

Contents

<i>List of figures</i>	xv
<i>List of tables</i>	xvii
<i>About the author</i>	xix
<i>Preface</i>	xxi
<i>Acknowledgments</i>	xxiii
1. Introduction	1
1.1 History of Risk Management	3
2. What Is a Medical Device?	5
3. Why Do Risk-Management?	11
3.1 Legal and Regulatory Requirements	12
3.1.1 United States	12
3.1.2 European Union	12
3.1.3 MDD/AIMDD and Transition to EU MDR	14
3.2 Business Reasons	14
3.2.1 Cost Efficiency	14
3.2.2 Avoiding Recalls and Field Corrective Actions	16
3.2.3 Better Communications	16
3.3 Moral and Ethical Reasons	16
4. The Basics	17
4.1 Vocabulary of Risk Management	17
4.1.1 Reasonably Foreseeable Misuse	21
4.2 Hazard Theory	22
4.3 Systems and System Types	24
5. Understanding Risk	27
5.1 Risk Definitions	28
5.2 Types of Risk	29
5.3 Contributors to Risk	30
5.4 Risk Perception	30
5.5 Risk Computation	31
6. Risk Management Standards	35
6.1 ISO 14971 History and Origins	36
6.2 Harmonized Standards	37

7. Requirements of the Risk Management Process	39
7.1 Risk Management Process	39
7.1.1 Risk Analysis	40
7.1.2 Risk Evaluation	41
7.1.3 Risk Control	41
7.1.4 Evaluation of Overall Residual Risk	41
7.1.5 Risk Management Review	42
7.1.6 Production and Post-Production Activities	42
8. Quality Management System	45
9. Usability Engineering and Risk Analysis	47
9.1 Key Terms	49
9.2 Distinctions	51
9.3 User-Device Interaction Model	52
9.4 Use Errors	54
9.5 Environmental Factors	55
9.6 Design Means to Control Usability Risks	55
9.7 Task Analysis	56
9.8 Usability and Risk	56
9.8.1 Elimination of Hazardous Situation	57
9.8.2 Data Gathering	58
9.8.3 Risk Reduction and Compliance with IEC 62366 Process	58
10. Biocompatibility and Risk Management	59
11. Influence of Security on Safety	63
12. The BXM Method	67
12.1 System Decomposition	68
12.2 Integration	69
12.3 Quantitative Risk Estimation	69
13. Risk Management Process	71
13.1 Management Responsibilities	74
13.1.1 Policy for Establishing Risk Acceptance Criteria	75
13.2 Risk Management File	76
13.3 Risk Management Plan	77
13.3.1 Criteria for Risk Acceptability	78
13.3.2 Other Considerations for Risk Reduction End-Point	80
13.4 Hazard Identification	81

13.5	Clinical Hazards List	81
13.6	Exceptions to the CHL	83
13.7	Harms Assessment List	83
13.7.1	How to Create a HAL	85

14. Risk Analysis Techniques **89**

14.1	Fault Tree Analysis	89
14.1.1	Introduction	89
14.1.2	Theory	91
14.1.3	Symbols	94
14.1.4	Methodology	95
14.1.5	Ground Rules	97
14.2	Mind Map Analysis	98
14.2.1	Introduction	98
14.2.2	Theory	98
	Methodology	99
14.3	Preliminary Hazard Analysis	99
14.3.1	Introduction	99
14.3.2	Methodology	100
14.4	Failure Modes and Effects Analysis	103
14.4.1	Facilitation of FMEAs	105
14.4.2	Hierarchical Multi-Level FMEA	105
14.4.3	Failure Theory	107
14.4.4	Ground Rules	108
14.4.5	Criticality Ranking	109
14.4.6	Benefits of FMEA	112
14.4.7	FMEA Weaknesses	114
14.4.8	Ownership of FMEA	114
14.4.9	Deciding When to Perform an FMEA	115
14.4.10	Making Your Way Through the FMEA	115
14.4.11	Revisiting FMEAs	118
14.5	FMEA in the context of Risk Management	118
14.6	Design Failure Modes and Effects Analysis (DFMEA)	120
14.6.1	DFMEA Workflow	122
14.7	Process Failure Modes and Effects Analysis (PFMEA)	133
14.7.1	PFMEA Workflow	134
14.8	Use/Misuse Failure Modes and Effects Analysis (UMFMEA)	141
14.8.1	Distinctions	142
14.8.2	Use Specification vs. Intended Use	144
14.8.3	UMFMEA Workflow	145
14.9	P-Diagram	150

14.9.1	Input Signals	150
14.9.2	System	150
14.9.3	Control Factors	151
14.9.4	Noise Factors	151
14.9.5	Ideal Function	151
14.9.6	Error States	151
14.9.7	Workflow	151
14.10	Comparison of FTA, FMEA	152
15.	Software Risk Management	155
15.1	Software Types	156
15.2	Software Risk Analysis	160
15.2.1	Does Software Fail 100% of the Time?	162
15.3	Software FMEA (SFMEA)	162
15.3.1	SFMEA Workflow	163
15.4	Software Safety Classification	168
15.5	The BXM Method for Software Risk Analysis	172
15.5.1	Case 1 — Probability of Software Failure Is Available	173
15.5.2	Case 2 — Probability of Software Failure Is Not Available	173
15.6	Risk Management File Additions	174
15.7	Risk Controls	175
15.8	Legacy Software	176
15.9	Software of Unknown Provenance	177
15.10	Software Maintenance and Risk Management	178
15.11	Software Reliability vs. Software Safety	178
15.12	Tips for Developing Safety-Critical Software	179
16.	Integration of Risk Analysis	183
16.1	Hierarchical Multi-Level FMEA	183
16.2	Integration of Supplier Input into Risk Management	187
17.	Risk Estimation	189
17.1	Qualitative Method	189
17.2	Semi-Quantitative Method	190
17.3	Quantitative Method	192
17.4	Individual and Overall Residual Risks	195
17.5	Pre/Post Risk	196
17.6	Risks That Cannot Be Estimated	197
18.	Risk Controls	199
18.1	Single-Fault-Safe Design	199
18.2	Risk Control Option Analysis	201

18.3	Distinctions of Risk Control Options	201
18.4	Information for Safety as a Risk Control Measure	202
18.4.1	Criteria for Information for Safety	202
18.5	Distinction of Types of Information for Safety	205
18.6	Sample Risk Controls	205
18.7	Risk Controls and Safety Requirements	206
18.8	Completeness of Risk Controls	206
19.	Verification of Risk Controls	207
19.1	Verification of Implementation	208
19.2	Verification of Effectiveness	209
20.	On Testing	213
20.1	Types of Testing	213
20.2	Risk-Based Sample Size Selection	214
20.3	Attribute Testing	214
20.4	Variable Testing	216
21.	Risk Evaluation	219
21.1	Application of Risk Acceptance Criteria	219
21.1.1	How to Determine the State-of-the-Art	220
21.2	Risk Evaluation for Qualitative Method	222
21.3	Risk Evaluation for Semi-Quantitative Method	222
21.4	Risk Evaluation for Quantitative Method	222
22.	Risk Assessment and Control Table	225
22.1	RACT Workflow	226
22.1.1	Examine the CHL	226
22.1.2	Capture End-Effects with Safety Impact	226
22.1.3	Revisit the PHA	226
22.1.4	Populate the Initial Cause and Sequence of Events Columns	226
22.1.5	Populate Hazardous Situations Column	227
22.1.6	Populate the P1 Column	227
22.1.7	Populate the Risk-Controls Columns	227
22.1.8	Populate the Harm Column	228
22.1.9	Populate the P2 Columns	228
22.1.10	Compute Residual Risks	228
22.1.11	Risk Evaluation	228
22.2	Individual and Overall Residual Risks	228
22.3	Inherent Risks	229

23. Benefit-Risk Analysis	231
23.1 What Is a Benefit?	232
23.2 Balancing Benefits against Risks	233
23.3 Benefit-Risk Analysis in Clinical Studies	237
24. Risk Management Review	239
25. Production and Post-Production Activities	241
25.1 Regulatory Basis	243
25.2 The Purpose of Post-Market Activities	243
25.3 Post-Market Risk Management	243
25.4 The Elements of Post-Market Risk Management	245
25.4.1 Post-Market Surveillance	245
25.4.2 Post-Market Clinical Follow-up	249
25.4.3 Complaint Handling and Monitoring	251
25.4.4 Post-Market Risk Management Actions	253
25.5 Deliverables of Post-Market Risk Management	254
25.5.1 Summary of Safety and Clinical Performance	254
25.5.2 Periodic Safety Update Report	255
25.5.3 Post-Market Surveillance Report	257
25.5.4 Manufacturer Incident Report	258
25.5.5 Medical Device Reporting	259
25.6 Clinical Evaluation	259
25.6.1 Clinical Evaluation Plan	262
25.6.2 Clinical Evaluation Report	262
25.7 Frequency of Risk Management File Review	265
25.8 Feedback to Pre-Market Risk Management	265
25.9 Benefits of Post-Market Surveillance	267
26. Traceability	269
27. Lifetime of a Medical Device	271
28. Safety Versus Reliability	273
29. Risk Management for System of Systems	275
29.1 Definition of System of Systems	276
29.2 Direct and Indirect Harms	277
29.3 Assessment of the Risks of an SoS	278
30. Risk Management for Clinical Investigations	281
30.1 Terminology	282
30.2 Clinical Studies	283

30.3	Mapping of Risk Management Terminologies	284
30.4	Risk Management Requirements	285
30.5	Adverse Event Categorization	287
30.6	Risk Documentation Requirements	288
30.7	Information Flow Between ISO 14971 and ISO 14155	288
31.	Risk Management for Legacy Devices	291
32.	Risk Management for Combination Medical Devices	293
33.	Basic Safety and Essential Performance	297
33.1	How to Identify Basic Safety	297
33.2	How to Identify Essential Performance	297
34.	Relationship between ISO 14971 and other Standards	299
34.1	Interaction with IEC 60601-1	299
34.2	Interaction with ISO 10993-1	300
34.3	Interaction with IEC 62366	302
34.4	Interaction with ISO 14155	304
35.	Risk Management Process Metrics	305
35.1	Comparison with Historical Projects	305
35.2	Issue Detection History	306
35.3	Subjective Evaluation	306
36.	Risk Management and Product Development Process	307
36.1	Identification of Essential Design Outputs	308
36.2	Life Cycle Relevance of Risk Management	310
37.	Risk Management for Suppliers	313
37.1	Manufacturer Perspective	313
37.1.1	How to Incorporate Supplier Risk	314
37.2	Supplier Perspective	314
38.	Axioms	317
39.	Special Topics	319
39.1	The Conundrum	319
39.2	Cassandras	320
39.3	Personal Liability	320

39.4	Creating a Safety Culture	321
39.5	Predicting the Future	322
39.5.1	How to Better Predict the Future	323
40.	Critical Thinking and Risk Management	325
41.	Advice and Wisdom	329
	<i>Appendix A: Glossary</i>	333
	<i>Appendix B: Templates</i>	339
	<i>Appendix C: Example Device — Vivio</i>	375
	<i>Appendix D: Useful References</i>	507
	<i>References</i>	509
	<i>Index</i>	511