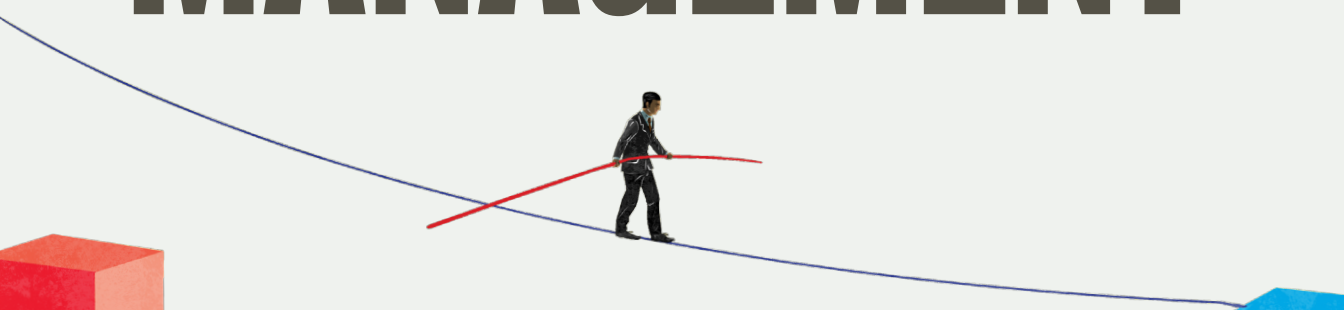
Foundations of QUALITY RISK MANAGEMENT



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



Jayet **MOON**

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

Foundations of Quality Risk Management

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

Foundations of Quality Risk Management

A Practical Approach to Effective Risk-Based Thinking

Jayet Moon



Quality Press
Milwaukee, Wisconsin

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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®

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

This book is dedicated to A. R. Moon

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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:

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

> *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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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:

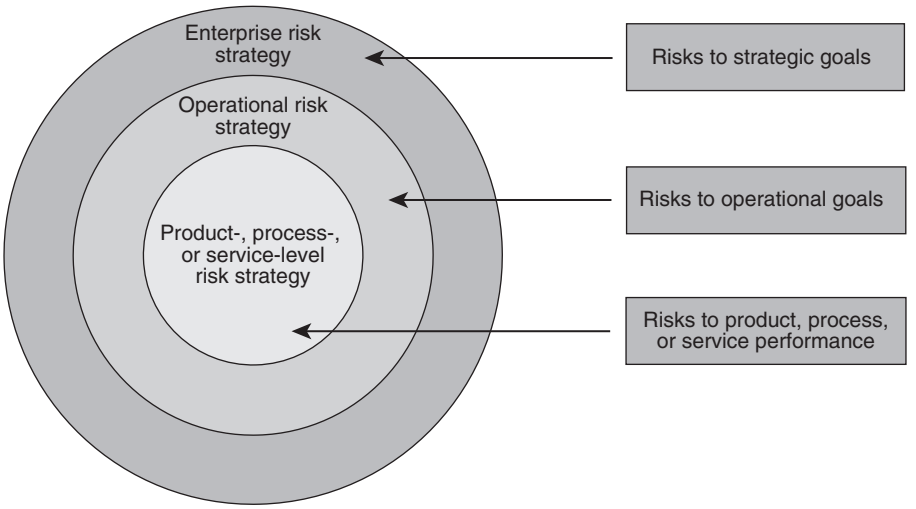
- Realistic assessment of the organizational objectives and path to their achievement
- Prevention of undesired outcomes
- Continuous improvement
- Value sustenance and value addition

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

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

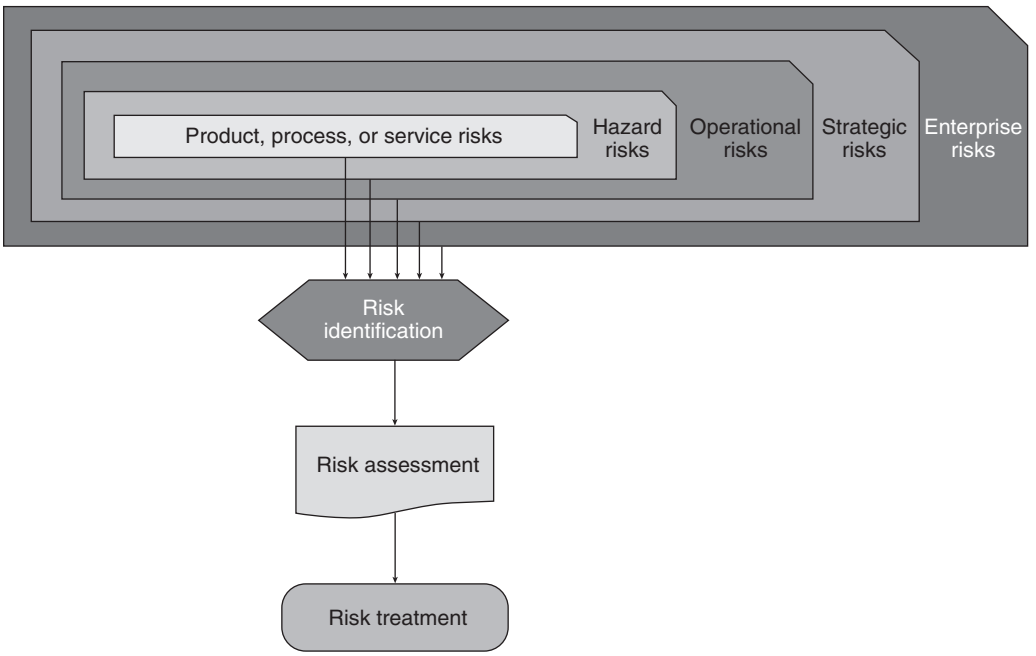
Risk governance varies tremendously from sector to sector and company to company. Some companies do not have any enterprise risk management at all, while others have no product-level risk management. Many companies have multiple decentralized risk management processes used by disparate functions and 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.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

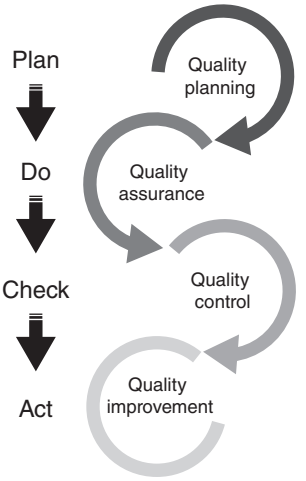
Quality control focuses on problem detection and reaction after an issue has been discovered. This is an important activity since now the risk to quality has been realized and detected. But detection and local solution of the issue do not add any long-term value to the system. The discovered issues must 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/.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

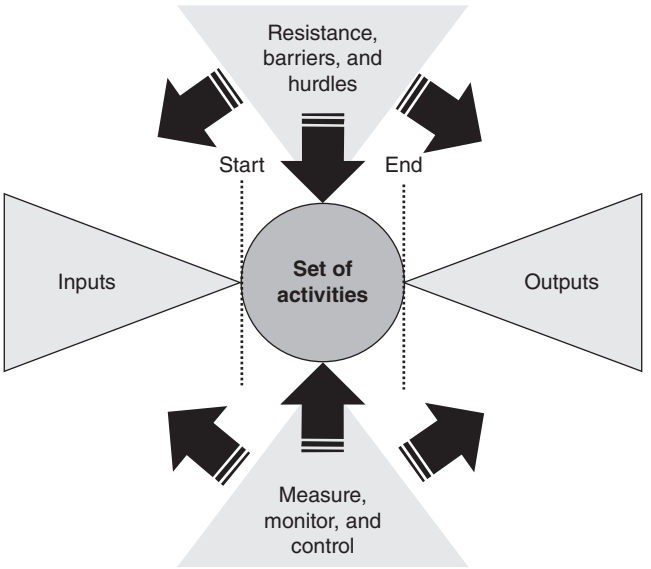
The *process approach* is an organizational strategy of managing and controlling a process and various interacting subprocesses within the organization. Any activity that has an input and output is a process. If a process is converting an input to an output, it means there are certain sets of subactivities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

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

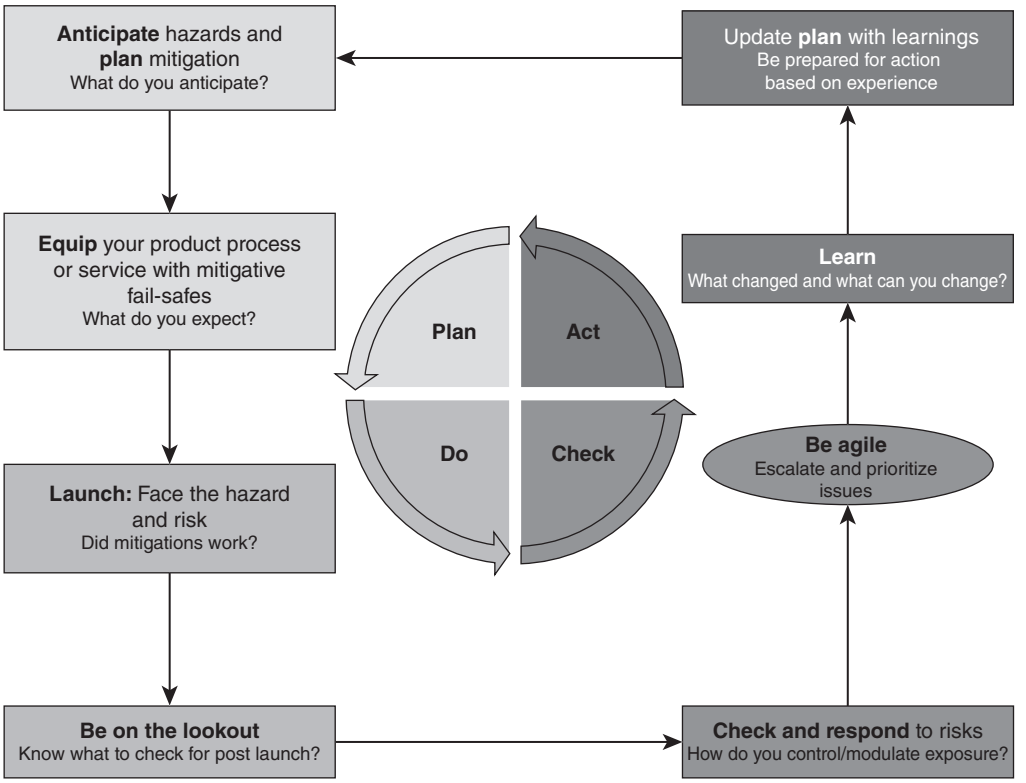
While enterprise risk management propagates a top-down approach to risk management, risk mitigation by design (RmD) aims for a bottom-up approach. ISO 9001:2015 removed the earlier preventive action clause and introduced risk-based thinking, which, by nature, is preventive in spirit. By practicing RmD (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

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

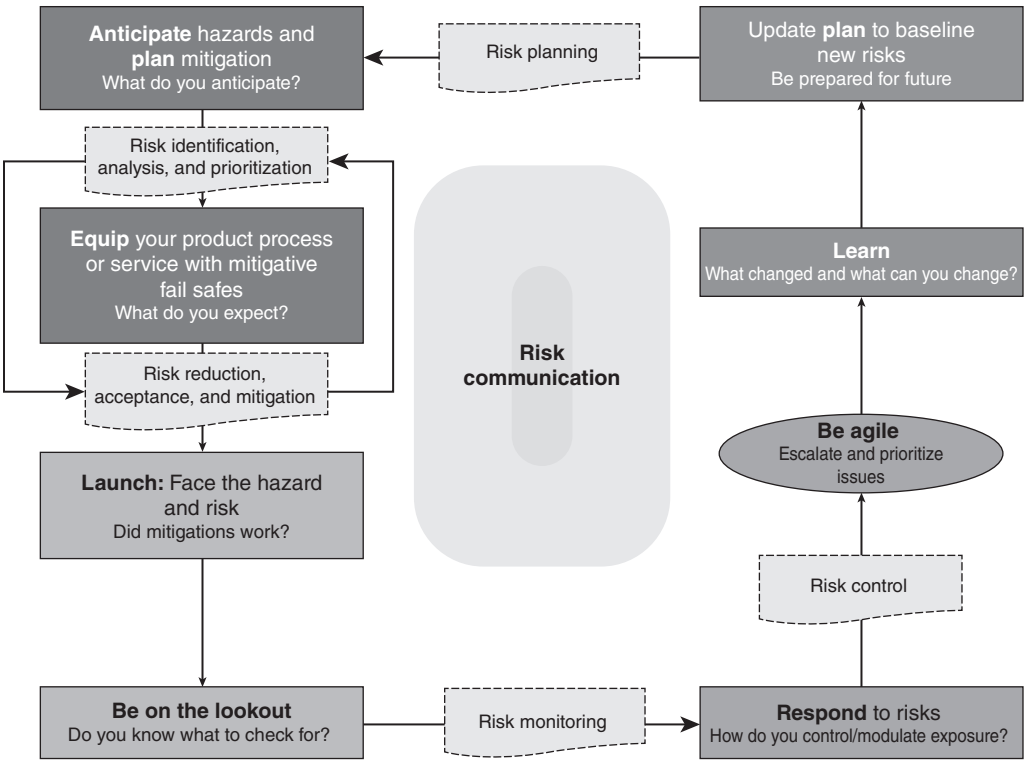


FIGURE 2.4 PDCA and risk management.



AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

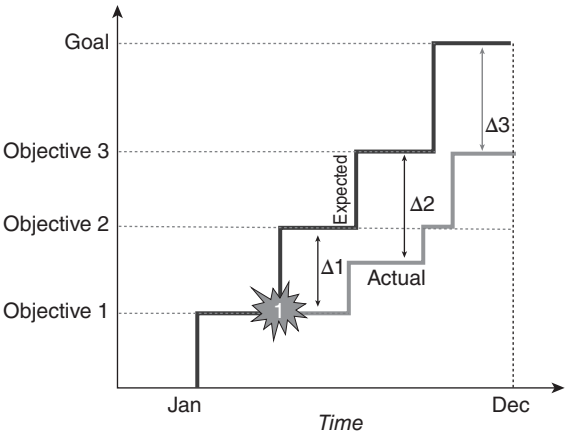
Similarly, in the scenario above, a positive event could have led the organization to get back on track and achieve the end goal before the end of the mandated time frame. If this were to happen, it would be an example of positive risk, the uncertainty due to events related to accelerated achievement 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.

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

AVA Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

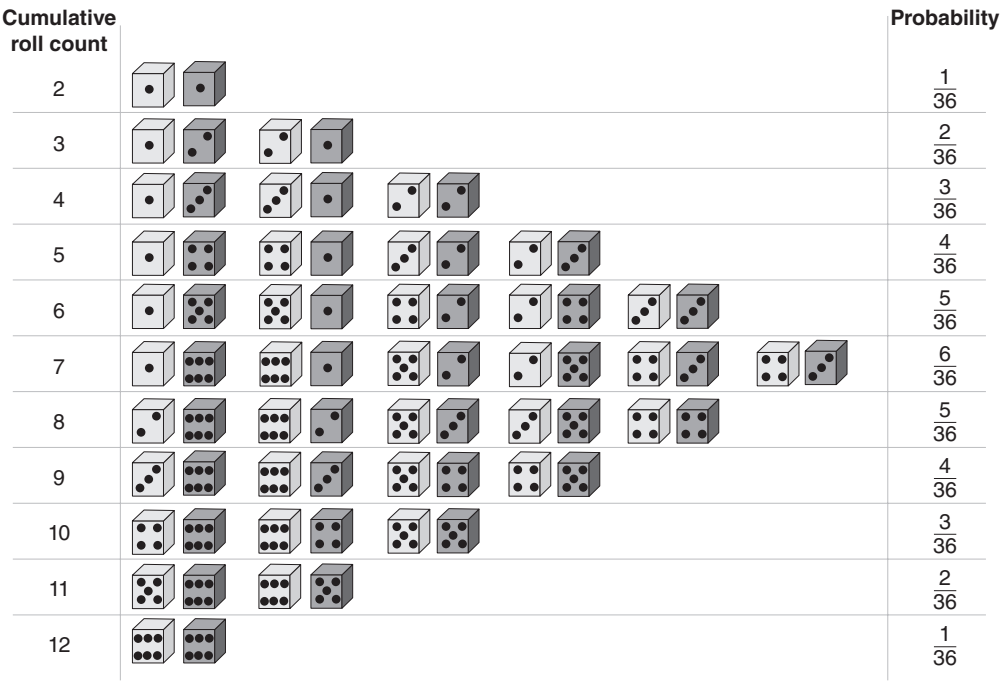
John chooses the number 5 because his father's birthday is on the fifth of the month. Steve uses concepts of probability to choose a number. Knowing that there are 36 outcomes in a double dice throw, per Figure 4.1, Steve calculates that the highest probability of occurrence is for the number 7.

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.



AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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

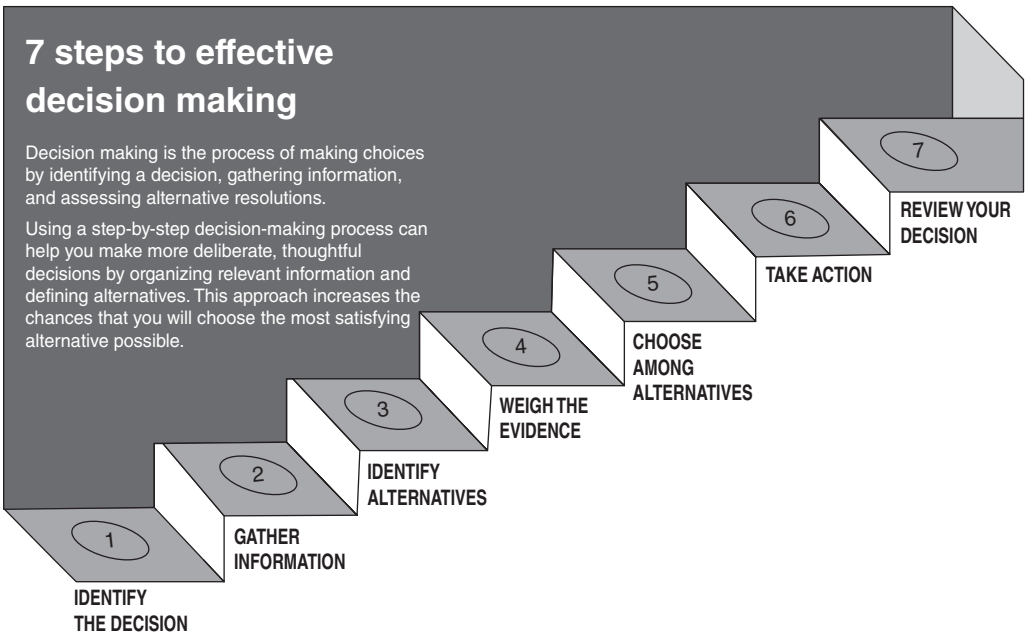
In this chapter we will focus on aspects of the decision structure. The coming chapters of this book will address risk and impact assessment in great detail.

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.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

FIGURE 5.2 Risk-based decision-making model.

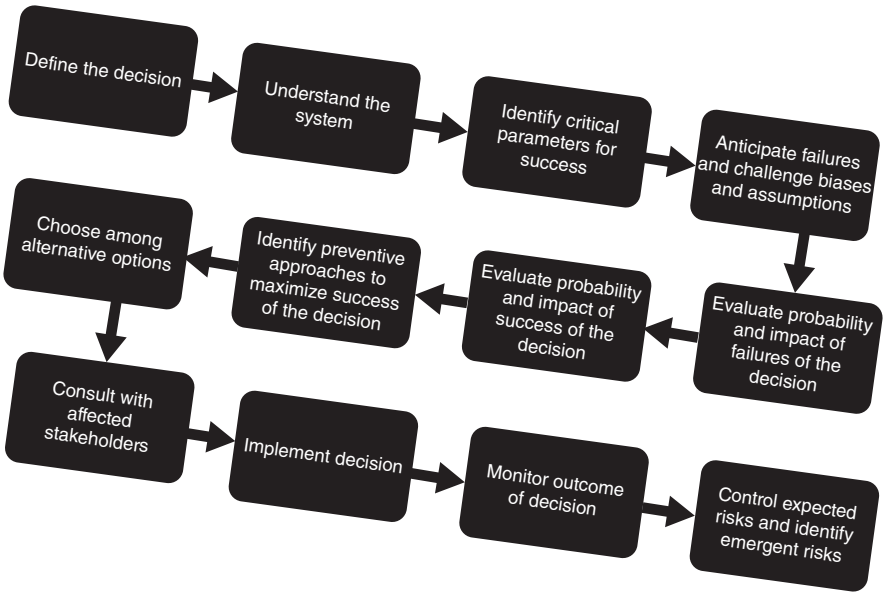
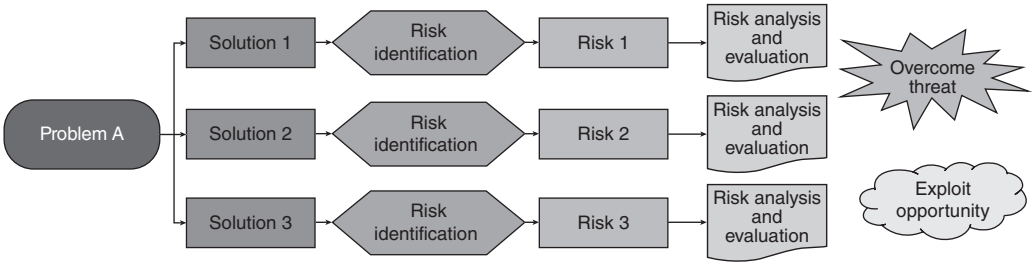


FIGURE 5.3 Risk-driven decision making leading to exploitation of opportunities and mitigation of threats.



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.

AVA Documents
Document Sharing Hub
Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking

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.

Documents
Document Sharing Hub

Full document details: Foundations of Quality Risk Management: A Practical Approach to Effective Risk-Based Thinking