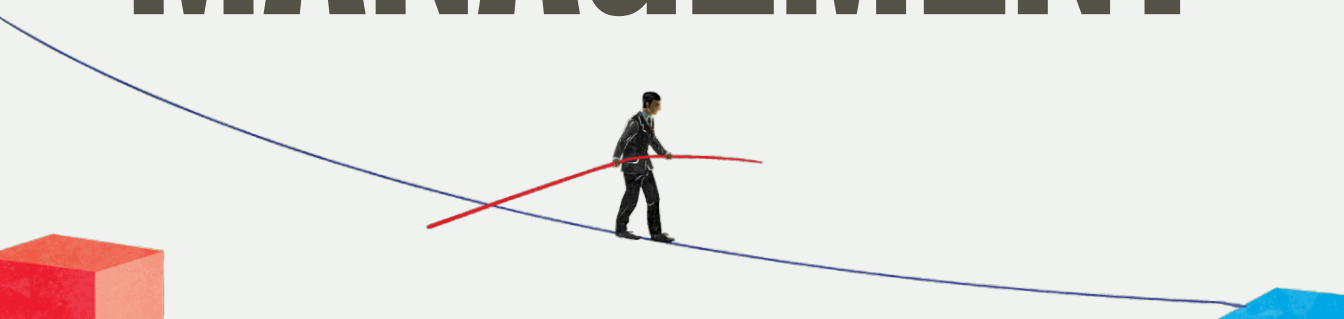
Foundations of QUALITY RISK MANAGEMENT



A Practical Approach to **EFFECTIVE RISK-BASED THINKING**



Jayet **MOON**

Foundations of Quality Risk Management

Risk management titles from Quality Press

Risk Management Using Failure Mode and Effect Analysis (FMEA)
D. H. Stamatis

Managing Organizational Risk Using the Supplier Audit Program
Lance B. Coleman Sr.

Quality Risk Management in the FDA-Regulated Industry, Second Edition
José Rodriguez-Pérez

The Art of Integrating Strategic Planning, Process Metrics, Risk Mitigation, and Auditing
Janet Bautista Smith

Problem-solving titles from Quality Press

Root Cause Analysis: The Core of Problem Solving and Corrective Action, Second Edition
Duke Okes

Introduction to 8D Problem Solving
Donald W. Benbow and Ali Zarghami

Innovative Business Management Using TRIZ
Sunil Kumar V. Kaushik

The Logical Thinking Process: A Systems Approach to Complex Problem Solving
H. William Dettmer

New from Quality Press

Connected, Intelligent, Automated: The Definitive Guide to Digital Transformation and Quality 4.0
N. M. Radziwill

Culture Is Everything: How to Become a True Culture Warrior and Lead Your Organization to Victory
Jeff Veyera

Beyond Compliance Design of a Quality System: Tools and Templates for Integrating Auditing Perspectives
Janet Bautista Smith with Robert Alvarez

The ASQ Certified Quality Improvement Associate Handbook, Fourth Edition
Eds. Grace L. Duffy and Sandra L. Furterer

For more information on Quality Press titles, please visit our website at: http://www.asq.org/quality-press

Foundations of Quality Risk Management

A Practical Approach to Effective Risk-Based Thinking

Jayet Moon



Quality Press
Milwaukee, Wisconsin

American Society for Quality, Quality Press, Milwaukee 53203
All rights reserved. Published 2020
© 2020 by Jayet Moon

No part of this book may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

The views, opinions, and materials presented in this book are the author's alone and do not in any way represent the views, opinions, or materials of the author's current or past employers or affiliations.

Library of Congress Cataloging-in-Publication Data

Names: Moon, Jayet, author.
Title: Foundations of quality risk management : a practical approach to effective risk-based thinking / Jayet Moon.
Description: First Edition. | Milwaukee : Quality Press, 2020. | Includes bibliographical references and index. | Summary: "A comprehensive reference and thorough introduction to risk management and risk-based thinking from a quality perspective and using quality tools"—Provided by publisher.
Identifiers: LCCN 2020029337 (print) | LCCN 2020029338 (ebook) | ISBN 9781951058326 (paperback) | ISBN 9781951058340 (adobe pdf) | ISBN 9781951058333 (epub)
Subjects: LCSH: Risk management. | Quality control.
Classification: LCC HD61 .M5866 2020 (print) | LCC HD61 (ebook) | DDC 658.15/5—dc23
LC record available at https://lccn.loc.gov/2020029337
LC ebook record available at https://lccn.loc.gov/2020029338

Publisher: Seiche Sanders
Managing Editor: Sharon Woodhouse

ASQ advances individual, organizational, and community excellence worldwide through learning, quality improvement, and knowledge exchange.

Bookstores, wholesalers, schools, libraries, businesses, and organizations: Quality Press books are available at quantity discounts for bulk purchases for business, trade, or educational uses. For more information, please contact Quality Press at 800-248-1946 or books@asq.org.

To place orders or browse the selection of all Quality Press titles, visit our website at: http://www.asq.org/quality-press

♾ Printed on acid-free paper

Printed in the United States of America

25 24 23 22 21 20 6 5 4 3 2 1



Quality Press
600 N. Plankinton Ave.
Milwaukee, WI 53203-2914
E-mail: authors@asq.org
The Global Voice of Quality®

This book is dedicated to A. R. Moon

If you don't run the risk of change, you don't have the benefit of advancement.

—Andrew Cuomo, governor of New York

If you only take small risks, you are only entitled to a small life.

—Robin Sharma, author of *The Monk Who Sold His Ferrari* book series

If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business.

—Gary Cohn, former director of the United States National Economic Council

Table of Contents

List of Tables and Figures . . . . . *xi*
Foreword . . . . . *xix*
Preface . . . . . *xxi*
Acknowledgments . . . . . *xxix*

1 Introduction to Risk Management 1
2 Quality and Risk Management 5
Risk Management and the Process Approach 6
3 So, What Is Risk? 10
4 Risk-Based Thinking 13
5 Risk-Based Decision Making 16
6 ISO 9001 and Risk Management 20
Risk, Opportunity, and ISO 9001 23
7 Basic Risk Identification and Analysis 24
8 Events and Consequences 31
9 Basic Risk Modification 36
10 The Stakeholder 40
11 Upside of Risk: Opportunity 44
12 Detailed Risk Identification 47
Where Do the Risks Come From? 52
How Do We Identify the Risks? 55
13 Chance and Possibilities 57
14 Organizational Context and Risk Management: The Working Details 64
15 Stakeholder Risk Attitude and Appetite 68
16 Organizational Context and Risk Management 2: The Top View 71
The Organizational Business Model 72
Organizational Culture 72
The Value Chain 73
17 Comprehensive Risk Management Maturity (CoRMM) Model 75
18 Risk Management Planning and Risk Management Plan 79
Integration of the Risk Management Plan and the Quality Management Plan 82

19 Risk Process Facilitation 83
Risk Management Teams 88
20 The Risk Repository (Risk Register or Hazard Log) 90
21 Detailed Risk Identification Tools 92
Risk Breakdown Structure 92
Structured What-If Technique (SWIFT) 94
Assumptions and Constraints Analysis 96
SWOT Analysis 98
22 Checkpoint: Risk Assessment—a Macro View 100
23 Hazard, Hazardous Situation, and Benefit and Harm 103
24 Detailed Consequence Analysis 109
Fault Tree Analysis (FTA) 110
Decision Tree Analysis 111
Event Tree Analysis (ETA) 112
Bow Tie Analysis 114
Cause and Consequence Analysis (CCA) 117
Scenario Analysis 118
Root Cause Analysis (RCA) 119
Preliminary Hazard Analysis (PHA) 122
25 Risk Analysis 125
26 The Risk Matrix and Its Constituents 128
27 Risk Evaluation 140
28 Risk Treatment/Modification Selection 149
Positive Risk Realization by Design 152
29 Risk Response Planning 157
The Concept of Secondary Risk 158
The Concept of Residual Risk 158
The Concept of Inherent Risk 159
Contingency Planning 160
30 Monitoring and Reviewing Risk 163
31 Monitoring and Reviewing Risk 2 167
What Are Trigger Conditions and Why Should They Be Monitored? 168
Risk Awareness 170
Risk Audits 170
32 Graphical Tools for Monitoring and Reviewing Risk 172
Pareto Charts 172
Scatter Plots 172

Bar Graphs and Histograms 175
Line and Time Series Charts 177
Run Charts 178
Control Charts 178
Pie Charts 180
Dotplots 181
Individual Value Plots 182
Radar Charts 182
Area Charts 183
J Charts 183
33 Visual Risk Exposure Tracker 187
34 A DMAIC Approach for Structured Risk-Based Trending 190
Applicability of Control Charts for Trending 190
What Is Risk-Based Trending? 191
The Five-Step DMAIC Process 191
Which Control Charts Should We Use? 194
Attribute Chart Assumptions 196
Real-World Application 197
35 Risk-Based Auditing 202
Audit Outcomes 203
Auditing Risks: Threats and Opportunities 204
36 Risk-Benefit Analysis 206
Generalized Method for Risk-Benefit Assessment for Drugs, Medical Devices, and Combination Products 213
37 Cognitive Science of Risk-Based Decision Making 222
38 Risk-Based Design Thinking: Risk Mitigation by Design 227
39 Supplier or Vendor Risk Oversight 232
Graphical Supplier Risk Representation 236
Preparing for Unanticipated Supplier Risks 237
40 Risk in Industry 4.0 239
41 Advanced Risk Tools: Failure Modes and Effects Analysis (FMEA) 242
Workflow for UFMEA 257
Workflow for PFMEA 257
Relationship between DFMEA and UFMEA 257
42 Advanced Risk Tools: Hazard Analysis 261
Identify the Hazard 261
Identify the Sequence of Events 262

Identify the Hazardous Situation 264
Identify the Harm 264
Estimate the Occurrence of the Harm 264
Select a Scoring System 265
Estimate the Severity of the Harm 265
Calculate the Risk 265
Identify the Cause 266
Implement Risk Control 266
Perform a Risk-Benefit Analysis 269
43 Advanced Risk Tools: Hazard and Operability Study (HAZOP) 270
44 Advanced Risk Tools: Hazard Analysis and Critical Control Points (HACCP) 280
Seven Principles of HACCP 281
45 Advanced Risk Tools: Fault Tree Analysis (FTA) 292
Risk Analysis Using FTA 294
46 Advanced Risk Tools: Monte Carlo Analysis. 298
47 Pandemic and Epidemic Risk Management 307
Step 1: Risk Identification 309
Step 2: Risk Analysis 310
Step 3: Risk Evaluation 311
Quantitative Risk Management. 315
Risk Mitigation 317
Risk Monitoring 317
Epidemic and Pandemic Preparedness for Businesses 323
Risk Perception 324

Bibliography 325
Index 333
About the Author 349

Tables and Figures

Figure 1.1 Risk management pillars 2
Figure 1.2 An example of hierarchical risk management 3
Figure 2.1 Quality management and PDCA 6
Figure 2.2 The process approach 7
Figure 2.3 Confluence of risk management, process approach, and PDCA with quality management 8
Figure 2.4 PDCA and risk management 8
Figure 2.5 PDCA to risk management with traditional steps 9
Figure 3.1 Time-based objectives realization 11
Figure 4.1 Probability distribution of two simultaneously cast fair dice 14
Table 4.1 Increasing the probability of winning via successive bets on number 7 15
Figure 5.1 Decision-making steps 17
Figure 5.2 Risk-based decision-making model 18
Figure 5.3 Risk-driven decision making leading to exploitation of opportunities and mitigation of threats 18
Table 6.1 Risk focus of ISO 9001:2015 clauses 22
Figure 6.1 Risk management process overview 23
Table 7.1 Dictionary definitions of risk 25
Table 7.2 Frequency or occurrence table 25
Table 7.3 Tabulation of events, outcomes, and their probabilities 26
Table 7.4 Severity table 27
Table 7.5 Tabulation of events, outcomes, probabilities, and severity levels 27
Table 7.6 3 × 3 risk matrix 28
Table 7.7 Tabulated risk assessment 29
Figure 7.1 Consequence–time series chart for aggregate risks 30
Table 8.1 Tabulated risk assessment 32
Table 8.2 Severity scale 33
Figure 8.1 The consequence polygon 33
Table 8.3 Expanded risk assessment with immediate and final consequences 34
Table 9.1 Tabulated risk assessment 36
Table 9.2 Tabulated risk assessment with a column for risk modification 37
Table 9.3 Tabulated risk assessment with modified probability and risk levels 38
Figure 9.1 Consequence–time series presentation of risk after mitigation (no unacceptable risks in this case) 39
Figure 10.1 Influence–engagement matrix 42
Figure 10.2 Influence–engagement matrix with stakeholder assignation 43
Table 10.1 An example of a RACI matrix 43

Table 11.1 Dictionary definitions of risk 45
Table 11.2 Expected monetary value analysis for a $5 bet 46
Figure 12.1 From risk source to outcome 49
Figure 12.2 Dirt road as a risk source leading to vibration as a hazard and dislodged components as a hazardous situation 49
Figure 12.3 Neighbor's rabbit farm as the risk source, rabbit as the hazard, rabbit's entry into the vegetable patch as the hazardous situation, and rabbit eating the lettuce crop as the negative outcome 50
Table 12.1 Tabular organization of cause, risky event, effect, classification, and risk line item 52
Figure 12.4 General sources of risk 54
Figure 12.5 Risk identification process: points to remember 55
Figure 12.6 Risk identification: past, present, and future 55
Table 13.1 Types of probability assignations 58
Table 13.2 Qualitative probability and its description 59
Table 13.3 Semiquantitative probability table 59
Figure 13.1 A causal probability tree for outcomes related to ringing of a doorbell 61
Figure 13.2 Causal probability chain related to storage of radioactive material in a sealed chamber 62
Figure 13.3 Causal probability chain template 62
Table 15.1 An example of risk attitude and corresponding appetite and tolerance 70
Table 17.1 CoRMM attributes and scoring key 76
Figure 19.1 Four stages of team performance 84
Figure 19.2 Zones of risk facilitation 85
Figure 19.3 Facilitation styles as team progresses through Tuckman's four stages 86
Table 21.1 Example of Risk Breakdown Structure (RBS) 93
Table 21.2 Another example of RBS 94
Figure 21.1 SWIFT process 95
Figure 21.2 SWIFT process example (car tire) 97
Figure 21.3 Assumptions/constraints analysis decision tree 98
Figure 21.4 SWOT analysis 99
Figure 22.1 Risk management process per ISO 31000:2018 101
Figure 23.1 Bottle of pesticide: a hazard 104
Figure 23.2 Baby near the bottle of pesticide: hazardous situation 105
Figure 23.3 Baby hurt by the spilled pesticide: harm 105
Figure 23.4 Hazard to harm 106
Table 23.1 Tabular representation of hazard to harm 106
Figure 23.5 Hazard to benefit 107
Figure 23.6 Spectrum of events that lead from hazard to hazardous situation on the left and spectrum of consequences on the right 107
Figure 23.7 An example of harm and benefit (negative and positive consequence) resulting from the same hazard 108
Figure 24.1 Effects analysis in light of uncertainty 110
Figure 24.2 Consequence analysis as a part of structured risk analysis 110

Figure 24.3 FTA example with top event of car sliding off the road 111
Figure 24.4 Decision tree analysis 112
Figure 24.5 Chance node and final quantitative outcomes of decision tree analysis 113
Figure 24.6 Expanded decision tree analysis. 113
Figure 24.7 ETA for initiating event of a short circuit 114
Figure 24.8 Frequency calculation of fire due to explosion 115
Figure 24.9 Simplified fundamentals of bow tie analysis 115
Figure 24.10 Simplified bow tie analysis for hazardous event of release of radioactive substance from a chamber 116
Figure 24.11 Complete bow tie analysis of release of radioactive substance from a chamber 117
Figure 24.12 Basic logic of CCA 118
Figure 24.13 Example of CCA: Brexit 118
Figure 24.14 Scenario analysis 119
Figure 24.15 Steps of RCA 120
Figure 24.16 Steps for creation of a fishbone diagram. 121
Figure 24.17 Example of 5 Whys tool. 122
Figure 24.18 Steps in PHA 123
Figure 24.19 From hazard to a variety of harms. 123
Table 24.1 PHA example 124
Figure 25.1 Consequence analysis and occurrence assignation together compose the risk analysis 126
Figure 25.2 Illustration aid for usage of risk metalanguage 127
Figure 25.3 Flow from hazard to effects (outcomes) 127
Figure 26.1 Risk as a combination of severity of earthquake impact and likelihood of earthquake occurrence 129
Figure 26.2 Severity scale for earthquakes. 130
Figure 26.3 Generic idea of an impact/consequence table 131
Table 26.1 Impact scale from ISO 14971 131
Table 26.2 Clavien-Dindo scale of surgical complications 132
Table 26.3 Severity scale from AIAG 133
Table 26.4 Severity scale from MIL-STD-882E. 133
Table 26.5 Risk consequence criteria from NASA S3001 Rev G 134
Figure 26.4 Generic idea of a probability table or occurrence scale 135
Table 26.6 Probability scale from ISO 14971:2007 135
Table 26.7 Occurrence scale from AIAG 136
Figure 26.5 A 2 × 2 risk matrix 137
Table 26.8 "X by X" risk matrix. 137
Table 26.9 5 × 5 risk matrix 137
Figure 26.6 Three-dimensional representation of a 5 × 5 risk matrix 138
Figure 26.7 Steps of risk level assignation 138
Table 27.1 A 5 × 5 risk matrix 141
Table 27.2 Risk levels and decision rules 142
Table 27.3 Risk matrix populated using RPN (Probability × Impact) 142

Table 27.4 Risk criticality levels and RPN 142
Table 27.5 Risk matrix coded for risk levels by acceptability decisions. 143
Table 27.6 Severity scale from ISO 14971:2007 144
Table 27.7 Occurrence scale from ISO 14971:2007 144
Table 27.8 3 × 3 risk matrix from ISO 14971:2007 144
Table 27.9 Probability scale from ISO 14971:2007 144
Table 27.10 Risk matrix shaded with acceptable and unacceptable risk levels. 145
Table 27.11 5 × 5 risk matrix from ISO 31010:2019 145
Table 27.12 5 × 4 risk matrix from MIL-STD-882E 146
Table 27.13 5 × 4 risk matrix from ANSI Z590.3-2011 146
Table 27.14 3 × 3 risk matrix 147
Table 27.15 5 × 5 risk matrix 147
Figure 27.1 Outcomes of the risk evaluation process 147
Figure 28.1 Four options for risk treatment or modification 150
Figure 28.2 Risk responses to positive and negative risks 152
Table 28.1 Risk matrix for design improvement reliability 153
Table 28.2 Risk matrix for risk-based resource considerations 153
Figure 28.3 Flowchart to assess risk-based opportunities 154
Figure 28.4 Use of flowchart to assess and act on opportunities based on risk 155
Figure 29.1 Risk response planning process 158
Figure 29.2 From original risk to residual risk 159
Figure 29.3 Residual risk and inherent risk. 160
Figure 29.4 Inherent risk, residual risk, and untreatable risk 160
Figure 29.5 Flowchart for risk response planning process 161
Figure 30.1 Risk monitoring example with KRIs 165
Figure 31.1 A holistic risk monitoring process. 169
Figure 32.1 Pareto chart example: production risks. 173
Figure 32.2 Pareto chart example: time in days for new product design 174
Figure 32.3 Scatter plot example: stock return and volatility 174
Figure 32.4 Scatter plot example: nonconformances and process sigma 175
Figure 32.5 Scatter plot with impact chart: nonconformances and process sigma 175
Figure 32.6 Bar chart example. 176
Figure 32.7 Histogram example: quality defects. 176
Figure 32.8 Time series plot example: defect counts 177
Figure 32.9 Time series plot (two variables) example: defect count of Machines A and B 178
Figure 32.10 Run chart example: defect count 179
Figure 32.11 C chart example: quality defects. 180
Figure 32.12 Pie chart example: operational costs 181
Figure 32.13 Dotplot example: quality defects 181
Figure 32.14 Dotplot (two variables) example: defect count for Machines A and B 181
Figure 32.15 Individual value plot example: calls attended at three stations 182
Figure 32.16 Radar chart: external failure costs 183
Figure 32.17 Radar chart: failure costs by plant 184

Figure 32.18 Radar chart: external and internal failure costs by plant 184
Figure 32.19 Area chart example: defect count by plant 185
Figure 32.20 J chart example: hypothetical failure mode leading to bleeding, hematoma, and infections. 185
Figure 32.21 J chart variation 186
Figure 33.1 Impact-probability chart 188
Table 33.1 Risk parameters for Figure 33.1 188
Table 33.2 Risk parameters for Figure 33.2 188
Figure 33.2 Impact-probability chart with qualitative x- and y-axes. 189
Figure 33.3 Use of impact-probability chart to show decrease in risk post-treatment 189
Figure 34.1 Risk-based trending. 191
Figure 34.2 Five-step process for risk-based complaints trending. 192
Figure 34.3 The Define phase 193
Figure 34.4 An example of targeted problem solving using control charts, risk assessment, and quality tools 195
Figure 34.5 Example anatomy of a control chart of post-launch consumer complaint events. 196
Figure 34.6 Anatomy of a U chart 197
Table 34.1 Adverse event reports by month 198
Figure 34.7 C chart of device failures from June 2009 to June 2011 199
Figure 34.8 C chart of pre- and post-recall catheter failure 199
Figure 34.9 Risk level correlation with KRI—pre-trending issue risk level is low. 200
Figure 34.10 Risk level correlation with KRI—increase in level due to uptick in complaints picked up by KRI. 200
Figure 34.11 High occurrence rate and high severity—drastic increase in risk level 201
Figure 35.1 Elements of a risk-based approach to auditing 203
Table 35.1 Risk matrix for classifying nonconformities during audits 204
Figure 35.2 Major inputs of risk audits 205
Figure 36.1 Time series chart of asset value showing volatility in value over time 208
Table 36.1 Grading of main aspects of negative risks 210
Table 36.2 R score associated with adverse effects 211
Table 36.3 B score associated with benefit. 212
Table 36.4 RB balance: the TURBO diagram 213
Table 36.5 Clavien-Dindo-based risk matrix 214
Table 36.6 Clavien-Dindo severity scale 214
Table 36.7 Probability scale 215
Figure 36.2 Clavien-Dindo grade-based risk factor model for risk-benefit analysis 216
Table 36.8 Weighted Clavien-Dindo risk matrix 217
Figure 36.3 Calculation of QALY 218
Table 36.9 Cost and QALYs. 219
Table 36.10 Cost and DALYs. 219
Figure 36.4 CEA plane 220
Figure 37.1 Uncertainty, risk attitude, and decision making 225

Table 38.1 Risk matrix for rating requirements 229
Table 38.2 Risk matrix for rating requirements based on consequences of design input on objective 229
Table 38.3 Risk matrix for rating requirements based on consequences of output on objective 229
Figure 38.1 A process for risk mitigation by design. 230
Figure 38.2 Hierarchy of controls for risk mitigation by design. 231
Figure 39.1 Kraljic matrix 233
Figure 39.2 Risk indicators for a supplier 234
Figure 39.3 Risk indicators, risk level, and tiers 235
Table 39.1 Elements of a comprehensive risk index. 235
Figure 39.4 Bubble chart as graphical indicator of supplier risk exposure 236
Figure 40.1 Sources of data and decision making in industry from 2.0 to 4.0 240
Figure 40.2 Data points in 4.0 241
Figure 41.1 System output and variability 243
Figure 41.2 Cause and effect 243
Figure 41.3 Failure mode, cause, and effect. 244
Figure 41.4 Cause, effect, and failure mode 244
Figure 41.5 Example of failure modes and their causes. 245
Figure 41.6 Probability tree for failure mode and failure effects 246
Table 41.1 Occurrence scale 246
Table 41.2 Severity scale. 247
Figure 41.7 Filling out an FMEA 247
Figure 41.8 The FMEA process. 249
Table 41.3 DFMEA column headers in a worksheet 250
Figure 41.9 Hierarchy of elements for failure study. 251
Table 41.4 Component and function 252
Table 41.5 Component and failure mode 252
Table 41.6 Component and failure effect. 253
Table 41.7 Component and cause of the failure 253
Table 41.8 Component and failure mode, effect, and cause 254
Table 41.9 Severity table. 254
Table 41.10 Occurrence table 254
Table 41.11 Detection table 255
Table 41.12 FMEA snippet for a mobile phone display. 256
Figure 41.10 The UFMEA process 258
Figure 41.11 The PFMEA process 259
Figure 42.1 Relation among hazard, hazardous situation, impact (harm), and risk 262
Figure 42.2 Hazard analysis process. 263
Figure 42.3 Probability path from hazard to harm. 264
Figure 42.4 Probability path from the hazard of slippery ice to the harm of breaking a leg 265
Figure 42.5 Probability path from the hazard of slippery ice to the harm of death. 265

Figure 42.6 Pictorial example of the relationship between hazard, sequence of events, hazardous situation, and harm 266
Table 42.1 Column headers for hazard analysis worksheet. 267
Table 42.2 Hazard analysis for infusion pump 268
Figure 43.1 An example of a study node: waveform conversion 271
Figure 43.2 Another example of a study node: the chemical reactor 271
Figure 43.3 The HAZOP process 273
Table 43.1 "More" and "less" guide words 274
Table 43.2 Examples of deviations and their associated guide words 275
Figure 43.4 HAZOP examination process. 276
Figure 43.5 Detailed HAZOP process workflow 277
Table 43.3 HAZOP table 278
Figure 43.6 Architecture of system under study. 279
Figure 44.1 HACCP process 281
Figure 44.2 Seven principles of HACCP 281
Figure 44.3 Decision tree to determine CCP 283
Table 44.1 Hazard identification worksheet 285
Table 44.2 Determination of a critical control point 285
Table 44.3 Headers for an HACCP plan 285
Figure 44.4 Process flow diagram of system under study 286
Table 44.4 Hazard analysis for creation of vanilla ice cream from milk 286
Table 44.5 CCP determination for creation of vanilla ice cream from milk. 288
Table 44.6 HACCP plan for creation of vanilla ice cream from milk 289
Figure 45.1 Top view of the FTA process. 293
Table 45.1 Fault tree symbols, names, and corresponding descriptions 293
Figure 45.2 FTA symbols and their definitions 295
Figure 45.3 FTA for top event of alarm system failure 296
Figure 45.4 Making cut sets for FTA 297
Figure 46.1 Monte Carlo analysis steps 299
Figure 46.2 Simulation results of a fair coin flip experiment with two flips. 300
Figure 46.3 Simulation results of a fair coin flip experiment with 10 flips 300
Figure 46.4 Simulation results of a fair coin flip experiment with 20 flips 301
Figure 46.5 Simulation results of a fair coin flip experiment with 50,000 flips 301
Figure 46.6 Parameters of the model and limiting values 303
Figure 46.7 The model for total deaths and infected population 303
Figure 46.8 Monte Carlo simulation output for number of deaths 304
Figure 46.9 Monte Carlo simulation output for number of infected people 304
Figure 46.10 Sensitivity analysis 305
Figure 46.11 Monte Carlo simulation output of reduced deaths based on parameter adjustment as a result of sensitivity analysis 305
Figure 47.1 Contexts based on the spread of a disease 308
Figure 47.2 The risk assessment process with special stress on communication and information dissemination 309
Table 47.1 Disease risk assessment example 312

Figure 47.3 Risk triangle with definitions showing original and reduced risk. 313
Figure 47.4 Risk rhomboid with definitions showing original and reduced risk 313
Figure 47.5 A model for predicting total number of beds and total deaths for an ongoing epidemic or pandemic 316
Figure 47.6 Parameters of the model and their limiting values 316
Figure 47.7 Monte Carlo simulation output for total number of people infected 316
Figure 47.8 Monte Carlo simulation output for total number of beds needed 316
Figure 47.9 Monte Carlo simulation output for total number of deaths. 317
Table 47.2 References for advanced epidemic risk assessment with their respective risk parameters and methods. 318
Figure 47.10 The risk management process 320
Figure 47.11 Percentage of visits for ILI in the United States from September 29, 2019, to April 11, 2020. 320
Figure 47.12 J chart for trending infections and outcomes. 321
Figure 47.13 Pneumonia-, influenza-, or COVID-related mortality with epidemic threshold mortality 322
Figure 47.14 Real-time reproduction number of SARS-CoV-2 in Hong Kong from February to April 2020 323

Foreword

Over the few decades we have spent in the industry, we have seen risk management evolve, mature, and incrementally broaden in scope. Decades after the introduction of risk management concepts into the mainstream, we saw these often implemented without application of the right mindset and rigor that can provide real results that affect the bottom line. In this world of ever-changing implications of risk, it is more important that we focus on the right process, one that is agile enough to make a desired impact in an uncertain business climate; this book suitably addresses how a risk-based approach can be used toward accomplishing this. Generally, risk is considered a negative term in most industries, but considering its positive aspects can really help us leverage organizational strengths to capitalize on opportunities in a climate of uncertainty. It was high time that quality management embraced the true definition of risk, beyond its negative side. After ISO 9001:2015's refocus on risk, there was a need for a guidebook that could help harmonize QMS and risk management. We see great value in this book, not only for beginners, who can take advantage of the simplicity with which complex concepts have been explained, but also for experts, who can use this text, as the author has suggested in the Preface, as a self-calibration tool and a reference manual.

Jayet has dedicated much of his career to mastering risk management. In this book, Jayet uses his passion for the topic to make risk management an exciting and intriguing concept for the reader. It is not uncommon for ambiguous "risk management" documentation to be created and applied at a surface level in hopes of achieving compliance to standards; however, this book makes it clear why this should not be the intended process or only outcome. Jayet has ensured the reader will understand exactly what risk management is and understand how to apply practical, value-added risk management methods and tools to identify, prevent, and solve the most important real-world problems. This is the real value of risk management. Jayet's ability to use modern examples from various industries and practical life situations helps articulate a clear case for the importance of risk management. This book highlights why and how the field of risk management is evolving and rapidly growing. It is becoming ever more critical within quality, engineering, business, services, and beyond. With this book, Jayet has created a single-source reference for the most influential risk management processes, standards, concepts, and tools. We highly recommend it to anyone looking to gain knowledge on the topic.

Arun Mathew
Associate Director, Quality Risk Management
Abbvie, Inc.
Chicago, IL

Michael Michetti
Design Quality Engineering Manager
Medtronic
Boulder, CO

Preface

Risk management is compulsory.
Risk management is indispensable.
Risk management is necessary for compliance.

We have heard this many times. Almost every industry has its own niche version of risk management and has some resources dedicated to its organizational processes for management of risk. But here is the truth:

Risk management often fails.
Risk management often becomes a paper exercise.
Risk management becomes reactive and passive.

These points apply to many industries, from national security and banking to healthcare, from the food industry to medical devices and beyond. Banks, which historically have had large armies staffed in risk management departments, could not foresee the U.S. housing market crash of 2008. The automotive industry has a very detailed, hierarchical, and industry-standard risk-based failure modes analysis process, yet is hit by losses of millions of dollars each year due to safety-related recalls. Each year, the food and medical device industries, where risk management is legally mandated by the U.S. Food and Drug Administration, recall hundreds of products released from their production sites that can severely harm people. The spread of COVID-19 to pandemic levels could be attributed to flaws in healthcare security intelligence, which in turn resulted from incorrect risk identification, risk assessments, and risk communication.

Is risk management even worth it? The answer is: more than ever before. Let us discuss why.

Before diving into this book, I would like to tell you a few *actual truths* about risk management, which are:

1. **Risk management is wired into us.**

   Evolution has bestowed upon us humans, by way of certain neuronal connections, a brain that continually processes risk. Everything in this book, or any standard or any other book on risk management, at its fundamental base really draws from what we often do subconsciously. When you walk in a crowded street, you are continually identifying risks, assessing them, evaluating them, and monitoring them. Your sense of risk is high when it's a new street or a new town. The sense of risk is low when it's a familiar street. The same applies in business and organizational environments. It's the same brain that thinks for

you in a boardroom or in a strange alley. The trick here is to understand another truth, which is that risk management is "exhausting" for the brain. The brain has a mind of its own. So, in seemingly normal situations, the brain will underplay risks and, at times, try to normalize scenarios that really aren't normal. While there may have been some survival advantages gained in doing so for the early *Homo sapiens,* this becomes a great weakness for the modern human who is called on to make risk-based decisions at the workplace on a routine basis. At the base of all the failures of risk management in all industries, you will find that incorrect perceptions, due in part to incorrect assumptions and biases, led to incorrect risk responses, which in turn led to organizational disasters.

This book, with its foundations in solid, proven theory, will refresh your brain, engender self-awareness, and reset your mind's risk calibration, whether it be for complex organizational decisions or day-to-day departmental decision making. The book itself is calibrated to major ISO, ANSI, and IEC standards, whose references you will find in almost every chapter. So the next time you have that gut feeling for an important business decision, pass it through the lens of risk-based thinking and risk-based decision making, as described in Chapters 4 and 5, and overcome your internal biases by reading up on the theory of cognitive aspects of risk-based decision making in Chapter 37.

2. **Risk management is proactive.**

Reactive risk management is a misnomer. It really means disaster management. This book is not for that. Risk management involves a lot of "futures thinking," which is quite hard. This book provides a platform and structure, along with methods and tools, to accomplish this difficult task. Again, many failures of risk management activities in the past have resulted from poor understanding of organizational context. This is critical to ensure proactiveness. Chapters 14 and 16, coupled with Chapters 10 and 15, delve into this and guide the reader in comprehending the organizational context such that the risk processes may be customized and consequently be most effective and efficient. The fundamental base of this book is built on the risk management framework per ISO 31000:2018. Proactive thought is embedded in this framework. Chapter 6 explains how this transfers over and forms the base of preventive risk-based thought championed by ISO 9001 since its 2015 edition. Multiple chapters in the middle of the book deal with major steps in the risk management framework by first introducing the fundamentals and then, in complementary chapters, going into detailed theory (e.g., see Chapters 7 and 12 for risk identification; Chapters 7, 25, and 27 for risk analysis; Chapters 13, 26, and 27 for risk evaluation; and Chapters 9 and 28 for risk modification). These activities within the risk management framework are preconditions for a proactive system that is flexible and adaptable enough to mount effective and efficient risk responses to anticipated and unanticipated risks.

3. **Risk management is holistic.**

   One problem with traditional quality risk management is that it is often very siloed. This book takes a slightly different approach to presenting risk management concepts. While it presents many old and proven techniques, it also dares to bring to the reader's attention some bold new methods and theories. The first of these are presented in Chapter 1, which describes the scope of risk management right from the enterprise level to the product, process, or service level. Traditionally, product-, process-, or service-level risk management has been the mainstay of quality teams in manufacturing organizations. What about the other levels? They may or may not exist on paper, but people are certainly making decisions at those levels and considering risks, consciously or subconsciously, while making those decisions, which will no doubt impact product-, process-, or service-level risk. Chapter 1 aims to make the reader aware of this hierarchy. When you set this hierarchy in your organizational context, you will be able to locate yourself and be aware of the rungs of decision making above and below you, which not only affect the risks at your level but also affect the success or failure of risk management efforts at your level. All theory in this book is based on the ISO 31000:2018 framework that applies to risk management for all levels in an organizational hierarchy.

4. **Risk management is an essential part of continual improvement and change management.**

   ISO 31000:2018 talks about continual improvement of risk management through learning and experience. This book talks about engendering continual improvement through risk management. Risk mitigation by design, discussed in Chapter 38, introduces new concepts to help guide improvements not only through initial design but also via specific redesigns as needs for change emerge. Risk vigilance through risk monitoring and review (described in Chapters 30, 31, and 32) will reveal many opportunities for improvement. Risk management acts as the first line of defense when indications of a risk emerge for preemptive action and can guide efforts to permanently improve the system to make it risk resilient. Chapter 34 provides an approach for risk-based monitoring of internal organizational processes, while Chapter 39 provides approaches for risk-based supplier and vendor oversight. Modern organizations are much more dynamic than those of 50 years ago. There is greater volatility, uncertainty, complexity, and ambiguity (see Chapter 12), which makes it incumbent upon the organization to install robust change management systems that form the base of adaptability and flexibility in the face of changing internal and external conditions. Here, too, risk management plays a central role. By correct and timely identification, analysis, and evaluation of upcoming risks, proper and commensurate risk responses can be planned, which protect, sustain, and create value for the organization.

5. **Risk response is different than risk reaction.**

   Risk management occurs with or without a structured or documented process in an organization. As mentioned, we are continually making decisions by factoring in a variety of risks in our daily lives. The same is true for organizational decision makers. For example, the COVID-19 pandemic affected all businesses. Even within different companies in the same sector, we see different risk outcomes based on risk planning (Chapters 18 and 19) or a lack thereof. In the face of uncertainty, top executives tried to manage external risk by modulating internal response. Some failed, while some fared better. Adoption of risk management practices and methods, many of them explained in detail in this book, will lead to risk readiness and a better response in the face of a realized risk, as opposed to a knee-jerk reaction, which will often be misguided. This even holds true in cases of unanticipated risks. The existing risk management framework working in synchrony with change management systems will always fare better than an emergency ad hoc response. Monitoring and review of leading indicators of risks (Chapters 30 and 31) can help the organization apply preemptive risk responses to prevent larger impacts from negative risks.

6. **Risk is the effect of uncertainty on objectives.**

   The etymological roots of the word "risk" can be traced back to the Arabic word رزق (pronounced *rizq*), which translates to "God's favor or fate." As humans became more seafaring, this word morphed with and into the Greek word ριζα (pronounced *rhiza*) for "roots," which was a Homeric metaphor for avoiding danger. Latins associated this word with cliffs, and the words *resicum*, *risco,* and *riscus* came to mean cliffs (and the risk associated with them), which were to be avoided and sailed around as they jutted out from the sea like "roots" and damaged ships nearing land. In this word lies the etymological root of the Spanish *riesgo* and the French *risque*. In sixteenth-century Germany, as massive profits were made by sea traders who undertook long, risky voyages to bring back valuable commodities from the East, the word morphed into *rysigo*, which came to mean "a daring or enterprising undertaking." This was the first time a positive connotation was associated with the word. Indeed, the human anthropological journey can be said to be reflected in the etymological journey of this word. The progression from leaving everything in gods' hands to venturing out cautiously, to undertaking dangerous ventures *suo moto* for profit, shows the increasing agency in human actions through the ages.

   In this book we follow the definition of risk from ISO 31000:2018, which looks at both the upside and downside of risk—its positive and negative aspects. To some readers, this may be a new concept. One-tailed definitions of risk (based on reduction and avoidance of negative risk only) will lead to one-dimensional risk management, which at best will result in zero losses. No company becomes successful by aiming for zero loss; they become successful by aiming for large profits and gains. Two-tailed definitions of risk management

allow us to leverage the existing risk management framework for organizational benefit and not just prevention of loss. Chapters 2, 3, 6, and 11 discuss this issue in detail, and other chapters further advance this thinking. While the theory and tools in this book apply to both types of risk, a reader who is familiar with only the negative aspects will come to realize the power of this expanded scope as they progress through the book.

7. **Risk management leads to greater efficiency and profits.**

   When risk is identified, assessed, and evaluated in a structured manner, keeping the organizational context front and center, it leads to good decision making in terms of risk modifications and treatments. It also leads to greater risk readiness and well-defined risk responses. An overall increase in organizational risk maturity (Chapter 17) leads to risk-intelligent decision making, which often leads to great benefits for the organization.

8. **Risk management is difficult.**

   It is easy to convert risk management into a paper exercise, conduct token risk assessments, and have signed, sealed, and approved files for minimal compliance purposes. It is much harder to holistically and effectively conduct risk management activities that actually affect the organization's bottom line in a positive manner. The hurdles are manifold. First, it's easy to get the context of risk management wrong. It is not a plug-and-play process; it needs to be nurtured and grown specific to an organizational environment, with due consideration to internal and external environment and the relevant interfaces. Second, even if the context is right, there may not be sufficient inclusivity and pervasiveness of the risk management processes and apparatus. If key stakeholders are missed or if risk management remains a siloed, single-level exercise, it may not affect the organization in a positive and meaningful way. Third, even if the context is right and sufficient inclusivity is realized, there needs to be a strong framework for risk governance that encompasses all levels of decision making, encourages ethical and independent thought, and challenges conventions. Finally, all people involved in the risk management process should have the applicable knowledge, skills, and abilities to participate and contribute to structured risk assessments and consequent processes. Chapters 21, 23, 24, 32, 33, 36, 41, 42, 43, 44, 45, and 46 present a plethora of tools and methods for the reader to choose from. By themselves, these standalone tools will not add any value. It is only when they are used in the right context, by the right stakeholders, at the right time, with the right interpretation, and in conjunction with the right processes, that their usage can result in value creation.

9. **Risk management should be harmonized with data analysis.**

   In Industry 4.0, there is no dearth of data (i.e., information). Industry 4.0 takes the digitization engendered by 3.0 and magnifies it to provide near-universal accessibility and connectivity. Capacity for accurate data gathering

has increased like never before, entering our personal devices, homes, cars, and sometimes even our bodies. These increased data points and enhanced analytics can together be used to enhance predictive, risk-based decision making. The effect of 4.0, however, is only as good as an organization's infrastructure to leverage the connectedness of systems. Even if an artificial intelligence (AI) with an IQ greater than 200 could be provided, smartness in terms of business decision making involves "futures thinking" and consequence analysis (Chapters 8 and 24). It means processing the final decision by considering multiple parameters, which include cascading effects, material outcomes, financial outcomes, and even emotional outcomes, to assign a probability of success to one decision. In short, the ultimate AI is equipped with risk-based thinking. Data analysis within a risk management framework can help make sense of the continual inflow of information and ensure visualization of the state of business by ranking and filtering. It can also help manage the connectedness of the business footprint by exposing gaps and prioritizing actions (Chapter 40). Organizations should reassess data analysis as it pertains to risk management processes, as many new sources of data mean newer sources of information not only for risk identification but also for risk monitoring. A risk management system from Industry 3.0 based on small data sets and lesser data points will be significantly less effective than a risk management system that embraces and leverages the power of big data and connectedness.

The scope of this book goes slightly beyond the traditional definition of "quality risk." This is in harmony with the adoption of a two-tailed definition of risk (including positive and negative aspects) from ISO 31000 by ISO 9001 in 2015. This expansion of scope in the gold standard framework for quality management systems (QMS) was done to embed preventive thought in systems, but the proactiveness gained by this integration of QMS with risk management can be leveraged to promote, manage, and sustain beneficial change and enrich the value of the organizational work product (Chapters 11, 22, 23, and 38). Our environment is fraught with internal and external uncertainties. Risk management allows us to make sense of these uncertainties in objective terms and challenges us to inculcate adaptability and flexibility to not only sail through volatility but, where possible, to profit from it.

Since 2015, many national and international standards have adopted risk-based approaches (e.g., ISO 19011:2018, as detailed in Chapter 35) and prescribe activities commensurate to and driven by risk. This book was not written to fulfill compliance with any of these standards but instead was compiled in a way that can allow a reader of any level of expertise to immediately use concepts of risk management for organizational benefit. In learning and implementing risk-based practices as described in this book, you will find that many clauses in these standards that are based on risk management foundations are automatically satisfied.

I would like to end this preface with some words from New York governor Andrew Cuomo's April 26, 2020, coronavirus briefing:

> *So, it's hard, it's hard to make change. It's hard to make change in your own life, let alone on a societal collective level. But if you don't change, you don't grow. And if you don't run the risk of change, you don't have the benefit of advancement.*[1]

Whether you are a novice or an expert, this book will help you by providing knowledge, theory, methods, and tools to do just that—to *run the risk of change* for the *benefit of advancement*.

—Jayet Moon

1. "Video, Audio & Rush Transcript: Governor Cuomo Announces Completion of Nation-Leading L Project Tunnel Rehabilitation with No Shutdown," New York State, April 26, 2020, https://www.governor.ny.gov/news/video-audio-rush-transcript-governor-cuomo-announces-completion-nation-leading-l-project-tunnel.

Acknowledgments

The author is deeply thankful to his family for their constant support and motivation. He is greatly indebted to Arun Mathew of Chicago, IL, for his help, guidance, and contributions to this manuscript.

The author also thanks Adam Brooks of Baltimore, MD, and Patricia Fleenor of Denver, CO, for their help.

This book also would not have been possible without Sharon Woodhouse and the patience, understanding, and encouragement of the Quality Press team.

Finally, the author thanks ASQ for being the thought leader in quality and continually providing forums for quality professionals around the globe to learn and excel.

CHAPTER 1

Introduction to Risk Management

PRODUCTS, SERVICES, SYSTEMS, AND ORGANIZATIONS continually face a multitude of risks that may hamper their functioning and lead to a variety of failures. These risks may be operational, commercial, environmental, technological, financial, political, or even social and cultural. In today's world, management of risk is not only an aspiration but a necessity for a successful organization to maintain its profits and reputation.

On a basic level, holistic organizational risk strategy is based on the following three pillars (see Figure 1.1):

1. Enterprise risk management
2. Operational risk management
3. Product-, process-, or service-level risk management

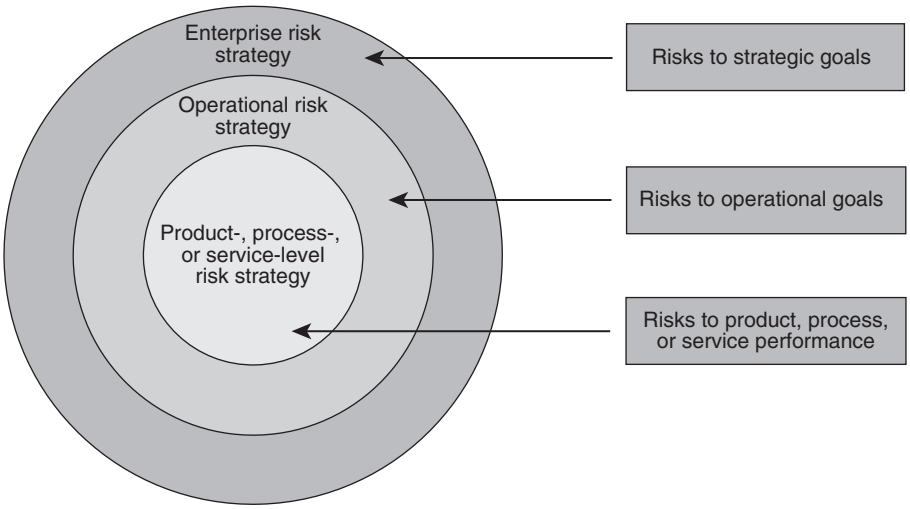
Enterprise risk management is the coordinated approach for centralized management of risks and their cascade from the strategic mission level.
Operational risk management is the coordination and control of all risky activities of the system at the operational business unit or functional level in order to successfully achieve the predefined expected operational outputs and objectives.
Product-, process-, or service-level risk management focuses on managing the day-to-day ground-level risks in terms of the specific end deliverables of the organization to its customers.

The aim of all risk management activities is the following:

- Realistic assessment of the organizational objectives and path to their achievement
- Prevention of undesired outcomes
- Continuous improvement
- Value sustenance and value addition

The organization can use the vehicle of risk management to leverage strengths to act on opportunities and assess weaknesses to mitigate threats. These actions in response to risk should be proportionate to the potential impact of the risk on the organization

FIGURE 1.1 Risk management pillars.



and its products or services. The success of risk management is dependent on a large extent to the organizational risk governance.

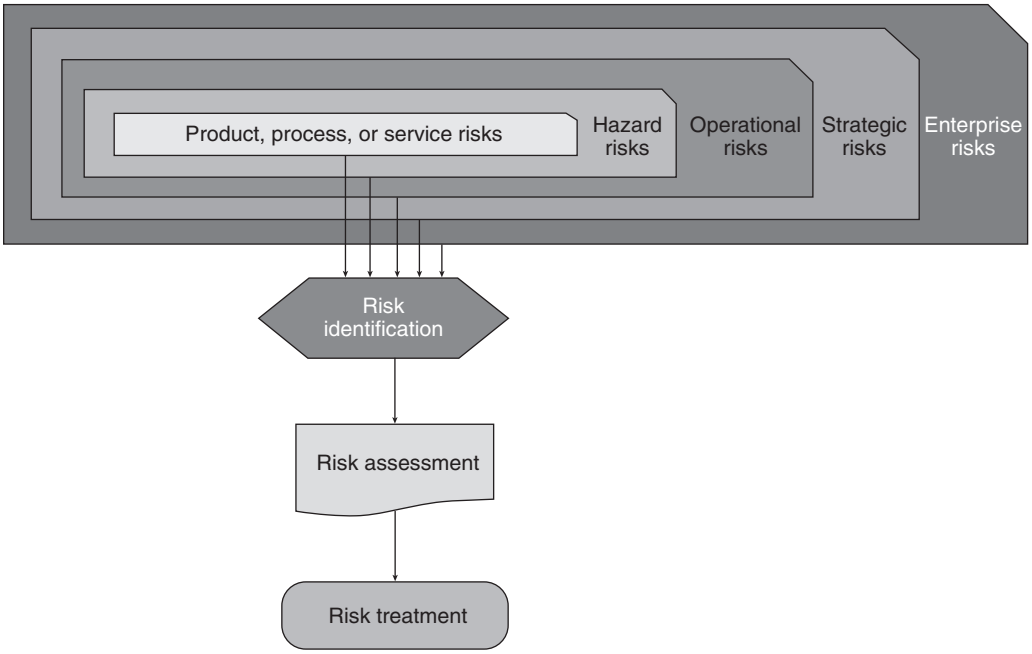
> **Risk governance** refers to the structural framework that governs the organizational risk management activities and related decision making. It encompasses policies, procedures, and processes that dictate risk management approaches, methods, and oversight.

Risk governance varies tremendously from sector to sector and company to company. Some companies do not have any enterprise risk management at all, while others have no product-level risk management. Many companies have multiple decentralized risk management processes used by disparate functions and departments. It is important for a quality and risk professional to understand the criticality of the risk management framework of one's organization and the governance of that framework to ensure success. This entails defining levels of accountability and ownership of cascading risks. It also entails identifying current risk policies, procedures, and stakeholder responsibilities in terms of risk and risk escalation pathways.

While it is easy to get lost in the myriad interpretations of and approaches to risk management, this book attempts to distill the basic risk management concepts into a practical risk-based approach. Fundamentally, for a risk professional, the risk-based approach depends on a clear understanding of the system itself, the threats and opportunities that surround it, and, finally, finding ways to modify risks for organizational benefit.

From a top level, the aim of enterprise risk management is to look at aggregate risk. While there is significant value in doing so, assessment of risk at succeeding levels of tactical planning is equally important to ensure effective risk management.

FIGURE 1.2 An example of hierarchical risk management.



A version of such hierarchical risk management at succeeding levels is shown in Figure 1.2.

After understanding the organizational context, the risk management practitioner must structurally break down the basic drivers of risks at various levels to assess and evaluate the same per organizational needs. This evaluation should be captured in risk assessments that serve not only as documentation of the comprehensive efforts for identification, analysis, and evaluation of potentially risky events but also as a risk register according to which these events are documented and correspondingly monitored and controlled.

The level at which the risk is assessed, analyzed, and treated is important. Hierarchical risk management starts from the enterprise level, flows over to the functional level, and then moves on to the subsequent levels of products, processes, and services.

In Figure 1.2, five levels are shown. Depending on the industry or company, these may change, and further levels may be added or deleted. In the hierarchical context, for this model, the five levels shown here are defined as follows:

1. **Enterprise risk management**—The overarching high-level risk management process that looks at risks as aggregate threats to or opportunities for the enterprise. This process will directly affect strategy setting.
2. **Strategic risk management**—The management of risks to an organization's achievement of strategic goals and objectives that have been set earlier.

3. **Operational risk management**—The management of risks that affect the routine workflows set in place to deliver organizational goals. These risks will affect the operational goals that cascade from the strategic goals.
4. **Hazard risk management**—An iterative process of risk management that focuses on the hazards faced by systems. Daily operations of an organization occur despite the presence of multiple hazards and hazardous situations. Hazard risk management scientifically looks at the exposure afforded by these hazards in terms of probability and consequence. Often, this significantly overlaps with risk management at other levels.
5. **Product, process, or service risk management**—This most detailed rung of risk management focuses on individual and specific failure modes arising from the hazards and attempts to assess each failure separately in order to manage component-specific risk. Often, this falls in the realm of quality departments in manufacturing and some service organizations.

An enterprise-wide risk management framework is just as important as functional expertise in product, process, or service risk management. Generally, in many sectors, the risk management functions are decentralized and uncoordinated. The value of dealing with risk holistically from an enterprise standpoint is the following:

1. Leadership support and high-level attention, thereby ensuring correct resource allocation
2. Strategic objectives at front and center, and synchrony between top-level and bottom-level risks, thereby allowing for effective end-to-end risk management
3. High-level steering control in terms of risk culture, risk appetite, and loss tolerance

It must be clarified that certain publications define hazard risk management through the lens of enterprise risk management as exposures that can cause loss without any possibility of a gain. They define hazards as major adverse events such as fires and earthquakes. This view of hazard risks is noninclusive and looks at hazards from financial or insurance standpoints only. This book does not take that approach. Hazards are continually present in the world around us. Normal operations take place despite them, and, indeed, we aim to mitigate the formation of hazardous situations from hazards continually so that benefits can be obtained despite the presence of the hazard. For example, it was understood that traffic at intersections was hazardous, so traffic lights were installed. A petroleum refinery has a risk of fire, so not only do we insure the refinery but also use fire-retardant materials as much as we can and take many other precautions.

When hazards are seen from an operational standpoint, they can help us define specific product, process, and service risks as well—as we shall do in the coming chapters of this book. Let us now turn our attention to the confluence of quality management and risk management.

CHAPTER 2

Quality and Risk Management

THE AMERICAN SOCIETY FOR QUALITY (ASQ) defines *quality* as:

> *1) the characteristics of a product or service that bear on its ability to satisfy stated or implied needs;*
> *2) a product or service free of deficiencies.*[1]

Quality management is an organizational process that ensures consistent quality to satisfy and, where possible, delight the customer. Quality management includes, as appropriate, quality planning, quality assurance, quality control, and quality improvement. The Plan–Do–Check–Act (PDCA) cycle is inherent in this definition, as shown in Figure 2.1.

Quality planning not only details the expected systemic activities and methods to ensure sustained quality, but also comprises preventive strategies and proposed actions in a structured format composed of system, operational, and functional deliverables.

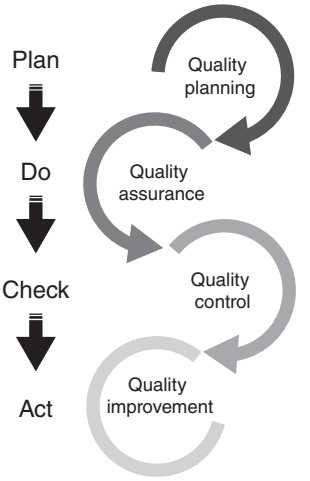
Quality assurance is the immediate outcome of the plan, which puts the preventive thought into action by focusing on problem or error prevention. This is a creative phase where hazards are anticipated and resulting issues are attempted to be mitigated by robust design thinking during formative stages. This is, in effect, risk mitigation by design. Risk management can assist and enable a structured quality assurance function since foundationally both are based on the same preventive philosophy.

Quality control focuses on problem detection and reaction after an issue has been discovered. This is an important activity since now the risk to quality has been realized and detected. But detection and local solution of the issue do not add any long-term value to the system. The discovered issues must be analyzed in the broader context and a level of response must be decided. Using risk management, this risk can not only be anticipated with ready mitigations but also be qualitatively and quantitatively measured, prioritized, and controlled throughout the life cycle.

Quality improvement starts with an analysis of performance to discover deficiencies, and focuses on a systematic approach to improving performance in order to achieve and

1. American Society for Quality, "Quality Glossary of Terms, Acronyms & Definitions: ASQ," ASQ, accessed June 20, 2020, https://asq.org/quality-resources/quality-glossary/.

FIGURE 2.1 Quality management and PDCA.



exceed goals and objectives. A quality improvement is realized as a positive effect of a change engendered to prevent issues. Again, phased risk management, which continually anticipates, measures, and tracks risk, becomes a yardstick for the quality improvement process and provides a meaningful baseline to measure changes and their effects.

Quality and risk management work in natural harmony, and together magnify the proactive, prevention-based approach, reducing the reactive defect detection and rejection to practicably low levels.

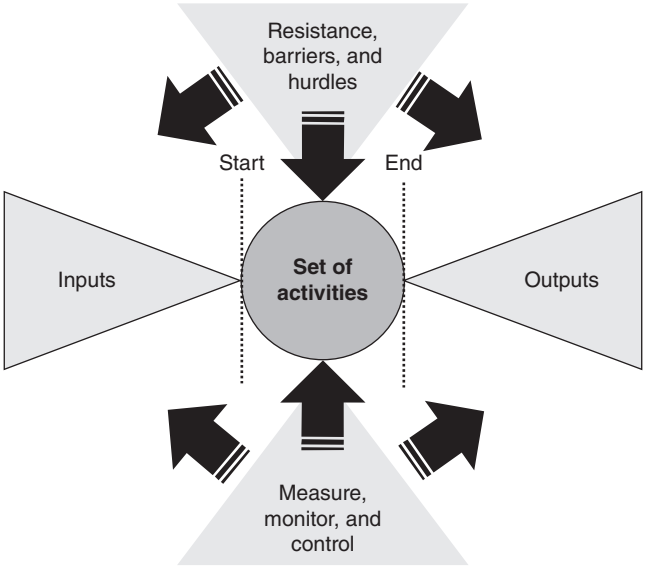
RISK MANAGEMENT AND THE PROCESS APPROACH

The *process approach* is an organizational strategy of managing and controlling a process and various interacting subprocesses within the organization. Any activity that has an input and output is a process. If a process is converting an input to an output, it means there are certain sets of subactivities within the process that enable this change.

Figure 2.2 shows a simple representation of a process. The realization of outputs of the process is contingent not only on the inputs but also on the actual "processing" step, whereby the activities convert the input to output. The success of this set of activities depends on overcoming resistance, barriers, or hurdles and monitoring their output and modulating parameters to ensure desired output.

A risk-based process approach focuses on anticipation of the resistance, barriers, and hurdles—and their preemptive mitigation to an acceptable level—such that the desired level of output is maintained. Resistance, barriers, and hurdles can be hazards, hazardous situations, faults, or failures that hamper operability and negatively affect the process outputs. To control the process, one must understand its hazards and anticipate the outcome of the realization of hazards on the process outcome.

FIGURE 2.2 The process approach.



This can be accomplished by incorporating risk management by using the PDCA approach:

- Risk planning to ensure a systematic scheme or framework for realization of risk management activities
- Risk identification by analyzing the set of activities within the process and its critical points
- Risk analysis and prioritization to consider preventive mitigations or level of risk acceptance
- Risk monitoring and control to keep an eye out for pain points and emergent issues

Thus, risk management, PDCA, and the process approach are all part of quality management and feed into and from one another (Figure 2.3).

Risk-based thinking is a *philosophy* and not a set of tools. Risk-based thinking will not automatically follow by simply creating a risk analysis document or a risk manager position within a company. Risk-based thinking must be tied and aligned to the culture of a company, such that its objectives, whether they be individual or organizational, incorporate this approach.

While enterprise risk management propagates a top-down approach to risk management, risk mitigation by design (RmD) aims for a bottom-up approach. ISO 9001:2015 removed the earlier preventive action clause and introduced risk-based thinking, which, by nature, is preventive in spirit. By practicing RmD (more details in Chapter 38) in its true form, the designers of products, processes, and services adopt a risk-based mindset to preemptively mitigate subsystem-specific, foreseeable risks. This results in low-risk products, processes, and services, which in turn allow greater tolerances for operational

FIGURE 2.3 Confluence of risk management, process approach, and PDCA with quality management.



FIGURE 2.4 PDCA and risk management.

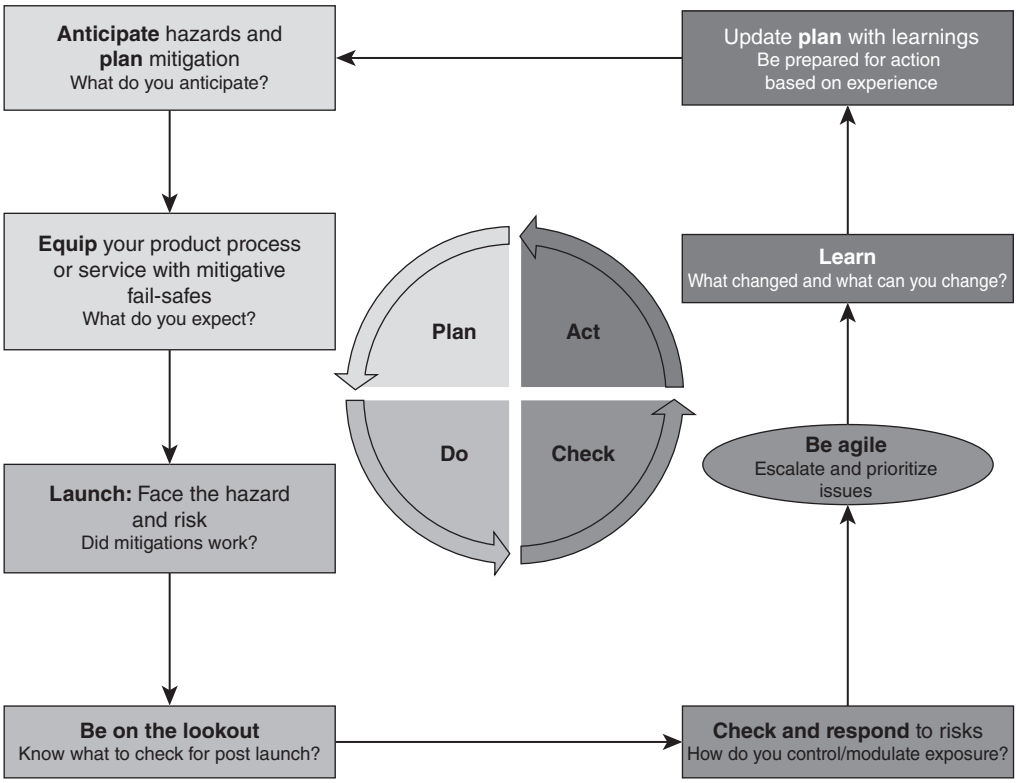
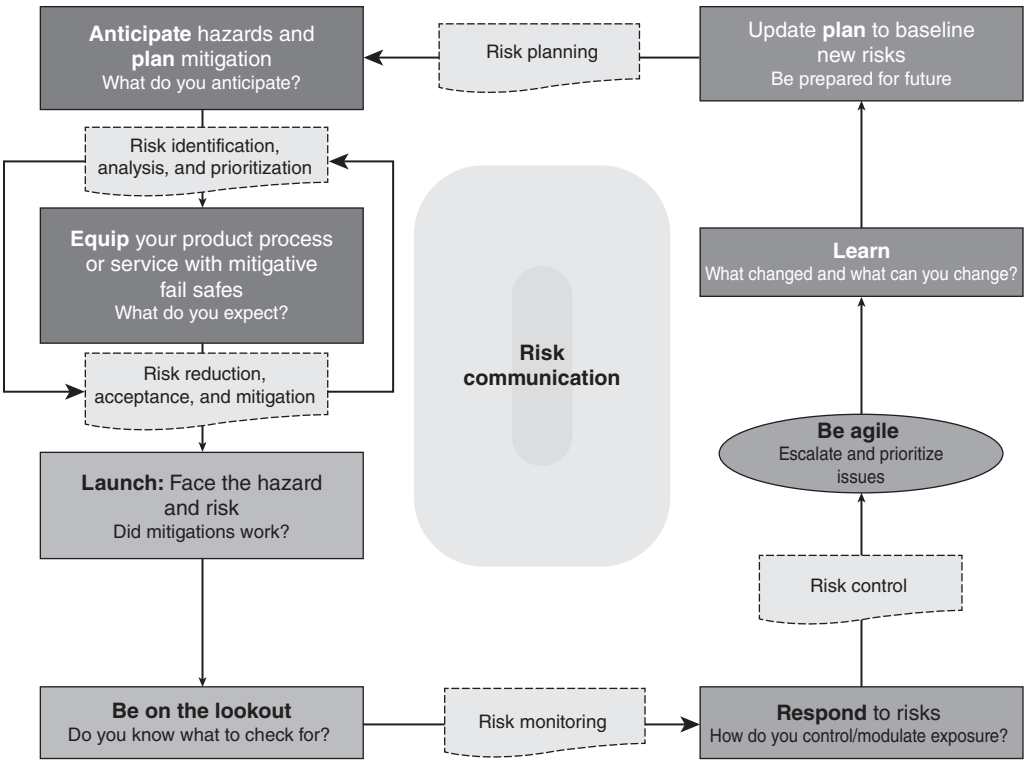


FIGURE 2.5 PDCA to risk management with traditional steps.



and subsequently strategic risks. Safe products and processes may encourage positive risk taking by engendering confidence in top management, which in turn will lead them to strategically leverage strengths to capitalize on business opportunities.

Thus, risk managed at one level allows for opportunities for value creation at other levels. Mismanaged risks at top level may lead to significant reduction in value because risks may magnify as they shift through levels.

Another way to look at the process in terms of product-, process-, or service-level decision making is through the prism of PDCA as shown in Figure 2.4.

We start by anticipating the risks to plan proactive mitigations and preventive controls for them in the Plan phase. In the Do phase, we launch the product, process, or service. In the Check phase, we determine if the design-based mitigations worked (monitoring) and if the residual risk was indeed as expected, if any alarm signals or risk warnings appeared, and if any unforeseen risks emerged. In the Act phase, we implement the learnings for the risks that occurred in the earlier phases by enabling better preventive controls in the system. We document the new risks and assess their impact on the system, which is then followed by new controls for the same.

The traditional steps of risk management are added to these steps and shown in Figure 2.5. We will continue to discuss these steps in the coming chapters.

CHAPTER 3

So, What Is Risk?

TO BEGIN, let us look at the most basic, universal, and simple—yet most conceptual—definition of risk. Per ISO 31000:2018, *risk* is defined as:

Effect of uncertainty on objectives.[1]

It means that any *effect* due to any *cause*, which leads to deviation from expectation, is risk. In organizational enterprise terms, the effect of not meeting objectives is the consequence of risk. These objectives may be safety related, performance related, or related to failure reduction or sales growth.

Moreover, these effects can be positive or negative. Positive effects will accelerate an organization's achievement of goals, while negative effects will hinder this achievement. The achievement of *objectives* is the purpose of the organization and thus is the purpose of risk management. These objectives can be systemic; can be strategic; can be product, process, or service related; and can pertain to any or all functional levels of the organization. The objective can also be nonfailure of the product or successful intended use of the product.

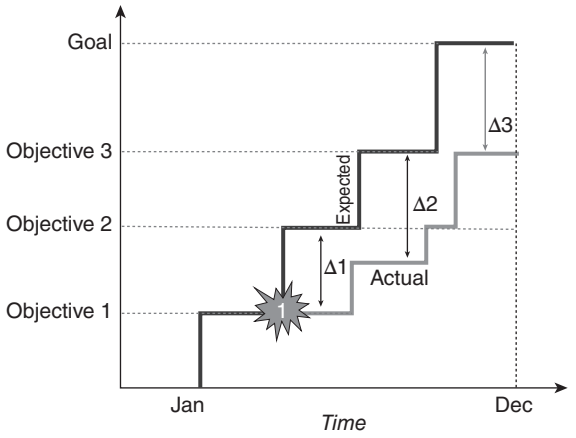
To further understand the definition of risk, let us consider an example. The organization in Figure 3.1 adopted a staggered approach to its end goal by defining three time-based interim objectives in its action plan.

An impactful adverse event, "1," just before achievement of Objective 2, derailed the schedule, and the deviation from plan objectives (delta 1 and delta 2) led to the failure to achieve the end goal. This is an example of negative risk, the uncertainty due to events related to nonachievement of objectives.

Similarly, in the scenario above, a positive event could have led the organization to get back on track and achieve the end goal before the end of the mandated time frame. If this were to happen, it would be an example of positive risk, the uncertainty due to events related to accelerated achievement of objectives. A positive risk is known as upside risk or can simply be called an opportunity (an opportunity with uncertain

1. ©ISO. This material is reproduced from ISO 31000:2018, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

FIGURE 3.1 Time-based objectives realization.



possibility of a gain). In some industries, such as the financial sector, where two-tailed risks are obvious (e.g., a stock market investment that can lead to profit or loss), this definition is well subscribed to. In other industries, such as the medical device sector, risk has been historically associated with a negative connotation. Here, the relevant ISO standards for medical devices (ISO 13485:2016 and ISO 14971:2019) slightly differ from ISO 31000:2018. Some risks, indeed, may not have a positive outcome or an opportunity associated with them. Still, medical device risk management aims to address the positive aspects of a treatment by using risk-benefit analyses, which are detailed in a separate chapter in this book. ISO 9001:2015, on the other hand, is well aligned with the definition in ISO 31000:2018 and uses the word "opportunity" for upside risk. The theory presented in this book applies to both aspects of risk, and a practitioner in any industry will be able to use the theory and tools presented in the coming chapters for holistic organizational risk management. A risk need not always be avoided, regardless of positive or negative aspects, but should always be managed to reduce disruptions related to uncertainty.

Any event with the potential to impact objectives, either alone or in combination, may give rise to risk. Risk management is simply the management of potential negative and positive events, by timely assessment and evaluation, to assess threats and opportunities in order to modify them to achieve sustained or accelerated achievement of goals.

ISO/Guide 73:2009 defines *uncertainty* as:

> *State of deficiency of information related to, understanding or knowledge of an event, its consequence or likelihood.*[2]

2. ©ISO. This material is reproduced from ISO Guide 73:2009, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

The whole concept of risk-based thinking depends on the reaction to uncertainty. The cornerstone of risk management is science-based uncertainty management. If the organization in the example above had managed uncertainty, it could have maintained control of the schedule by leveraging possible positive events and minimizing negative events. As the book progresses, we will discuss, in a lot of detail, the final product-, service-, or process-level risk management and present various tools and methods for the same. Here, we take some time to present the very top view of risk management. As risk management progresses from enterprise level to lower levels, the negative aspects of risk tend to become more pronounced than the positive aspects, as focus shifts to prevention of failures.

In the next chapter, we will look at the foundational concepts of risk-based thinking and how it treats event uncertainty.

CHAPTER 4

Risk-Based Thinking

THE GOOD NEWS IS THAT, as humans, we are natural risk takers. We are pioneers who constantly seek to conquer uncharted territory. The bad news is that risk-taking traits in humans are a gift of natural selection, which takes a brute-force approach to evolution, thereby exposing most of us to major mistakes.

For example, one caveman could choose to trust his gut and enter an unknown dark cave while another caveman could choose to wait in the bush for a few hours to check if the cave already housed a saber-toothed tiger. We may find the confident and gutsy caveman who traipses into the cave very daring, but if there did happen to be a tiger in the cave, we would have to admire the other caveman's level-headed approach.

The factor that differentiates gut-based thinking and risk-based thinking is the human attitude toward uncertainty. The *Cambridge English Dictionary* defines *uncertainty* as:

> *A situation where something is not known.*[1]

The next important realization in the development of risk-based thinking is that, by default, the probability of an uncertain event is *unknown*. Thus, the risk of an uncertain event is unknown as well. However, if we can use objective information to assign a probability to a previously uncertain event, then we can ascribe a risk to an event. *Probability* is defined as:

> *The level of possibility of something happening or being true, or, in mathematics, a number that represents how likely it is that a particular thing will happen.*[2]

The modern theory of probability was inspired by games of chance. The seventeenth-century Frenchman and mathematician Pierre de Fermat proved to a gambler that certain combinations of dice in the long term had a higher probability of winning than other

1. Cambridge English Dictionary, s.v., "uncertainty," accessed June 22, 2020, https://dictionary.cambridge.org/us/dictionary/english/uncertainty.
2. "The Possibility That Something Will Happen - Synonyms and Related Words," Macmillan Dictionary, accessed July 7, 2020, https://www.macmillandictionary.com/us/thesaurus-category/american/the-possibility-that-something-will-happen.

combinations. In Fermat's eyes, this was not a game of chance but a game of probabilities, and a person who understood the die's probabilistic distribution could *probably* profit from it. The profit would be commensurate to the risk a gambler was willing to take.

To clarify, consider a game where people bet money on the outcome of a double dice toss. For example, John and Steve both participate in this game and each bets $100. John is a gut thinker and Steve is a scientific thinker.

John chooses the number 5 because his father's birthday is on the fifth of the month. Steve uses concepts of probability to choose a number. Knowing that there are 36 outcomes in a double dice throw, per Figure 4.1, Steve calculates that the highest probability of occurrence is for the number 7.

It does not mean that Steve is guaranteed a win, but by using a science-based method, Steve progressively increases his chances of winning as the dice are rolled successively, as can be seen in Table 4.1.

Thus, Steve has used a risk-based approach to this game by quantifying probability, or the occurrence of success. John, on the other hand, has a much lower probability of winning if he bets on 5 every time; and if he randomly chooses new numbers for every bet, no prediction can be made regarding his chances, which have now become uncertain.

Probability theory led to a great transformative change in the business of insurance and gave birth to the field of actuarial science. James Dodson developed mortality tables, which predicted the probability of death or survivorship of certain populations;

FIGURE 4.1 Probability distribution of two simultaneously cast fair dice.

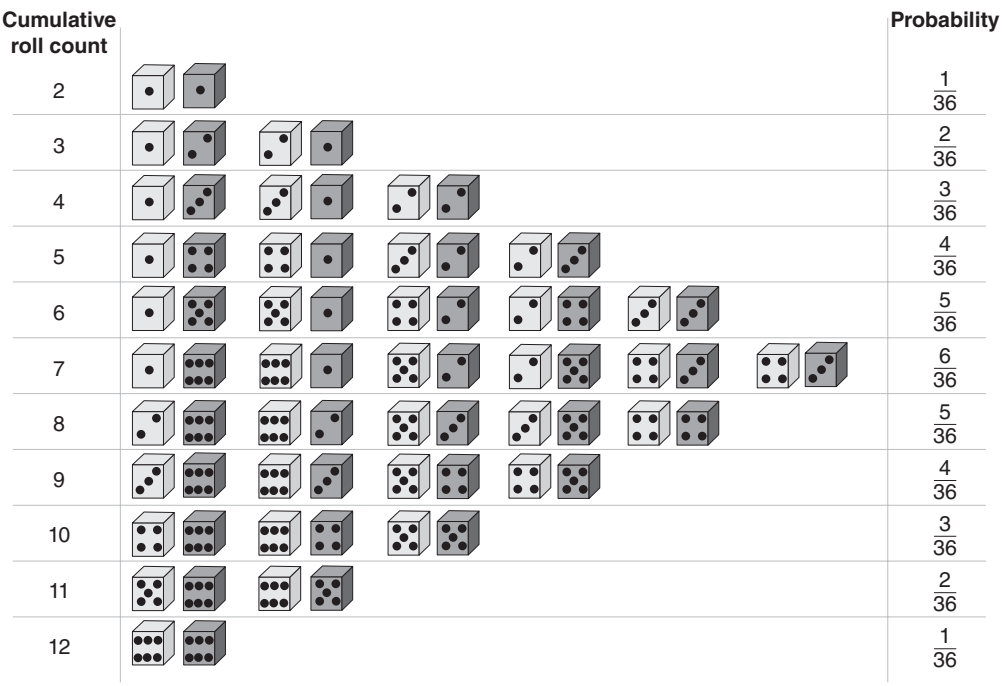


TABLE 4.1 Increasing the probability of winning via successive bets on number 7.

Throw number	Probability of Steve's win
1	16.60%
2	30.50%
3	42.10%
4	51.70%
5	59.80%
6	66.50%
7	72.10%
8	76.70%
9	80.60%
10	83.80%
11	86.50%
12	88.70%
13	90.65%

these tables were used to decide long-term insurance premiums. This was the first notable application of probability and consequence in large-scale commerce. These tables were immediately successful, and insurance companies that did not use these tables often found themselves failing.

Now that we have discussed the importance of probability in risk, let us discuss *the consequence*. *Consequence* is defined as:

A result or effect of an action or condition.[3]

To adopt a risk-based approach means to place the impact or consequence of risk front and center. While the probabilities of different impacts or consequences may differ, one must consider all possible consequential scenarios to not only measure various risk impacts but, where possible, determine aggregate risk.

Risk-based thinking is preventive thinking. It focuses on prevention of problems before they occur. Consequence analysis is a critical step in achieving this. To prevent a problem, one has to foresee it. Most importantly, one must foresee the consequence along with the probability of the consequence.

Thus, the essence of risk-based thinking is to inculcate a mindset that leads us to foresee threats and opportunities and estimate them with an objective level of certainty such that targeted modifications and controls can be built into the design and surveillance of systems.

3. Lexico, s.v., "consequence," accessed July 7, 2020, https://www.lexico.com/definition/consequence.

CHAPTER 5

Risk-Based Decision Making

RISK-BASED THINKING is not only preventive but also preemptive. A dynamic risk management system will engender preemptive thinking that will lead the system owners to deploy mitigations or modifications in anticipation of developing or emerging changes in the risk landscape. The foundation of preventive and preemptive thought lies in the decision-making process. At its core, risk-based thinking is simply a science-based decision-making process founded on risk.

The University of Massachusetts Dartmouth published the graphic shown in Figure 5.1 to explain an effective decision-making process.

This model has been shown here since almost all decision-making models follow this simple framework in one form or another with only slight modifications. Leveraging the Dartmouth model, for the purposes of this book, *risk-based decision making* can be defined as:

> *A structured process for identifying necessary and appropriate courses of action based on analysis of relevant information and evaluation of known or anticipated risks associated with each alternative action.*

Joseph J. Myers from the U.S. Coast Guard has presented a process for risk-based decision making, which is based on the following sequential order:[1]

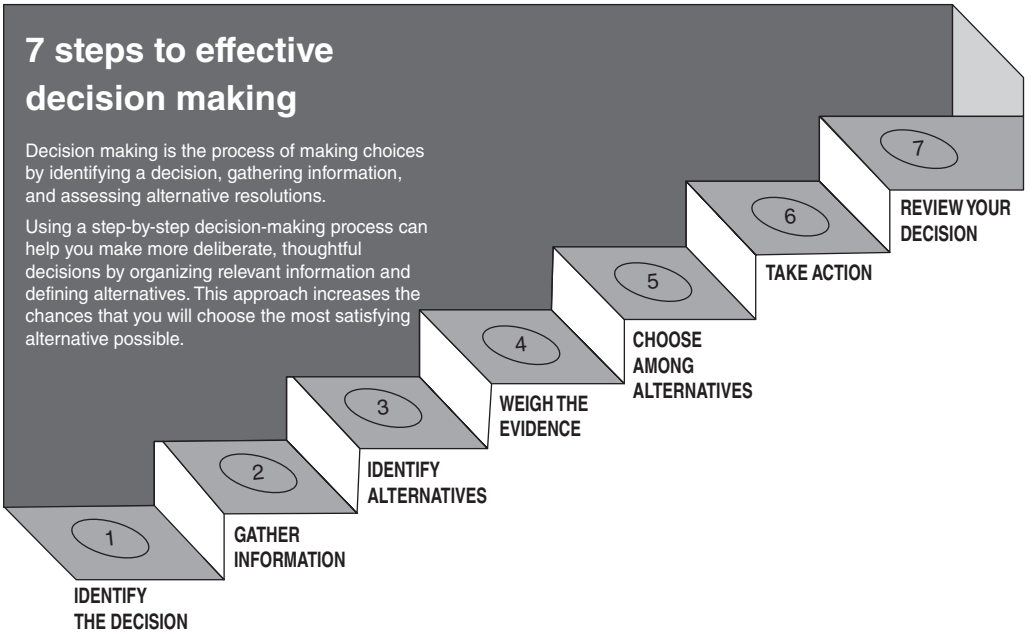
- Establish the decision structure
- Perform the risk assessment
- Apply the results to risk management decision making
- Monitor effectiveness through impact assessment
- Facilitate risk communication

In this chapter we will focus on aspects of the decision structure. The coming chapters of this book will address risk and impact assessment in great detail.

It is necessary to define the decision structure such that the decision-making flow incorporates the views of and, where necessary, the approval of relevant stakeholders.

1. J. J. Myers, "Risk-Based Decision Making," *Journal of Safety and Security at Sea* 64, no. 1 (2007): 6–10.

FIGURE 5.1 Decision-making steps.



Source: University of Massachusetts Dartmouth, "Decision-Making Process," First Year Course Modules, UMass Dartmouth, accessed June 22, 2020, https://www.umassd.edu/fycm/decision-making/process/.

These stakeholders must be supplied with, where appropriate, risk assessments that allow all parties to be on the same page and to discuss targeted implications and/or consequences (along with constraints) for further top-level review and judgment. Such a method relies on the formulation of making a decision first and then assessing its impact and acceptability. Aven and Kørte have given a model that fits these principles.[2] In their model, the issue and decision alternatives undergo a risk and decision analysis, which is then viewed through the lens of stakeholder values, goals, criteria, and preferences coupled with management review and judgment to finally arrive at a decision. At times, the final decision may be to evaluate other decision options, and the cycle is continued.

In this book, we will propound a new model of risk-based decision making based on the Dartmouth model, which leverages risk-based thinking to pinpoint success and failure factors of a decision and builds on Aven and Kørte's model as shown in Figure 5.2.

This model embeds the preventive approach during the formulation phase of the decision by forcing the anticipation of failures and, where possible, evaluating their impacts. Thus, instead of making a decision and assessing its risk, we are using principles of risk management to formulate and modify the decision as the risk-based process progresses.

2. T. Aven and J. Kørte, "On the Use of Risk and Decision Analysis to Support Decision-Making," *Reliability Engineering & System Safety* 79, no. 3 (2003): 289–299.

FIGURE 5.2 Risk-based decision-making model.

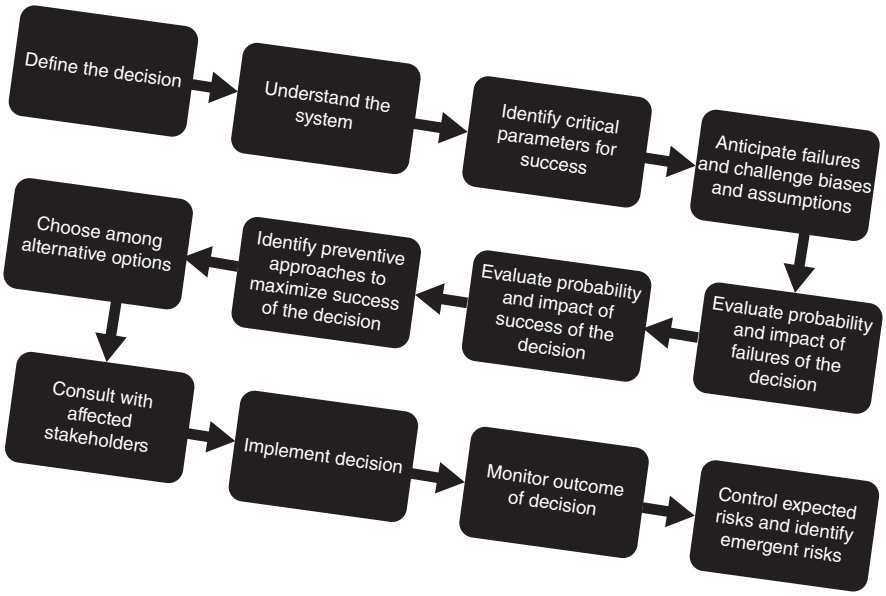
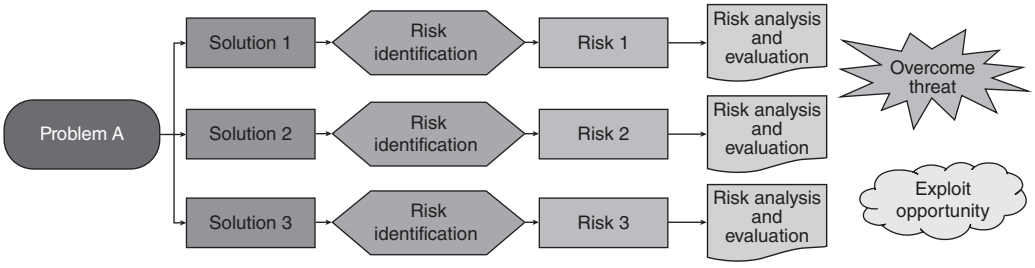


FIGURE 5.3 Risk-driven decision making leading to exploitation of opportunities and mitigation of threats.



Risk-based thinking and risk-based decision making should lead to risk-based solution determination. As quality and risk professionals, we continually find ourselves facing choices among multiple paths in the face of problems. The theory of risk management provides a structured method to deal with such situations and arrive at solutions.

The application of concepts of risk management does not mean that we take the path of least resistance or the path of least risk. It means that we assess and evaluate threats and opportunities and take the path that will leverage our strengths for maximum value. Risk management may not, at all times, aim to lower risks as much as possible, but instead helps to anticipate problems and their solutions so that commensurate preparations can be made in case of risk realization.

In Figure 5.3, Risk 1, which is associated with Solution 1, need not be "less" than Risks 2 or 3. Per risk-based solution determination, the deciding factor should be whether the organization has relevant strengths to convert the risk into an opportunity. If not, the risk should be deemed a threat to steer clear of. If there are no upsides to risks and all the risks are negative, then the solution associated with the risk with the lowest threat level should be chosen. The coming chapters will go into great detail about risk identification, analysis, and evaluation.

CHAPTER 6

ISO 9001 and Risk Management

ISO 9001 IS THE INTERNATIONAL standard that specifies requirements for a quality management system (QMS). Organizations across the globe pursue certification to this standard, which is used to demonstrate commitment to quality along with consistent customer-focused value creation and sustenance in the products and services created or marketed by the organization.

In Clause 0.1, ISO 9001:2015 mentions that the standard employs the PDCA cycle and risk-based thinking. It goes on to say:

> *Risk-based thinking enables an organization to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise.*[1]

ISO 9001, in its 2015 version, also removed the section on preventive actions. The idea is that life-cycle risk identification, analysis, evaluation modification, and monitoring, which are outcomes of the risk management process, are, by nature, preventive.

The standard draws attention to the risks associated with organizational contexts and objectives. It specifically mentions the risks again in the clauses outlined on p. 21.[2]

The focus of these clauses is summarized in Table 6.1.

The standard expects the risk management to stem from the organizational leadership, which echoes the foundational message of enterprise risk management. On the other end of the spectrum, the standard also expects in Clause 5 that a risk that affects conformity of products must be identified and addressed, thus covering the whole gamut of the hierarchical risk spectrum discussed earlier. Implicitly, one may interpret

1. ©ISO. This material is reproduced from ISO 9001:2015, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
2. ©ISO. This material is reproduced from ISO 9001:2015, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

Clause 4.4.1

The organization shall determine the processes needed for the quality management system and their application throughout the organization, and shall address the risks and opportunities as determined with requirements of Clause 6.1.

Clause 5.1.1

The top management shall demonstrate leadership and commitment with respect to quality management system by promoting the use of process approach and risk-based thinking.

Clause 5.1.2

Top management shall demonstrate leadership and commitment with respect to customer focus by ensuring that the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed.

Clause 6.1

When planning for the quality management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) give assurance that the quality management system can achieve its intended result(s);
b) enhance desirable effects;
c) prevent, or reduce, undesired effects;
d) achieve improvement.

Clause 6.1.2

The organization shall plan:

a) actions to address these risks and opportunities;
b) how to:
    1) integrate and implement the actions into its quality management system processes (see 4.4);
    2) evaluate the effectiveness of these actions.

Actions taken to address risks and opportunities shall be proportionate to the potential impact on the conformity of products and services.

NOTE 1: Options to address risks can include avoiding risk, taking risk in order to pursue an opportunity, eliminating the risk source, changing the likelihood or consequences, sharing the risk, or retaining risk by informed decision.

NOTE 2: Opportunities can lead to the adoption of new practices, launching new products, opening new markets, addressing new clients, building partnerships, using new technology and other desirable and viable possibilities to address the organization's or its customers' needs.

Clause 9.1.3

The organization shall analyze and evaluate appropriate data and information arising from monitoring and measurement. The results of analysis shall be used to evaluate the effectiveness of actions taken to address risks and opportunities.

Clause 9.3.2

The management review shall be planned and carried out taking into consideration the effectiveness of actions taken to address risks and opportunities.

Clause 10.2.1

When a nonconformity occurs, including any arising from complaints, the organization shall update risks and opportunities determined during planning, if necessary.

TABLE 6.1 Risk focus of ISO 9001:2015 clauses.

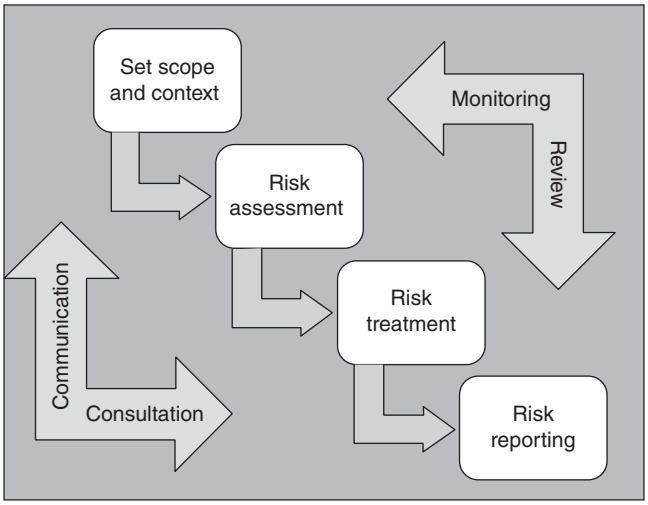
Clause	Focus
4.4.1	QMS processes should address the upside and downside of risks
5.1.1	Enterprise support for risk-based thinking
5.1.2	Product- and service-level risk management
6.1	Ensuring outcomes of risk management through QMS planning
6.1.2	Integration of QMS and risk management; focus on the upside of risk as opportunity
9.1.3	Monitoring of risk outcomes
9.3.2	Risk oversight by leadership
10.2.1	Post-market / life-cycle risk management

that the standard is asking the organization to implement risk management at various levels corresponding to the quality activities at those levels, which may include strategic, operational, and program, product, and service level via scope/context setting, risk assessments, risk evaluations, and risk treatment as shown in Figure 6.1.

It should be clarified that the standard is not explicitly asking for a formal risk management process, and that certification to this standard may not be contingent on such a requirement. It simply directs attention toward risk management—a set of practices and techniques that can significantly accelerate the accomplishment of the same goals as ISO 9001 in a structured fashion that:

1. Improves organizational governance
2. Establishes and sustains a continual improvement culture and framework
3. Enables evidence-based decision making
4. Improves customer satisfaction
5. Ensures consistent quality by accomplishing all of the above

FIGURE 6.1 Risk management process overview.



RISK, OPPORTUNITY, AND ISO 9001

In section 0.3.3, the standard mentions:

> Opportunities can arise as a result of a situation favourable to achieving an intended result, for example, a set of circumstances that allow the organization to attract customers, develop new products and services, reduce waste or improve productivity. Actions to address opportunities can also include consideration of associated risks. Risk is the effect of uncertainty and any such uncertainty can have positive or negative effects. A positive deviation arising from a risk can provide an opportunity, but not all positive effects of risk result in opportunities.[3]

The standard addresses the fact that positive deviations arise from risk and must be considered. Risks may not always have a negative outcome and is not always to be avoided.

Now that we have a high-level overview of risk and its nature, let us get into the details and talk about risk identification and analysis.

3. ©ISO. This material is reproduced from ISO 9001:2015, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

CHAPTER 7

Basic Risk Identification and Analysis

IN POPULAR MODERN DICTIONARIES, risk is defined as shown in Table 7.1.

The first common theme here (among these definitions) is the reference to chance or possibility. It follows that when the probability of an adverse event increases, the risk increases proportionally.

It is much riskier to walk on ice than concrete because the probability of slipping is higher on ice. Note that we have not yet even considered the level of consequence of slipping, which may result in a bruise, bleeding, broken bones, and so on.

Probability, like risk, is everywhere around us. For example, the probability of you driving to work in a snowstorm depends on the following:

1. If you can walk through the snow to get to your car
2. If you can start your car in the freezing conditions
3. If the road is icy and slippery
4. If you can drive on icy roads
5. If a minor accident blocks the road
6. If a major pileup halts traffic
7. If the snowstorm turns into a whiteout blizzard

Obviously, the probability of each event happening is different, and, even if the event occurs, it may still be likely that you will be able to reach work. On a qualitative scale, the probabilities range from very certain to extremely unlikely. One might argue that a person could also die from the cold while driving and never reach work. The chance of "dying due to cold" is so low that it sounds preposterous. At the same time, if that does happen, it will be the event with the most severe outcome. Such events are called *black swan* events. These are events of such low probability that they cannot be predicted with any amount of computational accuracy. These events are extremely impactful and usually are far beyond the normal realm of practical expectations. I have included this here only to introduce the concept of a black swan. One could never hope to complete risk assessments practically if all imaginable black swan events were included.

Now, let's say I am your friend and my objective is to ensure that you get to work safely. I will do everything in my power to maximize your probability of getting to

TABLE 7.1 Dictionary definitions of risk.

Source	Definition of risk
Macmillan	"The *possibility* that something *unpleasant* or *dangerous might happen*"
Merriam-Webster	"*Possibility* of *loss* or *injury*"
Dictionary.com	"Exposure to the *chance* of *injury* or *loss*; a *hazard* or *dangerous chance*"
Cambridge	"The *possibility* of *danger, defeat*, or *loss*"
Oxford	"*Chance* or *possibility* of *danger, loss, injury* or other *adverse consequences*"

Sources: Macmillan Dictionary, s.v., "risk," accessed June 15, 2020, https://www.macmillandictionary.com/us/dictionary/american/risk_1; Merriam-Webster Dictionary, s.v., "risk," accessed June 15, 2020, https://www.merriam-webster.com/dictionary/risk; Dictionary.com, s.v., "risk," accessed June 22, 2020, https://www.dictionary.com/browse/risk?s=t; Cambridge Dictionary, s.v., "risk," accessed June 15, 2020, https://dictionary.cambridge.org/us/dictionary/english/risk; Oxford Learner's Dictionaries, s.v., "risk," accessed June 15, 2020, https://www.oxfordlearnersdictionaries.com/us/definition/english/risk_1?q=risk.

TABLE 7.2 Frequency or occurrence table.

Term	Description
High	Occurrence is likely (often or frequent)
Medium	May occur but not often or frequently
Low	Rare occurrence (unlikely)

work. But I have limited resources and I need to prioritize the probabilities to ensure I use my resources in the best way possible. So, using the key shown in Table 7.2, I assign a "probability" to each event listed earlier (see Table 7.3).

Now, I could go ahead and reduce all high-probability events, or pick the easiest ones to reduce, but there is another way. If another dimension is introduced, I can focus my resources and expend them in a still more efficient manner. This dimension is *consequence*, also known as *impact* or *severity*.

Per the dictionary definitions of risk we reviewed earlier, the second common theme we see is in the mention of loss, injury, and adverse events. Negative risk proportionally increases based on the severity of an adverse event.

The severity is the consequence of the risky event. In this case, severity is the level of disruption caused, as seen in Table 7.4.

Table 7.5 includes a column for "severity" of each outcome as described earlier in Table 7.3 and reproduced here in the second column.

A simple definition of risk that lends itself to mathematical conversion is:

Risk is the combination of the probability of the occurrence of a consequence and the severity or impact of the consequence.

Similarly, by focusing on the negative outcome of *harm* as the injury or damage to people, property, or environment, ISO Guide 63:2019 defines *risk* as:

TABLE 7.3 Tabulation of events, outcomes, and their probabilities.

Ways in which you do not get to work	Outcome	Probability of event happening	Rationale for the probability
Slipping and falling while walking through snow to get to the car	You get a bruise, get first aid, and get to work late	Medium	You do not have snowboots
Slipping and falling while walking through snow to get to the car	You break a bone and cannot go to work	Low	You have strong bones and will likely break the fall
Car does not start due to dead battery	You take a cab and arrive slightly late	High	You have not replaced the battery in a long time
Car skids on icy roads but you control the car	You arrive at work slightly late	Medium	Roads are very icy and you have worn tires
Car skids on icy roads and you are unable to control the car	You lose control and go off the road; you need to be towed and do not get to work	High	Your path has lots of iced-over bridges and you have worn tires
A minor accident on the road has slowed traffic	You arrive at work late	Medium	Icy roads can often cause minor accidents leading to slow but moving traffic
A major pileup on the road halts traffic	You arrive at work late	High	The road has many bridges that ice over, traffic is usually fast, and this often causes large accidents
The snowstorm grows into a whiteout blizzard	You cannot drive and do not reach work	Low	The area has not had whiteout blizzards in five years

TABLE 7.4 Severity table.

Term	Description
Significant	You cannot reach work at all
Moderate	You reach work late (>30 minutes)
Negligible	You reach work slightly late (<30 minutes)

TABLE 7.5 Tabulation of events, outcomes, probabilities, and severity levels.

Ways in which you do not get to work	Outcome	Probability of event happening	Rationale for the probability	Severity level
Slipping and falling while walking through snow to get to the car	You get a bruise, get first aid, and get to work late	Medium	You do not have snowboots	Moderate
Slipping and falling while walking through snow to get to the car	You break a bone and cannot go to work	Low	You have strong bones and will likely break the fall	Significant
Car does not start due to dead battery	You take a cab and arrive slightly late	High	You have not replaced the battery in a long time	Negligible
Car skids on icy roads but you control the car	You arrive at work slightly late	Medium	Roads are very icy and you have worn tires	Negligible
Car skids on icy roads and you are unable to control the car	You lose control and go off the road; you need to be towed and do not get to work	High	Your path has lots of iced-over bridges and you have worn tires	Significant
A minor accident on the road has slowed traffic	You arrive at work late	Medium	Icy roads can often cause minor accidents leading to slow but moving traffic	Moderate
A major pileup on the road halts traffic	You arrive at work late	High	The road has many bridges that ice over, traffic is usually fast, and this often causes large accidents	Moderate
The snowstorm grows into a whiteout blizzard	You cannot drive and do not reach work	Low	The area has not had whiteout blizzards in five years	Significant

TABLE 7.6 3×3 risk matrix.

Probability level		Severity level		
		Negligible	Moderate	Significant
	High	Reduce risk	Reduce risk	Reduce risk
	Medium	Acceptable risk	Acceptable risk	Reduce risk
	Low	Acceptable risk	Acceptable risk	Acceptable risk

Combination of the probability of occurrence of harm and the severity of that harm.[1]

In this vein, let's combine the probability and occurrence to find out the real risk of the harm of the events listed earlier. The easiest way to define this is through a key. Various ISO standards provide risk tables or risk matrices to accomplish this. The key in Table 7.6 is adapted from ISO 14971:2007.[2]

In Table 7.7 we finish our sample risk assessment based on Table 7.6.

Voila! We have now prioritized the items with the highest risk levels using a structured risk analysis such that targeted actions can be taken to reduce risk to an acceptable level.

When conducting risk analyses and evaluations, a major factor is stakeholder communication and consultation. In this case, I was able to come up with a few scenarios of potential failures, but they may not be all-encompassing. For example, if I had consulted your car mechanic in this exercise, she or he may have provided me with new information that could either add a failure mode or change the occurrence or severity of an already identified failure mode. If your mechanic had told me that your car's alternator belt was old and very susceptible to cracking in freezing conditions, I would have identified and added an event with significant severity. Conversely, if I had known that you just installed a state-of-the-art slip detection system in your car, that would make me reduce the probability of uncontrolled skidding of the car from high to low.

The following are benefits of stakeholder communication in the risk identification process:

1. Drawing from different areas of expertise to assign accurate severity and occurrence values
2. Using stakeholder expertise to cover all possible failures and consequences
3. Ensuring all stakeholders are aligned on assigned risk levels

1. ©ISO. This material is reproduced from ISO/IEC Guide 63:2019, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

2. ©ISO. This material is reproduced from ISO 14971:2007, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

TABLE 7.7 Tabulated risk assessment.

Risk	Probability of event happening	Severity level	Risk level
Slipping and falling while walking through snow to get to the car	Medium	Moderate	Acceptable
Slipping and falling while walking through snow to get to the car	Low	Significant	Acceptable
Car does not start due to dead battery	High	Negligible	Reduce risk
Car skids on icy roads but you control the car	Medium	Negligible	Acceptable
Car skids on icy roads and you are unable to control the car	High	Significant	Reduce risk
A minor accident on the road has slowed traffic	Medium	Moderate	Acceptable
A major pileup on the road halts traffic	High	Moderate	Reduce risk
The snowstorm grows into a whiteout blizzard	Low	Significant	Acceptable

Involvement of stakeholders is not only important for risk identification but is also critical post–risk assessment when risk treatments and communication plans have to be developed.

Another thing to consider is aggregate risk. In this case, the aggregate risk is the summation of risks that prevent the realization of the objective of reaching work on time. One way to show this graphically is as a consequence–time series chart, as shown in Figure 7.1.

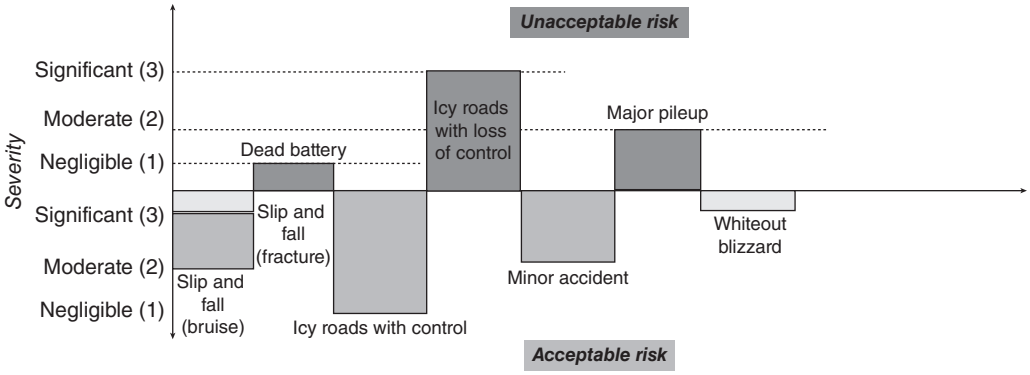
It is important to consider the successive appearance of risks in time sequence or, in some cases, even the simultaneous occurrence of risks. In this particular example, since the risks occur sequentially, a chart like Figure 7.1 shows their progression and level of acceptability or unacceptability as they stand without any treatment. This shows the net position of the risks in terms of comparative acceptability. I know that the risk with the maximum footprint is the loss of control of the car on icy roads, which has the most severe impact, while risk of dead battery is also unacceptable but has a negligible impact on the objective. It also shows that we have three unacceptable levels of threats to our objective of reaching work. After attempts to reduce risks, this figure can be compared with the original levels to check net loss of risk.

Let us summarize three important definitions:

risk identification

The process of finding, recognizing, describing, and recording risks. Risk identification involves the identification of risk sources, events, their causes, and their potential consequences.

FIGURE 7.1 Consequence–time series chart for aggregate risks.



risk analysis

The process for comprehending the nature of risk and determining the level of risk.

risk evaluation

The final phase of risk assessment, where the results of risk analysis are compared with criteria and assigned a level of acceptability based on which additional actions to modify or maintain risk are determined.

CHAPTER 8

Events and Consequences

IN THE LAST CHAPTER, we used a simple and structured analysis to qualitatively assign risk levels to individual events. To correctly assess risk, one must understand what an *event* means.

ISO-31000:2018 defines an *event* as:

Occurrence or change of a particular set of circumstances.[1]

An event may have several causes and may or may not have consequences. It may be previously seen or experienced or may be just plain theoretical.

ISO 31000:2018 defines *consequence* as follows:

Outcome of an event affecting objectives.[2]

When we evaluated the list of possible events in the previous chapter, the severity was assigned based on the consequence. Table 8.1 clarifies this in regard to the previous example.

Consequence is simply the scale of severity we used earlier. It is, in fact, the measure of the impact.

It is critical that risk professionals understand event and consequence. Mistakes here could lead to the analysis being overly redundant and, in the worst case, incorrect. The following are common mistakes in this regard:

- The idea that one event can have only one consequence
- The idea that consequences must be certain
- Use of only the final consequence

1. ©ISO. This material is reproduced from ISO 31000:2018, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
2. ©ISO. This material is reproduced from ISO 31000:2018, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

TABLE 8.1 Tabulated risk assessment.

Risk	Probability of event happening	Consequence	Severity level
Slipping and falling while walking through snow to get to the car	Medium	Reach work late (more than 30 minutes)	Moderate
Slipping and falling while walking through snow to get to the car	Low	Cannot reach work at all	Significant
Car does not start due to dead battery	High	Reach work slightly late (less than 30 minutes)	Negligible
Car skids on icy roads but you control the car	Medium	Reach work slightly late (less than 30 minutes)	Negligible
Car skids on icy roads and you are unable to control the car	High	Cannot reach work at all	Significant
A minor accident on the road has slowed traffic	Medium	Reach work late (more than 30 minutes)	Moderate
A major pileup on the road halts traffic	High	Reach work late (more than 30 minutes)	Moderate
The snowstorm grows into a whiteout blizzard	Low	Cannot reach work at all	Significant

One event may lead to various different consequences, each with varying levels of probability. The consequence of the impact may be positive or negative. There arises a need to distinguish the level of impact so that the consequences can be compared and evaluated. This is usually done with the help of a ratings scale. In the previous example, the scale shown in Table 8.2 was used.

To classify the negative impacts, the term "severity" is commonly used. The severity measures the level of negative impact so that it can be classified as a category using a ratings scale as shown in Table 8.2.

In the earlier example, to keep it simple, we used only one consequence for most of the risky events. For slipping and falling, we used two consequences on purpose to demonstrate the various possibilities and probabilities of event outcomes. This event can be further expanded, as shown in Table 8.3. The need for detail must be assessed by the risk professional. In case you are conducting risk analysis for a complex system that has possibilities of multiple user or customer harms, you may want to explore the consequences in much greater detail.

TABLE 8.2 Severity scale.

Severity	Term	Description
3	Significant	You cannot reach work at all
2	Moderate	You reach work late (>30 minutes)
1	Negligible	You reach work slightly late (<30 minutes)

FIGURE 8.1 The consequence polygon.

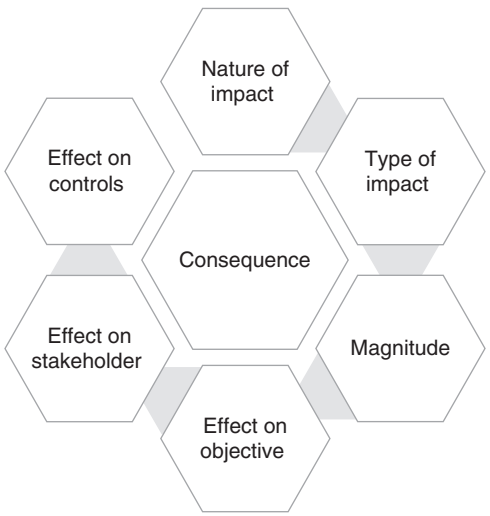


TABLE 8.3 Expanded risk assessment with immediate and final consequences.

Ways in which you do not get to work (sequence of events)	Probability of event happening	Immediate consequence	Final consequence*	Severity
Slipping while walking through snow to get to the car	Medium	Fall leading to a bruise	Reach work late (more than 30 minutes)	Moderate
Slipping while walking through snow to get to the car	Low	Fall leading to a broken femur	Cannot reach work at all	Significant
Slipping while walking through snow to get to the car	High	You regain balance and do not fall	Reach work on time	No impact / negligible

*Considering no other events occur after this event

The activity of drawing out consequences and analyzing them is known as *consequence analysis*.

A consequence analysis exercise can be done using the consequence polygon shown in Figure 8.1, which takes into account the following:

1. **Nature of impact**—chronic or acute
2. **Type of impact**—short or long term
3. **Magnitude**—scope of the impact (local vs. global, immediate vs. trailing)
4. **Effect on objective**—positive or negative
5. **Effect on stakeholder**—user, manufacturer, or layman effects
6. **Effect on control**—change in modification/mitigation strategy

One may choose not to include every section in the final risk analysis document, but it is important to have these points in mind during the consequence analysis activity.

CHAPTER 9

Basic Risk Modification

IN THE PREVIOUS CHAPTERS, we learned the basic concepts of risk identification, analysis, and evaluation. These are informative assessments that set the stage for modification of the assessed risk for organizational benefit. Risk modification, depending on the nature of risk response, can be called *risk treatment*, *risk mitigation*, or *risk control*.

Modification of risk is expected to reduce the adverse effects and, where possible, increase the beneficial effects of an endeavor such that the predetermined objectives are met with the fewest issues along the way.

In the previous example, we looked at the risk from driving in the snow. We identified certain unacceptable risks for reduction listed in Table 9.1.

The two obvious ways of reducing risks are to take actions to induce reduction in the probability and to take actions to induce reduction in the severity. In this example, it is much easier to effect a change in probability. The best way to approach risk modification is to modify the root cause of risk. Table 9.2 shows some modifications.

The addition of mitigation, in this case, is an anticipation to reduce the probability that an event will happen. Thus, we must update this register with the new anticipated probabilities and recalculate risk to confirm their acceptability. This is done as shown in Table 9.3.

In this case, we have reduced all risks to an acceptable level individually. Let us now look at the aggregate risks using the consequence–time series chart in Figure 9.1.

While we have reduced all unacceptable risks, we still need to be on the lookout for some high-severity risks as we embark on our objective to drive through the snow to reach

TABLE 9.1 Tabulated risk assessment.

Ways in which you do not get to work (sequence of events)	Probability of event happening	Severity level	Risk level
Car does not start due to dead battery	High	Negligible	Reduce risk
Car skids on icy roads and you are unable to control the car	High	Significant	Reduce risk
A major pileup on the road halts traffic	High	Moderate	Reduce risk

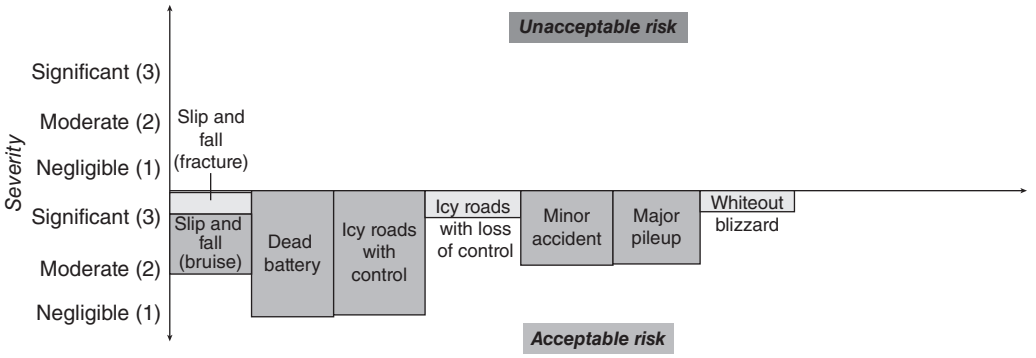
TABLE 9.2 Tabulated risk assessment with a column for risk modification.

Ways in which you do not get to work (sequence of events)	Probability of event happening	Severity level	Risk level	Modification
Car does not start due to dead battery	High	Negligible	Reduce risk	Check and replace battery when cold weather sets in
Car skids on icy roads and you are unable to control the car	High	Significant	Reduce risk	Change tires and check all systems as cold weather sets in
A major pileup on the road halts traffic	High	Moderate	Reduce risk	Use an app to find alternate routes with low-speed traffic

TABLE 9.3 Tabulated risk assessment with modified probability and risk levels.

Ways in which you do not get to work (sequence of events)	Probability of event happening	Severity level	Risk level	Mitigation	New probability	New risk level
Car does not start due to dead battery	High	Negligible	Reduce risk	Check and replace battery before winter	Medium	Acceptable
Car skids on icy roads and you are unable to control the car	High	Significant	Reduce risk	Change tires and check all systems	Low	Acceptable
A major pileup on the road halts traffic	High	Moderate	Reduce risk	Use an app to find alternate routes with low-speed traffic	Medium	Acceptable

FIGURE 9.1 Consequence–time series presentation of risk after mitigation (no unacceptable risks in this case).



our office. One cannot be carefree as a result of this exercise, as there are many subjective factors involved in this assessment. It is easier to predict an impact or consequence than the probability. Since no one can predict the future with 100% certainty, there is always some error involved in prediction regardless of the rigor of the methodology used.

A monitoring and review phase is essential to continually assess the level of risk and to check whether the predicted profile is maintained. In this example, a driver will continually monitor the road and snow conditions. If the conditions worsen, one may decide to turn back. As objectives become more complex with the involvement of more processes and people, a need arises to structurally define the roles and responsibilities of the risk management process. There arises a need for understanding the stakeholders and planning the whole process to ensure it is inclusive, streamlined, and effective.

Risk modification, for example, should always be a balance between practicality and effectiveness. Outside the simple scenario we've been examining, this can translate into a lot of complex factors in an organizational context, including attitudes toward risk and the availability of the resources for modification. Therefore, a primary consideration before beginning organization-wide risk management activity should be to identify and engage stakeholders.

In this chapter, we focus on risk modification, which can be defined as:

risk modification (treatment)

The method of selection and implementation of options for addressing risk, which usually involves a measure that maintains and/or modifies risk.

CHAPTER 10

The Stakeholder

EVEN BEFORE WE BEGIN identification of the risks, we must begin the identification of the *stakeholders*. These are the cross-functional entities that have a stake in the product, process, or system for which the risk is being analyzed. ISO 31000:2018 defines a *stakeholder* as:

> *Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.*[1]

Thus, any individual or organization that is directly or indirectly involved with, or is affected by, organization decision or activities can be a stakeholder. It is incumbent on the organization (and risk professionals) to identify the most relevant stakeholders based on their impact to the objectives.

The level of interest and influence a stakeholder has in the activity must also be noted. A structured method of doing this is through these two simple phases:

1. Identification
2. Engagement

In the *identification* phase, the interests, interdependencies, and "stake" of the stakeholders must be noted. It is important here to note the risk attitude of the stakeholder. They may have a risk-taking attitude or a risk-averse attitude. For example, an investment company with spare cash may want to invest in a high-risk, high-return market, while a maker of implantable medical devices may have a very conservative risk-averse attitude. Detailed discussion on risk attitudes can be found in Chapter 15.

In the *engagement* phase, the risk professional must foster positive engagement with the stakeholder, which leads to mutual benefit. This means managing the needs and expectations of the stakeholder and paying commensurate attention to their stake in the activity. Communication and cross-functional facilitation are key to success in this process.

---

1. ©ISO. This material is reproduced from ISO 31000:2018, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

The level of engagement with a stakeholder is defined by the level of interest and influence (the *stake* of the stakeholder). Some stakeholders will eventually act as risk owners, and such identification is necessary early on to avoid confusion later in the risk monitoring phase.

The following are the levels of stakeholder engagement mentioned by the *Guide to Project Management Body of Knowledge*.[2] These can be leveraged during the risk management process for easy categorization:

1. **Unaware**—unaware of risks
2. **Resistant**—resistant to risk management efforts
3. **Neutral**—neither supportive of nor resistant to the risk management efforts
4. **Supportive**—aware of risk impacts and active participant in the risk management process
5. **Leading**—supportive and actively engaged in ensuring that the risk management plan is a success

Another method to categorize stakeholders is with the influence–engagement matrix. This is a variation of Mendelow's matrix, a tool that analyzes stakeholders on the basis of their interest in objectives and influence (power) in the organization. For risk management, engagement of important stakeholders is essential at each step, and this has been made evident on the x-axis in Figure 10.1. Instead of *interest* in objectives, we will plot the *impact* on the objective. This allows us to identify not only the stakeholders with the most skin in the game but also the ones who impact the "game" itself. Based on these two foundational parameters, the stakeholders can be classified into three categories:

1. **Key stakeholders:** These are the people whose engagement is crucial to the success of the risk management activities. For those key stakeholders with high engagement, maximum attention must be given, and efforts must be taken, to ensure that their engagement in risk management activities is sustained. For the key stakeholders who have low engagement in risk management activities, targeted efforts for reengagement must be taken to ensure that this is corrected. This starts with uncovering the root cause of disengagement and then gaining alignment, spending more resources, involving management, and so on.
2. **Active stakeholders:** These are the people who have low impact on the objectives but are actively involved in the risk management efforts. Such stakeholders must be shown consideration and their engagement must be sustained as long as doing so does not take resources away from the key stakeholders. Such stakeholders usually add value by uncovering issues that key high-level or executive stakeholders sometimes cannot due to their routine familiarity with the objectives. Involvement of the active stakeholders allows for a review by new and different sets of eyes.

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

3. **Satellite stakeholders:** These are the people who have low influence on outcomes—and low engagement in risk management activities. These stakeholders are usually deserving of the least attention because not much value addition is expected of them. Still, their impact on objectives must be reassessed frequently. It is quite common for the influence/impact of some stakeholders to be misjudged early on, possibly leading to issues midway.

Throughout the risk management process or the product or service life cycle, if the expectation is that engagement and influence of stakeholders may change, then plan to redraw the chart in Figure 10.1 for different phases.

After the identification of the stakeholders is complete, chart various stakeholders as shown in Figure 10.2 such that a targeted determination can be made for their reengagement into risk management activities.

Once the stakeholders who need additional engagement have been identified, they must be approached with a proposition that ensures benefits and value creation for them arising from their participation in the risk management activities. While self-interest is the best motivator, at times, authoritative enforcement by top management is needed to ensure engagement, depending on the urgency and state of stakeholder participation.

After categorization of the stakeholders, it is useful to form an RACI matrix, which can help manage deliverables as the implementation of the risk management plan moves forward. RACI stands for responsible, accountable, consulted, and informed, which are defined as follows:

1. **Responsible:** This stakeholder is responsible for completing a risk management task or specific deliverable. The deliverables can be wide ranging and can encompass system, operational, functional, or document-creation-related

FIGURE 10.1 Influence–engagement matrix.

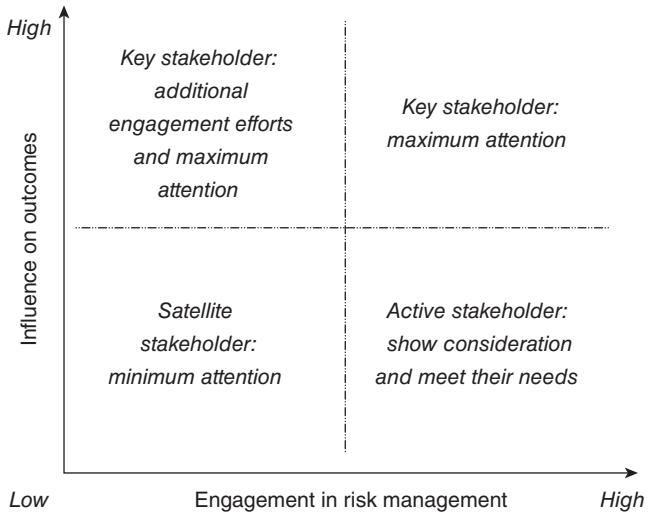


FIGURE 10.2 Influence–engagement matrix with stakeholder assignation.

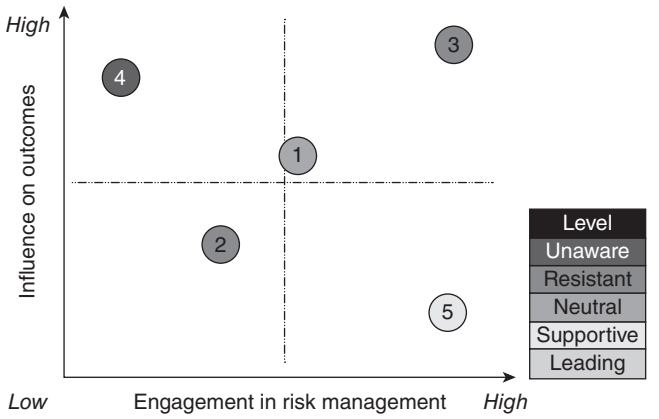


TABLE 10.1 An example of a RACI matrix.

Task	Risk manager	Stakeholder 1	Stakeholder 2	Stakeholder 3
Risk management plan development	R	R	C	I
Risk identification	A	R	R	C
Risk analysis	A	C	R	I
Risk response	A	C	C	I
Risk monitoring	A	C	C	I

tasks. The task will be completed by this stakeholder, and there can be more than one responsible stakeholder.

2. **Accountable:** This stakeholder is the person who owns the deliverable in terms of the completion liability and is the final approving authority. The accountable stakeholder may delegate the task and act as a reviewer or may also be the responsible party in some cases. It is a best practice to ensure that only one stakeholder is assigned the accountable status to avoid confusion.
3. **Consulted:** These are the stakeholders whose feedback is important by virtue of their expertise in the subject matter or routine association with the deliverable.
4. **Informed:** These stakeholders are periodically informed on the progress of the task or the deliverable. The communication is often one-way as opposed to two-way communication with the consulted stakeholders.

The RACI matrix can be created based on individual risk levels, at the level of hazards, or on the planning level, as shown in Table 10.1.

As we discussed earlier in the first example, engagement of the stakeholders leads to accurate identification, categorization, and classification of the risks. A lot of stakeholders will be the eventual risk owners, and they all must be on the same page in terms of escalation, action responses, communication, and documentation techniques.

CHAPTER 11

Upside of Risk: Opportunity

LOOKING AT ONLY THE DOWNSIDE OF RISK is akin to considering a coin to have only one side. Table 11.1 reproduces the dictionary definitions of the term "risk."

There is certainly a negative connotation of the term "risk." But let us dispel this falsehood early on.

We saw a few definitions of risk in earlier chapters, some with broader scope than others. Let us contrast two standard definitions and discuss their implications.

ISO 13485:2016 (*Medical Devices—Quality Management Systems*) defines risk as:

> *Combination of the probability of occurrence of harm and the severity of that harm.*[1]

ISO 9000:2015 (*Quality Management Systems—Fundamentals and Vocabulary*), from which ISO 9001:2015 derives all terms and definitions, defines risk as:

> *Effect of uncertainty.*
> *Note 1 to entry: An effect is a deviation from the expected—positive or negative.*[2]

ISO 31000:2018 (*Risk Management—Guidelines*) defines risk as:

> *Effect of uncertainty on objectives.*
> *Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.*[3]

---

1. ©ISO. This material is reproduced from ISO 13485:2016, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
2. ©ISO. This material is reproduced from ISO 9001:2015, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
3. ©ISO. This material is reproduced from ISO 31000:2018, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

TABLE 11.1 Dictionary definitions of risk.

Source	Definition of risk
Macmillan	"The *possibility* that something *unpleasant* or *dangerous might happen*"
Merriam-Webster	"*Possibility* of *loss* or *injury*"
Dictionary.com	"Exposure to the *chance* of *injury* or *loss*; a *hazard* or *dangerous chance*"
Cambridge	"The *possibility* of *danger, defeat,* or *loss*"
Oxford	"*Chance* or *possibility* of *danger, loss, injury* or other *adverse consequences*"

Sources: Macmillan Dictionary, s.v., "risk," accessed June 15, 2020, https://www.macmillandictionary.com/us/dictionary/american/risk_1; Merriam-Webster Dictionary, s.v., "risk," accessed June 15, 2020, https://www.merriam-webster.com/dictionary/risk; Dictionary.com, s.v., "risk," accessed June 22, 2020, https://www.dictionary.com/browse/risk?s=t; Cambridge Dictionary, s.v., "risk," accessed June 15, 2020, https://dictionary.cambridge.org/us/dictionary/english/risk; Oxford Learner's Dictionaries, s.v., "risk," accessed June 15, 2020, https://www.oxfordlearnersdictionaries.com/us/definition/english/risk_1?q=risk.

As we can see from the three separate definitions, the scope of risk and risk management went from negative to positive. So which definition is right? The answer is, all of them.

The context of the organization as detailed in Chapters 14 and 16 really defines the context of risk management. In the first definition, the negative aspect of risk is stressed since, in the context of medical devices, it makes sense to consider every possible failure of the device in detail from a safety and reliability standpoint. This one-tailed approach to risk arms the user with singlemindedness and specificity of scope (i.e., confined to failure and safety). But here too, one may argue that addition or deletion of design features may be opportunities that may well benefit from a risk and failure assessment. One can also argue that if one considers opportunities or upsides of risk right at the beginning, a more beneficial device can be manufactured.

ISO 9001:2015 and ISO 31000:2018 are more universal standards that take the two-tailed approach to risk, which includes positive and negative aspects. The benefits of this approach are apparent in system-level, operational, strategic, and enterprise risk management. But when we get to the product, process, or service level, as the risks tend to become more and more specific, many practitioners find it difficult and at times redundant to incorporate the opportunity side.

To simplify, let us define an *event*, which is full of uncertainty (i.e., full of risk), as follows:

A risky event is an event whose occurrence is uncertain,
but if it were to occur, it may have a negative or positive impact
on the product, process, or system.

This risky event may be turning a screw in a spinal implant or choosing a new indication for a drug or adding a new navigation feature to a car. A potential failure mode is still a risk event but only with negative risk.

Let us now look at an example that clarifies the concepts above related to risk, uncertainty, and positive and negative aspects. Let us consider a game where the

TABLE 11.2 Expected monetary value analysis for a $5 bet.

Outcome	Probability	Impact	Probability × Impact
Tails	50%	–$5	–2.5
Heads	50%	+$10	+5

correct guess on the outcome of a fair coin toss doubles your wager. We are aware that a fair coin toss has 50% probability of heads or tails. So here, the risky event is the coin toss, with a two-tailed risk.

If I flip a coin on a $5 wager and call heads, tails brings a 50% possibility of loss and financial injury to me, but heads brings a 50% possibility of profit for me. I could have chosen not to place the wager and not take a risk, but I decided that there was an opportunity for me to benefit by taking that risk. When such situations present themselves, how do you decide which path to take? Is the risk worth it?

A risk-benefit analysis can help drive a decision in such cases. Below is one that I performed on the fly for this simple two-outcome event by doing the following:

1. Assigning probability to the positive outcome
2. Assigning impact level to the positive outcome
3. Assigning probability to the negative outcome
4. Assigning impact level to the negative outcome
5. Comparing total risk between the two outcomes by using a risk equation

Table 11.2 shows my tabulated risk-benefit analysis.

Table 11.2, in fact, is known as expected monetary value analysis (commonly used in project management) and is often used to quantify aggregate risk by multiplying the likelihood of the outcome by the impact of the outcome. This multiplicative product gives an expected monetary value for each outcome, which can be added across all outcomes to give a final level of risk. The aggregate expected output here is $2.50, which does not mean I will earn $2.50 but if I play this game over and over again multiple times, I will probably end up with an average gain of $2.50.

So, the question I need to answer in this simple risk-benefit analysis is: Am I fine with the expected monetary value of $2.50? or Am I fine with a 50% chance of losing $5 for a 50% chance to gain $10?

The key concept here is that risk is involved for all outcomes borne out of uncertainty. Some of these outcomes are beneficial and have a positive risk or an opportunity associated with them. Risk-benefit analysis is mentioned in detail in Chapter 36.

CHAPTER 12

Detailed Risk Identification

BEFORE WE BEGIN THE RISK-IDENTIFICATION PROCESS, we must ask ourselves, Why do we perform risk management? Previously, we learned that all risk is the effect of uncertainty. Uncertainty is everywhere around us, and some of that uncertainty carries threats while some carries opportunities. And, some uncertainty just doesn't matter. That my car may or may not start when I leave for work today is an uncertainty that matters tremendously to me since the impact would mean that I would miss an important meeting. The number of red lights I encounter is an uncertainty that doesn't matter to me as I start my day well ahead of time to ensure stopping at red lights doesn't become a factor in arriving at work on time.

In the words of David Hillson, risk is "uncertainty that matters."[1] And why do only some uncertainties matter? Because they affect an end goal. In an organization, these end goals may be classified as outcomes, objectives, or outputs.

Risk identification is the process of determining which risks affect the end goals, intended uses, or objectives. This determination in the risk-identification phase involves finding, defining, and documenting these risks. Thus, the data and evidence gathering and consolidation within the organizational context (see Chapters 14 and 16 for details on organizational context) is most important to begin this process. On a high level, the data must:

1. Provide a comprehensive review of the function within the scope of risk management activities
2. Be verifiable and reliable
3. Be relevant to the context
4. Be inclusive of all relevant stakeholders
5. Consider internal and external sources
6. Take into account existing controls
7. Take into account past, present, and future states
8. Take into account all risk sources
9. Take into account all risk drivers

1. D. Hillson, ed., *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk* (London: Kogan Page Publishers, 2016).

Risk sources are defined by ANSI/ASIS/RIMS RA.1-2015 as:

> *A factor with the potential to create uncertainty in achieving objectives.*[2]

Risk drivers are defined by ANSI/ASIS/RIMS RA.1-2015 as:

> *Event, individual(s), process, or trends having impact on the objectives of the organization.*[3]

Risk sources have a large scope and include the tangible and intangible factors. ISO 31000:2018 describes risk sources as having intrinsic potential to engender risk. They are the true root originators of risk. These can be things as broad as political environments and as narrow as a small design feature in a product. Risk source is simply the source of the hazard. Risk drivers are actuators of the risks from the risk sources. These are specific events, individuals, processes, actions, sets of decisions, and so on that actuate the risk at its source and increase its probability of realization by giving rise to a hazard. Consequently, sometimes risk sources are also known as hazard sources. The relationship between risk source, risk driver, hazard, sequence of events, and hazardous situation is shown in Figure 12.1.

While it is great to know a risk or hazard source for mitigation purposes, in terms of risk assessment, hazard identification is where the traditional risk identification process begins.

The process of risk identification may start with identification of the hazards:

> *A hazard is a potential condition that, through a sequence of events, can cause a consequence.*

Hazards can, and mostly do, exist without the occurrence of a failure. For example, the excessive vibration of internal components while driving a car on a dirt road is a hazard. It leads to a hazardous situation and failure only when some important component gets displaced and causes the car to stop or break down. Conversely, one may be able to drive the car for a long time without encountering any failures despite components being misplaced. This can be explained using the graphic in Figure 12.2.

In the example above, the dirt road is the risk source, and the risk driver is the need to traverse the dirt road (due to some objective, such as rural delivery). This leads to the appearance of a hazard, which is mechanical vibration. Overspeeding on a bad patch of road leads to magnification of vibration and dislodges a few components. This may lead to total stoppage of the car or may not lead to any event.

Thus, hazards are potential sources of risky events that may cause consequences (harmful, benign, or in some cases even beneficial).

---

2. *Risk Assessment*, ANSI/ASIS/RIMS RA.1-2015 (Alexandria, VA: American National Standards Institute, 2015), 3.1.
3. *Risk Assessment*, ANSI/ASIS/RIMS RA.1-2015 (Alexandria, VA: American National Standards Institute, 2015), 3.1.

FIGURE 12.1 From risk source to outcome.

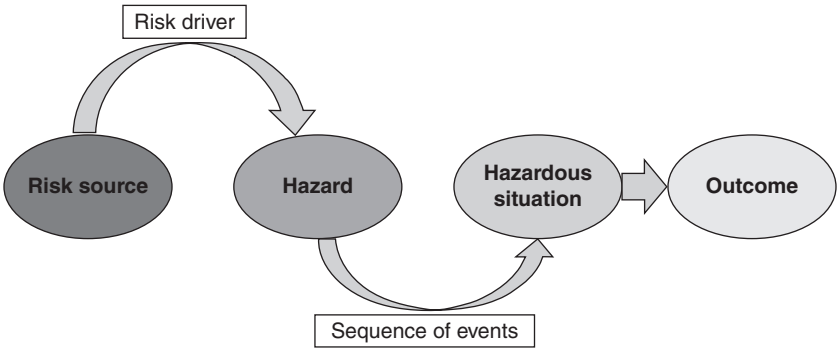
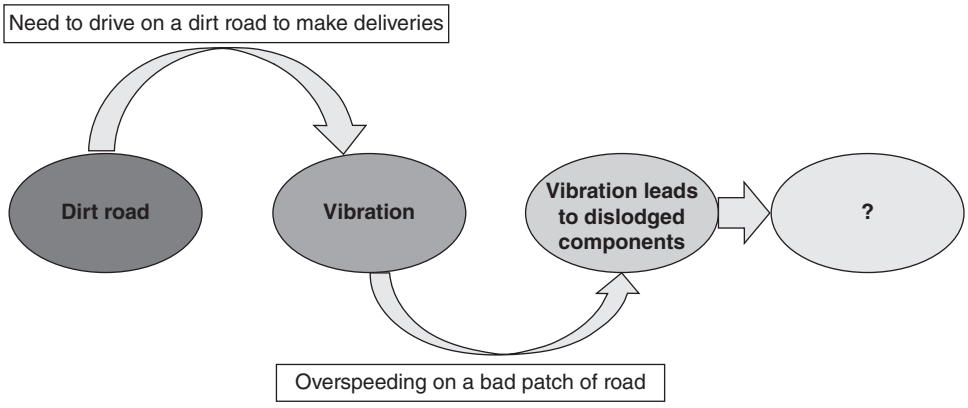


FIGURE 12.2 Dirt road as a risk source leading to vibration as a hazard and dislodged components as a hazardous situation.



ISO 12100:2010 describes *safety hazard* as:

> *A potential source of harm.*
> *It can be ever present, or it can appear unexpectedly.*[4]

A *hazardous situation* is:

> *A circumstance in which the user or system is exposed to a hazard with possibility of an impactful consequence.*

4. ©ISO. This material is reproduced from ISO 12100:2010, with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

In the example above, the hazardous situation is the dislodgement of the car's internal components due to exposure to vibration. This has the possibility of an impactful occurrence of total stoppage of the car.

Let us look at the full spectrum of events from risk/hazard source to outcome using the example in Figure 12.3.

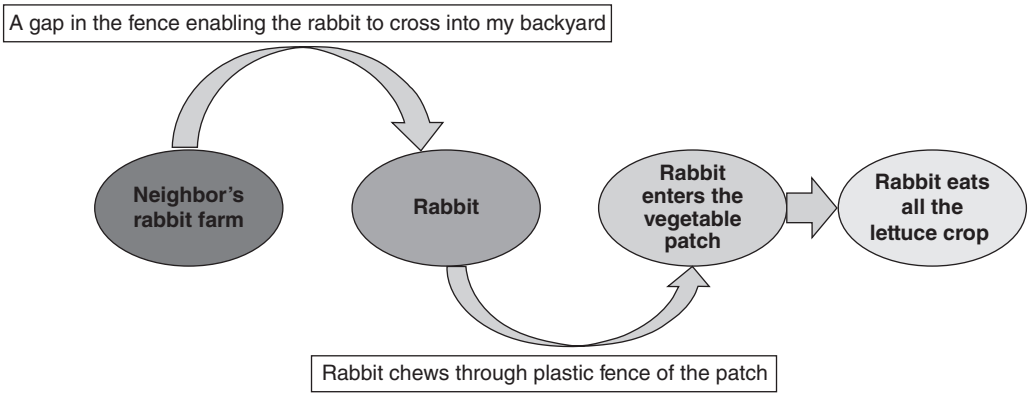
Here,

Risk/hazard source: neighbor's rabbit farm
Risk driver: a gap in the fence enabling a rabbit to cross into my backyard
Sequence of events that lead to a hazardous situation: rabbit chews through the plastic fence of my vegetable patch
Hazardous situation: rabbit enters the vegetable patch
Harm: rabbit eats all the lettuce crop

For the product, process, or system, the risk professional should be able to classify the various hazards that surround the activities. During hazard identification, the following questions should be asked:

1. What is the hazard?
2. Is the hazard time dependent?
3. Is the hazard location dependent?
4. What events lead the hazard to become a hazardous situation?
5. What are the multiple hazardous situations caused by the hazard due to each initiating event or risk drivers?
6. Are there any events or risk sources that trigger the hazard itself?
7. Can the hazard be quantified? Does the quantification have an impact on the risk engendered by the hazard?
8. What are the consequences of the hazardous situations?
9. What the best- and worst-case scenarios of the hazardous situation, and what needs to be done to achieve or mitigate those?

FIGURE 12.3 Neighbor's rabbit farm as the risk source, rabbit as the hazard, rabbit's entry into the vegetable patch as the hazardous situation, and rabbit eating the lettuce crop as the negative outcome.



Sometimes there can be confusion between a hazard and a source or even a hazard and a hazardous situation. In such cases, it is most important to consider the context of the situation. Also important to consider is the definitions of terms themselves. Always remember that there can be many ways of doing the right thing. Different industries have different categories of hazards. For example, for medical devices, the following could be the hazards list:

1. Electromagnetic energy
2. Line voltage
3. Leakage current
4. Electric fields
5. Thermal energy
6. Mechanical energy
7. Gravity
8. Vibration
9. Biological agents
10. Bacteria
11. Viruses

For disaster management, a list such as the following could apply:

1. Drought/famine
2. Storms/floods
3. Heat/cold waves
4. Earth movements
5. Eruptions
6. Landslides
7. Biological events
8. Epidemics
9. Infestations

These hazard lists essentially act as prompts to guide the formulators of risk assessment to the potential failures that may manifest as threats or opportunities.

The questions we are trying to answer during the risk identification process are as follows:

- What could affect us?
- What could go wrong?

To answer these questions, the hazards list must be broken down into specific and sensible individual line items that may represent failures encompassing opportunities and threats. Here, we move from hazard identification into risk identification.

TABLE 12.1 Tabular organization of cause, risky event, effect, classification, and risk line item.

Hazard	Cause	Risky event	Effect	Classification	Risk verbiage
Icy road	Worn tires	Driving car on icy roads	Slippage and crash	Threat	Due to driving with worn tires on icy roads, the car can slip and crash

The key to the success of risk management lies here at this first step: *What level of specificity do you use to document the risk?* A simple technique for this is to follow the *risk metalanguage* described in the *Practice Standard for Risk Management*:[5]

Due to <cause>, <risk> can occur, which will lead to <effect>

The cause and effect loop must be clarified for the risk line to lend itself to proper usage. Another idea is to organize the cause, risky event, effect, and classification (threat, failure, or opportunity) in separate columns as in Table 12.1.

I have used neutral terms here to emphasize that there can be positive and negative aspects of risk. In certain industries, like medical devices, a risk may be specifically categorized in technical terms as *failure mode* and a negative effect may be a *harm*. It must be noted that there is a difference between *failure* and *failure mode*. This difference will be analyzed in more depth in Chapter 41 on failure modes and effects analysis.

As greater details are populated during the risk-identification exercise, it must be noted that some causes, effects, and risks will show up again and again. This is because one risk or failure may have more than one cause and, upon occurrence, could have more than one effect, which could be threats or opportunities. The cause and subsequent sequence of events can create the possibility of the negative or positive outcome through the activating agency of the risk.

WHERE DO THE RISKS COME FROM?

I mentioned that the lists of hazards act like prompts and help in targeted identification of risks from their very source. But to ensure that most of the risks are captured, engagement of the stakeholders is essential. The identification of the stakeholders precedes the risk identification and is extremely important since, many times, the success of risk identification depends on the success of cross-functional engagement of the stakeholders.

5. Project Management Institute, *Practice Standard for Project Risk Management* (Newtown Square, PA: Project Management Institute, 2009).

On an enterprise level, the high-level risks may be said to arise from volatility, uncertainty, complexity, and ambiguity (VUCA). The U.S. Army War College introduced the concept of VUCA to define the issues facing a fractured and weaponized world at the end of the Cold War. All systems and organizational challenges, on a base level, can be fit into the following four definitions:

1. **Volatility:** Volatility denotes the likelihood of changing rapidly and unpredictably. In risk contexts, volatility refers to the challenge of organizational control over the dynamics of change. In the risk-identification phase, we ask: *What rapidly changing liabilities does the organization face?* (stock market? consumer choice? etc.)
2. **Uncertainty:** While volatility looks at ups and downs, uncertainty looks toward problems faced due to lack of predictability. With anticipation comes awareness, understanding, and eventual evaluation of the issue in a risk management context.
3. **Complexity:** Complexity refers to the multitude of interwoven and interconnected risks that can confound their correct identification and defeat a risk response. Complex risks take effort to be defined through a simple causal nexus and can possibly lead to confusion. Using the risk metalanguage can diagnose such risks in the identification phase.
4. **Ambiguity:** Reality and outcomes are open to more than one interpretation; so are risks. Ambiguity regarding a risk impact or risk cause leads to incorrect risk evaluations.

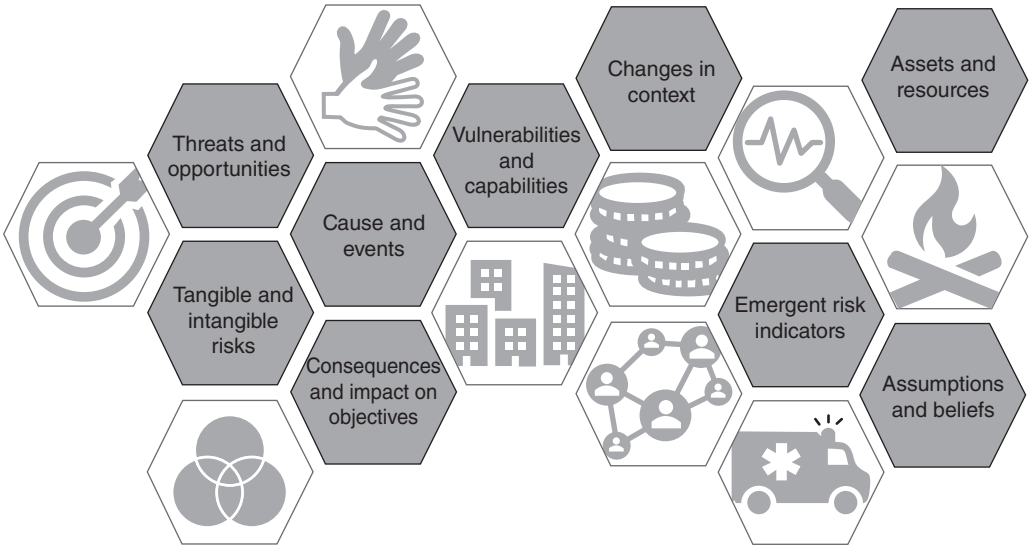
VUCA is a good place to start risk identification as it has a very broad scope. Knowledge arms us against being victims of VUCA, and by looking through the VUCA lens, we may identify specific risks that may be more complex than they seem.

ISO 31000:2018 goes a layer deeper than VUCA and mentions general sources of risk, as shown in Figure 12.4.

In addition to the above items, a variety of sources should be scanned for potential risks. A few of them are listed below:

1. Design and development plan / project plan / action plan
2. Specification and constraints
3. Human resources management plan
4. Cost and schedule documentation
5. Assumptions
6. Stakeholder list
7. Quality management plan
8. Technical documentation
9. Supplier quality and procurement documentation
10. Academic and published studies
11. Quality checklists and forms
12. Standard operating procedures
13. Historical similar activities and their risk management plans

FIGURE 12.4 General sources of risk.



In this chapter we have learned how and where to identify risks. This is only the first part of the risk-identification process. In coming chapters we will see how to assign qualitative and quantitative probabilities to these identified risks.

It is important that the risk-identification process generate sufficient detail such that it may be properly qualitatively or quantitatively assessed and be assigned to a risk owner. In addition, the already identified risk may be updated as time passes and more knowledge becomes available; the risk-identification process must allow for such iterative identification. Most importantly, the process must allow for identification and proper documentation and assessment of emergent risks. New risks that were not identified during the initial identification phase should be prioritized for evaluation by quick formal identification supported by due process. This is summarized in Figure 12.5.

HOW DO WE IDENTIFY THE RISKS?

After the relevant cross-functional team has been identified and engaged, a comprehensive review of all the documentation stated above must be completed. The assumptions, requirements, and constraints must be tested, and a preliminary list of possible issues compiled.

As shown in Figure 12.6, for holistic risk identification, similar products, processes, or services must be reviewed in conjunction with assessment of relevant present conditions of the current product process or service under study. Finally, risks must be anticipated using an informed reflection about future states through the anticipated life cycle of the system.

FIGURE 12.5 Risk identification process: points to remember.

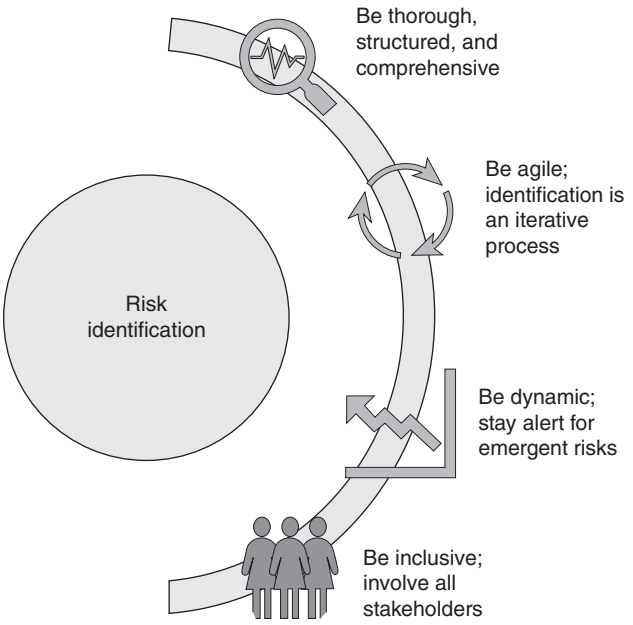
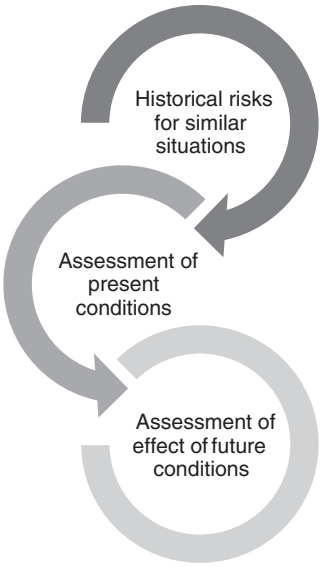


FIGURE 12.6 Risk identification: past, present, and future.



Information-gathering techniques are of immense benefit in this stage as they stimulate creativity. A few techniques are written below:

1. **Brainstorming:** Have a set of multidisciplinary experts who have good knowledge of the system essentially put the system through an imaginary pressure test that focuses on things going wrong and their consequences. This technique generates a lot of risk in a short amount of time and, if facilitated properly, can form the foundation of the risk-identification phase. A list of hazards can then be used as a starting point to generate conversation and automatically categorize the compiled risk list.
2. **Delphi Technique:** A questionnaire is used to solicit opinions on risk from various experts in the field, one at a time. These opinions are summarized and recirculated for further opinions, again and again, until consensus is reached on a list of risks. This technique, though time intensive, provides anonymity to the experts and allows them to finish the task of risk identification in their own time. This ensures that no one person dominates the discussion, and quashes the possibility of groupthink.
3. **Interviewing:** The risk manager takes on the role of an interviewer and summarizes the thoughts of the experts in a list of risks. This saves time but places more responsibility on the risk manager to ensure the efficacy of the process. Interviews can be coupled with surveys that include questions regarding survey takers' functional or departmental uncertainties and their perceived probability and impact rating of the risks.

For complex products, processes, and systems, root cause analysis may be needed at certain times to clarify the risk. This can be diagrammatically accomplished using the Ishikawa (fishbone) diagram and flowcharts.

CHAPTER 13

Chance and Possibilities

RISK, BY NATURE, IS BORNE OUT OF UNCERTAINTY. If there is a 100% probability of an event occurring, then that event is an actual hurdle or issue and no longer considered a risk. The probability of the occurrence of a risk is the likelihood of the occurrence of the risky event. While probability theory is an advanced subject in itself, for practical risk management purposes, we need only state some fundamentals.

An approach to probability is based on classical theory, which calculates the probability of an event based on favorability of the desired event over all events. This is given by the following equation:

$$Probability\ of\ an\ Event\ E = \frac{Number\ of\ times\ Event\ E\ can\ occur}{Number\ of\ all\ events} \tag{13.1}$$

This formula can be used to calculate probability of a unique event from a set of events, where all events have similar probabilities, such as drawing specific cards from a full deck of cards or the probability of a number showing in the throw of a die. The total probability is always 1 (100%), and it is composed of the probability of the desired event plus the probability of the undesired events.

This can be written as:

$$\begin{aligned} &Probability\ of\ final\ outcome \\ &= Probability\ of\ desired\ Event\ E + Probability\ of\ all\ other\ events = 1 \end{aligned} \tag{13.2}$$

The key point here is that the probability of all (which includes each and every outcome) events totals one (1). Out of this, the challenge for us is to extract the probability of our outcome of interest under study.

The classical approach to probability is simplistic since it assumes that all outcomes have an equal chance of occurring. While this approach is great for certain tools like decision trees and fault tree analysis, in real-world business scenarios, we know sometimes this may not be the case.

A second approach to probability calculation is the *frequentist approach*. This approach depends on testing a sample size to gauge the relative frequency of occurrence of an event in the population. A small representative group is tested once or

many times, depending on the need for statistical power, and the frequency of an event is ascertained. Many times, risk professionals do not have the luxury of conducting tests like these, and, often, the nature of risks under study does not lend itself to this approach at all (e.g., enterprise risks).

The last approach to probability accepts the fact that decisions regarding probability of risks are largely subjective, based on opinions, viewpoints, and beliefs grounded in available evidence. The probability is assigned according to the measure of degree of belief one has for the event. This does not mean ad hoc assignation, but a logical decision based on available facts that inform the belief.

An obvious drawback of the subjective approach is that it is more than likely to be off target. There are various methods to reduce subjective inaccuracy that will be discussed later in this chapter. A modern approach is to use Bayesian statistics, which I will discuss briefly.

The *Bayesian approach* gives us a mathematical formula to incorporate any new evidence into the old probability calculation so that the probability can be updated. The formula is as follows:

$$\begin{array}{r}\textit{Probability of a risk A' knowing that}\\ \textit{an information x' is true}\end{array} = \frac{\begin{array}{c}(\textit{Probability of information x' being}\\ \textit{true knowing that probability of risk}\\ \textit{A' is true}) * (\textit{Probability of risk A being true})\end{array}}{(\textit{Probability of information x' being true})} \quad (13.3)$$

The Bayes theorem is an easy method to update previously assigned probabilities and iteratively arrive at an accurate probability level for any given risk as new evidence becomes available.

The foundational distinctions in assignation of probability for purposes of risk analysis have been summarized by Lt. Duane Boniface of the U.S. Coast Guard in Table 13.1.

As risk management professionals, we are continually challenged to ensure the correct assignation of probability. Many approaches exist to reduce errors by increasing objectivity in assignation. Use of structured methods by decomposing constituent scenarios and sequence of events, analyzing the causal nexus between events preceding

TABLE 13.1 Types of probability assignations.

Probability Interpretation	Description
Classical	The probability of an event is the ratio of the number of outcomes with the attributes of the event to the total number of equally likely and different ways.
Frequency	The probability of an event is given by the limit of its relative frequency as the number of samples becomes large.
Subjective	The probability of an event is a measure of the degree of belief that one holds for that event.

Source: Duane Boniface, Lt., U.S. Coast Guard, "Risk-Based Decision-Making Guidelines," accessed July 7, 2020, https://www.hsdl.org/?view&did=471178.

impact, and leveraging historical information is a good start, but we must be prepared to review and reassess the initially assigned probabilities as and when evidence emerges that may change our prediction. Depending on the risk methods, the probabilities assigned can be qualitative, semiquantitative, or quantitative.

The following five approaches for probability assignation are discussed in the rest of the chapter:

1. Expert opinion
2. Parametric analysis
3. Analogous analysis
4. Probabilistic analysis
5. Cause and effect analysis

In our first example, we assigned the probability based on an opinion, which though practical and obvious was subjective. A broken femur was a remote and unlikely-to-happen event, so the probability was assigned as low per Table 13.2.

Table 13.2 keeps things simple but does not allow us to assign a number to the actual rate of the events. To allow for such a detail, a table such as Table 13.3 may be used.

Now the question arises, How could one actually assign an exact value? The answer is that we don't. The table above has ranges instead of set exact values. The advantage of assigning a range is that we can capture a low estimate and a high estimate since pinpointing an exact value would be extremely difficult and have a high chance of being inaccurate. This is a semiquantitative method of assigning a range of occurrence to an event. Our aim is to use expert opinion to assign a measure to the randomness of the risky event. In realization of this goal, as far as possible, we should try to convert a qualitative assessment to a semiquantitative one using such tables. The range of the

TABLE 13.2 Qualitative probability and its description.

Term	Description
High	Occurrence is likely (often or frequent)
Medium	May occur but not often or frequently
Low	Rare occurrence (unlikely)

TABLE 13.3 Semiquantitative probability table.

Rank	Description
0	≤**0.001%** Extremely unlikely—up to 1 in 100,000 cases
1	>**0.001% and** ≤**0.01%** Occasional—up to 1 in 10,000 cases
2	>**0.01% and** ≤**0.1%** Moderately probable—up to 1 in 1,000 cases
3	>**0.1% and** ≤**0.5%** Reasonably probable—up to 1 in 200 cases
4	>**0.5% and** ≤**100%** Highest rank—inclusive of failure occurring in every case

values in the table can vary and should be set in accordance with the nature of risks encountered according to industry sectors. Keep in mind that the aim is to set a range of probability with about 90% confidence. The main fallacy is that people set the range too narrow, which is a behavioral bias of overconfidence or excessive optimism.

Likewise, I may have a previous activity that is similar to my current activity, and, thus, I may choose to assign similar values of probability. This combines past experience, historical information, and expert judgment. For example, a company may make valves and produce different product lines with minor modifications. If a new product line is introduced, the company may choose to leverage the risk probability information from the previous product lines to form a baseline performance based on probability of various failures of similar products. This method is known as *analogous estimating*. A major drawback of this technique is that it relies on heuristics of availability and representativeness—that is, some data may be easily available, leading them to be assumed to be more important, and some data may be easily stereotyped, leading to a narrow viewpoint.

Parametric analysis uncovers a statistical relationship between the subject activity and the previous activity to arithmetically calculate probability based on ratios in terms of failure rates, cost, or schedule. For example, if there are data that the valves of a certain product line fail at the inlet flap 1000 times per million opportunities, and if we know that the inlet flap is strengthened on the new product line by 50%, then we can assume based on the parametric relationship that the new valve will fail 50% less often. So, we will then assign a probability of failure as 500 per million. The drawback of this technique is that it is susceptible to the anchoring and adjustment heuristic (see Chapter 37). This occurs when a risk owner attempts to forcefully draw a parametric estimate from insufficient data. Thus, the nature of the data must be understood before drawing any inferential conclusion(s), however simple they may appear.

The *probabilistic analysis* combines the following three:

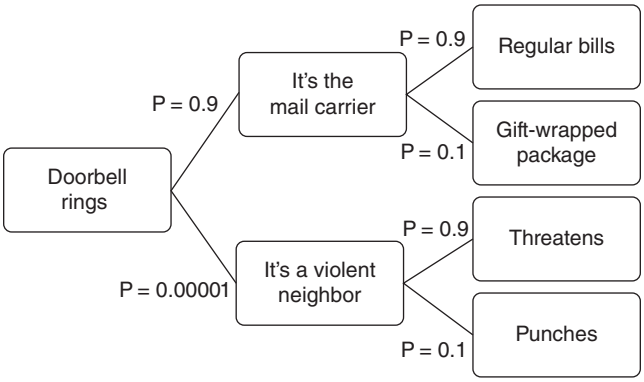
1. Historical data for same or similar product, or a product with similar features
2. A forecast based on cumulative or conditional probabilities of successive fault levels in a system
3. Subject matter expert opinion

An accurate way of calculating probability is by using *probability theory*. This method works the best for systems that can be represented by subsystems.

In Figure 13.1, the probability of the doorbell ringer being the mail carrier delivering the regular bills is 0.18, which translates to about one in five times, as opposed to the probability of the doorbell ringer being a violent neighbor throwing punches, which is one in a million. An important thing to keep in mind is that for each level of consequence, the probabilities must ideally add up to one, which means that you have considered all possible outcomes. In this case, the probabilities do not add up to one, which means there could be other consequences of the bell ringing.

In certain industries, use of quantitative methods such as the *Monte Carlo simulation* is common. This method provides estimates by incorporating the overall system

FIGURE 13.1 A causal probability tree for outcomes related to ringing of a doorbell.



risk rather than just one individual failure mode. In this discussion, we will limit ourselves to risk analysis for specific individualized failures. Monte Carlo analysis is detailed in Chapter 46.

Usage of expert opinion should be formalized and not ad hoc. For example, if you are soliciting expert opinion on failure of a noncritical software feature on an airplane, different pilots may have different opinions depending on their technique, experience, and training. The software engineers may have a completely different viewpoint than the pilots, though they are both subject matter experts (SMEs). Similarly, in the health-care field, surgeons and doctors are often used as SMEs, but the onus is on the owner of the risk analysis to reduce subjectivity of the expert opinions. A few ways in which the objectivity of an SME opinion can be maintained are the following:

1. Pairing the opinion with historical data and investigating for gaps
2. Pairing the opinion with peer opinion and investigating gaps
3. Assigning weights to several factors and comparing weighted opinions among experts
4. Pairing the opinion with probability analysis methods discussed earlier

If there is a set causal nexus between events in a sequence, then the probabilities of preceding events can be multiplied to give the final consequence. Sometimes, events under study can be easily resolved into successive sets of causes and effects.

In Figure 13.2, a probability is assigned independently for every cause and effect pair in sequence. The final probability of lethal exposure to radioactivity due to the hazard of radioactive material storage in a chamber with poor sealant doors is $P1 \times P2 \times P3 = 0.00125$ or 0.125%.

This causal chain can be explained in terms of system, fault condition, fail-safe failure, and outcome, as shown in Figure 13.3.

The probability of harm in this case due to this specific causal chain is $P1 \times P2 \times P3 \times P4$. Care must be taken to not become narrow-minded in any step. One system may have several hazards, or there may be several fault conditions that lead

FIGURE 13.2 Causal probability chain related to storage of radioactive material in a sealed chamber.

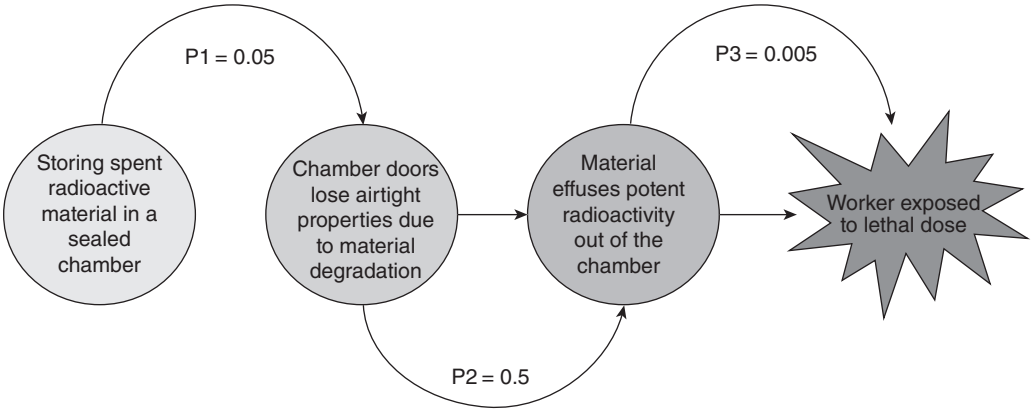
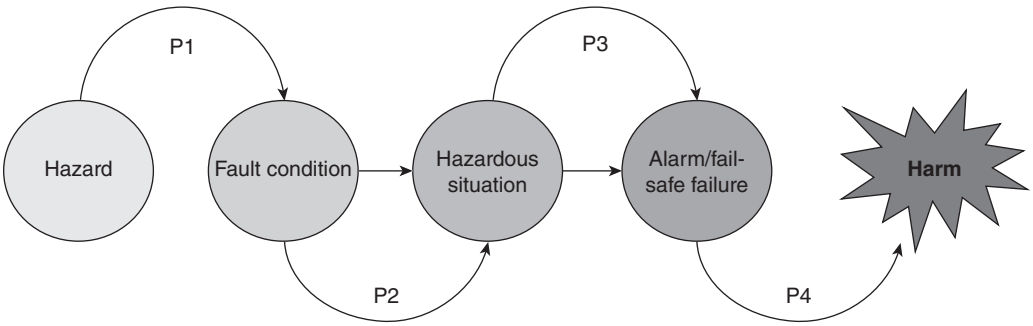


FIGURE 13.3 Causal probability chain template.



to different hazardous situations. This diagram, while being very applicable in this example, is not a universal standard, and the hazard may appear after occurrence of a fault condition depending on the system and the context. The actual assignation of step-wise probabilities can be accomplished by any of the estimating methods detailed earlier. The subjective aspect of these methods must be understood before using them.

The subjectivity of a probability estimate is based on the perception of the person assigning the estimate, which is in turn based on the person's knowledge and experiences in general. It is the risk professional's job to refocus this knowledge and experience toward the event under study. This can be done by supplying as much data and information as possible regarding the event and the system within which the event will occur. If it is common to hear, "Oh, that happens all the time. It's more than a 90% rate," then the risk management professional must uncover why and challenge the experts' assumptions by supplying the same nature of information on which the initial decision of >90% rate was made, to check whether the assumptions are still valid.

In this chapter, we learned the exercise of *likelihood analysis*, also known as *probability estimation*, which along with *consequence analysis* forms an important pillar of risk assessment:

probability estimation

The exercise of assessing likelihood of occurrence of risk and quantitatively, semiquantitatively, or qualitatively assigning a value to the assessed estimate.

Bibliography

American Society for Quality. "Quality Glossary of Terms, Acronyms, & Definitions: ASQ." ASQ. Accessed June 20, 2020. https://asq.org/quality-resources/quality-glossary/.

American Society of Safety Engineers. *Prevention through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes*. ANSI/ASSE Z590.3-2011. Des Plaines, IL: American Society of Safety Engineers, 2011.

ANSI/ASIS/RIMS. *Risk Assessment.* ANSI/ASIS/RIMS RA.1-2015. Alexandria, VA: American National Standards Institute, 2015. https://webstore.ansi.org/standards/asis/ansiasisrimsra2015.

Automotive Industry Action Group. *The FMEA Handbook: Failure Mode and Effects Analysis*. Southfield, MI: Automotive Industry Action Group, 2019.

Aven, T. "Safety Is the Antonym of Risk for Some Perspectives of Risk." *Safety Science* 47, no. 7 (2009): 925–930.

Aven, T. "SRA Glossary Draft." Society for Risk Analysis. Accessed June 20, 2020. https://www.sra.org/sra-glossary-draft.

Aven, T., and J. Kørte. "On the Use of Risk and Decision Analysis to Support Decision-Making." *Reliability Engineering & System Safety* 79, no. 3 (2003): 289–299.

Bank, K. F. K. *Mendelow's Matrix*. London: Kaplan Financial, 2012.

Benefit-Risk Balance for Marketed Drugs. Geneva, Switzerland: CIOMS, 2004.

Bennett, N., and J. Lemoine. "What VUCA Really Means for You." *Harvard Business Review* 92, nos. 1–2: 27.

Benneyan, J. C. "Statistical Quality Control Methods in Infection Control and Hospital Epidemiology, Part I Introduction and Basic Theory." *Infection Control & Hospital Epidemiology* 19, no. 3 (1998): 194–214.

Berger, S. "Vaginal Mesh Has Caused Health Problems in Many Women, Even as Some Surgeons Vouch for Its Safety and Efficacy." *Washington Post*, January 20, 2019. https://www.washingtonpost.com/national/health-science/vaginal-mesh-has-caused-health-problems-in-many-women-even-as-some-surgeons-vouch-for-its-safety-and-efficacy/2019/01/18/1c4a2332-ff0f-11e8-ad40-cdfd0e0dd65a_story.html.

Blackhurst, J. V., K. P. Scheibe, and D. J. Johnson. "Supplier Risk Assessment and Monitoring for the Automotive Industry." *International Journal of Physical Distribution & Logistics Management* 38, no. 2 (2008): 143–165.

Boada, J. N., C. Boada, M. García-Sáiz, M. García, E. Fernandez, and E. Gomez. "Net Efficacy Adjusted for Risk (NEAR): A Simple Procedure for Measuring Risk: Benefit Balance." *PloS One* 3, no. 10 (2008): e3580.

Bossert, J. L., ed. *The Supplier Management Handbook*. Milwaukee, WI: ASQ Quality Press, 2004.

Breban, R., J. Riou, and A. Fontanet. "Interhuman Transmissibility of Middle East Respiratory Syndrome Coronavirus: Estimation of Pandemic Risk." *Lancet* 382, no. 9893 (2013). https://doi.org/10.1016/S0140-6736(13)61492-0.

Campbell, A., J. Whitehead, and S. Finkelstein. "Why Good Leaders Make Bad Decisions." *Harvard Business Review* 87, no. 2 (2009): 60–66.

Center for Devices and Radiological Health. "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval and De Novo Classifications." August 29, 2019. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/factors-consider-when-making-benefit-risk-determinations-medical-device-premarket-approval-and-de.

Center for Food Safety and Applied Nutrition. "HACCP Principles & Application Guidelines." U.S. Food and Drug Administration, August 14, 1997. https://www.fda.gov/food/hazard-analysis-critical-control-point-haccp/haccp-principles-application-guidelines.

Chen, J. "Pathogenicity and Transmissibility of 2019-NCoV—A Quick Overview and Comparison with Other Emerging Viruses." *Microbes and Infection* 22, no. 2 (2020): 69–71.

Chen, K.-S., T.-C. Chang, K.-J. Wang, and C.-T. Huang. "Developing Control Charts in Monitoring Service Quality Based on the Number of Customer Complaints." *Total Quality Management & Business Excellence* 26, no. 5–6 (2015): 675–689.

Chuang-Stein, C. "A New Proposal for Benefit-Less-Risk Analysis in Clinical Trials." *Controlled Clinical Trials* 15, no. 1 (1994): 30–43.

Chuang-Stein, C., R. Entsuah, and Y. Pritchett. "Measures for Conducting Comparative Benefit: Risk Assessment." *Drug Information Journal* 42, no. 3 (2008): 223–233.

Chuang-Stein, C., N. R. Mohberg, and M. S. Sinkula. "Three Measures for Simultaneously Evaluating Benefits and Risks Using Categorical Data from Clinical Trials." *Statistics in Medicine* 10, no. 9 (1991): 1349–1359.

CIOMS Working Group IV. *Benefit–Risk Balance for Marketed Drugs: Evaluating Safety Signals*. Geneva, Switzerland: Council for International Organizations of Medical Sciences, 1998. https://cioms.ch/wp-content/uploads/2017/01/benefit-risk.pdf.

Clavien, P. A., J. Barkun, M. L. De Oliveira, J. N. Vauthey, D. Dindo, R. D. Schulick, E. De Santibañes, et al. "The Clavien-Dindo Classification of Surgical Complications: Five-Year Experience." *Annals of Surgery* 250, no. 2 (2009): 187–196.

Cortez, A. *The Complete Idiot's Guide to Risk Management: Get Dynamic Growth and Profitability through Successful Risk Strategies*. Indianapolis, IN: Penguin, 2010.

Crichton, D. "The Risk Triangle." *Natural Disaster Management* 102, no. 3 (1999): 103.

Crouch, E. A., and R. Wilson. *Risk-Benefit Analysis*, 2nd ed. Cambridge, MA: Harvard Center for Risk Analysis, 2001.

Department of Defense. *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017.

Dindo, D. "The Clavien–Dindo Classification of Surgical Complications." In *Treatment of Postoperative Complications after Digestive Surgery*, pp. 13–17. London: Springer.

Edwards, I. R., B. E. Wiholm, and C. Martinez. "Concepts in Risk-Benefit Assessment." *Drug Safety* 15, no. 1 (1996): 1–7.

Elahi, B. *Safety Risk Management for Medical Devices*. Academic Press, 2018.

Forna, A., P. Nouvellet, I. Dorigatti, and C. A. Donnelly. "Case Fatality Ratio Estimates for the 2013–2016 West African Ebola Epidemic: Application of Boosted Regression Trees for Imputation." *Clinical Infectious Diseases* 70, no. 12 (2020): 2476–2483. https://doi.org/10.1093/cid/ciz678.

Gaylor, D. W. "Risk/Benefit Assessments of Human Diseases: Optimum Dose for Intervention." *Risk Analysis: An International Journal* 25, no. 1 (2005): 161–168.

Goddard Space Flight Center. *Risk Management Reporting*. GFSC-STD-002. Greenbelt, MD: NASA, 2009.

Goleman, D. *Emotional Intelligence*. New York: Bantam, 2006.

Goleman, D. *Emotional Intelligence and Working with Emotional Intelligence*. London: Bloomsburg Publishing, 2004.

Goleman, D. "How Emotionally Intelligent Are You?" Daniel Goleman. April 22, 2015. http://www.danielgoleman.info/daniel-goleman-how-emotionally-intelligent-are-you/.

Goleman, D. "Leadership That Gets Results." *Harvard Business Review* 78, no. 2 (2000): 4–17.

Goleman, D. "What Makes a Leader." *Organizational Influence Processes* 82 (2003): 229–241.

Goleman, D., R. E. Boyatzis, and A. McKee. *Primal Leadership: Unleashing the Power of Emotional Intelligence*. Boston: Harvard Business Press.

Goleman, D., R. E. Boyatzis, A. McKee, and S. Finkelstein. *HBR's 10 Must Reads on Emotional Intelligence (with featured article "What Makes a Leader?" by Daniel Goleman)*. Boston: Harvard Business Review Press, 2015.

Hampton, J. *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity*. New York: Amacom, 2009.

Hare, L. B. "Statistics Roundtable: Follow the Rules." American Society for Quality. Accessed June 20, 2020. http://asq.org/quality-progress/2013/01/statistics-roundtable/follow-the-rules.html.

Her Majesty's Treasury. *The Orange Book*. Government Finance Function, 2020. https://www.gov.uk/government/publications/orange-book.

Hillson, D. *Risk Facilitation Made Easy*. Paper presented at PMI Global Congress 2015 EMEA, London, England. Newtown Square, PA: Project Management Institute, 2015.

Hillson, D., ed. *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk*. London: Kogan Page Publishers, 2016.

Hillson, D. "Towards a Risk Maturity Model." *International Journal of Project & Business Risk Management* 1, no. 1 (1997): 35–45.

Hillson, D. "Use a Risk Breakdown Structure (RBS) to Understand Your Risks." *Proceedings of the Project Management Institute Annual Seminars & Symposium* 10 (October 2002). https://www.pmi.org/learning/library/risk-breakdown-structure-understand-risks-1042.

Hillson, D. "Using a Risk Breakdown Structure in Project Management." *Journal of Facilities Management* 2, no. 1 (2003): 85–97.

Hillson, D., and R. Murray-Webster. "Understanding and Managing Risk Attitude." In *Proceedings of 7th Annual Risk Conference,* held in London, UK, on November 26, 2004.

Holden, W. L., J. Juhaeri, and W. Dai. "Benefit-Risk Analysis: A Proposal Using Quantitative Methods." *Pharmacoepidemiology and Drug Safety* 12, no. 7 (2003): 611–616.

Hopkin, P. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. London: Kogan Page Publishers, 2018.

Hugonnet, S., and D. Pittet. "Transmission of Severe Acute Respiratory Syndrome in Critical Care: Do We Need a Change?" *American Journal of Respiratory and Critical Care Medicine* 169, no. 11. https://doi.org/10.1164/rccm.2403004.

Hunink, M. G., M. C. Weinstein, E. Wittenberg, M. F. Drummond, J. S. Pliskin, J. B. Wong, and P. P. Glasziou. *Decision Making in Health and Medicine: Integrating Evidence and Values*. 2nd ed. Cambridge: Cambridge University Press, 2014.

Hutchins, G. *ISO: Risk Based Thinking*. Portland, OR: Quality Plus Engineering, 2016.

Hutchins, G. *ISO 31000:2018 Enterprise Risk Management*. Portland, OR: Greg Hutchins, 2018.

International Electrochemical Commission. *Failure Modes and Effects Analysis (FMEA and FMECA)*. IEC 60812:2018. Geneva, Switzerland: International Electrochemical Commission, 2018. https://webstore.iec.ch/publication/26359.

International Electrochemical Commission. *Fault Tree Analysis (FTA)*. IEC 61025:2006. Geneva, Switzerland: International Electrochemical Commission, 2006. https://webstore.iec.ch/publication/26359.

International Electrochemical Commission. *Hazard and Operability Studies (HAZOP Studies)—Application Guide*. IEC 61882:2016. Geneva, Switzerland: International Electrochemical Commission, 2016. https://webstore.iec.ch/publication/24321.

International Electrotechnical Commission. *Risk Management: Part 3 Guide to Risk Analysis of Technological Systems*. IEC 60300-3-9:1995. Geneva, Switzerland: International Electrotechnical Commission, 1995.

International Organization for Standardization. *Application of Risk Management to Medical Devices*. ISO 14971:2019. Geneva, Switzerland: International Organization for Standardization, 2019. https://www.iso.org/standard/72704.html.

International Organization for Standardization. *Automation Systems and Integration—Key Performance Indicators (KPIs) for Manufacturing Operations Management—Part 2: Definitions and Descriptions of KPIs*. ISO 22400-2:2014. Geneva, Switzerland: International Organization for Standardization, 2014.

International Organization for Standardization. *Food Safety Management Systems—Requirements for Any Organization in the Food Chain*. ISO 22000:2018. Geneva, Switzerland: International Organization for Standardization, 2018. https://www.iso.org/standard/65464.html.

International Organization for Standardization. *Guidelines for Auditing Management Systems*. ISO 19011:2018. Geneva, Switzerland: International Organization for Standardization, 2018. https://www.iso.org/standard/70017.html.

International Organization for Standardization. *Quality Management Systems—Requirements*. ISO 9001:2015. Geneva, Switzerland: International Organization for Standardization, 2015. https://www.iso.org/standard/62085.html.

International Organization for Standardization. *Risk Management—Guidelines*. ISO 31000:2018. Geneva, Switzerland: International Organization for Standardization, 2018. https://www.iso.org/standard/65694.html.

International Organization for Standardization. *Risk Management—Risk Assessment Techniques*. ISO 31010:2019. Geneva, Switzerland: International Organization for Standardization, 2019. https://www.iso.org/standard/72140.html.

International Organization for Standardization. *Risk Management—Vocabulary*. ISO Guide 73:2009. Geneva, Switzerland: International Organization for Standardization, 2009. https://www.iso.org/standard/44651.html.

Johnson, F. R., S. Özdemir, C. Mansfield, S. Hass, C. A. Siegel, and B. E. Sands. "Are Adult Patients More Tolerant of Treatment Risks Than Parents of Juvenile Patients?" *Risk Analysis: An International Journal* 29, no. 1 (2009): 121–136.

Jones, B. "Breast Implant Scandal: What Went Wrong?" CNN, January 27, 2012. https://edition.cnn.com/2012/01/27/world/europe/pip-breast-implant-scandal-explained/index.html.

Karwowski, W., and A. Mital. "Potential Applications of Fuzzy Sets in Industrial Safety Engineering." *Fuzzy Sets and Systems* 19, no. 2 (1986): 105–120.

Katayama, H., Y. Kurokawa, K. Nakamura, H. Ito, Y. Kanemitsu, N. Masuda, Y. Tsubosa, et al. "Extended Clavien-Dindo Classification of Surgical Complications: Japan Clinical Oncology Group Postoperative Complications Criteria." *Surgery Today* 46, no. 6 (2016): 668–685.

King, M. *Statistics for Process Control Engineers: A Practical Approach*. Hoboken, NJ: Wiley, 2017.

Kraljic, P. "Purchasing Must Become Supply Management." *Harvard Business Review* 61, no. 5 (1983): 109–117.

Lam, J. *Enterprise Risk Management: From Incentives to Controls*. Hoboken, NJ: John Wiley & Sons, 2014.

Lee, J. H., D. J. Park, H. H. Kim, H. J. Lee, and H. K. Yang. "Comparison of Complications after Laparoscopy-Assisted Distal Gastrectomy and Open Distal Gastrectomy for Gastric Cancer Using the Clavien–Dindo Classification." *Surgical Endoscopy* 26, no. 5 (2012): 1287–1295.

Levitan, B. "A Concise Display of Multiple End Points for Benefit–Risk Assessment." *Clinical Pharmacology & Therapeutics* 89, no. 1 (2011): 56–59.

Levitan, B. S., E. B. Andrews, A. Gilsenan, J. Ferguson, R. A. Noel, P. M. Coplan, and F. Mussen. "Application of the BRAT Framework to Case Studies: Observations and Insights." *Clinical Pharmacology & Therapeutics* 89, no. 2 (2011): 217–224.

Macesker, B., J. J. Myers, V. H. Guthrie, D. A. Walker, and S. G. Schoolcraft. "Quick-Reference Guide to Risk-Based Decision Making (RBDM): A Step-by-Step Example of the RBDM Process in the Field." Air University. Accessed October 25, 2008. http://www.au.af.mil/au/awc/awcgate/uscg/risk-qrg.pdf.

Markowski, A. S., and M. S. Mannan. "Fuzzy Risk Matrix." *Journal of Hazardous Materials* 159, no. 1 (2008): 152–157.

Ministry of Defence. *Safety Management Requirements for Defence Systems*. Standard 00-56. Ministry of Defence, Directorate of Standardisation, Kentigern House, 2007.

Moon, J. "An Investigation into the Use of Laney U Chart as a Visual Schedule Tracker to Graphically Monitor the Schedule Performance Index." *Journal of Engineering, Project, and Production Management* 10, no. 1 (2020): 35–41.

Moon, J. "Effect of Emotional Intelligence and Leadership Styles on Risk Intelligent Decision Making and Risk Management." *Journal of Engineering, Project, and Production Management* 11, no. 1 (2021; in press).

Moon, J. "Theory and Application of J Charts for Holistic Risk Based Statistical Adverse Event Trending." *International Journal of Health and Economic Development* 4, no. 1 (2018): 9–31.

Mt-Isa, S., C. E. Hallgreen, N. Wang, T. Callréus, G. Genov, I. Hirsch, S. F. Hobbiger, et al. "Balancing Benefit and Risk of Medicines: A Systematic Review and Classification of Available Methodologies." *Pharmacoepidemiology and Drug Safety* 23, no. 7 (2014): 667–678.

Mussen, F., S. Salek, and S. R. Walker. *Benefit-Risk Appraisal of Medicines: A Systematic Approach to Decision-Making*. Chichester, UK: Wiley-Blackwell, 2009.

Myers, J. J. "Risk-Based Decision Making." *Journal of Safety and Security at Sea* 64, no. 1 (2007): 6–10.

Mylotte, J. M. "Analysis of Infection Surveillance Data in a Long-Term Care Facility: Use of Threshold Settings." *Infection Control and Hospital Epidemiology* 17, no. 2 (1996): 101–107.

NASA. *IV&V Management System, Guidelines for Risk Management*. S3001, rev. G. Fairmont, WV: NASA, 2017. https://www.nasa.gov/sites/default/files/atoms/files/s3001_guidelines_for_risk_management_-_ver_g_-_10-25-2017.pdf.

Ni, H., A. Chen, and N. Chen. "Some Extensions on Risk Matrix Approach." *Safety Science* 48, no. 10 (2010): 1269–1278.

Oka, T., H. Matsuda, and Y. Kadono. "Ecological Risk–Benefit Analysis of a Wetland Development Based on Risk Assessment Using 'Expected Loss of Biodiversity.'" *Risk Analysis* 21, no. 6 (2001): 1011–1024.

Ouellet, D. "Benefit–Risk Assessment: The Use of Clinical Utility Index." *Expert Opinion on Drug Safety* 9, no. 2 (2010): 289–300.

Pérez, J. R. *Handbook of Investigation and Effective CAPA Systems*. Milwaukee, WI: ASQ Quality Press.

Pérez, J. R. *Quality Risk Management in the FDA-Regulated Industry*. Milwaukee, WI: ASQ Quality Press, 2012.

Pluchino, A., G. Inturri, A. Rapisarda, A. E. Biondo, R. Le Moli, C. Zappala, N. Giuffrida, G. Russo, and V. Latora. "A Novel Methodology for Epidemic Risk Assessment: The Case of COVID-19 Outbreak in Italy." arXiv preprint arXiv:2004.02739 (2020).

Popov, G., B. K. Lyon, and B. Hollcroft. *Risk Assessment: A Practical Guide to Assessing Operational Risks*. Hoboken, NJ: John Wiley & Sons.

Porter, M. E. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press, 1998 [1985].

Preston, G., J. Moon, R. Simon, S. Allen, and E. Kossi. "The Relevance of Emotional Intelligence in Project Leadership." *Journal of Information Technology and Economic Development* 6, no. 1 (2015): 16.

Pritchard, C. L. *Risk Management: Concepts and Guidance*. Boca Raton, FL: Auerbach Publications.

Project Management Institute. *A Guide to the Project Management Body of Knowledge*. 5th ed. Newtown Square, PA: Project Management Institute, 2013.

Project Management Institute. *Practice Standard for Project Risk Management*. Newtown Square, PA: Project Management Institute, 2009.

Rausand, M. *Risk Assessment: Theory, Methods, and Applications.* Vol. 115. Hoboken, NJ: John Wiley & Sons.

Raz, T., and D. Hillson. "A Comparative Review of Risk Management Standards." *Risk Management* 7, no. 4 (2005): 53–66.

"Regulation (EU) 2017/745 of the European Parliament." EUR-Lex. April 5, 2017. https://eur-lex.europa.eu/eli/reg/2017/745/oj.

Rose, K. H. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. Newtown Square, PA: Project Management Institute, 2013.

Sarac, S. B., C. H. Rasmussen, M. A. Rasmussen, C. E. Hallgreen, T. Søeborg, M. Colding-Jørgensen, P. K. Christensen, S. Thirstrup, and E. Mosekilde. "A Comprehensive Approach to Benefit–Risk Assessment in Drug Development." *Basic & Clinical Pharmacology & Toxicology* 111, no. 1 (2012): 65–72.

Shiroiwa, T., A. Igarashi, T. Fukuda, and S. Ikeda. "WTP for a QALY and Health States: More Money for Severer Health States?" *Cost Effectiveness and Resource Allocation* 11 (2013): https://doi.org/10.1186/1478-7547-11-22.

Sibthorpe, C. "Coronavirus Pandemic: What Does This Mean - and What Happens Next?" *Sky News*, March 12, 2020. https://news.sky.com/story/coronavirus-pandemic-what-does-this-mean-and-what-happens-next-11955553.

Simchi-Levi, D., W. Schmidt, and Y. Wei. "From Superstorms to Factory Fires: Managing Unpredictable Supply Chain Disruptions." *Harvard Business Review* 92, no. 1–2 (2014): 96–101.

Standards Australia. *Risk Management Guidelines - Companion to AS/NZS ISO 31000:2009*. SA/SNZ HB 436:2013. Sydney: Standards Australia, 2013. https://infostore.saiglobal.com/en-us/Standards/SA-SNZ-HB-436-2013-119721_SAIG_AS_AS_250882/.

Tuckman, B. W. "Developmental Sequence in Small Groups." *Psychological Bulletin* 63, no. 6 (1965): 384–399.

University College London. "Irrational Decisions Driven by Emotions." ScienceDaily, August 3, 2006. www.sciencedaily.com/releases/2006/08/060803171138.htm.

U.S. Department of Defense. *Department of Defense Standard Practice: System Safety*. MIL-STD-882E. Washington, DC: U.S. Department of Defense, 2012.

U.S. Department of Energy. *Risk Management Guide*. DOE G 413.3-7. Washington, DC: U.S. Department of Energy. https://www.directives.doe.gov/directives-documents/400-series/0413.3-EGuide-07a.

Van Vreeswijk, M., J. Broersen, and M. Nadort. *The Wiley-Blackwell Handbook of Schema Therapy: Theory, Research, and Practice*. John Wiley & Sons, 2012.

Weber, E. U., A. R. Blais, and N. E. Betz. "A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors." *Journal of Behavioral Decision Making* 15, no. 4 (2002): 263–290.

Wilkinson, L. "Revising the Pareto Chart." *American Statistician* 60, no. 4 (2006): 332–334.

Wood, H. O., and F. Neumann. *Modified Mercalli Intensity Scale of 1931*. Albany, CA: Seismological Society of America, 1931.

Woolhouse, M., F. Scott, Z. Hudson, R. Howey, and M. Chase-Topping. "Human Viruses: Discovery and Emergence." *Philosophical Transactions of the Royal Society B* 367 (2012): 2864–2871.

World Health Organization. *Pandemic Influenza Risk Management: A WHO Guide to Inform and Harmonize National and International Pandemic Preparedness and Response*. Geneva, Switzerland: World Health Organization, 2017.

Yoon, P. D., V. Chalasani, and H. H. Woo. "Use of Clavien-Dindo Classification in Reporting and Grading Complications after Urological Surgical Procedures: Analysis of 2010 to 2012." *Journal of Urology* 190, no. 4 (2013): 1271–1274.

Zadeh, L. A. "Fuzzy Sets." *Information and Control* 8, no. 3 (1965): 338–353.

Zimmer, B. "'Hazard': From Medieval Dice to the Risks Faced by Frontline Workers." *Wall Street Journal*, May 14, 2020. https://www.wsj.com/articles/hazard-from-medieval-dice-to-the-risks-faced-by-frontline-workers-11589481761.

Zsidisin, G. A., L. M. Ellram, J. R. Carter, and J. L. Cavinato. "An Analysis of Supply Risk Assessment Techniques." *International Journal of Physical Distribution & Logistics Management* 34, no. 5 (2004): 397–413.

The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Index

Note: Page numbers followed by *f* or *t* refer to figures or tables, respectively.

A

accountability of stakeholders, 43. *See also* RACI matrix
advanced risk tools. *See also specific tools*
  Failure Modes and Effects Analysis, 242–260
  fault tree analysis, 292–297
  hazard analysis, 261–269
  hazard analysis and critical control points, 280–291
  hazard and operability study, 270–279
  Monte Carlo analysis, 298–306
aerospace and aviation industry, organizational context for, 64–65
affect heuristic, 223
aggregate risk
  definition of, 29
  enterprise risk management of, 2, 3
  monitoring and reviewing, 168
  risk appetite for, 69
  risk-based thinking on, 15
  risk identification and analysis of, 29, 30*f*
  risk management planning for determination of, 81
AI (artificial intelligence), xxvi, 239
AIAG (Automotive Industry Action Group) risk matrix, 130, 133*t,* 135, 136*t*
ambiguity, as risk source, 53
American Society for Quality (ASQ)
  on control charts, 179–180
  on histograms, 177
  quality, defined, 5
analogous estimating of probability, 60
anchoring and adjustment heuristic, 60, 222
ANSI/ASIS/RIMS RA.1-2015
  risk drivers and sources defined in, 48
ANSI Z590.3-2011
  risk-based design thinking in, 227–228, 229, 231
  risk matrix in, 145, 146*t*
area charts, 183, 185*f*
artificial intelligence (AI), xxvi, 239
ASQ. *See* American Society for Quality
assumptions and constraints analysis, 96, 98*f*
auditing, risk-based. *See* risk-based auditing
automotive industry
  HAZOP for, 277, 278*t,* 279, 279*f*
  inherent risk in, 159–160
  risk analysis in, 126
  risk management failures in, xxi
  risk matrix for, 130, 133*t,* 135, 136*t*
  risk modification in, 150–151
  SWIFT process applied to, 97*f*
Automotive Industry Action Group (AIAG) risk matrix, 130, 133*t,* 135, 136*t*
availability heuristic, 222
Aven, T., 17

B

banking and financial services industry
  hazards and hazardous situations in, 108, 108*f*
  Monte Carlo analysis in, 298
  positive and negative risk consequences in, 10–11, 108*f*
  risk-benefit analysis in, 206–208, 208*f*
  risk management failures in, xxi
  root cause analysis of mortgage crisis in, 122*f*
bar graphs, 175, 176*f,* 186, 186*f*. *See also* histograms
baselines, in trend analysis, 193
Bayesian approach to probability, 58
benchmarking
  of organizational context, 65
  for pandemic and epidemic risk management, 311
  for risk monitoring and review, 168
benefits. *See also* opportunities
  definition of, 105
  from hazards and hazardous situations, 105, 107–108, 107*f*–108*f,* 110*f*
  risk-benefit analysis of, 46, 46*t,* 108, 129–130, 132*t,* 206–221, 266
Betz, N. E., 225
black swan events, 24, 307–308
Blais, A. R., 225
Boniface, Duane, 58
bounded rationality, 222
bow tie analysis, 114–116, 115*f*–117*f*
brainstorming
  for hazard identification, 262, 281–282
  for opportunities, 152
  for risk identification, 56, 88
  in risk process facilitation, 87, 88
  in root cause analysis, 120
bubble charts
  for risk monitoring and review, 187, 188*f*–189*f,* 188*t*
  for supplier risk representation, 236, 236*f*
budgets, planning, 80–81

C

Campbell, A., 223, 224
causal chain, 61–62, 62*f,* 117, 118*f*
causal nexus, 61, 117
causal probability tree, 61*f*
cause and consequence analysis (CCA), 117, 118*f*
cause and effect analysis. *See also* root cause analysis
  cause and consequence analysis as, 117, 118*f*
  consequence analysis using, 109–124, 110*f*
  FMEA including, 243–245, 243*f*–246*f,* 252, 253*t*–254*t*
  for probability, 61–62, 61*f*–62*f*
  in risk identification, 52, 52*t*
CCA (cause and consequence analysis), 117, 118*f*
CEA (cost effectiveness analysis), 218–221, 218*f,* 219*t,* 220*f*
Centers for Disease Control and Prevention (CDC), 319
chance and possibilities. *See* probability
change management, xxiii, xxvi–xxvii. *See also* risk modification
check sheets/checklists
  in HACCP, 284
  in hazard identification, 261
  risk identification from, 53
  in root cause analysis, 121
Chuang-Stein, C., 210
Clavien-Dindo scale, 129–130, 132*t,* 213, 214*t,* 215–217, 216*f,* 217*t*
cognitive science of risk-based decision making, 222–226
  cognitive bias in, 223, 224, 324
  emotional intelligence in, 224–226, 225*f*
  emotional tagging in, 223, 224
  failed perceptions and, xxii
  heuristics in, 222–223, 224, 324
  in pandemics and epidemics, 324
competition
  benchmarking to, 65, 168, 311
  in organizational context, 64–65
complexity, as risk source, 53
Comprehensive Risk Management Maturity (CoRMM) Model, 75–78
  levels of maturity in, 75, 78
  parameters assessed in, 75, 76*t*–77*t*
  risk management planning informed by, 79
confirmation bias, 223
consequence analysis, 109–124
  bow tie analysis for, 114–116, 115*f*–117*f*
  cause and consequence analysis for, 117, 118*f*
  cause and effect analysis in, 109–124, 110*f*
  consequence polygon for, 33*f,* 35
  decision tree analysis for, 111–112, 112*f*–113*f*
  definition of, 35, 109
  event tree analysis for, 112–114, 114*f*–115*f*
  fault tree analysis for, 110–111, 111*f*
  hazards and hazardous situations in, 109, 110*f,* 114–116, 115*f*–117*f,* 122–124, 123*f,* 124*t*
  HAZOP including, 272
  preliminary hazard analysis for, 122–124, 123*f,* 124*t*
  probability in, 109, 112, 113*f,* 114, 115*f,* 117
  risk analysis including, 109, 110*f,* 125–126, 126*f*
  in risk-based thinking, 15
  root cause analysis for, 119–122, 120*f*–122*f*
  scenario analysis for, 118–119, 119*f*
  severity in, 109
  of two consequences, 33, 34*t*
consequences
  consequence analysis (*See* consequence analysis)
  definition of, 15, 31, 128
  events and (*See* events and consequences)
  failure effect as, 243–246, 244*f*–246*f,* 247*t,* 249, 252–253, 253*t*–254*t*
  hazards defined in relation to, 48–49
  positive vs. negative, 10–12, 23, 33, 44–45, 52, 152–156 (*See also* harm; opportunities)
  risk-based thinking on, 15
  severity based on, 31–33, 32*t*–33*t* (*See also* severity)
consequence-time series charts
  for aggregate risk, 29, 30*f*
  of risk after risk modification, 39*f*
constituent risk factors, 66, 67
consultation with stakeholders, 43. *See also* RACI matrix
context
  organizational (*See* organizational context)
  for pandemic and epidemic risk management, 308–309, 308*f*
contingency planning
  for risk monitoring and review, 168
  for risk response planning, 160, 162
  for supplier risk oversight, 233
continual improvement, xxiii, 190–191
control charts
  control limits in, 197
  criteria for valid, 196
  elements of, 196–197, 196*f*–197*f*
  for risk monitoring and review, 178–180, 180*f*
  for trend analysis, 190–191, 194–201, 195*f*–197*f,* 199*f*
  types of, 196
CoRMM model. *See* Comprehensive Risk Management Maturity (CoRMM) Model
coronavirus. *See* COVID-19
cost effectiveness analysis (CEA), 218–221, 218*f,* 219*t,* 220*f*
COVID-19 (coronavirus-2019)
  growth from change due to, xxvi–xxvii
  healthcare risk management failures and, xxi
  Monte Carlo analysis of, 301–306, 303*f*–305*f,* 315–317, 316*f*–317*f*
  risk evaluation of, 311, 312*t*
  risk monitoring of, 319–323, 320*f*–323*f*
  as white vs. black swan event, 307–308
  zoonotic spillover of, 307
Crichton, David, 312

critical control points, 282, 283*f,* 285*t,* 288*t*. *See also* hazard analysis and critical control points
critical limits, in HACCP, 282–283
Crouch, E. A., 208–209
Cuomo, Andrew, xxvi–xxvii
cut sets, in FTA, 294–295, 297*f*

D

DALYs (disability adjusted life years), 218–220, 219*t*
data analysis
  baselines from historical, 193
  flowcharts for, 121
  of Industry 4.0 risk, xxv–xxvi, 239–241, 240*f*–241*f*
  in organizational context, 47
  in pandemic and epidemic risk management, 311
  probability (*See* probability)
  risk identification from, 47
  risk management harmonization with, xxv–xxvi
  risk management planning for, 79
  in root cause analysis, 121
  stratification in, 194, 195*f*
decision making. *See* risk-based decision making
decision tree analysis
  for consequence analysis, 111–112, 112*f*–113*f*
  for HACCP critical points determination, 283*f*
deductive reasoning, 87, 88
Delphi technique, 56, 88
Deming, W. E., 190
design Failure Modes and Effects Analysis (DFMEA), 248, 249, 250*t,* 257
design risk
  FMEA evaluation of, 229, 247, 248, 249, 250*t,* 257
  HAZOP evaluation of, 229, 271–272
  monitoring and review of, 229
  risk-based design thinking, 227–231
  Risk Breakdown Structure for, 94*t*
  risk mitigation by design, 7, 227–231, 229*t,* 230*f*–231*f*
detection, pandemic, 311
DFMEA (design Failure Modes and Effects Analysis), 248, 249, 250*t,* 257
disability adjusted life years (DALYs), 218–220, 219*t*
disaster management
  hazards in, 51
  risk matrix for, 128–129, 129*f*–130*f*
DMAIC approach to trend analysis, 191–194, 193*f*–194*f*
documents. *See* information; reporting; risk repository
Dodson, James, 14
dotplots, 181, 181*f*
Dutch Council for Public Health and Care, 220–221

E

Ebola, 307, 312*t*
emotional intelligence, 224–226, 225*f*
emotional tagging, 223, 224
enterprise risk management
  definition of, 1
  in hierarchical risk management, 2–4, 3*f*
  leadership support for, 4, 20
  as pillar of risk management, 1, 2*f*
  supplier risk oversight in, 236
epidemic risk management. *See* pandemic and epidemic risk management
escalation of commitment, 222
ETA (event tree analysis), 112–114, 114*f*–115*f*
events and consequences, 31–35. *See also* consequences
  basic, intermediate, and top events, in FTA, 292
  basic events, 110, 111*f,* 292
  black swan events, 24, 307–308
  consequence, defined, 15, 31, 128
  consequence analysis of, 33–35, 33*f,* 34*t* (*See also* consequence analysis)
  event, defined, 31, 45
  normal events, 110, 111*f*
  probability of (*See* probability)
  severity of, 25, 27*t*–28*t,* 31–33, 32*t*–33*t* (*See also* severity)
  trigger conditions for (*See* trigger conditions)
  white swan events, 307
event tree analysis (ETA), 112–114, 114*f*–115*f*
expected monetary value analysis, 46, 46*t*
expert opinions. *See also* subject matter experts
  HACCP critical limits set by, 283
  probability based on, 59–60, 59*t,* 61, 246
  for risk identification brainstorming, 56

F

facilitation. *See* risk process facilitation
Failure Modes and Effects Analysis (FMEA), 242–260
  acceptability criteria in, 255
  action results from, 255
  action taken from, 255
  advantages and disadvantages of, 256
  cause and effect analysis in, 243–245, 243*f*–246*f,* 252, 253*t*–254*t*
  current control in, 255
  data gathering in, 248
  definition of, 242
  design risk evaluation in, 229, 247, 248, 249, 250*t,* 257
  detection table in, 253, 255*t*
  failure, defined for, 242
  failure effect in, 243–246, 244*f*–246*f,* 247*t,* 249, 252–253, 253*t*–254*t*
  failure mode in, 52, 243–246, 244*f*–246*f,* 249, 252, 252*t,* 254*t*
  hierarchy of elements studied in, 251, 251*f*
  item function identified in, 251, 252*t*
  J charts comparison, 186
  monitoring of, 255
  probability in, 245–247, 246*f,* 246*t,* 253, 254*t*
  process and stages of, 247–248, 247*f,* 249*f,* 257, 258*f*–259*f,* 260
  purpose of, 248
  recommended action in, 255

risk matrix for, 130, 133*t,* 136*t*
for risk modification, 242
risk priority numbers in, 247, 255
risk process facilitation using, 87
risk repository in, 91
root cause analysis in, 244, 244*f*–245*f*
scope of, 248
severity in, 246–247, 248*t,* 249, 253, 254*t*
stakeholders in, 248
structured what-if technique in, 94
of system inputs and outputs, 242, 243*f*
system/subsystem/component studied in, 251, 251*f,* 252*t*–254*f*
types of, 248, 249, 257, 258*f*–259*f,* 260
worksheets for, 250*t,* 251–256, 256*t*
Failure Modes and Effects Criticality Analysis (FMECA), 186, 246
familiarity heuristic, 223
fault tree analysis (FTA), 292–297
advantages and disadvantages of, 295, 297
basic level events in, 292
as consequence analysis, 110–111, 111*f*
cut sets in, 294–295, 297*f*
definition of, 292
intermediate events in, 292
process of, 292, 293*f*
risk analysis using, 294–295, 296*f*–297*f*
symbols in, 293*t*–294*t,* 295*f*
top events in, 292
Fermat, Pierre de, 13–14
financial resources. *See also* profits
budgets detailing, 80–81
cost effectiveness analysis of, 218–221, 218*f,* 219*t,* 220*f*
hazard risks in relation to, 4
risk management planning for, 79, 80–81, 323
financial sector. *See* banking and financial services industry
Finkelstein, S., 223, 224
fishbone diagrams, 87, 120, 121, 121*f*
5 Whys, 120, 121–122, 122*f,* 272
flowcharts
for data analysis, 121
for FMEA process, 249*f,* 258*f*–259*f*
in HACCP, 280, 282, 284, 286*f*
for HAZOP process, 277*f*
for opportunities assessment, 153, 154*f*–155*f,* 156
for risk modification, 153, 154*f*–155*f,* 156
for risk response planning, 161*f*
FMEA. *See* Failure Modes and Effects Analysis
FMECA (Failure Modes and Effects Criticality Analysis), 186, 246
Food and Drug Administration, U.S., 64, 283
food industry
HACCP in, 280, 283, 286*f,* 286*t*–290*t,* 291
organizational context for, 64
risk management failures in, xxi
Ford, 150–151
frequentish approach to probability, 57–58, 58*t*
FTA. *See* fault tree analysis

G

gap analysis, 79
governance. *See* risk governance
graphical tools, 172–186. *See also specific tools below*
area charts, 183, 185*f*
bar graphs, 175, 176*f,* 186, 186*f*
bubble charts, 187, 188*f*–189*f,* 188*t*
control charts, 178–180, 180*f*
dotplots, 181, 181*f*
histograms, 176*f,* 177
individual value plots, 182, 182*f*
J charts, 183, 185*f*–186*f,* 186, 321, 321*f*
line charts, 177
Pareto charts, 172, 173*f*–174*f*
pie charts, 180, 181*f*
radar charts, 182, 183*f*–184*f*
run charts, 178, 179*f*
scatter plots, 172–174, 174*f*–175*f*
time-series charts, 177–178, 177*f*–178*f*
guide words, in HAZOP, 270, 273–274, 274*t*–275*t*

H

H1N1, 307
H7N9, 312*t*
HACCP. *See* hazard analysis and critical control points
harm. *See also* hazards and hazardous situations; threats
definition of, 104
from hazards and hazardous situations, 104–105, 105*f*–106*f,* 106*t,* 107–108, 108*f,* 110*f,* 123*f,* 124, 124*t,* 261, 262*f,* 264–265, 264*f*–266*f*
hazards defined in relation to, 49
organizational context for, 52
probability of (*See* probability)
risk-benefit analysis of, 108, 213–215, 214*t,* 217
risk defined in relation to, 261
risk identification and analysis of, 25, 28, 50–52, 264
severity of (*See* severity)
hazard analysis, 261–269. *See also* hazard analysis and critical control points
cause identification in, 266
definition of, 261
harm identification in, 264
harm occurrence estimation in, 264–265, 264*f*–266*f*
hazard identification in, 261–262
hazardous situation identification in, 264
preliminary hazard analysis, 122–124, 123*f,* 124*t*
probability in, 261, 262*f,* 264, 264*f*–266*f*
process of, 261–269, 263*f*
risk-benefit analysis in, 266
risk calculation in, 265
risk control implementation in, 266, 269
scoring system selection in, 265
sequence of events identification in, 262
severity of harm estimation in, 265
worksheets for, sample, 267*t*–268*t*

hazard analysis and critical control points (HACCP), 280–291
corrective actions in, 284
critical control points determination in, 282, 283*f,* 285*t,* 288*t*
critical limits determination in, 282–283
definition of, 280
design risk evaluation in, 229
documentation procedures in, 284–285
example of, 285, 286*f,* 286*t*–290*t,* 291
hazard identification and evaluation in, 280–282, 285*t,* 286*f,* 286*t*–287*t*
monitoring procedures in, 283–284
principles of, 281–285, 281*f,* 285*t*
process of, 281*f,* 280
risk repository in, 91
structured what-if technique in, 94
team conducting, 280, 281, 285
verification procedures in, 284
worksheets for, 285*t,* 289*t*–290*t*
hazard and operability study (HAZOP), 270–279
advantages and disadvantages of, 279
consequence analysis in, 272
definition of, 270
definition phase of, 272
design intent interpretation for, 271–272
design risk evaluation in, 229, 271–272
deviation of output in, 270–271, 271*f,* 274*t*–275*t*
documentation phase of, 274, 276
examination phase of, 273–274, 276*f*
example of, 277, 278*t,* 279, 279*f*
guide words in, 270, 273–274, 274*t*–275*t*
preparation phase of, 273
process and phases of, 272–276, 273*f,* 274*t*–275*t,* 276*f*–277*f*
risk repository in, 91
root cause analysis in, 272
structured what-if technique in, 94
study nodes in, 270–271, 271*f*
team performing, 272
worksheets for, 270, 276, 278*t*
hazard log. *See* risk repository
hazards and hazardous situations, 103–108. *See also* harm; threats
benefits or opportunities from, 105, 107–108, 107*f*–108*f,* 110*f*
bow tie analysis of, 114–116, 115*f*–117*f*
consequence analysis consideration of, 109, 110*f,* 114–116, 115*f*–117*f,* 122–124, 123*f,* 124*t*
definition of, 48–49, 103–105, 107, 261
harm from, 104–105, 105*f*–106*f,* 106*t,* 107–108, 108*f,* 110*f,* 123*f,* 124, 124*t,* 261, 262*f,* 264–265, 264*f*–266*f*
hazard analysis, 122–124, 261–269
hazard analysis and critical control points, 91, 94, 229, 280–291
hazard and operability study, 91, 94, 229, 270–279
hazard risk management of, 3*f,* 4
hazard sources, 48–51, 49*f*–50*f*
in hierarchical risk management, 3*f,* 4
organizational context for, 108
in pandemic and epidemic risk management, 312, 313*f*
process approach anticipating, 6, 8*f*–9*f*
risk analysis of, 126–127, 127*f*
risk identification including, 48–51, 49*f*–50*f,* 261–262, 264, 281–282, 285*t*
risk management planning for categorization of, 80
sequence of events between, 105, 106*f*–108*f,* 106*t,* 107–108, 115, 123*f,* 124, 124*t,* 126, 262, 266*f*
HAZOP. *See* hazard and operability study
healthcare industry. *See also* medical device industry; pandemic and epidemic risk management; pharmaceutical industry
cost effectiveness analysis in, 218–221, 218*f,* 219*t,* 220*f*
FMEA for, 245, 245*f*
inherent risk in, 160
risk analysis in, 126
risk management failures in, xxi
risk matrix for, 129–130, 132*t,* 146*t*
risk monitoring and review in, 170, 177, 186, 186*f*
subject matter experts in, 61
trend analysis in, 190
heuristics
affect heuristic, 223
anchoring and adjustment heuristic, 60, 222
availability heuristic, 222
definition of, 222
escalation of commitment, 222
familiarity heuristic, 223
representativeness heuristic, 223
in risk-based decision making, 222–223, 224, 324
hierarchical risk management, 2–4, 3*f*
hierarchy of control, 229, 231, 231*f*
Hillson, David, 47, 85–86, 92
histograms, 177, 176*f*
HIV, 307
holistic risk management, xxiii, 4, 101
House of Quality, 228

I

IAEA (International Atomic Energy Association) hazardous situations guidance, 103
ICER (incremental cost effectiveness ratio), 218–220, 219*t,* 220*f*
IEC 60812:2006
failure definition in, 242
IEC 60812:2008
failure effect definition in, 243
IEC 61025:2006
top event definition in, 292
IEC 61882:2016
guide words in, 273, 275*t*
HAZOP phases in, 272–276, 273*f,* 275*t,* 277*f*
impact. *See* severity
inclusivity, xxv, 77*t,* 314
incremental cost effectiveness ratio (ICER), 218–220, 219*t,* 220*f*

independent reviewers, in risk process facilitation, 83, 86–87, 88
individual value plots, 182, 182*f*
inductive reasoning, 87, 88
Industry 4.0 risk, xxv–xxvi, 239–241, 240*f*–241*f*
influence-engagement matrix, 41–42, 42*f*–43*f*
influenza, 307, 312*t,* 322*f*
information
  for hazard identification, 262
  pandemic and epidemic risk management of, 309, 310, 314–315
  for risk identification and analysis, 56, 87, 262
  risk repository of, 90–91
  to stakeholders, 28–29, 43, 52, 148 (*See also* RACI matrix)
  tangible vs. intangible sources of, 72
inherent risk, 159–160, 160*f*
insurance industry
  hazard risks in, 4
  Industry 4.0 risk management in, 241
  probability in, 14–15
International Atomic Energy Association (IAEA) hazardous situations guidance, 103
interviews, 56, 121
Ishikawa diagrams, 87, 120, 121, 121*f*
ISO 51:2014
  hazards and hazardous situations in, 103–104
ISO 63:2019
  risk definition in, 25, 28
ISO 73:2009
  organizational context in, 64, 65
  risk tolerance in, 69
ISO 9000:2015
  risk definition and description in, 44
ISO 9001:2015, 20–23
  on opportunities, 23, 44–45
  quality management standards in, 20
  on risk-based thinking, 7, 20
  risk definition and description in, 11, 44–45
  risk management standards in, 20–23, 22*t,* 23*f*
ISO 12100:2010
  hazards and hazardous situations in, 49–50, 103–104
ISO 13485:2016
  risk definition and description in, 11, 44–45
ISO 14971:2007
  risk matrix in, 28, 129, 131*t,* 135, 135*t,* 144*t*–145*t*
ISO 14971:2019
  hazards and hazardous situations in, 103, 261, 264–265, 266*f*
  risk definition and description in, 11
ISO 19011:2018
  risk-based auditing in, 202, 203, 204
ISO 22000:2018
  HACCP critical limits in, 282
  HACCP monitoring procedures in, 284
ISO 31000:2018
  consequence definition in, 31
  event definition in, 31
  organizational context in, 65
  pandemic and epidemic risk management based on, 309, 314
  risk analysis in, 125
  risk assessment process in, 100, 101*f*
  risk definition and description in, xxiv–xxv, 10–11, 44–45
  risk evaluation in, 140
  risk identification in, 92, 99
  risk management framework in, xxii, xxiii, 309
  risk monitoring and review in, 164
  risk sources in, 48, 53
  stakeholder definition in, 40
ISO 31010:2018
  criteria for risk monitoring and review in, 66
ISO 31010:2019
  bow tie diagram in, 116
  risk matrix in, 142–143, 145*t*

J

J charts, 183, 185*f*–186*f,* 186, 321, 321*f*

K

key performance indicators (KPIs), 164–165, 205
key risk indicators (KRIs)
  definition of, 163–164
  monitoring and reviewing, 163–167, 165*f,* 168, 169, 177, 179
  in pandemic and epidemic risk management, 319, 321
  supplier risk oversight based on, 234–236, 234*f*–235*f*
  trend analysis of, 168, 177, 179, 190, 194, 200*f*
  trigger conditions for, 169
key stakeholders, xxv, 41
knowledge, skills, and abilities (KSAs)
  CoRMM Model assessment of, 76*t*
  expert (*See* expert opinions; subject matter experts)
  for risk management process, xxv
  for risk process facilitation, 84
Kørte, J., 17
Kraljic, Peter, 232, 236
Kraljic matrix, 232–234, 233*f*

L

leadership
  audit, 203
  CoRMM Model assessment of, 76*t*
  enterprise risk management support from, 4, 20
  ISO 9001 standards for, 20, 21, 22*t*
  in organizational context, 65
  risk acceptance by, 150
  risk attitude of, 68, 70, 223, 226
  risk-based decision making by (*See* risk-based decision making)
  risk culture reflecting, 68, 70, 223, 226

life-cycle risk management
FMEAs in, 247–248
risk monitoring and review in, 65, 163, 168
risk process facilitation using, 87–88, 89
supplier risk oversight as, 233
likelihood analysis, 63, 125, 132. *See also* probability
line charts, 177. *See also* run charts; time-series charts
literature reviews, for hazard identification, 262
logarithmic scales, 320–321
loss aversion bias, 223

M

machine learning, 239
magnitude of consequences. *See* severity
management team. *See* leadership
Marburg filovirus, 307
MAUDE (U.S. Manufacturer and User Facility Device) database, 87
maximum drawdown (MDD), 207
medical device industry
hazard analysis for, 268*t*
hazards in, 51, 268*t*
opportunities in, 154*f*–155*f,* 156
organizational context for, 64
positive and negative risk consequences in, 11, 52
residual risk in, 159
risk analysis in, 126
risk-benefit analysis in, 213
Risk Breakdown Structure applied to, 93*t*–94*t*
risk defined for, 44, 45
risk management failures in, xxi
risk matrix for, 28, 129, 131*t,* 135, 135*t,* 143, 144*t*–145*t*
risk modification in, 154*f*–155*f,* 156
trend analysis in, 191, 197–201, 198*t,* 199*f*–201*f*
Mendelow's matrix, 41
Middle East respiratory syndrome (MERS-CoV), 307, 312*t*
MIL-STD-882
preliminary hazard analysis in, 124
risk matrix in, 131, 133*t,* 143, 146*t*
mining industry risk-benefit analysis, 208–209
modification of risk. *See* risk modification
Mohberg, N. R., 210
monitoring and reviewing risk. *See* risk monitoring and review
Monte Carlo analysis, 298–306
adjusting parameters in, 304–306, 305*f*
advantages and disadvantages of, 306
COVID-19 example of, 301–306, 303*f*–305*f,* 315–317, 316*f*–317*f*
defining model for, 303, 303*f,* 315, 316*f*
definition of, 298
input and output variables in, 302
intermediate and final outputs from, 302–303
limiting values assigned in, 303, 303*f,* 316*f*
probability distributions in, 298–301, 300*f*–301*f,* 302, 303
process of, 299*f,* 302–306
for quantitative probability, 60–61, 302, 305
random sampling in, 298, 300
running simulation of, 303–304, 304*f,* 315–317, 316*f*–317*f*
sensitivity analysis in, 304–305, 305*f*
Myers, Joseph J., 16

N

NASA
HACCP developed by, 280
risk matrix, 131, 134*t*
National Center for Health Statistics, 321
National Institute for Health and Care Excellence (NICE), 219, 220

O

objectives
risk-based auditing prioritizing, 202–203
risk evaluation of significance to, 140
risk management to achieve, 10–11, 11*f,* 47
risk modification to achieve, 149
observations, in root cause analysis, 121
operational risk management
definition of, 1
in hierarchical risk management, 3*f,* 4
organizational context for, 72
as pillar of risk management, 1, 2*f*
opportunities, 44–46. *See also* benefits
flowcharts for assessing, 153, 154*f*–155*f,* 156
from hazards and hazardous situations, 105, 107–108, 107*f*–108*f,* 110*f*
Industry 4.0 risk and, 241
ISO 9001 on, 23, 44–45
organizational context for, 72
probability for, 45–46, 46*t*
risk attitude and appetite for seeking, 69–70
risk-based auditing evaluating, 202–203, 204–205, 205*f*
in risk-based decision making, 18–19, 18*f*
risk-based design thinking on, 228
risk-benefit analysis of, 46, 46*t,* 108, 208
risk defined in relation to, 44–45
risk identification of, 51–52
risk modification for, 150–156, 152*f,* 153*t,* 154*f*–155*f*
SWOT analysis of, 98–99, 99*f*
organizational business model, 72
organizational context, 64–67, 71–74. *See also specific industries*
benchmarking of, 65
competition in, 64–65
data analysis in, 47
establishing of, 64
external context, 64–65
hazards and hazardous situations in, 108
hierarchical risk management in, 2–4, 3*f*
internal context, 65–67

organizational business model and, 72
organizational culture in, 72–73 (*See also* risk culture)
pandemic and epidemic preparedness in, 323–324
regulatory influences in, 64
risk-based auditing in, 202–203
risk-based decision making in, 71
risk-based design thinking in, 228
risk definition specific to, 45
risk evaluation specific to, 140–141
risk governance in, 2, 65, 71–73
risk management framework in, 65
risk management planning informed by, 79
risk matrix appropriate for, 128–132, 129*f*–131*f,* 131*t*–136*t,* 135
risk monitoring and review in, 65–67, 165–166
stakeholders considered in, 65
value chains in, 73–74
organizational culture, 72–73. *See also* risk culture
organizational leaders. *See* leadership
overconfidence bias, 223

P

pandemic and epidemic risk management, 307–324
black vs. white swan events and, 307–308
business preparedness for, 323–324
communication and information management in, 309, 310, 314–315
context for, 308–309, 308*f*
COVID-19 (*See* COVID-19)
customized approach to, 314
data analysis in, 311
detection or testing protocols in, 311
dynamic approach to, 314
epidemic and pandemic, defined for, 308
example of, 319–323, 320*f*–323*f*
failures in, xxi
growth from change in, xxvi–xxvii
hazards in, 312, 313*f*
inclusivity in, 314
Monte Carlo analysis for, 301–306, 303*f*–305*f,* 315–317, 316*f*–317*f*
probability or occurrence in, 310–311, 312, 313*f,* 315–317, 316*f*–317*f*
quantitative approach to, 315–317, 316*f*–317*f,* 318*t*–319*t*
risk analysis in, 310–311
risk assessment for, 309–317, 309*f,* 312*t,* 316*f*–317*f,* 318*t*–319*t*
risk evaluation in, 311, 312*t*
risk identification in, 309–310
risk mitigation in, 311, 317, 320*f*
risk monitoring and review in, 317, 319–323, 320*f*–323*f*
risk perception in, 324
risk response planning in, xxiv, 323–324
risk triangle/rhomboid in, 312, 313*f*
severity or virulence determination in, 310–311, 312, 313*f*
structured and comprehensive approach to, 314
viral exposure evaluation for, 317
zoonotic spillover in, 307
parametric analysis for probability, 60
Pareto charts, 172, 173*f*–174*f*
Patient Protection and Affordable Care Act (2010), 221
PDCA (Plan-Do-Check-Act) cycle, 5–7, 6*f,* 8*f*–9*f,* 9
pervasiveness, xxv, 77*t*. *See also* severity
PFMEA (process Failure Modes and Effects Analysis), 248, 249, 257, 259*f,* 260
PHA (preliminary hazard analysis), 122–124, 123*f,* 124*t*
pharmaceutical industry
organizational context for, 64
risk-benefit analysis in, 209–217, 210*t*–215*t,* 216*f,* 217*t*
supplier risk oversight in, 236
trend analysis regulations in, 191
pictograms, in root cause analysis, 121
pie charts, 180, 181*f*
Plan-Do-Check-Act (PDCA) cycle, 5–7, 6*f,* 8*f*–9*f,* 9
planning
contingency planning, 160, 162, 168, 233
planning fallacy, 223
quality planning, 5, 6*f,* 82
risk management planning, 7, 9*f,* 79–82, 142, 233, 323–324
risk response planning, xxiv, 72, 157–162, 190, 204, 323–324
Pluchino, A., 312
policies and procedures
for pandemic and epidemic risk management, 309
for risk governance, 2
risk identification from standard, 53
Porter, Michael, 73
preemptive thinking, 16
preliminary hazard analysis (PHA), 122–124, 123*f,* 124*t*
preventive thinking
FMEA as tool for, 242
risk-based decision making based on, 17
risk-based design thinking as, 227–228, 231
risk-based thinking as, 15
proactive risk-based thinking, xxii
probability, 57–63
analogous estimating of, 60
Bayesian approach to, 58
causal probability chain on, 61–62, 62*f*
causal probability tree on, 61*f*
cause and effect analysis for, 61–62, 61*f*–62*f*
classical approach to, 57, 58*t*
consequence analysis using, 109, 112, 113*f,* 114, 115*f,* 117
definition of, 13, 57, 128
expert opinion informing, 59–60, 59*t,* 61, 246
in fault tree analysis, 292, 294
in FMEA, 245–247, 246*f,* 246*t,* 253, 254*t*
frequentish approach to, 57–58, 58*t*
in hazard analysis, 261, 262*f,* 264, 264*f*–266*f*
in impact-probability bubble charts, 187, 188*f*–189*f,* 188*t*

likelihood analysis or probability estimation, 63, 125, 132
Monte Carlo analysis of, 60–61, 298–306, 315–317
for opportunities, 45–46, 46*t*
in pandemic and epidemic risk management, 310–311, 312, 313*f,* 315–317, 316*f*–317*f*
parametric analysis for, 60
probabilistic analysis for, 60, 61*f*
probability distributions, 298–301, 300*f*–301*f,* 302, 303
probability theory on, 60
qualitative probability, 59, 59*t*
quantitative probability, 60–61, 302, 305
risk-based thinking on, 13–15, 14*f*–15*f*
in risk-benefit analysis, 214*t*–215*t,* 214–217
risk identification and analysis of, 24–25, 25*t*–26*t,* 125–126, 126*f,* 310
risk management planning for definition of, 80
risk matrix based on, 128, 129*f,* 132, 135–137, 135*f,* 135*t*–137*t,* 137*f*–138*f,* 139, 140–143, 141*t*–146*t,* 147, 147*t*
risk modification altering, 38*t,* 149, 150–152, 153*t*
risk probability numbers, 67, 141–142, 142*t,* 187, 188*t*
semiquantitative probability, 59–60, 59*t*
subjective approach to, 58, 58*t,* 62
trend analysis of, 199–200, 201*f*
process approach
definition of, 6
to quality risk management, 6–9, 7*f*–9*f*
to risk-based decision making, 16
in risk process facilitation, 83–89, 96
process Failure Modes and Effects Analysis (PFMEA), 248, 249, 257, 259*f,* 260
product-, process-, or service-level risk management
definition of, 1
FMEAs in, 248–249, 257, 259*f,* 260
in hierarchical risk management, 3*f,* 4
life cycle management, 87–88
as pillar of risk management, 1, 2*f*
profits
benefits defined in relation to, 105
probability estimation increasing, 14
risk management benefits to, xxv
risk modification affecting, 150–151
supplier risk oversight based on, 232–233
Pugh matrix, 228

Q

quality
continual improvement of, xxiii, 190–191
definition of, 5
House of Quality, 228
ISO 9001 standards for, 20
PDCA cycle on, 5–7, 6*f,* 8*f*–9*f,* 9
process approach to, 6–9, 7*f*–9*f*
quality assurance, 5, 6*f*
quality control, 5, 6*f*
quality improvement, 5, 6*f* (*See also* continual improvement)
quality planning, 5, 6*f,* 82
risk management and, xxvi, 5–9, 82 (*See also* risk management)
supplier risk management of, 234, 234*f*
quality adjusted life years (QALYs), 218–221, 218*f,* 219*t*
questionnaires
for hazard identification, 262
for risk identification, 56

R

R_1 charts, 322, 323*f*
RACI (responsible, accountable, consulted, and informed) matrix, 42–43, 43*t,* 80, 89
radar charts, 182, 183*f*–184*f*
ranking of risk, 66. *See also* risk priority numbers
RBS (Risk Breakdown Structure), 92–94, 93*t*–94*t*
RCA. *See* root cause analysis
regulations
FMEA use to meet, 248
HACCP critical limits set in, 282
hazard identification by reviewing, 262
organizational context influenced by, 64
risk acceptability criteria in, 141
trend analysis under, 191
reporting
HACCP, 284–285
HAZOP, 274, 276
risk management planning for, 81
on risk monitoring and review, 170
risk repository for reports, 90–91
representativeness heuristic, 223
residual risk, 158–159, 159*f*–160*f,* 229
responsibility of stakeholders, 42–43, 80
responsible, accountable, consulted, and informed (RACI) matrix, 42–43, 43*t,* 80, 89
risk
definition and description of, xxiv–xxv, 10–12, 24–25, 25*t,* 28, 44–45, 45*t,* 47, 104, 214–215, 261
etymological roots of, xxiv
risk acceptability
active acceptance, 150
criteria for, 67, 140–141, 142*t*–143*t,* 148, 255
passive acceptance, 149
risk attitude, appetite, and tolerance for, 40, 67, 68–70, 70*t,* 73, 81, 87, 140–141, 142*t,* 143, 148, 223, 225–226, 225*f*
risk culture reflecting (*See* risk culture)
risk evaluation of (*See* risk evaluation)
risk management planning for, 79, 80
risk modification not needed with, 149–150, 150*f,* 152*f*
scoring criteria based on, 67
risk analysis, 24–30, 125–127
of aggregate risk, 29, 30*f*
basic, 24–30
consequence analysis in, 109, 110*f,* 125–126, 126*f* (*See also* consequence analysis)

definition of, 30, 100
fault tree analysis for, 294–295, 296*f*–297*f*
of hazards and hazardous situations, 126–127, 127*f*
in hierarchical risk management, 3, 3*f*
in pandemic and epidemic risk management, 310–311
probability in, 24–25, 25*t*–26*t,* 125–126, 126*f,* 310
in process approach, 7, 9*f*
purpose of, 125, 127
risk assessment from, sample, 29*t,* 36*t*
risk assessment including, 100–102, 101*f,* 125, 310–311 (*See also* risk assessment)
risk-based auditing of, 204
in risk-based decision making, 18–19, 18*f*
risk defined for, 24, 25*t*
risk matrix for, 28*t,* 127, 131
risk metalanguage in, 126, 127*f*
risk modification based on, 36, 36*t,* 88–89
risk repository of information from, 90
risk teams conducting, 83–89
severity in, 25, 27*t*–28*t,* 125, 310
stakeholder communication in, 28–29
risk appetite
definition of, 69
organizational culture influencing, 67, 73
risk attitude and, 69–70, 70*t*
risk evaluation reflecting, 140, 148
stakeholders', 69, 73, 148
risk assessment, 100–102
in hierarchical risk management, 3, 3*f*
overview of, 100–102
for pandemic and epidemic risk management, 309–317, 309*f,* 312*t,* 316*f*–317*f,* 318*t*–319*t*
phases of, 100, 101*f*
reassessment for risk monitoring and review, 163, 167, 169
risk analysis for, 29*t,* 36*t,* 100–102, 101*f,* 125, 310–311 (*See also* risk analysis)
risk-based auditing of, 203, 204
risk-based thinking underlying, 101
risk evaluation for, 100, 101*f,* 102 (*See also* risk evaluation)
risk identification for, 29*t,* 36*t,* 100–102, 101*f,* 309–310 (*See also* risk identification)
risk management planning for, 79–80
risk modification and, 36–39, 36*t*–38*t,* 88–89, 141, 148
risk repository of information from, 90
risk triangle/rhomboid for, 312, 313*f*
in supplier risk oversight, 238
risk attitude. *See also* risk acceptability; risk culture
definition of, 68
identification of, 40
organizational culture influencing, 67, 73, 223, 225–226, 225*f*
risk appetite and, 69–70, 70*t*
risk-averse attitude, 69–70, 70*t*
risk-based decision making influenced by, 223, 225–226, 225*f*
risk-neutral attitude, 69–70, 70*t*
risk process facilitation considering, 87
risk-seeking attitude, 69–70, 70*t*
risk-tolerant attitude, 69–70, 70*t*
stakeholders', 40, 68–69, 73
risk avoidance
definition of, 149
loss aversion bias and, 223
risk-averse attitude and, 69–70, 70*t*
as risk modification, 149, 150*f,* 152*f*
risk awareness, 170
risk-based auditing, 202–205
elements of, 203*f*
major inputs of, 205*f*
opportunities and threats evaluated in, 202–203, 204–205
organizational context for, 202–203
outcomes of, 203–204, 204*t*
process of, 171, 202
risk matrix for, 204, 204*t*
of risk monitoring and review, 170–171, 204
risk-based decision making, 16–19
cognitive bias in, 223, 224, 324
cognitive science of, xxii, 222–226, 324
definition of, 16
emotional intelligence in, 224–226, 225*f*
emotional tagging in, 223, 224
heuristics in, 222–223, 224, 324
models of effective, 16–18, 17*f*–18*f*
Monte Carlo analysis for, 305
opportunities and threats assessment in, 18–19, 18*f*
in organizational context, 71
process of, 16
risk-based auditing for, 205
risk-based thinking underlying, 16 (*See also* risk-based thinking)
stakeholder role in, 16–17
risk-based design thinking, 227–231
design inputs in, 228, 229*t*
design outputs from, 228–229, 229*t*
hierarchy of control for, 229, 231, 231*f*
in organizational context, 228
requirements identification in, 228, 229*t*
risk matrix for, 228, 229*t*
risk mitigation by design as, 7, 227–231, 229*t,* 230*f*–231*f*
risk-based thinking, 13–15. *See also* risk-based decision making; risk-based design thinking
in artificial intelligence, xxvi, 239
on consequences, 15
data analysis informing, xxvi
definition of, 16
ISO 9001 on, 7, 20
as philosophy, 7
as preemptive thinking, 16
as preventive thinking, 15
proactive vs. reactive, xxii
probability estimation using, 13–15, 14*f*–15*f*
risk assessment based on, 101
on uncertainty, 13

risk-based trend analysis, 191–194
control charts for, 190–191, 194–201, 195*f*–197*f,* 199*f*
definition of, 191
DMAIC approach to, 191–194, 193*f*–194*f*
graphical tools for, 172, 177–180, 183, 186
of key risk indicators, 168, 177, 179, 190, 194, 200*f*
probability and severity in, 199–200, 201*f*
real-world example of, 197–201, 196*t,* 199*f*–201*f*
for risk monitoring and review, 168, 172, 177–180, 183, 186
risk response planning interface with, 190
source data for, 190, 191*f*
trigger conditions in, 192, 193–194
risk-benefit analysis, 206–221
in banking and financial services industry, 206–208, 208*f*
Clavien-Dindo scale for, 129–130, 132*t,* 213, 214*t,* 215–217, 216*f,* 217*t*
cost effectiveness analysis as, 218–221, 218*f,* 219*t,* 220*f*
definition of, 108, 208
of degree of benefit, 211–212, 212*t*
global risk-benefit score, 210
of harm, 108, 213–215, 214*t,* 217
hazard analysis including, 266
in healthcare industry, 218–221, 218*f,* 219*t,* 220*f*
maximum drawdown as, 207
in mining industry, 208–209
of opportunities, 46, 46*t,* 108, 208
in pharmaceutical industry, 209–217, 210*t*–215*t,* 216*f,* 217*t*
probability in, 214*t*–215*t,* 214–217
risk matrix approach to, 213–215, 214*t*–215*t,* 217*t*
severity in, 210–211, 211*t,* 214*t,* 214–216
Sharpe ratio as, 206–207
of threats, 108, 208
TURBO model for, 210, 213*t*
weighted counts in, 213–215, 215*t,* 217, 217*t*
Risk Breakdown Structure (RBS), 92–94, 93*t*–94*t*
risk control. *See* risk modification
risk culture
definition of, 68, 73
in organizational context, 40, 67, 68–70, 71, 73, 140–141, 142*t,* 143, 223, 226, 225*f*
risk attitude, appetite, and tolerance in, 40, 67, 68–70, 70*t,* 73, 81, 87, 140–141, 142*t,* 143, 148, 223, 225–226, 225*f*
risk drivers, 48, 49*f*–50*f,* 50
risk enhancement, 150–151, 152*f*
risk evaluation, 140–148
decisions rules for, 141–142, 142*t*–143*t*
definition of, 30, 100, 140
in HACCP, 281–282
organizational context for, 140–141
outcomes of, 148
in pandemic and epidemic risk management, 311, 312*t*
risk acceptability criteria for, 140–141, 142*t*–143*t,* 148
risk analysis informing, 125
risk assessment including, 100, 101*f,* 102 (*See also* risk assessment)
risk-based auditing of, 204
in risk-based decision making, 18–19, 18*f*
risk levels for prioritization in, 139, 141–143, 141*t*–147*t,* 145–148, 147*f*
risk management planning for, 79, 142
risk matrix in, 139, 141–143, 141*t*–147*t,* 145–148, 147*f*
risk modification based on, 36, 36*t,* 141, 148
risk repository of information from, 90
risk teams conducting, 86, 88
stakeholder communication in, 28–29, 148
risk exploitation, 151, 152*f*
risk exposure
acceptability of (*See* risk acceptability)
KRIs presenting, 164
to pandemic or epidemic, 312, 313*f,* 317
risk analysis of, 125 (*See also* risk analysis)
visual risk exposure tracker, 187–189, 311
risk governance
CoRMM Model assessment of, 76*t*
definition of, 2
in organizational context, 2, 65, 71–73
policies and procedures for (*See* policies and procedures)
risk identification, 24–30, 47–56
of aggregate risk, 29, 30*f*
basic, 24–30
brainstorming for, 56, 88
cause and effect analysis in, 52, 52*t*
consequence analysis in, 109 (*See also* consequence analysis)
data analysis for, 47
definition of, 29, 47, 100
Delphi technique for, 56, 88
detailed, 47–56
hazard identification in, 48–51, 49*f*–50*f,* 261–262, 264, 281–282, 285*t*
in hierarchical risk management, 3, 3*f*
methods of, 56, 55*f,* 88
in pandemic and epidemic risk management, 309–310
probability in, 24–25, 25*t*–26*t*
in process approach, 7, 9*f*
process of, 55*f*
purpose of, 92
risk assessment from, sample, 29*t,* 36*t*
risk assessment including, 100–102, 101*f,* 309–310 (*See also* risk assessment)
risk-based auditing of, 204, 205
in risk-based decision making, 18–19, 18*f*
risk defined for, 24, 25*t*
risk drivers in, 48, 49*f*–50*f,* 50
risk matrix for, 28*t*
risk metalanguage for, 52, 53, 98, 126
risk modification based on, 36, 36*t,* 88–89
risk repository of information from, 90

risk sources in, 48–51, 49*f*–50*f,* 52–54, 54*f*
risk teams conducting, 83–89
root cause analysis for, 56
severity in, 25, 27*t*–28*t*
stakeholder communication in, 28–29, 52
tools for (*See* risk identification tools)
risk identification tools, 92–99
assumptions and constraints analysis, 96, 98*f*
Risk Breakdown Structure, 92–94, 93*t*–94*t*
strengths-weaknesses-opportunities-threats analysis, 98–99, 99*f*
structured what-if technique, 94–96, 95*f,* 97*f*
risk management
challenges of, xxv
characteristics of, xxi–xxvi
CoRMM Model, 75–78, 79
data analysis and (*See* data analysis)
definition of, 11
events and consequences in (*See* consequence analysis; consequences; events and consequences)
evolutionary origins of, xxi–xxii, 13
hazards necessitating (*See* hazards and hazardous situations)
hierarchical, 2–4, 3*f*
holistic approach to, xxiii, 4, 101
of Industry 4.0 risk, xxv–xxvi, 239–241
ISO standards for (*See* ISO *entries*)
opportunities in (*See* opportunities)
organizational context for (*See* organizational context)
overview of, 1–4
pandemic and epidemic risk management (*See* pandemic and epidemic risk management)
PDCA cycle on, 5–7, 6*f,* 8*f*–9*f,* 9
pillars of, 1, 2*f*
probability in (*See* probability)
process approach to, 6–9, 7*f*–9*f*
quality and, xxvi, 5–9, 82 (*See also* quality)
risk, defined, xxiv–xxv, 10–12, 24–25, 25*t,* 28, 44–45, 45*t,* 47, 104, 214–215, 261
risk assessment in (*See* risk analysis; risk assessment; risk evaluation; risk identification)
risk-based auditing in, 170–171, 202–205
risk-based decision making in (*See* risk-based decision making)
risk-based thinking in (*See* risk-based design thinking; risk-based thinking)
risk-based trend analysis in (*See* risk-based trend analysis)
risk-benefit analysis in (*See* risk-benefit analysis)
risk governance framework for (*See* risk governance)
risk management planning in (*See* risk management planning)
risk matrix in (*See* risk matrix)
risk modification in (*See* risk modification)
risk monitoring and review in (*See* risk monitoring and review)
risk process facilitation in, 83–89, 96
risk repository in, 90–91
risk response planning in (*See* risk response planning)
stakeholders in (*See* stakeholders)
supplier risk oversight in, 232–238
tools for (*See* advanced risk tools; graphical tools; risk identification tools)
risk management planning, 79–82
for aggregate risk determination, 81
for budgets, 80–81
CoRMM Model informing, 79
elements addressed in, 79–81
gap analysis in, 79
for hazard categorization, 80
organizational context informing, 79
for pandemic and epidemic risk management, 323–324
for probability and severity definitions, 80
in process approach, 7, 9*f*
quality management planning integration with, 82
for reporting, 81
for risk acceptability, 79, 80
for risk evaluation, 79, 142
for risk modification metrics, 81
for risk monitoring and review, 81, 323
for risk tolerance, 81
sample risk management plan, 81–82
for stakeholder roles and responsibilities, 80
supplier risk oversight in, 233
risk matrix, 128–139
bubble charts vs., 187
definition of, 135–136
Kraljic matrix as, 232–234, 233*f*
organizational context for, 128–132, 129*f*–131*f,* 131*t*–136*t,* 135
probability in, 128, 129*f,* 132, 135–137, 135*f,* 135*t*–137*t,* 137*f*–138*f,* 139, 140–143, 141*t*–146*t,* 147, 147*t*
purpose of, 145–147
for risk acceptability determination, 67
for risk analysis, 28*t,* 127, 131
risk-based auditing using, 204, 204*t*
for risk-based design thinking, 228, 229*t*
for risk-benefit analysis, 213–215, 214*t*–215*t,* 217*t*
risk definition as basis for, 214–215
for risk evaluation, 139, 141–143, 141*t*–147*t,* 145–148, 147*f*
for risk identification, 28*t*
risk levels in, 66, 137, 137*f*–138*f,* 137*t,* 139, 141–143, 141*t*–147*t,* 145–148, 147*f*
for risk modification, 152–153, 153*t*
risk response planning using, 159, 159*f*
severity in, 128–131, 129*f*–131*f,* 131*t*–134*t,* 135–137, 137*f*–138*f,* 137*t,* 139, 140–143, 141*t*–147*t*
for supplier risk oversight, 232–234, 233*f*
risk metalanguage, 52, 53, 98, 126, 127*f,* 152
risk mitigation
definition of, 149
in pandemic and epidemic risk management, 311, 317, 320*f*

risk mitigation by design, 7, 227–231, 229*t,* 230*f*–231*f*
as risk modification, 149, 150*f,* 152*f* (*See also* risk modification)
in supplier risk oversight, 238
risk modification, 35–39, 149–156
basic, 35–39
consequence-time series charts of risk after, 39*f*
definition of, 39
flowcharts for, 153, 154*f*–155*f,* 156
FMEAs for, 242
hazard analysis implementation of, 266, 269
in hierarchical risk management, 3*f*
implementation of (*See* risk response planning)
for opportunities, 150–156, 152*f,* 153*t,* 154*f*–155*f*
positive risk realization by design, 152–156, 153*t,* 154*f*–155*f*
preliminary hazard analysis leading to, 122, 123*f,* 124, 124*t*
probability modification with, 38*t,* 149, 150–152, 153*t*
purpose of, 149
risk acceptance without, 149–150, 150*f,* 152*f*
risk assessment and, 36–39, 36*t*–38*t,* 88–89, 141, 148
risk avoidance as, 149, 150*f,* 152*f*
risk-based auditing of, 204
risk enhancement as, 150–151, 152*f*
risk evaluation leading to, 36, 36*t,* 141, 148
risk exploitation as, 151, 152*f*
risk identification and analysis informing, 36, 36*t,* 88–89
risk management planning for measuring effectiveness of, 81
risk matrix for, 152–153, 153*t*
risk mitigation as, 149, 150*f,* 152*f* (*See also* risk mitigation)
risk mitigation by design as, 7, 227–231, 229*t,* 230*f*–231*f*
risk monitoring and review for, 39, 89
risk repository of information from, 90
risk sharing as, 151, 152*f*
risk teams for, 88–89
risk transfer as, 149, 150*f,* 152*f*
selection of, 149–156
severity modification with, 36, 39, 149, 150–152, 153*t*
stakeholders' engagement in, 39
risk monitoring and review, 163–171
aggregation for, 168
benchmarking for, 168
contingency planning for, 168
of design risk, 229
FMEA monitoring as, 255
graphical tools for (*See* graphical tools)
in HACCP, 283–284
key risk indicators for, 163–167, 165*f,* 168, 169, 177, 179
logarithmic scales for, 320–321
organizational context for, 65–67, 165–166
in pandemic and epidemic risk management, 317, 319–323, 320*f*–323*f*
in process approach, 7, 9*f*
process of, 169*f*
reassessment for, 163, 167, 169
reporting on, 170
risk awareness and, 170
risk-based auditing of, 170–171, 204
risk level measurements for, 167
risk management planning for, 81, 323
for risk modification, 39, 89
in risk process facilitation, 88, 89
risk response planning using, xxiv
scoring criteria for, 66–67
trend analysis for, 168, 172, 177–180, 183, 186
trigger conditions and, 167, 168–169
visual risk exposure tracker for, 187–189, 311
risk priority numbers (RPNs), 247, 249*f,* 255, 258*f*–259*f*
risk probability numbers (RPNs), 67, 141–142, 142*t,* 187, 188*t*
risk process facilitation, 83–89
independent reviewers in, 83, 86–87, 88
inductive and deductive reasoning in, 87, 88
knowledge, skills, and attitudes for, 84
life cycle management in, 87–88, 89
risk attitude considered in, 87
risk facilitation, defined, 83
risk monitoring and review in, 88, 89
for risk teams, 83–89, 84*f,* 86*f,* 96
for SWIFT process, 96
zones/styles of facilitation, 85–86, 85*f*–86*f*
risk ranking, 66. *See also* risk priority numbers
risk register. *See* risk repository
risk repository, 90–91
risk response planning, 157–162
contingency planning in, 160, 162
elements addressed in, 157–158
flowcharts for, 161*f*
inherent risk analysis in, 159–160, 160*f*
in organizational context, 72
for pandemics and epidemics, xxiv, 323–324
process of, 158*f,* 161*f*
purpose of, 157
residual risk analysis in, 158–159, 159*f*–160*f*
risk-based auditing of, 204
risk-based trend analysis interface with, 190
risk matrix in, 159, 159*f*
risk reaction distinguished from, xxiv
secondary risk analysis in, 158
risk sharing, 151, 152*f*
risk sources, identification of, 48–51, 49*f*–50*f,* 52–54, 55*f*
risk teams
for HACCP performance, 280, 281, 285
for HAZOP performance, 272
independent reviewers in, 83, 86–87, 88
risk process facilitation for, 83–89, 84*f,* 86*f,* 96
stages of team performance, 84–85, 84*f,* 86*f*
stakeholders in, 88–89, 96
for SWIFT process, 96
zones/styles of facilitation with, 85–86, 85*f*–86*f*

risk tolerance
definition of, 69
organizational culture influencing, 67, 73
risk attitude and, 69–70, 70*t*
risk evaluation reflecting, 140–141, 142*t,* 143
risk management planning for, 81
risk-tolerant attitude, 69–70, 70*t*
stakeholders', 69, 73, 81
risk transfer, 149, 150*f,* 152*f*
risk treatment. *See* risk modification
risk triangle, 312, 313*f*
RmD (risk mitigation by design), 7, 227–231, 229*t,* 230*f*–231*f*
root cause analysis (RCA)
brainstorming in, 120
consequence analysis using, 119–122, 120*f*–122*f*
fault tree analysis for, 294
fishbone diagrams in, 120, 121, 121*f*
5 Whys in, 120, 121–122, 122*f,* 272
FMEA including, 244, 244*f*–245*f*
hazard analysis including, 266
HAZOP including, 272
for risk identification, 56
steps in, 119–121, 120*f,* 121*f*
RPNs. *See* risk priority numbers; risk probability numbers
run charts, 178, 179*f*

S

SARS-CoV (severe acute respiratory syndrome), 307, 312*t*
SARS-CoV-2. *See* COVID-19
satisficing, in decision making, 222
scatter plots, 172–174, 174*f*–175*f*
scenario analysis, 118–119, 119*f*
secondary risk, 158
self-awareness, 224, 225*f*
self-management, 224, 225*f*
sensitivity analysis, 304–305, 305*f*
sequence of events
causal nexus between, 61, 117
fault tree analysis of, 110–111, 292–297
hazard analysis identification of, 262
in hazardous situations, 105, 106*f*–108*f,* 106*t,* 107–108, 115, 123*f,* 124, 124*t,* 126, 262, 266*f*
risk identification including, 48, 49*f*–50*f,* 50
service Failure Modes and Effects Analysis, 248
severe acute respiratory syndrome (SARS-CoV), 307, 312*t*
severity
consequence analysis using, 109
consequences as scale of, 31–33, 32*t*–33*t*
definition of, 25, 128
in FMEA, 246–247, 247*t,* 249, 253, 254*t*
hazard analysis estimation of, 265
in impact-probability bubble charts, 187, 188*f*–189*f,* 188*t*
in pandemic and epidemic risk management, 310–311, 312, 313*f*
in risk-benefit analysis, 210–211, 211*t,* 214*t,* 214–216
risk identification and analysis of, 25, 27*t*–28*t,* 125, 310
risk management planning for definition of, 80
risk matrix based on, 128–131, 129*f*–131*f,* 131*t*–134*t,* 135–137, 137*f*–138*f,* 137*t,* 139, 140–143, 141*t*–147*t*
risk modification altering, 36, 39, 149, 150–152, 153*t*
trend analysis of, 199–200, 201*f*
Sharpe ratio, 206–207
Shewhart, W. A., 190
Simchi-Levi, D., 237
Simon, Herbert, 222
Sinkula, M. S., 210
SMEs. *See* subject matter experts
social awareness, 224, 225*f*
Society of Risk Analysis, hazards definition, 107
software Failure Modes and Effects Analysis, 248
software industry, subject matter experts in, 61
stakeholders, 40–43
active stakeholders, 41
definition of, 40
engagement of, 39, 40–42, 42*f*–43*f,* 52
in FMEA, 248
identification of, 40–42, 52
inclusivity of, xxv, 77*t,* 314
influence-engagement matrix of, 41–42, 42*f*–43*f*
key stakeholders, xxv, 41
organizational context consideration of, 65
RACI matrix for, 42–43, 43*t,* 80, 89
reporting to (*See* reporting)
risk attitude, appetite, and tolerance of, 40, 68–70, 73, 81, 148
risk-based decision making role of, 16–17
risk evaluation communication with, 28–29, 148
risk identification and analysis communication with, 28–29, 52
risk management planning for roles and responsibilities of, 80
risk modification engagement of, 39
risk team involvement of, 88–89, 96 (*See also* risk teams)
satellite stakeholders, 42
storage of risk information. *See* risk repository
strategic risk management
in hierarchical risk management, 3, 3*f*
organizational context for, 72
stratification, in data analysis, 194, 195*f*
strengths-weaknesses-opportunities-threats (SWOT) analysis, 98–99, 99*f*
structured what-if technique (SWIFT), 94–96, 95*f,* 97*f*
subject matter experts (SMEs). *See also* expert opinions
in HAZOP team, 272
probability informed by, 61, 246
risk teams augmented with, 87, 88, 272
supplier risk oversight, 232–238
FMEA performance and, 249
graphical representation of risk in, 236, 236*f*
key risk indicators informing, 234–236, 234*f*–235*f*

Kraljic matrix for, 232–234, 233*f*
preparing for unanticipated risks in, 237–238
reactive and proactive quality management in, 234, 234*f*
risk index for, 234–236, 235*t*
risk mitigation in, 238
supplier agreements on, 232
supplier risk assessment in, 238
time to recovery analysis in, 237–238
SWIFT (structured what-if technique), 94–96, 95*f,* 97*f*
SWOT (strengths-weaknesses-opportunities-threats) analysis, 98–99, 99*f*

T

Taleb, Nassim Nicholas, 307
teams. *See* risk teams
Tesla, 151
testing, pandemic, 311
thinking, risk-based. *See* risk-based design thinking; risk-based thinking
threats. *See also* harm; hazards and hazardous situations
organizational context for, 72
risk attitude toward, 69
risk-based auditing evaluating, 202–203, 204–205, 205*f*
risk-based decision making assessment of, 18–19, 18*f*
risk-based design thinking on, 228
risk-benefit analysis of, 108, 208
risk defined in relation to, 44, 45
risk identification of, 51–52, 52*t*
risk modification for, 149–151, 150*f,* 152*f*
SWOT analysis of, 98–99, 99*f*
timelines
Pareto charts over, 174*f*
risk management planning for, 80
time to recovery in supply chain, 237–238
time-series charts
consequence-time series charts, 29, 30*f,* 39*f*
control charts as, 178–180, 180*f,* 196*f*–197*f,* 197
in risk-benefit analysis, 208*f*
for risk monitoring and review, 177–178, 177*f*–178*f*
tools for risk management. *See* advanced risk tools; graphical tools; risk identification tools
top event, in fault tree analysis, 292
Toyoda, Sakichi, 122
Toyota, 122, 151
tracking risk. *See* risk monitoring and review
Transparent Uniform Risk Benefit Overview (TURBO) model, 210, 213*t*
trend analysis. *See* risk-based trend analysis
trigger conditions
for hazardous situations, 103, 104, 115–116
monitoring, 167, 168–169
risk identification of, 95*f,* 96, 97*f*
risk management planning for, 81
in trend analysis, 192, 193–194
Tuckman, B. W., 84
TURBO (Transparent Uniform Risk Benefit Overview) model, 210, 213*t*

U

UFMEA (use Failure Modes and Effects Analysis), 248, 257, 258*f*
Ulam, Stanislaw, 298
uncertainty
consequence analysis consideration of, 109, 110*f*
definition of, 11, 13
design risk with, 227
risk-based thinking on, 13
risk-benefit analysis quantifying, 206
risk defined in relation to, 10–12, 44–45, 47
as risk source, 53
use Failure Modes and Effects Analysis (UFMEA), 248, 257, 258*f*
U.S. Manufacturer and User Facility Device (MAUDE) database, 87

V

value chains, 73–74
value creation, 77*t*
vendor risk oversight. *See* supplier risk oversight
viral exposure evaluation, 317
visual risk exposure tracker, 187–189, 311
volatility
definition of, 53
as hazard, 107*f*
Monte Carlo analysis of, 298
risk analysis of, 125
risk-benefit analysis quantifying, 206–207, 208*f*
as risk source, 53
scatter plot graphing, 173, 174*f*
VUCA (volatility, uncertainty, complexity, ambiguity), xxiii, 53
vulnerability
to pandemic or epidemic, 312, 313*f,* 324
risk analysis of, 125
risk identification of, 99

W

Weber, E. U., 225
what-if techniques
for hazard analysis, 262
structured what-if technique, 94–96, 95*f,* 97*f*
Whitehead, J., 223, 224
white swan events, 307
Wilson, R., 208–209

Z

zoonotic spillover, 307

About the Author

Jayet Moon is a Senior ASQ member and holds ASQ CQE, CSQP, and CQIA certifications. He has earned a master's degree in biomedical engineering from Drexel University in Philadelphia and is a Project Management Institute (PMI) Certified Risk Management Professional (PMI-RMP). He is also an Enterprise Risk Management Certified Professional (ERMCP) and a Risk Management Society (RIMS) certified Risk Management Professional (RIMS-CRMP), a certification that holds official accreditation from the American National Standards Institute (ANSI) under ISO/IEC 17024:2012. He is a doctoral candidate in Systems and Engineering Management at Texas Tech University.



ASQ'S ONLINE QUALITY RESOURCES IS THE PLACE TO:

- Stay on top of the latest in quality with Editor's Pick and Most Popular
- Browse topics in Learn About Quality
- Find definitions in the Quality Glossary
- Search ASQ's collection of articles, books, tools, training, and more

QUALITY RESOURCES
www.asq.org/quality-resources

Connect with ASQ staff for personalized help hunting down the knowledge you need, the networking opportunities that will keep your career and organization moving forward, and the publishing opportunities that offer the best fit for you.

www.asq.org/quality-resources

ASQ
Excellence Through Quality™

TRAINING CERTIFICATION CONFERENCES MEMBERSHIP PUBLICATIONS

ASK A LIBRARIAN!



Have questions?
Looking for answers?
In need of information?
ASK A LIBRARIAN!

Customized research assistance from ASQ's research librarian is one of the many benefits of membership. ASQ's research librarian is available to answer your research requests using the ever-expanding library of current and credible resources, including journals, conference proceedings, case studies, and Quality Press publications.

For more information or to submit a question, visit **asq.org/quality-resources/ask-a-librarian**

ASQ
Excellence Through Quality®

TRAINING CERTIFICATION CONFERENCES MEMBERSHIP PUBLICATIONS



VIRTUAL EDUCATION TO FIT YOUR SCHEDULE AND BUDGET

ASQ provides a range of e-learning options designed to meet your unique professional education needs during this extraordinary time of uncertainty – and we've added new courses to our virtual training catalog!

Now, you can continue your education with high-caliber content and outstanding instructors, in the convenience of your own home or office.

Whether you choose to learn on your own with web-based instruction materials, or with virtual training led by subject matter experts, ASQ is ready to help you grow your professional knowledge and skills.

Visit **asq.org/training/catalog**
to learn more about our virtual course options.

ASQ
Excellence Through Quality®



ASQ MEMBERSHIP: MAKE YOUR MEMBER BENEFITS WORK FOR YOU!

You're dedicated to excellence through quality. At ASQ, we're committed to helping advance your quality career as your primary source of industry news, emerging trends, professional development, quality tools, and career resources.

Here's how you can make the most of your ASQ membership:

- **Increase your quality knowledge:** Gain print and digital access to the latest quality news with ASQ publications.
- **Develop skills to advance your career:** Continue your professional development through e-learning and virtual courses.
- **Connect and collaborate:** Join quality peers and thought leaders through myASQ.
- **Invest in your future:** Demonstrate your commitment to quality with ASQ certifications.

Develop your skills. Expand your network. Advance your career.

Visit **asq.org/membership** for details and to join or renew your membership.

ASQ
Excellence Through Quality®