project failing*, this is probably going to be useful knowledge.

For Developers

Risk-First is a tool you can deploy to immediately improve your ability to plan your work.

Frequently, as developers we find software methodologies "done to us" from above. Risk-First is a toolkit to help *take apart* methodologies like Scrum, Lean and Prince2, and understand them. Methodologies are *bicycles*, rather than *religions*. Rather than simply *believing*, we can take them apart and see how they work.

For Project Managers and Team Leads

All too often, Project Managers don't have a full grasp of the technical details of their projects. And this is perfectly normal, as the specialization belongs below them. However, projects fail because risks materialize, and risks materialize because the devil is in those details.

This seems like a lost cause, but there is hope: the ways in which risks materialize on technical projects is the same every time. With Risk-First we are attempting to name each of these types of risk, which allows for a dialog with developers about which risks they face, and the order they should be tackled.

Risk-First allows a project manager to pry open the black box of development and talk with developers about their work, and how it will affect the project. It is another tool in the (limited) arsenal of techniques a project manager can bring to bear on the task of delivering a successful project.

How

One of the original proponents of the Agile Manifesto, Kent Beck, begins his book Extreme Programming by stating:

"It's all about risk" > Kent Beck

This is a promising start. From there, he introduces his methodology, Extreme Programming, and explains how you can adopt it in your team, the features to observe and the characteristics of success and failure. However, while *Risk* has clearly driven the conception of Extreme Programming, there is no clear model of software risk underpinning the work, and the relationship between the practices he espouses and the risks he is avoiding are hidden.

In this book, we are going to introduce a model of software project risk. This means that in **Book Two** (Risk-First: Tools and Practices), we can properly analyse Extreme Programming (and Scrum, Waterfall, Lean and all the others) and *understand* what drives them. Since they are designed to deliver successful software projects, they must be about mitigate risks, and we will uncover *exactly which risks are mitigated* and *how they do it*.

Where

All of the material for this book is available Open Source on github.com[1], and at the risk-first.org[2] website. Please visit, your feedback is appreciated.

There is no compulsion to buy a print or digital version of the book, but we'd really appreciate the support. So, if you've read this and enjoyed it, how about buying a copy for someone else to read?

A Note on References

Where possible, references are to the Wikipedia[3] website. Wikipedia is not perfect. There is a case for linking to the original articles and papers, but by using Wikipedia references are free and easy for everyone to access, and hopefully will exist for a long time into the future.

On to The Executive Summary

[1] https://github.com

[2] https://risk-first.org

[3] https://wikipedia.org

Executive Summary

1. There are Lots of Ways of Running Software Projects

There are lots of different ways to look at a project. For example, metrics such as “number of open tickets”, “story points”, “code coverage” or “release cadence” give us a numerical feel for how things are going and what needs to happen next. We also judge the health of projects by the practices used on them - Continuous Integration, Unit Testing or Pair Programming, for example.

Software methodologies, then, are collections of tools and practices: “Agile”, “Waterfall”, “Lean” or “Phased Delivery” (for example) all suggest different approaches to running a project, and are opinionated about the way they think projects should be done and the tools that should be used.

None of these is necessarily more “right” than another- they are suitable on different projects at different times.

A key question then is: **how do we select the right tools for the job?**

2. We can Look at Projects in Terms of Risks

One way to examine a project in-flight is by looking at the risks it faces.

Commonly, tools such as RAID logs and RAG status reporting are used. These techniques should be familiar to project managers and developers everywhere.

However, the Risk-First view is that we can go much further: that each item of work being done on the project is mitigating a particular risk.

Risk isn't something that just appears in a report, it actually drives *everything we do*.

For example:

- A story about improving the user login screen can be seen as reducing *the risk of users not signing up*.
- A task about improving the health indicators could be seen as mitigating *the risk of the application failing and no-one reacting to it*.
- Even a task as basic as implementing a new function in the application is mitigating *the risk that users are dissatisfied and go elsewhere*.

One assertion of Risk-First therefore, is that every action you take on a project is to mitigate some risk.

3. We Can Break Down Risks on a Project Methodically

Although risk is usually complicated and messy, other industries have found value in breaking down the types of risks that affect them and addressing them individually.

For example:

- In manufacturing, *tolerances* allow for calculating the likelihood of defects in production.
- In finance, reserves are commonly set aside for the risks of stock-market crashes, and teams are structured around monitoring these different risks.
- The insurance industry is founded on identifying particular risks and providing financial safety-nets for when they occur, such as death, injury, accident and so on.

Software risks are difficult to quantify, and mostly, the effort involved in doing so *exactly* would outweigh the benefit. Nevertheless, there is value in spending time building *classifications of risk for software*. That's what Risk-First does: describes the set of *risk patterns* we see every day on software projects.

With this in place, we can:

- Talk about the types of risks we face on our projects, using an appropriate language.
- Expose Hidden Risks that we hadn't considered before.
- Weigh the risks against each other, and decide which order to tackle them.

4. We Can Analyse Tools and Techniques in Terms of how they Mitigate Risk

If we accept the assertion above that *all* the actions we take on a project are about mitigating risks, then it stands to reason that the tools and techniques available to us on a project are there for mitigating different types of risks.

For example:

- If we do a Code Review, we are partly trying to mitigate the risks of bugs slipping through into production, and also mitigate the Key-Man Risk of knowledge not being widely-enough shared.
- If we write Unit Tests, we're also mitigating the risk of bugs going to production, but we're also mitigating against future changes breaking our existing functionality.
- If we enter into a contract with a supplier, we are mitigating the risk of the supplier vanishing and leaving us exposed. With the contract in place, we have legal recourse against this risk.

Different tools are appropriate for mitigating different types of risks.

5. Different Methodologies for Different Risk Profiles

In the same way that our tools and techniques are appropriate to dealing with different risks, the same is true of the methodologies we

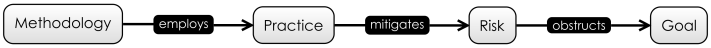


Figure 1: Methdologies, Risks, Practices

use on our projects. We can use a Risk-First approach to examine the different methodologies, and see which risks they address.

For example:

- **Agile** methodologies prioritise mitigating the risk that requirements capture is complicated, error-prone and that requirements change easily.
- **Waterfall** takes the view that coding effort is an expensive risk, and that we should build plans up-front to avoid it.
- **Lean** takes the view that risk lies in incomplete work and wasted work, and aims to minimize that.

Although many developers have a methodology-of-choice, the argument here is that there are tradeoffs with all of these choices. Methodologies are like *bicycles*, rather than *religions*. Rather than simply *believing*, we can take them apart and see how they work.

We can place methodologies within a framework, and show how choice of methodology is contingent on the risks faced.

6. Driving Development With a Risk-First Perspective

We have described a model of risk within software projects, looking something like this:

How do we take this further?

The first idea we explore is that of the Risk Landscape: Although the software team can't remove risk from their project, they can take actions that move them to a place in the Risk Landscape where the risks on the project are more favourable than where they started.

From there, we examine basic risk archetypes you will encounter on the software project, to build up a Taxonomy of Software Risk, and look at which specific tools you can use to mitigate each kind of risk.

Then, we look at different software practices, and how they mitigate various risks. Beyond this we examine the question: *how can a Risk-First approach inform the use of this technique?*

For example:

- If we are introducing a **Sign-Off** in our process, we have to balance the risks it *mitigates* (coordination of effort, quality control, information sharing) with the risks it *introduces* (delays and process bottlenecks).
- If we have **Redundant Systems**, this mitigates the risk of a *single point of failure*, but introduces risks around *synchronizing data* and *communication* between the systems.
- If we introduce **Process**, this may make it easier to *coordinate as a team* and *measure performance* but may lead to bureaucracy, focusing on the wrong goals or over-rigid interfaces to those processes.

Risk-First aims to provide a framework in which we can *analyse these choices* and weigh up *accepting* versus *mitigating* risks.

Still interested? Then dive into reading the introduction.

Part I

Introduction

Part II

Risk

CHAPTER 1

Agency Risk

Coordinating a team is difficult enough when everyone on the team has a single Goal. But, people have their own goals, too. Sometimes, the goals harmlessly co-exist with the team's goal, but other times they don't.

This is Agency Risk. This term comes from finance and refers to the situation where you (the "principal") entrust your money to someone (the "agent") in order to invest it, but they don't necessarily have your best interests at heart. They may instead elect to invest the money in ways that help them, or outright steal it.

> "This dilemma exists in circumstances where agents are motivated to act in their own best interests, which are contrary to those of their principals, and is an example of moral hazard." - Principal-Agent Problem, *Wikipedia*[1]

The less visibility you have of the agent's activities, the bigger the risk. However, the whole *point* of giving the money to the agent was that you would have to spend less time and effort managing it.

Agency Risk clearly includes the behaviour of Bad Actors[2]. But, this is a very strict definition of Agency Risk. In software development, we're not lending each other money, but we are being paid by the project sponsor, so they are assuming Agency Risk by employing us.

[1] https://en.wikipedia.org/wiki/Principalagent_problem

[2] https://en.wiktionary.org/wiki/bad_actor

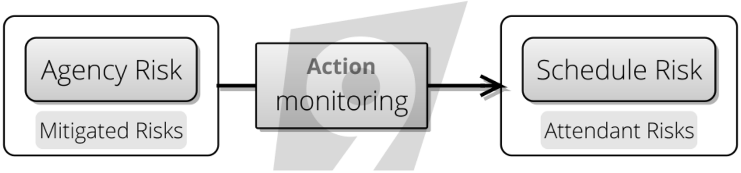


Figure 1.1: Mitigating Agency Risk Through Monitoring

As we saw in the previous section on Process Risk, Agency Risk doesn't just apply to people: it can apply to *running software* or *whole teams*.

Let's look at some examples of borderline Agency Risk situations, in order to sketch out where the domain of this risk lies.

1.1 Personal Lives

We can't (shouldn't) expect people on a project to sacrifice their personal lives for the success of the project, right? Except that "Crunch Time"[3] is exactly how some software companies work:

> "Game development... requires long working hours and dedication from their employees. Some video game developers (such as Electronic Arts) have been accused of the excessive invocation of"crunch time"."Crunch time" is the point at which the team is thought to be failing to achieve milestones needed to launch a game on schedule.
> " - Crunch Time, *Wikipedia*

People taking time off, going to funerals, looking after sick relatives and so on are all Agency Risk, but they should be *accepted* on the project. They are a necessary Attendant Risk of having *staff* rather than *slaves*.

[3] https://en.wikipedia.org/wiki/Video_game_developer#%22Crunch_time%22

1.2 The Hero

> "The one who stays later than the others is a hero." - Hero Culture, *Ward's Wiki*[4]

Conversely, Heroes put in more hours and try to rescue projects single-handedly, often cutting corners like team communication and process in order to get there.

Sometimes, projects don't get done without heroes. But other times, the hero has an alternative agenda than just getting the project done:

- A need for control, and for their own vision.
- A preference to work alone.
- A desire for recognition and acclaim from colleagues.
- For the job security of being a Key Man[5].

A team *can* make use of heroism, but it's a double-edged sword. The hero can becomes a bottleneck to work getting done, and because want to solve all the problems themselves, they under-communicate.

1.3 Consultancies

When you work with an external consultancy, there is *always* more Agency Risk than with a direct employee. This is because as well as your goals and the employee's goals, there is also the consultancy's goals.

This is a good argument for not using consultancies, but sometimes the technical expertise they bring can outweigh this risk.

Also, try to look for *hungry* consultancies: if you being a happy client is valuable to them, they will work at a discount (either working cheaper, harder or longer or more carefully) as a result.

[4] http://wiki.c2.com/?HeroCulture

[5] https://en.wikipedia.org/wiki/Key_person_insurance

1.4 CV Building

This is when someone decides that the project needs a dose of "Some Technology X", but in actual fact, this is either completely unhelpful to the project (incurring large amounts of Complexity Risk), or merely less useful than something else.

It's very easy to spot CV building: look for choices of technology that are incongruently complex compared to the problem they solve, and then challenge by suggesting a simpler alternative.

1.5 Career Risk

1.6 Devil Makes Work

Heroes can be useful, but *underused* project members are a nightmare. The problem is, people who are not fully occupied begin to worry that actually, the team would be better off without them, and then wonder if their jobs are at risk.

The solution to this is "busy-work": finding tasks that, at first sight, look useful, and then delivering them in an over-elaborate way (Gold Plating[6]) that'll keep them occupied. This will leave you with more Complexity Risk than you had in the first place.

Even if they don't worry about their jobs, doing this is a way to stave off *boredom*.

1.7 Pet Projects

> A project, activity or goal pursued as a personal favourite, rather than because it is generally accepted as necessary or important. - Pet Project, *Wiktionary*[7]

Sometimes, budget-holders have projects they value more than others without reference to the value placed on them by the business. Perhaps

[6] https://en.wikipedia.org/wiki/Gold_plating_(software_engineering)

[7] https://en.wiktionary.org/wiki/pet_project

the project has a goal that aligns closely with the budget holder's passions, or its related to work they were previously responsible for.

Working on a pet project usually means you get lots of attention (and more than enough budget), but due to Map and Territory Risk, it can fall apart very quickly under scrutiny.

1.8 Morale Risk

> Morale, also known as Esprit de Corps is the capacity of a group's members to retain belief in an institution or goal, particularly in the face of opposition or hardship - Morale, *Wikipedia*[8]

Sometimes, the morale of the team or individuals within it dips, leading to lack of motivation. Morale Risk is a kind of Agency Risk because it really means that a team member or the whole team isn't committed to the Goal, may decide their efforts are best spent elsewhere. Morale Risk might be caused by:

- External factors: Perhaps the employees' dog has died, or they're simply tired of the industry, or are not feeling challenged.
- If the team don't believe a goal is achievable, they won't commit their full effort to it. This might be due to to a difference in the evaluation of the risks on the project between the team members and the leader.
- If the goal isn't considered sufficiently worthy, or the team isn't sufficiently valued.
- In military science, a second meaning of morale is how well supplied and equipped a unit is. This would also seem like a useful reference point for IT projects. If teams are under-staffed or under-equipped, this will impact on motivation too.

1.9 Hubris & Ego

It seems strange that humans are over-confident. You would have thought that evolution would drive out this trait but apparently it's

[8] https://en.wikipedia.org/wiki/Morale

not so:

> "Now, new computer simulations show that a false sense of optimism, whether when deciding to go to war or investing in a new stock, can often improve your chances of winning." - Evolution of Narcissism, *National Geographic*[9]

In any case, humans have lots of self-destructive tendencies that *haven't* been evolved away, and we get by.

Development is a craft, and ideally, we'd like developers to take pride in their work. Too little pride means lack of care, but too much pride is *hubris*, and the belief that you are better than you really are. Who does hubris benefit? Certainly not the team, and not the goal, because hubris blinds the team to hidden risks that they really should have seen.

Although over-confidence might be a useful trait when bargaining with other humans, the thesis of everything so far is that Meeting Reality will punish your over-confidence again and again.

Perhaps it's a little unfair to draw out one human characteristic for attention. After all, we are riddled with biases. There is probably an interesting article to be written about the effects of different biases on the software development and project management processes. (This task is left as an exercise for the reader.)

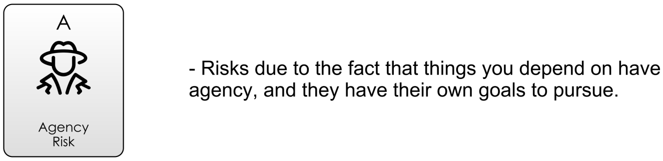
1.10 Software Processes And Teams

Agency Risk doesn't just refer to people - it refers to anything which has agency over it's actions.

> "Agency is the capacity of an actor to act in a given environment... Agency may either be classified as unconscious, involuntary behavior, or purposeful, goal directed activity (intentional action)." - Agency, *Wikipedia*[10]

[9] https://news.nationalgeographic.com/news/2011/09/110914-optimism-narcissism-overconfidence-hubris-evolution-science-nature/

[10] https://en.wikipedia.org/wiki/Agency_(philosophy)



- Risks due to the fact that things you depend on have agency, and they have their own goals to pursue.

Figure 1.2: Agency Risk

There is significant Agency Risk in running software *at all*. Since computer systems follow rules we set for them, we shouldn't be surprised when those rules have exceptions that lead to disaster. For example:

- A process continually writing log files until the disks fill up, crashing the system.
- Bugs causing data to get corrupted, causing financial loss.
- Malware infecting a system, and sending your passwords and data to undesirables.

Agency Risk also covers *whole teams* too. It's perfectly possible that a team within an organisation develops Goals that don't align with those of the overall organisation. For example:

- A team introduces excessive Bureaucracy in order to avoid work it doesn't like.
- A team gets obsessed with a particular technology, or their own internal process improvement, at the expense of delivering business value.
- A marginalised team forces their services on other teams in the name of "consistency". (This can happen a lot with "Architecture", "Branding" and "Testing" teams, sometimes for the better, sometimes for the worse.)

1.11 It's About Goals

We've looked here at some illustrative examples of Agency Risk. But as we stated at the beginning, Agency Risk at any level comes down to differences of Goals between the different agents, whether they are *people*, *teams* or *software*.

So, having looked at agents *individually*, it's time to look more closely at Goals, and the Attendant Risks when aligning them amongst multiple agents.

On to Coordination Risk. . .

Part III

Preview

book1/Part3.md practices/Estimates.md

Glossary

Abstraction

Feedback Loop

Goal In Mind

Internal Model

The most common use for Internal Model is to refer to the model of reality that you or I carry around in our heads. You can regard the concept of Internal Model as being what you *know* and what you *think* about a certain situation.

Obviously, because we've all had different experiences, and our brains are wired up differently, everyone will have a different Internal Model of reality.

Alternatively, we can use the term Internal Model to consider other viewpoints: - Within an organisation, we might consider the Internal Model of a *team of people* to be the shared knowledge, values and working practices of that team. - Within a software system, we might consider the Internal Model of a single processor, and what knowledge it has of the world. - A codebase is a team's Internal Model written down and encoded as software.

An internal model *represents* reality: reality is made of atoms, whereas the internal model is information.

Meet Reality

Risk

Attendant Risk

Hidden Risk

Mitigated Risk

Take Action