

Table of Contents

1	Introduction	11
1.1	Purpose.....	12
1.2	Scope.....	13
1.3	EU AI Act.....	14
1.4	Supplier Aspects	14
1.5	Business Benefits	15
1.6	Structure	15
2	Key Concepts	17
2.1	Introduction	17
2.2	ISPE GAMP 5 (Second Edition) Key Concepts Overview	18
2.3	Additional Concepts Overview	20
2.4	Key Terms	21
3	Life Cycle Approach	31
3.1	Introduction	31
3.2	Life Cycles	31
3.3	Specification and Verification	34
3.4	AI-Enabled Computerized System Validation Framework and Critical Thinking.....	34
4	Life Cycle Phases.....	35
4.1	Introduction	35
4.2	Concept.....	35
4.3	Project.....	36
4.4	Operation	45
4.5	Retirement	48
5	Quality Risk Management (QRM)	49
5.1	Introduction	49
5.2	Overview	49
5.3	Science-Based QRM	49
5.4	QRM Process.....	51
6	Regulated Company Activities.....	55
6.1	Introduction	55
6.2	Governance for Achieving Compliance.....	55
6.3	System-Specific Activities	60
7	Supplier Activities.....	71
7.1	Introduction	71
7.2	Supplier Products, Applications, and Services.....	71
7.3	General Supplier Good Practices	72
7.4	Data Usage.....	76
7.5	AI-Specific Security Measures	77

Phase Appendices

8	Appendix P1 – Concept Phase.....	79
8.1	Introduction	79
8.2	Overview	79
8.3	PoC Structure	81
8.4	Business Need or Opportunity	83
8.5	Stakeholder Engagement and Planning of Communication	84
8.6	Solution Ideation	85
8.7	Context of Use and Scope Definition	85
8.8	Drafting Requirements	86
8.9	Initial Risk Assessment and Trustworthy AI Considerations	87
8.10	Feasibility Assessment.....	90
8.11	PoC Evaluation Criteria.....	93
8.12	Specifying Initial Requirements and Transition to Project Phase.....	93
9	Appendix P2 – Project Phase	95
9.1	Introduction	95
9.2	Overview	95
9.3	Planning	96
9.4	Model Requirement Specification and Definition of Model Design Space	97
9.5	Case Data Set Creation	101
9.6	Data Split	102
9.7	Iterative Experimentation	104
9.8	Model Release Candidate Selection	110
9.9	Testing of AI-Enabled Computerized Systems	110
9.10	Reporting and Release	117
10	Appendix P3 – Operation Phase	119
10.1	Introduction	119
10.2	Overview	119
10.3	Handover	120
10.4	Establishing and Managing Support Services	121
10.5	System Monitoring	121
10.6	Incident Management and Problem Management	123
10.7	CAPA.....	127
10.8	Operational Change and Configuration Management	128
10.9	Periodic Review	133
10.10	Business Continuity Management	134
10.11	Security Management.....	134
11	Appendix P4 – Retirement Phase	135
11.1	Introduction	135
11.2	Retirement Planning	136
11.3	Retirement Execution.....	136
11.4	Retirement Reporting.....	137
11.5	Lessons Learned and Improvements.....	137

Management Appendices

12 Appendix M1 – Quality by Design (QbD)	139
12.1 Introduction	139
12.2 General Considerations	139
13 Appendix M2 – Supplier Management	143
13.1 Introduction	143
13.2 Concept Phase	143
13.3 Project Phase	145
13.4 Operation Phase	146
13.5 Retirement Phase	147
14 Appendix M3 – Science-Based QRM	149
14.1 Introduction	149
14.2 Guidelines and Regulations	149
14.3 Benefits	150
14.4 Roles and Responsibilities	151
14.5 Scalability of the Process	154
14.6 Applying Risk Management Based on the Business Process	154
14.7 Risk Management Throughout the System Life Cycle	154
14.8 Hazard Identification Method	159
14.9 Risk Assessment Methods	160
14.10 Selection and Use of Controls	161
14.11 Residual Risk	163
14.12 Scaling Life Cycle Activities	163
14.13 Risk Communication and Documentation	163
14.14 Risk Management for Outsourced Activities	163
14.15 Risk Review	163
14.16 Risk Considerations when Applying XAI	164
14.17 Examples	164
15 Appendix M4 – Critical Thinking	167
15.1 Introduction	167
15.2 Concept Phase Considerations	169
15.3 Project Phase Considerations	169
15.4 Operation Phase Considerations	169
15.5 Retirement Phase Considerations	170
15.6 QRM Considerations	170
15.7 Supplier Assessment and Selection	170
15.8 Inspection Readiness	171
16 Appendix M5 – Knowledge Management and Building AI Literacy	173
16.1 Introduction	173
16.2 Knowledge Management	173
16.3 Building AI Literacy	175
17 Appendix M6 – Fit for Purpose Data and Data Quality	179
17.1 Introduction	179
17.2 Fit for Purpose Data	179
17.3 Data Quality	181

18 Appendix M7 – Data and Model Governance and Management	185
18.1 Introduction	185
18.2 Data and Model Governance Framework	186
18.3 Data Management	187
18.4 Data Access and Provision	190
18.5 Data Cleansing and Data Transformation	191
18.6 Data Augmentation	193
18.7 Model Management	194
18.8 Data Operations and Implications on Models	194
18.9 Roles and Responsibilities	197
18.10 Scaling of AI Use Cases	198
18.11 Data Sharing and Federated Learning	198
19 Appendix M8 – IT Infrastructure	199
19.1 Introduction	199
19.2 Data Storage	200
19.3 Data Catalog and Metadata Management	202
19.4 Data Collection and Ingestion	202
19.5 Data Pre-Processing and Transformation	203
19.6 Data Versioning	203
19.7 Data Security and Compliance	203
19.8 Data Pipeline Orchestration	204
19.9 Model and Artifact Management	204
19.10 Tracking of Iterative Experimentation	204
19.11 Model Monitoring and Drift Detection	205
19.12 Model Deployment and Serving	205
20 Appendix M9 – Trustworthy AI	207
20.1 Introduction	207
20.2 Human Autonomy and Control	207
20.3 Safety and Security	208
20.4 Fairness and Mitigation of Bias	208
20.5 Privacy and Data Protection	209
20.6 Transparency	209
20.7 Accountability	210
20.8 Sustainability	211
21 Appendix M10 – AI Maturity	213
21.1 Introduction	213
21.2 AI Sub-System Autonomy	213
21.3 AI Sub-System Adaptiveness	214
21.4 AI Maturity Levels	215
22 Appendix M11 – Categories of Software and Hardware	217
22.1 Introduction	217
22.2 Categories of Software	217
22.3 Categories of Hardware	218
22.4 Model Categories	219

Special Interest Topics Appendices

23 Appendix S1 – Organizational Changes.....	221
23.1 Introduction	221
23.2 General Considerations	221
24 Appendix S2 – AI Adoption and Challenges.....	223
24.1 Introduction	223
24.2 General Considerations	223
24.3 Challenges	224
25 Appendix S3 – Machine Learning (ML) Fundamentals	227
25.1 Introduction	227
25.2 Learning Strategies	227
25.3 Model Types	229
26 Appendix S4 – Explainable AI (XAI)	233
26.1 Introduction	233
26.2 XAI Principles	233
26.3 Stakeholder Contributions to XAI	234
26.4 XAI Methods	234
26.5 Use of Model Features for XAI	235
26.6 XAI Methods Based on Model Anatomy	235
26.7 Use of Proxy Models for XAI	235
27 Appendix S5 – Cybersecurity Challenges	237
27.1 Introduction	237
27.2 Data Protection, Privacy, and Confidential Information	237
27.3 Activities of Malevolent Actors	238
27.4 Software Supply Chains	238
27.5 Business Continuity	239
27.6 Moral and Ethical Considerations	239
27.7 Examples of Cybersecurity Threats	239
27.8 Cybersecurity Risk Mitigation	240
28 Appendix S6 – AI in and as Medical Devices	243
28.1 Introduction	243
28.2 Challenges in the Context of AI-Enabled Medical Devices	243
28.3 General Considerations	244
28.4 Governance	246
28.5 Design	249
28.6 Cybersecurity Aspects of AI in Medical Devices	251
28.7 Life Cycle Guidance	253
29 Appendix S7 – Statutes, Regulations, Standards, and Guidance.....	255

General Appendices

30 Appendix G1 – References	261
31 Appendix G2 – Glossary	273
31.1 Acronyms and Abbreviations	273
31.2 Definitions	276