Brady Field

Risk Management for Software Development

**Important points**

“A risk is a potential problem; a problem is a risk that has materialized” [261]

“Systematic risk management requires that initial apprehensions be turned into specific root causes, and that the probabilities and potential losses be established.” [261]

“Risks are thus viewed as potential problems that, should they occur, will impact project targets. If there are no quantified targets, then there is no danger that the targets will not be achieved; risk management is meaningless unless targets are defined in measurable terms.” [262]

“Generic risks are those risk factors common to all software projects.” [263]

“A risk management plan may contain both Action Plans and Contingency Plans.” [264]

“A project enters crisis mode when the maximum duration of a contingency plan is exceeded. A crisis is a ‘show-stopper;’ all available resources are focused on solving the problem until the crisis is resolved or the project is rescoped or terminated.” [264]

“Incremental development also lowers the risks of insufficient personnel and failure to meet a fixed delivery date (with, perhaps, less than full capability).” [265]

“Risk Assessment deals with determining the threats to a project, with particular emphasis placed on identifying, analyzing, and prioritizing major risk factors that might become problems.” [266]

“Risk identification is improved by relying on past experience, often in the form of checklists (sometimes structured and quantified with weightings from historical data). The most useful checklists are those derived from local experience.” [267]

“A risk factor may correspond to a single event, to a number of discrete events (any one of which may occur), or to a continuous distribution of possible events.” [267]

“As a project progresses, the operation is monitored to verify that risk factors are indeed being controlled and, if not, the project is redirected as appropriate, thus closing the control loop.” [268]

“The costs as well as the benefits of alternative courses of action must be considered; it is not sensible to spend more on risk reduction than the cost to fix the resulting problem, should it materialize.” [269]

“Risk monitoring (and reporting) on a regular, continuing basis have the goals of identifying risks that are about to become, or have become, problems, determining whether risks and problems are being successfully resolved, and gaining insight to identify new risk factors as they arise.” [270]

“Reporting is upward through the management chain. If possible, a risk factor is mitigated within the group that identifies it, and reported to the next level. A risk that cannot be mitigated within the bounds of authority of the group that identifies it is promoted to the next level for mitigation.” [272]

“Risk Reassessment is a continuous process. The risk management control loop depends on risk monitoring which leads to corrective action, risk reassessment, and adjustments to risk management plans to stay in control of the evolving risk factors.” [272]

“In many organizations the effective application of risk management depends on highly motivated individuals who understand risk management and who hold key positions in the organization.” [274]

**Disagreements**

I read the article a few times in search of a disagreement. I’m afraid I lack the necessary experience to find and soundly oppose a major point in this particular article.

**Questions**

I understood everything in the article.