software engineering glossary

Editor: Richard H. Thayer California State Univ., Sacramento thayer@csus.edu
Technical Reviewer: Merlin Dorfman Cisco Systems dorfman@computer.org

Software Risk Management

Richard E. Fairley

- **contingency plan:** A plan for dealing with a risk factor, should it become a problem.
- continuous risk management: The process of analyzing the progress of a planned activity, project, or program on a periodic, ongoing basis and handling identified risk factors; includes developing options and fallback positions to permit alternative solutions to reduce the impact if a risk factor becomes a problem.
- **crisis:** A critical state of affairs in which a decisive, probably undesirable outcome is impending.
- **crisis management:** Steps to take when a contingency plan doesn't solve the associated problem.
- problem: A negative situation to overcome. A risk factor becomes a problem when a risk metric (an objective measure) crosses a predetermined threshold (the problem trigger).
- **risk:** The probability of incurring a loss or enduring a negative impact.
- risk acceptance: Acknowledgment of a risk factor's existence along with a decision to accept the consequences if the corresponding problem occurs. Also called risk assumption.
- risk analysis: The process of examining identified risk factors for probability of occurrence, potential loss, and potential risk-handling strategies.
- risk avoidance: A course of action that removes a risk factor from further

- consideration (for example, by changing the requirements, extending the schedule, or transferring the risk factor to another domain).
- risk exposure: The product of probability times potential loss for a risk factor; usually expressed in monetary units or utility.
- risk factor: A potential problem that would be detrimental to a planned activity, project, or program, characterized by the probability of problem occurrence (0 and a potential loss (of life, money, property, reputation, and so on) should the problem occur. Both probability and potential loss might change over time.
- risk handling: A course of action taken in response to a risk factor; includes risk acceptance, risk avoidance, risk transfer, and risk mitigation.
- risk identification: An organized, systematic approach to determining the risk factors associated with a planned activity, project, or program.
- risk leverage factor (rlf): rlf = (reb rea)/rmc, where reb is risk exposure before risk mitigation, rea is risk exposure after risk mitigation, and rmc is the risk mitigation activity's cost. Larger rlfs indicate better mitigation strategies.
- risk management: An organized process for identifying and handling risk factors; includes initial identification and handling of risk factors as well as continuous risk management.

- risk metric: An objective measure associated with a risk factor to be mitigated.
- risk mitigation: A course of action taken to reduce the probability of and/or potential loss from a risk factor; includes executing contingency plans when a risk metric crosses a predetermined threshold (when a risk factor becomes a problem).
- risk reduction: Reducing the probability and/or potential impact of a risk factor. Risk reduction might involve research, prototyping, and other means of exploration.
- **risk transfer:** Transferring responsibility for managing a risk factor to another organization or functional entity better able to mitigate the risk factor.
- risk trigger: The predetermined threshold value of a risk metric that triggers invocation of a contingency plan when the risk metric crosses the threshold.
- **root-cause analysis:** Determination of a potential problem's (a risk factor's) underlying cause or causes.
- uncertainty: The result of not having accurate or sufficient knowledge of a situation; often the root cause of a risk factor.
- utility: A measure of value within a given value system, often measured on a scale of 0 to 100.

Richard E. Fairley is a computer science professor at Oregon Health and Science University's OGI School of Science and Engineering. Contact him at d.fairley@computer.org.