# Risk Management





---

***Lead Authors:*** *Ed Conrow, Ray Madachy, Garry Roedler,* ***Contributing Author:*** *Richard Turner*

---

The purpose of risk management is to reduce potential risks to an acceptable level before they occur, throughout the life of the product or project. Risk management is a continuous, forward-looking process that is applied to anticipate and avert risks that may adversely impact the project, and can be considered both a project management and a systems engineering process. A balance must be achieved on each project in terms of overall risk management ownership, implementation, and day-to-day responsibility between these two top-level processes.

For the SEBoK, risk management falls under the umbrella of Systems Engineering Management, though the wider body of risk literature is explored below.

☐

## Contents

# Risk Management Process Overview

Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints. It has the following two components (DAU 2003a):

1. the probability (or likelihood) of failing to achieve a particular outcome
2. the consequences (or impact) of failing to achieve that outcome

In the domain of catastrophic risk analysis, risk has three components: (1) threat, (2) vulnerability, and (3) consequence (Willis et al. 2005).

Risk management involves defining a risk management strategy, identifying and analyzing risks, handling selected risks, and monitoring the progress in reducing risks to an acceptable level (SEI 2010; DoD 2015; DAU 2003a; DAU 2003b; PMI 2013) (Opportunity and opportunity management is briefly discussed below).

The SE risk management process includes the following activities:

- risk planning
- risk identification
- risk analysis
- risk handling
- risk monitoring

ISO/IEC/IEEE 16085 provides a detailed set of risk management activities and tasks which can be utilized in a risk management process aligned with ISO 31000:2009, Risk management — Principles and Guidelines, and ISO Guide 73:2009,

Risk management — Vocabulary. ISO 9001:2008

standard provides risk-based preventive action requirements in subclause 8.5.3.

The Risk Management Process section of the INCOSE Systems Engineering Handbook: A Guide for Systems Life Cycle Processes and Activities, 4th Edition, provides a comprehensive overview of risk management which is intended to be consistent with the Risk Management Process section of ISO 15288.

## Risk Planning

Risk planning establishes and maintains a strategy for identifying, analyzing, handling, and monitoring risks within the project. The strategy, both the process and its implementation, is documented in a risk management plan (RMP).

The risk management process and its implementation should be tailored to each project and updated as appropriate throughout the life of the project.The RMP should be transmitted in an appropriate means to the project team and key stakeholders.

The risk management strategy includes as necessary the risk management process of all supply chain suppliers and describes how risks from all suppliers will be raised to the next level(s) for incorporation in the project risk process.

The context of the Risk Management process should include a description of stakeholders' perspectives, risk categories, and a description (perhaps by reference) of the technical and managerial objectives, assumptions and constraints. The risk categories include the relevant technical areas of the system and facilitate identification of risks across the life cycle of the system. As noted in ISO 31000 the aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

The RMP should contain key risk management information; Conrow (2003) identifies the following as key components of RMP:

- a project summary
- project acquisition and contracting strategies
- key definitions
- a list of key documents

- process steps
- inputs, tools and techniques, and outputs per process step
- linkages between risk management and other project processes
- key ground rules and assumptions
- risk categories
- buyer and seller roles and responsibilities
- organizational and personnel roles and responsibilities

Generally, the level of detail in an RMP is risk-driven, with simple plans for low risk projects and detailed plans for high risk projects.

## Risk Identification

Risk identification is the process of examining the project products, processes, and requirements to identify and document candidate risks. Risk identification should be performed continuously at the individual level as well as through formerly structured events at both regular intervals and following major program changes (e.g., project initiation, re-baselining, change in acquisition phase, etc.).

Conrow (2009) states that systems engineers should use one or more top-level approaches (e.g., work breakdown structure (WBS), key processes evaluation, key requirements evaluation, etc.) and one or more lower-level approaches (e.g., affinity, brainstorming, checklists and taxonomies, examining critical path activities, expert judgment, Ishikawa diagrams, etc.) in risk identification. For example, lower-level checklists and taxonomies exist for software risk identification (Conrow and Shishido 1997, 83-89, p. 84; Boehm 1989, 115-125, Carr et al. 1993, p. A-2) and operational risk identification (Gallagher et al. 2005, p. 4), and have been used on a wide variety of programs. The top and lower-level approaches are essential but there is no single accepted method — all approaches should be examined and used as appropriate.

Candidate risk documentation should include the following items where possible, as identified by Conrow (2003 p.198):

- risk title
- structured risk description

- applicable risk categories
- potential root causes
- relevant historical information
- responsible individual and manager

It is important to use structured risk descriptions such as an *if-then* format: *if* (an event occurs--trigger), *then* (an outcome or affect occurs). Another useful construct is a *condition* (that exists) that leads to a potential *consequence* (outcome) (Gluch 1994). These approaches help the analyst to better think through the potential nature of the risk.

Risk analysis and risk handling activities should only be performed on approved risks to ensure the best use of scarce resources and maintain focus on the correct risks.

## Risk Analysis

Risk analysis is the process of systematically evaluating each identified, approved risk to estimate the probability of occurrence (likelihood) and consequence of occurrence (impact), and then converting the results to a corresponding risk level or rating.

There is no *best* analysis approach for a given risk category. Risk scales and a corresponding matrix, simulations, and probabilistic risk assessments are often used for technical risks, while decision trees, simulations and payoff matrices are used for cost risk; and simulations are used for schedule risk. Risk analysis approaches are sometimes grouped into qualitative and quantitative methods. A structured, repeatable methodology should be used in order to increase analysis accuracy and reduce uncertainty over time.

The most common qualitative method (typically) uses ordinal probability and consequence scales coupled with a risk matrix (also known as a risk cube or mapping matrix) to convert the resulting values to a risk level. Here, one or more probability of occurrence scales, coupled with three consequences of occurrence scales (cost, performance, schedule) are typically used. Mathematical operations should not be performed on ordinal scale values to prevent erroneous results (Conrow 2003, p. 187-364).

Once the risk level for each risk is determined, the risks need to be prioritized. Prioritization is typically performed by risk level (e.g., low, medium, high), risk

score (the pair of max (probability), max (consequence) values), and other considerations such as time-frame, frequency of occurrence, and interrelationship with other risks (Conrow 2003, pp. 187-364). An additional prioritization technique is to convert results into an estimated cost, performance, and schedule value (e.g., probability budget consequence). However, the result is only a point estimate and not a distribution of risk.

Widely used quantitative methods include decision trees and the associated expected monetary value analysis (Clemen and Reilly 2001), modeling and simulation (Law 2007; Mun 2010; Vose 2000), payoff matrices (Kerzner 2009, p. 747-751), probabilistic risk assessments (Kumamoto and Henley 1996; NASA 2002), and other techniques. Risk prioritization can directly result from the quantitative methods employed. For quantitative approaches, care is needed in developing the model structure, since the results will only be as good as the accuracy of the structure, coupled with the characteristics of probability estimates or distributions used to model the risks (Law 2007; Evans, Hastings, and Peacock 2011).

If multiple risk facets exist for a given item (e.g., cost risk, schedule risk, and technical risk) the different results should be integrated into a cohesive three-dimensional *picture* of risk. Sensitivity analyses can be applied to both qualitative and quantitative approaches in an attempt to understand how potential variability will affect results. Particular emphasis should be paid to compound risks (e.g., highly coupled technical risks with inadequate fixed budgets and schedules).

## Risk Handling

Risk handling is the process that identifies and selects options and implements the desired option to reduce a risk to an acceptable level, given program constraints (budget, other resources) and objectives (DAU 2003a, 20-23, 70-78).

For a given system-of-interest (SoI), risk handling is primarily performed at two levels. At the system level, the overall ensemble of system risks is initially determined and prioritized and second-level draft risk element plans (REP's) are prepared for handling the risks. For more complex systems, it is important that the REP's at the higher SoI level are kept consistent with the system RMPs at the lower SoI level, and that the top-level RMP preserves continuing risk traceability across

the SoI.

The risk handling strategy selected is the combination of the most desirable risk handling option coupled with a suitable implementation approach for that option (Conrow 2003). Risk handling options include assumption, avoidance, control (mitigation), and transfer. All four options should be evaluated and the best one chosen for each risk. An appropriate implementation approach is then chosen for that option. Hybrid strategies can be developed that include more than one risk handling option, but with a single implementation approach. Additional risk handling strategies can also be developed for a given risk and either implemented in parallel with the primary strategy or be made a contingent strategy that is implemented if a particular trigger event occurs during the execution of the primary strategy. Often, this choice is difficult because of uncertainties in the risk probabilities and impacts. In such cases, buying information to reduce risk uncertainty via prototypes, benchmarking, surveying, modeling, etc. will clarify risk handling decisions (Boehm 1981).

### Risk Handling Plans

A risk handling plan (RHP - a REP at the system level), should be developed and implemented for all *high* and *medium* risks and selected *low* risks as warranted.

As identified by Conrow (2003, 365-387), each RHP should include:

- a risk owner and management contacts
- selected option
- implementation approach
- estimated probability and consequence of occurrence levels at the start and conclusion of each activity
- specific measurable exit criteria for each activity
- appropriate metrics
- resources needed to implement the RHP

Metrics included in each RHP should provide an objective means of determining whether the risk handling strategy is on track and whether it needs to be updated. On larger projects these can include earned value, variation in schedule and technical performance measures (TPMs), and changes in risk level vs. time.

The activities present in each RHP should be integrated

into the project's integrated master schedule or equivalent; otherwise there will be ineffective risk monitoring and control.

### Risk Monitoring

Risk monitoring is used to evaluate the effectiveness of risk handling activities against established metrics and provide feedback to the other risk management process steps. Risk monitoring results may also provide a basis to update RHPs, develop additional risk handling options and approaches, and re-analyze risks. In some cases, monitoring results may also be used to identify new risks, revise an existing risk with a new facet, or revise some aspects of risk planning (DAU 2003a, p. 20). Some risk monitoring approaches that can be applied include earned value, program metrics, TPMs, schedule analysis, and variations in risk level. Risk monitoring approaches should be updated and evaluated at the same time and WBS level; otherwise, the results may be inconsistent.

## Opportunity and Opportunity Management

In principle, opportunity management is the duality to risk management, with two components: (1) probability of achieving an improved outcome and (2) impact of achieving the outcome. Thus, both should be addressed in risk management planning and execution. In practice, however, a positive opportunity exposure will not match a negative risk exposure in utility space, since the positive utility magnitude of improving an expected outcome is considerably less than the negative utility magnitude of failing to meet an expected outcome (Canada 1971; Kahneman-Tversky 1979). Further, since many opportunity-management initiatives have failed to anticipate serious side effects, all candidate opportunities should be thoroughly evaluated for potential risks to prevent unintended consequences from occurring.

In addition, while opportunities may provide potential benefits for the system or project, each opportunity pursued may have associated risks that detract from the expected benefit. This may reduce the ability to achieve the anticipated effects of the opportunity, in addition to any limitations associated with not pursing an opportunity.

# Linkages to Other Systems Engineering Management Topics

The measurement process provides indicators for risk analysis. Project planning involves the identification of risk and planning for stakeholder involvement. Project assessment and control monitors project risks. Decision management evaluates alternatives for selection and handling of identified and analyzed risks.

# Practical Considerations

Key pitfalls and good practices related to systems engineering risk management are described in the next two sections.

## Pitfalls

Some of the key pitfalls encountered in performing risk management are below in Table 1.

**Table 1. Risk Management Pitfalls.** (SEBoK Original)

| Name | Description |
|---|---|
| Process Over-Reliance | • Over-reliance on the process side of risk management without sufficient attention to human and organizational behavioral considerations. |
| Lack of Continuity | • Failure to implement risk management as a continuous process. Risk management will be ineffective if it's done just to satisfy project reviews or other discrete criteria. (Charette, Dwinnell, and McGarry 2004, 18-24 and Scheinin 2008). |
| Tool and Technique Over-Reliance | • Over-reliance on tools and techniques, with insufficient thought and resources expended on how the process will be implemented and run on a day-to-day basis. |
| Lack of Vigilance | • A comprehensive risk identification will generally not capture all risks; some risks will always escape detection, which reinforces the need for risk identification to be performed continuously. |
| Automatic Mitigation Selection | • Automatically select the risk handling mitigation option, rather than evaluating all four options in an unbiased fashion and choosing the "best" option. |

| | |
|---|---|
| Sea of Green | • Tracking progress of the risk handling plan, while the plan itself may not adequately include steps to reduce the risk to an acceptable level. Progress indicators may appear “green” (acceptable) associated with the risk handling plan: budgeting, staffing, organizing, data gathering, model preparation, etc. However, the risk itself may be largely unaffected if the handling strategy and the resulting plan are poorly developed, do not address potential root cause(s), and do not incorporate actions that will effectively resolve the risk. |
| Band-Aid Risk Handling | • Handling risks (e.g., interoperability problems with changes in external systems) by patching each instance, rather than addressing the root cause(s) and reducing the likelihood of future instances. |

## Good Practices

Some good practices gathered from the references are below in Table 2.

**Table 2. Risk Management Good Practices.** (SEBoK Original)

| Name | Description |
|---|---|
| Top Down and Bottom Up | • Risk management should be both “top down” and “bottom up” in order to be effective. The project manager or deputy need to own the process at the top level, but risk management principles should be considered and used by all project personnel. |
| Early Planning | • Include the planning process step in the risk management process. Failure to adequately perform risk planning early in the project phase contributes to ineffective risk management. |
| Risk Analysis Limitations | • Understand the limitations of risk analysis tools and techniques. Risk analysis results should be challenged because considerable input uncertainty and/or potential errors may exist. |
| Robust Risk Handling Strategy | • The risk handling strategy should attempt to reduce both the probability and consequence of occurrence terms. It is also imperative that the resources needed to properly implement the chosen strategy be available in a timely manner, else the risk handling strategy, and the entire risk management process, will be viewed as a “paper tiger.” |

| | |
|---|---|
| Structured Risk Monitoring | • Risk monitoring should be a structured approach to compare actual vs. anticipated cost, performance, schedule, and risk outcomes associated with implementing the RHP. When ad-hoc or unstructured approaches are used, or when risk level vs. time is the only metric tracked, the resulting risk monitoring usefulness can be greatly reduced. |
| Update Risk Database | • The risk management database (registry) should be updated throughout the course of the program, striking a balance between excessive resources required and insufficient updates performed. Database updates should occur at both a tailored, regular interval and following major program changes. |

# References

## Works Cited


Boehm, B. 1981. *Software Engineering Economics*. Upper Saddle River, NJ, USA: Prentice Hall.

Boehm, B. 1989. *Software Risk Management*. Los Alamitos, CA; Tokyo, Japan: IEEE Computer Society Press: 115-125.

Canada, J.R. 1971. *Intermediate Economic Analysis for Management and Engineering*. Upper Saddle River, NJ, USA: Prentice Hall.

Carr, M., S. Konda, I. Monarch, F. Ulrich, and C. Walker. 1993. *Taxonomy-based risk identification*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-93-TR-6.

Charette, R., L. Dwinnell, and J. McGarry. 2004. "Understanding the roots of process performance failure." *CROSSTALK: The Journal of Defense Software Engineering* (August 2004): 18-24.

Clemen, R., and T. Reilly. 2001. *Making hard decisions*. Boston, MA, USA: Duxbury.

Conrow, E. 2003. *Effective Risk Management: Some Keys to Success,* 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).

Conrow, E. 2008. "Risk analysis for space systems." Paper presented at Space Systems Engineering and Risk Management Symposium, 27-29 February, 2008, Los Angeles, CA, USA.

Conrow, E. and P. Shishido. 1997. "Implementing risk management on software intensive projects." IEEE *Software.* 14(3) (May/June 1997): 83-9.

DAU. 2003a. *Risk Management Guide for DoD Acquisition: Fifth Edition,* version 2. Ft. Belvoir, VA, USA: Defense Acquisition University (DAU) Press.

DAU. 2003b. *U.S. Department of Defense extension to: A guide to the project management body of knowledge (PMBOK(R) guide), first edition*. Version 1. 1st ed. Ft. Belvoir, VA, USA: Defense Acquisition University (DAU) Press.

DoD. 2015. *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC, USA: Office of the Deputy Assistant Secretary of Defense for Systems Engineering/Department of Defense.

Evans, M., N. Hastings, and B. Peacock. 2000. *Statistical Distributions,* 3rd ed. New York, NY, USA: Wiley-Interscience.

Forbes, C., M. Evans, N. Hastings, and B. Peacock. 2011. “Statistical Distributions,” 4th ed. New York, NY, USA.

Gallagher, B., P. Case, R. Creel, S. Kushner, and R. Williams. 2005. *A taxonomy of operational risk*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-2005-TN-036.

Gluch, P. 1994. *A Construct for Describing Software Development Risks*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-94-TR-14.

ISO/IEC/IEEE. 2015. *Systems and Software Engineering -- System Life Cycle Processes*. Geneva, Switzerland: International Organisation for Standardisation / International Electrotechnical Commissions / Institute of Electrical and Electronics Engineers. ISO/IEC/IEEE 15288:2015.

Kerzner, H. 2009. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling.* 10th ed. Hoboken, NJ, USA: John Wiley & Sons.

Kahneman, D., and A. Tversky. 1979. "Prospect theory: An analysis of decision under risk." *Econometrica.* 47(2) (Mar., 1979): 263-292.

Kumamoto, H. and E. Henley. 1996. *Probabilistic Risk Assessment and Management for Engineers and Scientists,* 2nd ed. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers (IEEE) Press.

Law, A. 2007. *Simulation Modeling and Analysis,* 4th ed. New York, NY, USA: McGraw Hill.

Mun, J. 2010. *Modeling Risk,* 2nd ed. Hoboken, NJ, USA: John Wiley & Sons.

NASA. 2002. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,* version 1.1. Washington, DC, USA: Office of Safety and Mission Assurance/National Aeronautics and Space Administration (NASA).

PMI. 2013. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, 5th ed. Newtown Square, PA, USA: Project Management Institute (PMI).

Scheinin, W. 2008. "Start Early and Often: The Need for Persistent Risk Management in the Early Acquisition Phases." Paper presented at Space Systems Engineering and Risk Management Symposium, 27-29 February 2008, Los Angeles, CA, USA.

SEI. 2010. *Capability Maturity Model Integrated (CMMI) for Development,* version 1.3. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie Mellon University (CMU).

Vose, D. 2000. *Quantitative Risk Analysis,* 2nd ed. New York, NY, USA: John Wiley & Sons.

Willis, H.H., A.R. Morral, T.K. Kelly, and J.J. Medby. 2005. *Estimating Terrorism Risk*. Santa Monica, CA, USA: The RAND Corporation, MG-388.

## Primary References

Boehm, B. 1981. *Software Engineering Economics*. Upper Saddle River, NJ, USA:Prentice Hall.

Boehm, B. 1989. *Software Risk Management.* Los Alamitos, CA; Tokyo, Japan: IEEE Computer Society Press, p. 115-125.

Conrow, E.H. 2003. *Effective Risk Management: Some Keys to Success,* 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).

DoD. 2015. Risk, Issue, and Opportunity Management

Guide for Defense Acquisition Programs. Washington, DC, USA: Office of the Deputy Assistant Secretary of Defense for Systems Engineering/Department of Defense.

SEI. 2010. *Capability Maturity Model Integrated (CMMI) for Development,* version 1.3. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie Mellon University (CMU).

## Additional References

Canada, J.R. 1971. *Intermediate Economic Analysis for Management and Engineering*. Upper Saddle River, NJ, USA: Prentice Hall.

Carr, M., S. Konda, I. Monarch, F. Ulrich, and C. Walker. 1993. *Taxonomy-based risk identification*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-93-TR-6.

Charette, R. 1990. *Application Strategies for Risk Management.* New York, NY, USA: McGraw-Hill.

Charette, R. 1989. *Software Engineering Risk Analysis and Management.* New York, NY, USA: McGraw-Hill (MultiScience Press).

Charette, R., L. Dwinnell, and J. McGarry. 2004. "Understanding the roots of process performance failure." *CROSSTALK: The Journal of Defense Software Engineering* (August 2004): 18-24.

Clemen, R., and T. Reilly. 2001. *Making hard decisions*. Boston, MA, USA: Duxbury.

Conrow, E. 2010. "Space program schedule change probability distributions." Paper presented at American Institute of Aeronautics and Astronautics (AIAA) Space 2010, 1 September 2010, Anaheim, CA, USA.

Conrow, E. 2009. "Tailoring risk management to increase effectiveness on your project." Presentation to the Project Management Institute, Los Angeles Chapter, 16 April, 2009, Los Angeles, CA.

Conrow, E. 2008. "Risk analysis for space systems." Paper presented at Space Systems Engineering and Risk Management Symposium, 27-29 February, 2008, Los Angeles, CA, USA.

Conrow, E. and P. Shishido. 1997. "Implementing risk management on software intensive projects." IEEE

*Software.* 14(3) (May/June 1997): 83-9.

DAU. 2003a. *Risk Management Guide for DoD Acquisition: Fifth Edition.* Version 2. Ft. Belvoir, VA, USA: Defense Acquisition University (DAU) Press.

DAU. 2003b. *U.S. Department of Defense extension to: A guide to the project management body of knowledge (PMBOK(R) guide),* 1st ed. Ft. Belvoir, VA, USA: Defense Acquisition University (DAU) Press.

Dorofee, A., J. Walker, C. Alberts, R. Higuera, R. Murphy, and R. Williams (eds). 1996. *Continuous Risk Management Guidebook.* Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU).

Gallagher, B., P. Case, R. Creel, S. Kushner, and R. Williams. 2005. *A taxonomy of operational risk*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-2005-TN-036.

Gluch, P. 1994. *A Construct for Describing Software Development Risks*. Pittsburgh, PA, USA: Software Engineering Institute (SEI)/Carnegie-Mellon University (CMU), CMU/SEI-94-TR-14.

Haimes, Y.Y. 2009. *Risk Modeling, Assessment, and Management*. Hoboken, NJ, USA: John Wiley & Sons, Inc.

Hall, E. 1998. *Managing Risk: Methods for Software Systems Development.* New York, NY, USA: Addison Wesley Professional.

INCOSE. 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities,* version 4. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), INCOSE-TP-2014-001-04.

ISO. 2009. *Risk Management—Principles and Guidelines*. Geneva, Switzerland: International Organization for Standardization (ISO), ISO 31000:2009.

ISO/IEC. 2009. *Risk Management—Risk Assessment Techniques*. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 31010:2009.

ISO/IEC/IEEE. 2006. *Systems and Software Engineering - Risk Management*. Geneva, Switzerland: International

Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE). ISO/IEC/IEEE 16085.

ISO. 2003. *Space Systems - Risk Management.* Geneva, Switzerland: International Organization for Standardization (ISO), ISO 17666:2003.

Jones, C. 1994. *Assessment and Control of Software Risks.* Upper Saddle River, NJ, USA: Prentice-Hall.

Kahneman, D. and A. Tversky. 1979. "Prospect theory: An analysis of decision under risk." *Econometrica.* 47(2) (Mar., 1979): 263-292.

Kerzner, H. 2009. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling,* 10th ed. Hoboken, NJ: John Wiley & Sons.

Kumamoto, H., and E. Henley. 1996. *Probabilistic Risk Assessment and Management for Engineers and Scientists,* 2nd ed. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers (IEEE) Press.

Law, A. 2007. *Simulation Modeling and Analysis,* 4th ed. New York, NY, USA: McGraw Hill.

MITRE. 2012. *Systems Engineering Guide to Risk Management.* Available online: http://www.mitre.org/work/systems_engineering/guide/acquisition_systems_engineering/risk_management/. Accessed on July 7, 2012. Page last updated on May 8, 2012.

Mun, J. 2010. *Modeling Risk,* 2nd ed. Hoboken, NJ, USA: John Wiley & Sons.

NASA. 2002. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,* version 1.1. Washington, DC, USA: Office of Safety and Mission Assurance/National Aeronautics and Space Administration (NASA).

PMI. 2013. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, 5th ed. Newtown Square, PA, USA: Project Management Institute (PMI).

Scheinin, W. 2008. "Start Early and Often: The Need for Persistent Risk Management in the Early Acquisition Phases." Paper presented at Space Systems Engineering and Risk Management Symposium, 27-29 February 2008, Los Angeles, CA, USA.

USAF. 2005. *SMC systems engineering primer &*

*handbook: Concepts, processes, and techniques,* 3rd ed. Los Angeles, CA, USA: Space & Missile Systems Center/U.S. Air Force (USAF).

USAF. 2014. ''SMC Risk Management Process Guide. *Version 2. Los Angeles, CA, USA: Space & Missile Systems Center/U.S. Air Force (USAF).*

Vose, D. 2000. *Quantitative Risk Analysis.* 2nd ed. New York, NY, USA: John Wiley & Sons.

Willis, H.H., A.R. Morral, T.K. Kelly, and J.J. Medby. 2005. *Estimating Terrorism Risk*. Santa Monica, CA, USA: The RAND Corporation, MG-388.

---

< Previous Article | Parent Article | Next Article >
**SEBoK v. 2.10, released 06 May 2024**

---