Risk Management in Agile Projects

The inherent cadence and iterative nature of Agile practices make them well suited for the management of a wide range of risk commonly encountered in product development and related projects. Indeed, the nature and pace of change in such undertakings present considerable challenges for traditional methods that presume well-defined and stable requirements, together with known risk, that can be captured and modelled using classic techniques. For example, the manner in which understanding of requirements evolves (e.g., facilitated workshops, Agile modelling), the explorative fashion in which designs are implemented (e.g., prototyping, architectural spikes) and the incremental delivery of solutions all help to tackle uncertainty and to promote desired outcomes. This is particularly true of highly innovative solutions where both the customer and the delivery team must collaboratively work together to iteratively define the scope and content of the final solution while tackling both upside and downside risk.

However, throughout Agile literature, there is also a pronounced tendency to focus exclusively on the downside of risk without considering opportunities that can be exploited. This is evident from the view, expressed in many methodologies, that risk should necessarily be considered as an exposure to potentially negative outcomes. Moreover, there is a prevailing view that merely being Agile suffices and that there is also a pronounced tendency to focus exclusively on the downside of risk without considering opportunities that can be exploited. This is evident from the view, expressed in many methodologies, that risk should necessarily be considered as an exposure to potentially negative outcomes. Moreover, there is a prevailing view that merely being Agile suffices and that more explicit attention to the identification, assessment, treatment and monitoring of risk is, therefore, not warranted.

This notwithstanding, some methodologies, such as Agile Project Management (AgilePM), which is based on the dynamic systems development method (DSDM), do incorporate an approach to risk management that is more consistent with risk community practices. Furthermore, there is a growing appreciation within the Agile community of the link between risk (under in terms of uncertainty) and learning.

In reality, risk can be subtle and complex, making them difficult for the uninitiated to identify and manage. Irrespective of the chosen Agile methodology, it is incumbent on Agile risk management to address the following concerns:

- Recognition of threats and opportunities within a project in order to balance the desire for reward against the risk incurred in its pursuit. This requires not only a thorough understanding of risk appetite and tolerance within a project, but also an appreciation of the risk inclinations of individual team members and the impact of social and cultural influences on risk management.
- Identification and prioritisation of appropriate risk response strategies (e.g., accept, mitigate, exploit) based on risk exposure and in a manner that is consistent with Agile practices (e.g., inclusion of risk-related tasks in a product backlog or use of a risk-modified Kanban board, which is a planning tool in which activities are moved between lanes representing the phase of development in which they find themselves [e.g., Planned, In Progress, Done] and user story maps as described later in this article).
- Ability to judge whether or not risk is being managed in an effective and efficient manner through the monitoring of risk. This also includes awareness of the residual risk at the iteration level and how these impinge on the overall riskiness of the undertaking.

Thus, Agile risk management underpins project governance in whatever form this takes. In the Agile context, this translates into promoting the visibility of risk, ensuring collective ownership and accountability in relation to risk, and supporting informed decision making in an environment that is often founded on people-centric principles (e.g., collectivism, self-organisation and empowerment).
project risk or how they are contributing towards its management.

The integration of established risk management techniques into Agile projects requires care if the value of team heterogeneity, efficient feedback loops and lean decision making are not to be eroded. Accordingly, it becomes necessary to adapt the risk management approach in a manner consistent with the preferences and principles enshrined in the Agile manifesto rather than to simply graft traditional risk practice on top of an Agile process. Indeed, experience indicates that this is possible using artefacts already commonly found in Agile projects (e.g., product backlog or Kanban board), as illustrated in figure 1.

The natural cadence of Agile projects suggests that risk identification and assessment, along with the identification of risk measures, should be incorporated into iteration planning. In product-oriented methodologies (e.g., Scrum, XP), this corresponds to Sprint planning; whereas, in project-focused approaches (e.g., AgilePM), this ought to occur at the start of each Timebox (i.e., a structured and fixed time period that commences with initiation and planning activities that are followed by implementation work and concluded with a review). Thereafter, treatment and monitoring of risk can be embedded in the everyday practices at the iteration level.

One key difference between traditional and Agile project risk management is that ownership of risk is determined by project team members in a manner similar to the allocation of user stories (i.e., Agile requirements) and related tasks. This transforms the traditional role of the risk manager into one that has a more facilitative character that ensures attention to risk management. Such functions can easily be assumed by existing Agile roles (e.g., Scrum Master, DSDM Project Manager).

**RISK IDENTIFICATION AND ASSESSMENT**

Owing to the manner in which risk and effect are often confused, the identification of risk is harder than one would imagine. Consider, for example, a project to migrate a web application from a physical to a virtual infrastructure in which the concern is raised about whether or not the application will be accessible after the migration. Whilst many may consider the nonavailability of the web application to be a project risk, it is, in fact, the effect of an unsuccessful migration. The real risk resides in the uncertainty that gave rise to the inaccessibility of the web application in the first place (e.g., doubts about whether the configuration of the virtual infrastructure is correct or if the web application is addressable via the domain name system [DNS]).

This confusion between risk and effect is particularly pernicious owing to the manner in which it misdirects risk management activities.
Given the subtle issues surrounding the understanding of risk, one of the best techniques for Agile teams is based upon the what-why approach (figure 1). This entails a group brainstorming session to discover what might occur in a project followed by an analysis of why each event may occur. Whilst the former identifies effects, it is the latter that is concerned with risk. Indeed, it is not uncommon when discussing why an event might occur to hear explicit statements of uncertainty. For example, in the migration example cited previously, the inaccessibility of the web application (what) may be analysed further to reveal numerous risk (whys), such as the configuration of the virtual server or correctness of DNS entries, thereby enabling the identification of meaningful countermeasures. The advantage of this approach lies in its simplicity, especially for teams that may otherwise be unfamiliar with specialist risk management practices owing to the prevalence of more generalist skills. In addition, the diversity often found in Agile teams can be considered a strength in the search for possible risk, owing to the variety of business and technical perspectives. When conducting such sessions, however, do not focus on purely negative events (e.g., by asking what might go wrong), but rather keep the discussion open in order to admit possible opportunities that the project might exploit.

In keeping with traditional practices, risk should be recorded in a register. However, the visibility of this artefact must be maintained at all times and ownership of risk therein assumed by team members in much the same fashion as user stories or other Agile project tasks. This can be achieved by keeping the register in a place accessible to all team members and encouraging them to provide feedback as often and as early as possible (e.g., updates, omissions, corrections).

Risk assessment involves both the determination of risk exposure (where t-shirt sizing often suffices, e.g., using small, medium and large to denote magnitude) and the assignment of a risk score (to be used later during risk monitoring) that is based on the risk exposure band in which a risk falls. This score requires consideration of inherent risk and should accommodate not only what is involved in a requirement or task, but also how it is to done (e.g., use of risk-mitigating Agile techniques). Risk exposure is also central to risk prioritisation which, in turn, is an indication of the urgency with which learning must take place in order to tackle project risk.

**RISK TREATMENT**

Risk assessment provides the input required in order to determine risk responses (e.g., avoid, accept, exploit). Whilst some risk may be tackled by undertaking specific activities (referred to as “risk tasking” in Agile risk management), others require attention to the manner in which activities are undertaken (referred to as “risk tagging” in Agile risk management). For example, the presence of requirements risk when developing a product user interface may encourage the team to ensure that all such user stories are performed using pair programming, an Agile technique wherein two individuals work in tandem. Thus, the team identifies all affected activities and tags them as a reminder of this decision (e.g., perhaps using a double head icon as a visual cue to use pair programming as illustrated in figure 2) when they later perform the activities during the iteration.

A risk-modified Kanban board encourages the colour coding of risk-related tasks (e.g., green for opportunity, red for threat) to support the visualisation of risk. Incidentally, such practices can also be extended to other Agile artefacts, including Agile story maps that describe the relationship between epics and their constitute user stories as illustrated in figure 2. This enables an excellent visualisation of the distribution of risk and even enables detection of where risk analysis may have been deficient (e.g., a collection of user stories with no apparent upside or downside risk).

![Figure 2—Risk Modified User Story Map](source: Alan Moran. Reprinted with permission.)

**RISK MONITORING**

During risk assessment, the scores assigned to measure inherent risk can be used to construct a risk burndown chart that tracks overall risk management efforts. This device, which resembles the widely used story point burndown chart,
also makes clear to the team that there exists an iteration residual risk (comprised of the cumulative residual risk of user stories along with risk linked to transfer or sharing strategies) that cannot be entirely eliminated. Furthermore, it clearly exhibits the dynamics of risk management in a manner that might not otherwise have been clear (e.g., the fact that secondary risk may cause the chart to rise rather than fall). In a practice referred to as “risk walling,” it is recommended to co-locate the risk burnup alongside other risk-related artefacts (e.g., risk register, risk-modified Kanban or user story map) in order to enhance transparency and actively solicit feedback from the team.

CONCLUSION

As Agile becomes ever more widely used, its stance on risk management, governance and related matters remains an impediment in some organisations. This is, however, beginning to change as answers to these challenges are being found and integrated into Agile methodologies and project practices. This provides not only oversight and accountability in relation to risk management, but also ensures that the benefits of Agile in terms of the value it delivers are not eroded.

ENDNOTES

1 Moran, A.; Agile Risk Management, Springer Verlag, Germany, 2014
3 Op cit, Moran
5 Op cit, Moran