

Contents

Chapter 1	How to Use this Book	1
1.1	Purpose and Scope	1
1.2	The Way It Was...	2
1.3	The Way It Should Be...	3
1.4	Book Structure: Life to Death of a CDS	3
1.4.1	Chapter Structure	4
1.4.2	Part 1: Understanding the Basics	6
1.4.3	Part 2: Planning the Work	7
1.4.4	Part 3: Selecting the System	8
1.4.5	Part 4: Risk, Traceability, Configuration, Installation and Integration	9
1.4.6	Part 5: User Acceptance Testing	10
1.4.7	Part 6: Supporting Documentation and System Release	10
1.4.8	Part 7: Maintaining the Validation Status	11
1.4.9	Part 8: Records Retention and System Retirement	12
1.4.10	Part 9: When All Else Fails: Retrospective Validation of a CDS	12
1.4.11	Ensuring Data Integrity	12
1.4.12	Importance of the Second Person Review in Ensuring Data Integrity	13
1.5	Use Your Organisation's Computer Validation Procedures	13
1.5.1	Terminology Used in this Book	14
1.6	Why Does it Take so Long to Validate a CDS?	14
1.6.1	CDS Validation: The Way It Is	14

RSC Chromatography Monographs No. 20

Validation of Chromatography Data Systems: Ensuring Data Integrity, Meeting Business and Regulatory Requirements, 2nd Edition

By R. D. McDowall

© R.D.McDowall, 2017

Published by the Royal Society of Chemistry, www.rsc.org

1.6.2	CDS Validation: The Way It Should Be	14
1.6.3	The Core System	15
1.7	Ten Critical Success Factors for Fast CDS Validation	16
1.7.1	Management Involvement and Backing	16
1.7.2	Dedicated Key Project Team Members	17
1.7.3	Use an Appropriate Life Cycle Model	17
1.7.4	Knowledge of the CDS Application	18
1.7.5	Active and Flexible Quality Assurance Involvement	18
1.7.6	Effective and Compliant IT Participation	18
1.7.7	Use the Supplier Effectively	19
1.7.8	Planning, Planning and Planning	20
1.7.9	Focus on the Core System	20
1.7.10	Get More from Less Testing	21
1.8	Assumptions, Exclusions and Limitations	21
Chapter 2	What is a CDS? The Past, Present and Future	22
2.1	Introduction to Chromatography Data Systems	22
2.2	What is a Chromatography Data System?	22
2.2.1	Types of Chromatography Data System	23
2.2.2	Naming Conventions	25
2.2.3	Data Acquisition Files	25
2.2.4	Instrument Control Files	26
2.2.5	Sequence File	27
2.2.6	Acquisition of Chromatographic Data	27
2.2.7	Management of Data: Database or Files?	28
2.2.8	Interpretation of Chromatographic Data	28
2.2.9	System Suitability Test (SST) Calculations	30
2.2.10	Calibration	30
2.2.11	User Defined Analytical Run Parameters	31
2.2.12	Collation of Results and Reports	32
2.2.13	Architecture of a Networked CDS	32
2.3	Evolution of Chromatography Data Systems	33
2.3.1	CDS: Where Have We Come From?	33
2.3.2	The Evolutionary Ages of CDS	34
2.4	Stone Age: Paper Based Peak Measurement Techniques	35
2.4.1	Cut and Weigh	36
2.4.2	Ruler and Pencil	36
2.4.3	Disk Integrator	37
2.4.4	Summary of Stone Age CDS	37
2.5	Bronze Age: Electronic Peak Measurement	38
2.5.1	Central Data Systems	38
2.5.2	Computing Integrators	38
2.5.3	Summary of Bronze Age CDS	39

2.6	Iron Age: Expansion to Include Instrument Control	40
2.6.1	Standalone PCs: Extension to Instrument Control	40
2.6.2	PC Client–Server Networks	40
2.6.3	Summary of Iron Age CDS	41
2.7	Technology Age: Electronic Working and Regulatory Compliance	41
2.7.1	Migrating from Paper to Electronic Records	41
2.7.2	Part 11 Regulatory Compliance Features	42
2.7.3	Compliant Electronic Working Practices	42
2.7.4	Summary of Technology Age CDS	42
2.8	Think When You Use a CDS	43
2.9	Quo Vadis CDS?	43
2.9.1	Networked CDS Architecture	44
2.9.2	Data Management <i>via</i> a Database	45
2.9.3	Independent IT Support	46
2.9.4	Interfaces to Instruments and Systems	47
2.9.5	Open Data File Formats	47
2.9.6	Method Development Function	47
2.9.7	Analytical Procedure Validation	48
2.9.8	Trending Analytical Data	48
2.9.9	Additional Functions for Electronic Working	50
2.9.10	Laboratory Investigation Module	51
2.9.11	Documenting Configuration Settings	51
2.9.12	Automated Instrument Qualification	52
2.9.13	Securing Metadata for Ensuring Data Integrity	53
2.9.14	Improved Audit Trail Review	53
2.9.15	Compliance Control in Unattended Analysis	54
	References	55
Chapter 3	Laboratory Informatics and the Role of a CDS	57
3.1	Laboratory Informatics Applications	57
3.1.1	Instrument Data Systems	58
3.1.2	Electronic Laboratory Notebooks (ELN)	58
3.1.3	Scientific Data Management Systems (SDMS)	59
3.1.4	Laboratory Information Management Systems (LIMS)	59
3.1.5	Application Convergence	60
3.1.6	Data Analysis Applications	60
3.2	Islands of Automation in an Ocean of Paper	61
3.2.1	The Current Situation	61
3.2.2	Interfacing Laboratory Informatics Applications	61

3.2.3	Why Interface Laboratory Informatics Applications?	62
3.2.4	Interfacing in Detail	62
3.2.5	Overview of Interfacing a CDS to a LIMS	63
3.3	The Role of a CDS in Laboratory Informatics	65
3.3.1	The Laboratory Jig-Saw	65
3.4	The Operating Principles of an Electronic Laboratory	65
3.4.1	Standalone Data Systems Cannot be Integrated into an Electronic Laboratory	66
3.5	Developing a Strategy for an Electronic Laboratory	67
3.6	Strategic Planning for an Electronic Laboratory	67
3.7	Systems and the Operating Principles of the Electronic Laboratory	68
3.8	Phased Implementation of Systems	70
3.9	Justification of Individual Systems	72
	References	73
Chapter 4	Applicable GXP Regulations and Guidance for CSV	74
4.1	When All Else Fails Read and Understand the Regulations	74
4.1.1	Why Read the Regulations?	74
4.1.2	Approach to Regulations in this Book	75
4.2	Regulations and Guidance Impacting Computerised Systems	76
4.2.1	Scope of Regulations and Guidance	76
4.2.2	Computerised Systems are Often Equated to Equipment or Apparatus	76
4.3	Good Manufacturing Practice (GMP) Regulations and Guidance	78
4.3.1	FDA Good Manufacturing Practice (GMP) 21 CFR 211	78
4.3.2	Update of 21 CFR 211: 2007–2008	81
4.3.3	Inspection of Pharmaceutical Quality Control Laboratories	82
4.3.4	Compliance Program Guidance 7346.832 for Pre-Approval Inspections (PAI)	83
4.3.5	FDA Guidance for Industry: Circumstances that Constitute Delaying, Denying, Limiting, or Refusing a Drug Inspection	84
4.3.6	European Union GMP Regulations	84
4.3.7	EU GMP Part 2 & ICH Q7: GMP for Active Pharmaceutical Ingredients	85
4.3.8	Japanese GMP Regulations	86

4.3.9	Japanese GMP Guidance for Computerised Systems	88
4.3.10	PIC/S Guidance on Computerised Systems in GXP Environments	89
4.3.11	PIC/S Guidance for Validation Master Plans	90
4.3.12	WHO GMP Recommendations	90
4.3.13	FDA Level 2 GMP Guidance Records and Reports	91
4.3.14	Good Automated Manufacturing Practice (GAMP) Guidelines	92
4.3.15	GAMP Good Practice Guide for Validation of Laboratory Computerised Systems	93
4.4	Medical Device Good Manufacturing Practice	93
4.4.1	An Overview of Medical Device Regulations	93
4.4.2	Quality System Regulation for Medical Devices: 21 CFR 820	94
4.4.3	FDA Guidance: General Principles of Software Validation	95
4.4.4	ISO 13485 and EN 62304	96
4.5	Good Laboratory Practice Regulations and Guidance	96
4.5.1	Overview of GLP	96
4.5.2	Aims of GLP	97
4.5.3	GLP Regulations and Guidance Reviewed	98
4.5.4	US Good Laboratory Practice Regulations for Non-Clinical Studies (21 CFR 58)	98
4.5.5	Japanese Good Laboratory Practice Regulations	99
4.5.6	OECD Good Laboratory Practice Regulations	99
4.5.7	OECD GLP Guidance Document Number 10	100
4.5.8	OECD GLP Guidance Document Number 17	102
4.5.9	WHO GLP Handbook Second Edition 2009	103
4.5.10	Drug Information Association (DIA) Red Apple Guidance 1988 and 2008	104
4.5.11	Swiss AGIT GLP Guidance Documents	105
4.6	Good Clinical Practice Regulations	107
4.6.1	ICH Good Clinical Practice	107
4.6.2	Good Clinical Laboratory Practice	108
4.6.3	FDA Guidance Computerised Systems in Clinical Investigations	109
4.7	21 CFR 11 – Electronic Records and Electronic Signatures Regulation	112
4.7.1	21 CFR 11 is an Integrated Regulation	112

4.7.2	Interpret 21 CFR 11 by the Applicable Predicate Rule	113
4.7.3	The Need for 21 CFR Part 11 Assessment of Software	114
4.7.4	Current FDA Activities on 21 CFR 11	115
4.8	European Union GMP Annex 11 and Chapter 4	115
4.8.1	Introduction	115
4.8.2	EU GMP Overview	116
4.8.3	Increased Scope of Annex 11	116
4.8.4	Risk Management Throughout the Life Cycle	117
4.8.5	New Roles and Responsibilities	117
4.8.6	Suppliers and Service Providers	118
4.8.7	Validation	119
4.8.8	Annex 11 Controls for Ensuring Data Integrity	120
4.8.9	Electronic Signatures	121
4.8.10	IT Support of Validated Computer Systems	121
4.8.11	Maintaining Validation	122
4.8.12	What has been Omitted in the New Annex 11?	122
4.8.13	EU GMP Chapter 4: Major Changes	123
4.8.14	Principle: Define Raw Data	123
4.8.15	Generation and Control of Documentation	124
4.8.16	Dead as a Dodo: My Raw Data are Paper	125
4.8.17	Retention of Documents	125
4.9	United States Pharmacopoeia <1058> on Analytical Instrument Qualification	126
4.9.1	Overview of USP General Chapters	126
4.9.2	Origins of USP <1058> on Analytical Instrument Qualification	127
4.9.3	AIQ Life Cycle	128
4.9.4	The Data Quality Triangle	129
4.9.5	Classification of Apparatus, Instruments and Systems	133
4.9.6	Problems with the Current USP <1058>	134
4.9.7	Progress Updating USP <1058>	136
4.9.8	What has Changed in the In-Process Revisions of USP <1058>?	137
4.9.9	Is the Proposed USP <1058> Better?	137
4.9.10	Definition of Qualification	137
4.10	GXP Regulations and Guidance Summary for Computerised Systems	141
	References	141

Chapter 5	Concepts of Computer Validation	147
5.1	Why Bother to Validate Your Software?	147
5.1.1	Investment Protection	147
5.1.2	Consistent Product Quality	148
5.1.3	Compliance with Regulations	148
5.1.4	Ensure Data Integrity	148
5.1.5	Protection of Intellectual Property	148
5.2	What is Computerised System Validation (CSV)?	148
5.2.1	Definitions of Computerised System Validation	148
5.2.2	Key Concepts of Computer Validation	149
5.3	What is a Computerised System?	150
5.4	What Computer Validation is and is not	152
5.4.1	Principles of Computer Validation	152
5.4.2	Computer Validation Assumptions and Misconceptions	152
5.4.3	Problems with Computer Validation	152
5.5	Corporate Computer Validation Policy	157
5.6	Changing Approaches to CSV Due to Data Integrity Issues	159
5.6.1	Traditional Computerised System Validation	159
5.6.2	Process, Process, Process	160
5.6.3	A Validated System with Vulnerable Records Means Data Integrity Problems	162
5.6.4	Back to the Future?	162
5.6.5	Brave New CSV World?	163
5.6.6	Turning principles into practice	164
	References	165
Chapter 6	Understanding Software Categories and System Life Cycles	167
6.1	What Do the Regulators Want?	167
6.1.1	EU GMP Annex 11	167
6.1.2	FDA Guidance on General Principles of Software Validation	168
6.1.3	Regulatory Summary	168
6.2	Business Rationale	168
6.3	GAMP Software Categories	169
6.3.1	Origins of the GAMP Guide	169
6.3.2	GAMP 5 Software Classification Categories	169
6.3.3	Why Classify Software?	171
6.4	Software Classification Changes and their Laboratory Impact	171

6.4.1	Category 1: Greatly Expanded Scope – Infrastructure Software	171
6.4.2	Category 2: Ignore the Discontinuation of Firmware Classification – but with Care	173
6.4.3	Software Silos or Software Continuum?	176
6.4.4	Category 3 Software: What’s in a Name?	176
6.4.5	Category 4: Configured Products Refined	177
6.4.6	Category 4 and 5 Software: Configure <i>Versus</i> Customise – Where is the Line?	177
6.4.7	Category 5: Custom Applications, Macros and Modules	178
6.4.8	Users and the Software Screw-Up Factor	179
6.4.9	A Modified Software Classification	181
6.4.10	Do Not Use the Term COTS Software	182
6.5	Why is a System Life Cycle Model Important?	182
6.5.1	Overview	182
6.5.2	Using V Life Cycle Models	183
6.5.3	Do Not Forget Validation Control	184
6.5.4	Category 3 Life Cycle Model	185
6.5.5	Category 4 Life Cycle Model – Complex Version	185
6.5.6	Category 4 Life Cycle Model – Simple Version	187
6.5.7	System Life Cycle Summary	188
6.6	Defining the Documentation for a CDS Validation	188
6.6.1	A CDS is GAMP Category 4 Software	188
6.6.2	Compliance Health Warning	190
6.6.3	Interpreting the System Life Cycle Deliverables for a CDS	190
6.6.4	Document Controls	190
	References	193
Chapter 7	Ensuring Data Integrity for Chromatography Data Systems	194
7.1	What the Regulators Want	194
7.1.1	EU Good Manufacturing Practice	194
7.1.2	EU GMP Chapter 4 on Documentation	195
7.1.3	Overview of Regulatory Guidance for Data Integrity	195
7.1.4	FDA Compliance Program Guide 7346.832 on Pre Approval Inspections	197
7.1.5	PIC/S Guidance Documents	198
7.1.6	FDA Level 2 Guidance	198
7.1.7	Delaying, Denying, Limiting or Refusing an FDA Inspection	199

7.1.8	MHRA GMP Data Integrity Guidance	199
7.1.9	WHO Guidance on Good Data and Records Management Practices	200
7.1.10	FDA Guidance on Data Integrity and Compliance with cGMP	201
7.1.11	Regulations and Regulatory Guidance Summary	202
7.2	What is Data Integrity?	202
7.2.1	A Plethora of Definitions	202
7.2.2	What do the Definitions Mean?	202
7.2.3	Criteria for Integrity of Laboratory Data	203
7.3	Chromatography Data Systems in Falsification and Fraud	204
7.3.1	A Brief History of Data Falsification and Testing into Compliance	204
7.3.2	Able Laboratories Fraud Case 2005	204
7.3.3	Overview of Regulatory Citations for CDS in FDA Warning Letters	206
7.3.4	Quality Management System Failures	207
7.3.5	Equipment Citations	208
7.3.6	Citations for Lack of Laboratory Controls	209
7.3.7	Failure to Have Complete Laboratory Records	210
7.4	A Data Integrity Model	211
7.4.1	The Concept of Data Governance	211
7.4.2	Layers of Data Integrity	212
7.4.3	Focus on the Laboratory Levels of the Data Integrity Model	213
7.4.4	Foundation Layer: Right Corporate Culture for Data Integrity	213
7.4.5	Layer 1: Right Instrument and System for the Job	216
7.4.6	Layer 2: Right Analytical Procedure for the Job	216
7.4.7	Layer 3: Right Analysis for the Right Reportable Result	217
7.4.8	Linking the Data Integrity Model to the Analytical Process	217
7.4.9	Quality No Longer Owns Quality	219
7.5	Environmental Analysis and an Approach to Data Integrity	219
7.5.1	Background to EPA and Data Integrity	219
7.5.2	NELAC and Laboratory Accreditation	220
7.5.3	NELAC Quality System	220
7.5.4	NELAC Data Integrity Training	222
7.6	Data Integrity Foundation: Data Governance	223

7.6.1	Management Leadership and Oversight	226
7.6.2	Data Integrity Policy	226
7.6.3	Regulatory Requirements for GMP Training	227
7.6.4	Data Integrity Policy Training	229
7.6.5	Open Culture	231
7.6.6	Good Documentation Practice Training	231
7.6.7	Data Integrity Training for a Chromatography Data System: Operational SOPs	232
7.6.8	Data Integrity Audits and Investigations	232
7.7	Establishing Data Criticality and Inherent Integrity Risk	234
7.7.1	Regulatory Background	234
7.7.2	Spectrum of Laboratory Processes and Systems	235
7.7.3	The Data Life Cycle	237
7.7.4	Managing the CDS Data: Data Owners and Data Stewards	239
7.7.5	System Assessment and Remediation	240
7.8	CDS Compliance Commandments	242
7.8.1	Management are Responsible	243
7.8.2	Understand the Applicable Regulations for Laboratory Records	243
7.8.3	Use a CDS that is Networked and Uses a Database	246
7.8.4	Document the CDS Application Configuration Settings	246
7.8.5	Work Electronically	246
7.8.6	Identify Each User Uniquely and have Adequate Password Controls	246
7.8.7	Separate Roles with Different Access Privileges	247
7.8.8	Define Methods that Can and Cannot be Modified	248
7.8.9	An SOP for Chromatographic Integration	248
7.8.10	Control Changes to the System	248
7.8.11	Only Trained Staff Must Operate the System	249
7.8.12	Define and Document Electronic Records for the System	249
7.8.13	Review the Audit Trail Entries for Each Batch	251
7.8.14	Backup the System Regularly	251
7.8.15	Conduct Data Integrity Audits	252
7.8.16	Control Blank Forms	252
7.9	Audit Trails and an Introduction to Second Person Review	254
7.9.1	EU GMP Annex 11	254

7.9.2	FDA Guidance on Data Integrity and cGMP Compliance	254
7.9.3	Which Audit Trail Should Be Reviewed?	255
7.9.4	How Regular is a Regular Review of Audit Trail Entries?	256
7.10	Is The Chromatographic System Ready to Run?	259
7.10.1	“Test” or “Prep” Injections Using Samples	259
7.10.2	FDA Guidance for Using Actual Samples for SST Injections	259
7.10.3	Role of System Evaluation Injections	260
	References	261
Chapter 8	CDS Validation: Managing System Risk	266
8.1	What Do the Regulators Want?	266
8.1.1	EU GMP Annex 11	266
8.1.2	FDA Guidance on Part 11 Scope and Application	267
8.1.3	FDA General Principles of Software Validation	267
8.1.4	PIC/S Guidance on Computerised Systems in GXP Environments	267
8.1.5	OECD Guidance 17 on Application of GLP Principles to Computerised Systems	267
8.1.6	Regulatory Summary	268
8.2	Risk Management: Balancing Compliance and Non-Compliance	269
8.3	Overview of a System Risk Assessment	270
8.3.1	Overview of the Laboratory Risk Assessment	270
8.3.2	USP <1058> Based Integrated AIQ and CSV Risk Assessment	271
8.3.3	Risk Assessment Flow Chart	273
8.3.4	Define the Item and the Intended Use	274
8.3.5	Does the Item Carry Out Any GXP Work?	274
8.3.6	Identification of Software, Apparatus, Instrument or System?	276
8.3.7	Separating Instruments from Systems	277
8.3.8	Group C Systems – Documenting the GAMP Software Category	277
8.3.9	Group C Systems: Determining the Record Impact	280
8.3.10	Group C System Sub-Classification	280
	References	282

Chapter 9	Working Electronically and Using Electronic Signatures	284
9.1	What Do the Regulators Want?	285
9.1.1	EU GMP Annex 11	285
9.1.2	21 CFR 11 Main Electronic Signature Requirements	285
9.1.3	Signature Requirements in GXP Regulations	286
9.1.4	21 CFR 11 is an Integrated Regulation	286
9.1.5	FDA GMP Regulations: Number of Signatures and Order of Signing	286
9.1.6	Regulations Summary	287
9.2	Process Redesign is Essential for Working Electronically	287
9.2.1	Rationale for Using Electronic Signatures	287
9.2.2	Understand the Current Process	288
9.3	Process Mapping and Analysis	288
9.3.1	Importance of Understanding the Process	288
9.3.2	Map the Current Process	289
9.3.3	Other Benefits from Redesigning the Process	289
9.3.4	Leverage Benefits from Other Laboratory Applications	293
9.4	Case Study Descriptions	293
9.4.1	Case Study 1	293
9.4.2	Case Study 2	296
9.5	Optimising the Workflow for Electronic Signatures – Case Study 1	296
9.5.1	The Current Process	296
9.5.2	Basic Process Improvement Ideas	297
9.5.3	The Redesigned Process	297
9.6	Optimising the Workflow for Electronic Signatures – Case Study 2	298
9.6.1	The Current Process	298
9.6.2	The Redesigned Process	299
9.7	Using the CDS for Automated Compliance	300
9.8	Implementing Electronic Signatures Successfully	300
9.8.1	Understand the Process	300
9.8.2	Electronic Signatures Components	301
	References	302
Chapter 10	Writing the User and System Requirements	303
10.1	What Do the Regulators Want?	303
10.1.1	FDA GMP and GLP Predicate Rules	303
10.1.2	EU GMP Annex 11	303

10.1.3	PIC/S Guide Computerised Systems in GXP Environments	304
10.1.4	General Principles of Software Validation	304
10.1.5	Regulatory Summary	304
10.2	Business Rationale for Writing a URS	304
10.3	Contents of a Chromatography Data System URS	305
10.3.1	Writing a URS to Select a CDS and Supplier	305
10.3.2	Link the URS to a Specific Software Version	306
10.3.3	Sections of the URS	306
10.4	Guidance for Writing the Requirements	309
10.4.1	Sub-Divide the Major URS Sections	309
10.4.2	General Guidance for Requirements	309
10.4.3	URS Issues to Consider	310
10.4.4	Making the Requirements Traceable	311
10.4.5	Reviewing the URS	312
10.5	Writing Testable or Verifiable Requirements	312
10.5.1	How Not To Do It	312
10.5.2	Writing Well-Formed Requirements	313
10.5.3	Orphan Requirements	315
10.5.4	Key Criteria for User Requirements	315
10.6	Updating the URS	316
10.6.1	A URS is a Living Document	316
10.6.2	Maintaining Traceability with URS Updates	316
10.6.3	Helping the Reviewers of the Updated URS	316
10.7	Configuration Specification	317
10.7.1	Areas for Application Configuration in a CDS	317
	References	318
Chapter 11	Controlling the Validation	319
11.1	What Do The Regulators Want?	319
11.1.1	EU GMP Annex 11	319
11.1.2	EU GMP Annex 15 – Qualification and Validation	320
11.1.3	General Principles of Software Validation	320
11.1.4	PIC/S Guidance Document	320
11.1.5	Regulatory Requirements Summary	320
11.2	Validation Plan or Validation Master Plan?	321
11.2.1	What's in a Name?	321
11.2.2	Relationship Between a Validation Master Plan and Validation Plan	321
11.3	Content of the Validation Plan	322
11.3.1	Title of the Validation Plan: Include the Name and Version of the Application	323
11.3.2	Purpose of the Plan and Scope of the System	324

11.3.3	When to Write the Validation Plan?	324
11.3.4	Do not Include a System Description	325
11.3.5	Project Plan and Overall Timescales	325
11.3.6	One Validation Plan for the System Life or one for Each Software Version?	326
11.3.7	Roles and Responsibilities	326
11.3.8	Validation Team Considerations	328
11.3.9	Defining Life Cycle Tasks	329
11.4	Defining a Validation Strategy for Some CDS Systems	330
11.4.1	Validation Strategy for Four Instances of a CDS	331
	References	332
Chapter 12	System Selection	333
12.1	What Do the Regulators Want?	333
12.1.1	EU GMP Annex 11	333
12.1.2	PIC/S Guidance PI-011	334
12.1.3	Regulations Summary	334
12.2	Investment Protection <i>Versus</i> Seduction by Technology	334
12.3	The System Selection Process	335
12.3.1	Write an Initial URS for Selecting the System	335
12.3.2	Generate a List of Potential Suppliers	335
12.3.3	Determine Selection Criteria and Evaluation Tests Now	335
12.3.4	Prepare the Invitation to Tender/Request for Proposal	337
12.3.5	Evaluate the Supplier ITT Responses	338
12.3.6	Testing Systems Against Your Requirements	338
12.3.7	Consider User Training Now!	339
12.3.8	Visit or Talk with Existing Users	339
12.3.9	System Selection and Report	339
	References	340
Chapter 13	Assessing the CDS Supplier	341
13.1	What Do the Regulators Want?	341
13.1.1	EU GMP Annex 11	341
13.1.2	Preamble to 21 CFR 11 Final Rule	342
13.1.3	PIC/S Guide on Computerised Systems in GXP Environments	342
13.1.4	Regulatory Requirements Summary	342

13.2	Software Quality and Business Risk	343
13.3	Rationale for a Supplier Assessment	343
13.3.1	ISO 9000: Saint or Sinner?	343
13.3.2	ISO 9001 and ISO 9003	344
13.3.3	Supplier Certificates of Validation	345
13.3.4	Marketing Literature and Contracts	346
13.4	When Do I Assess the CDS Supplier?	346
13.4.1	First, Second or Third Party Assessment or Audit?	347
13.4.2	On-Site Audit or Remote Assessment?	347
13.4.3	Remote Supplier Audit	347
13.4.4	Remote Assessment with Follow-Up Conference Call	348
13.5	On-Site Supplier Audits	349
13.5.1	Preparation for an Audit	349
13.5.2	The Scope of an On-Site Audit	351
13.5.3	The Role of an Audit Checklist	353
13.5.4	Software Development – The Move to Agile	354
13.5.5	Writing the Audit Report	355
13.6	Using the Supplier Audit to Reduce PQ Testing	356
	References	357
Chapter 14	Negotiating the Contract and Purchasing the System	358
14.1	What Do the Regulators Want?	358
14.1.1	EU GMP Annex 11	358
14.1.2	Regulatory Requirements Summary	359
14.2	The Contract and Protection of Rights	359
14.2.1	Rationale for Negotiating the Contract	359
14.2.2	Overview of the Contract	359
14.2.3	Some Key Clauses of a Contract	360
14.3	Purchase Order: Defining the Initial Configuration	363
	References	363
Chapter 15	Planning the Installation of the System	364
15.1	What Do the Regulators Want?	364
15.1.1	US GMP 21 CFR 211: Subpart D – Equipment	364
15.1.2	EU GMP Chapter 3: Premises and Equipment	364
15.1.3	Regulatory Summary	365
15.2	Business Rationale for an Installation Plan	365
15.3	Preparing for System Installation	365
15.3.1	The CDS System Installation Plan	365
15.3.2	Laboratory Plan	366
	References	367

Chapter 16	CSV Risk Management Requirements Level Assessment	368
16.1	What Do the Regulators Want?	368
16.1.1	EU GMP Annex 11	368
16.1.2	FDA Guidance for Industry: Part 11 Scope and Application	369
16.1.3	PIC/S Guidance on Computerised Systems in GXP Environments	369
16.1.4	FDA General Principles of Software Validation	369
16.1.5	Regulatory Requirements Summary	369
16.2	You Need a Current URS Before Starting the Risk Assessment	370
16.2.1	Train Key Users	370
16.2.2	Understanding the New CDS System or Version	370
16.2.3	Stop Here Until You Have a Current URS	371
16.2.4	Revised URS? Update the Risk Assessment!	371
16.3	Risk Management Approach	371
16.3.1	Vocabulary Issues	372
16.3.2	ISO Guide 73 and ISO 14971: Risk Management Definitions	372
16.3.3	Risk Assessment is a Continuous Process	373
16.3.4	Application of Risk Assessment to a CDS	373
16.4	Risk Assessment at the Requirements Level	373
16.4.1	Outcome of Risk Management	373
16.4.2	Possible Risk Assessment Methodologies	373
16.4.3	Team Approach to Risk Assessment	374
16.5	Functional Risk Assessment (FRA)	375
16.5.1	Risk Analysis of Individual Functions	375
16.5.2	Managing the Mandatory and Critical Requirements	378
16.5.3	Allocating Requirements to Test Scripts	379
16.5.4	Application of FRA	379
16.6	Failure Mode Effects Analysis (FMEA)	379
16.6.1	Overview of FMEA	379
16.6.2	Conducting an FMEA Risk Assessment	380
16.6.3	An Example FMEA Assessment	382
16.6.4	Limitations of FMEA	384
16.7	Risk Acceptance and Risk Communication	384
	References	384
Chapter 17	Importance of the Traceability Matrix	386
17.1	What Do the Regulators Want?	386
17.1.1	EU GMP Annex 11	386
17.1.2	General Principles of Software Validation	386

17.1.3	PIC/S Guide PI-011: Computerised Systems in GXP Environments	387
17.1.4	Regulations Summary	387
17.2	Business Rationale for a Traceability Matrix	387
17.2.1	GAMP 5	388
17.3	A Life Cycle Model Refresher	388
17.3.1	Terms and Definitions	389
17.3.2	Why Bother to Trace Requirements?	390
17.4	Linking Requirements with Their Testing or Verification	392
17.5	Examples of Requirements Traceability	394
17.5.1	Traceability Between the URS and the Configuration Specification	394
17.5.2	Traceability Matrix Combined with Functional Risk Assessment	395
17.5.3	How Detailed Should User Acceptance Testing Traceability Be?	396
17.6	Using a Spreadsheet to Manage Traceability	398
17.6.1	Evolution and Further Refinement of User Requirements	400
17.7	The Traceability Treadmill?	401
	References	401
Chapter 18	Writing Configuration Specifications	403
18.1	What Do the Regulators Want?	403
18.1.1	FDA GMP Regulations	403
18.1.2	General Principles of Software Validation	404
18.1.3	Regulatory Requirements Summary	404
18.2	Business Rationale	404
18.3	Scope of CDS Configuration and Approach to Documentation	404
18.3.1	Application Configuration Areas of a CDS	404
18.3.2	Never Use Unconfigured CDS Software	405
18.3.3	Ways of Documenting Application Configuration	405
18.4	Application Configuration Specification	406
18.4.1	Training to Understand CDS System Settings	406
18.4.2	Prototype the Configured System	406
18.4.3	Document the Configuration	407
18.4.4	Defining User Types and Access Privileges	407
18.4.5	Ensure Linkage Between the URS and Configuration Specification	408
18.4.6	Confirming the Application Configuration	409
18.5	Controlling CDS Configuration by Procedure	409
	References	411

Chapter 19	Writing the Technical Specification	412
19.1	What Do the Regulators Want?	412
19.1.1	EU GMP Annex 11	412
19.1.2	FDA GMP 21 CFR 211	412
19.1.3	Regulatory Summary	413
19.2	Data Gathering for a Technical Specification	413
19.2.1	Input from the CDS Supplier	413
19.2.2	Corporate IT/IS Standards	414
19.2.3	URS Requirements	414
19.3	Initial Platform Design	415
19.4	Writing the Technical Specification	415
19.4.1	Hardware Architecture	415
19.4.2	Connections and Communications	417
19.4.3	Input into the Installation Qualification Phase	417
	References	417
Chapter 20	Installing and Integrating System Components	418
20.1	What Do the Regulators Want?	419
20.1.1	US GMP 21 CFR 211	419
20.1.2	EU GMP Chapter 3: Premises and Equipment	419
20.1.3	EU GMP Annex 11: Computerised Systems	419
20.1.4	PIC/S Guidance PI-011	419
20.1.5	USP <1058> Analytical Instrument Qualification	420
20.1.6	General Principles of Software Validation	420
20.1.7	Regulatory Summary	420
20.2	Overview of the Whole Qualification Process	420
20.3	Installing and Integrating the System Components	421
20.3.1	Co-Ordinating Suppliers	421
20.3.2	Computer Platform	422
20.3.3	CDS Application Components and Associated Documentation	422
20.3.4	Qualification of the Laboratory Data Servers	424
20.3.5	Connection and Qualification of Chromatographs	424
20.3.6	Establish the Initial CDS Configuration Baseline Now	425
20.4	How Much Value is there in a Software OQ?	425
20.4.1	Positioning of a Software Operational Qualification	425
20.4.2	Is an OQ Essential for a CDS Validation Project?	426

<i>Contents</i>	xxxi
20.4.3 An OQ Case Study	428
20.4.4 Do You Believe in Risk Management?	428
20.4.5 OQ for Configurable Software?	429
References	430
Chapter 21 Designing the User Acceptance Test Suite	431
21.1 What Do the Regulators Want?	432
21.1.1 EU GMP Annex 11	432
21.1.2 FDA General Principles of Software Validation	432
21.1.3 Regulatory Requirements Summary	432
21.2 Overview of the User Acceptance Testing Phase of Validation	433
21.2.1 Who Are You Writing the Test Documents For?	434
21.2.2 UAT/PQ Test Plan	434
21.2.3 Writing the Test Scripts	434
21.2.4 Executing the Test Scripts	435
21.3 The UAT/PQ Test Plan	435
21.3.1 Format of a Test Plan	435
21.3.2 Test Environment	436
21.3.3 Confirming the CDS Application Configuration	436
21.3.4 Overview of the Test Suite	436
21.3.5 Further Testing Considerations	439
21.3.6 Implementation Strategy 1: Same System Multiple Sites	440
21.3.7 Implementation Strategy 2: Single Instance with Phased Roll-Out	441
21.3.8 Tracing User Requirements to PQ Testing	441
21.3.9 Assumptions, Exclusions and Limitations of the Test Approach	442
21.3.10 Features Not Tested	443
21.3.11 Test Approach	444
21.4 Authorising the Test Plan and Test Scripts	445
21.4.1 PQ Test Plan	445
21.4.2 UAT Test Scripts	445
References	446
Chapter 22 Writing Test Scripts and Test Cases	447
22.1 What Do the Regulators Want?	447
22.1.1 EU GMP Annex 11	447
22.1.2 FDA General Principles of Software Validation	448

22.1.3	Regulatory Requirements Summary	448
22.2	Principles of Software Testing	448
22.2.1	Essentials of Software Testing	448
22.2.2	White Box and Black Box Testing	448
22.2.3	Understanding How the CDS Application Works	450
22.2.4	Test Coverage	451
22.2.5	Manual or Automated Testing?	451
22.2.6	Necessity for Pre-Defined Expected Results and Acceptance Criteria	452
22.2.7	Updating the URS During the UAT Phase	452
22.3	Functional and Non-Functional Testing of a CDS	453
22.3.1	Risk Assessment: Extent of Testing?	453
22.3.2	Functional Testing	454
22.3.3	Non-Functional Testing	455
22.4	UAT Test Script Structure and Contents	455
22.4.1	Purpose of the Test	455
22.4.2	Requirements to be Tested and Limitations to the Testing	455
22.4.3	Test Preparation	458
22.4.4	Identification of Personnel	459
22.4.5	Test Procedures	460
22.4.6	Collecting and Collating Documented Evidence	461
22.4.7	Acceptance Criteria	462
22.4.8	Test Execution Log	463
22.4.9	Test Summary Log and Test Script Sign-Off	463
22.4.10	Second Person Review of the Test Script	464
22.4.11	Approval of the Test Script	464
22.5	Designing Tests for Security and Access Control	464
22.5.1	Are the User Requirements Adequately Specified?	464
22.5.2	Logical Security	465
22.5.3	Access Control	465
22.5.4	Designing the Tests	466
22.5.5	Refining the Test Design	467
22.5.6	Writing Test Execution Instructions and Expected Results	468
22.6	Some Considerations for Testing Electronic Signature Use	470
22.7	Execution of Approved Test Scripts	470
	References	470
Chapter 23	Executing Test Scripts and Reporting the Results	472
23.1	What Do the Regulators Want?	472
23.1.1	EU GMP Annex 11	472

23.1.2	FDA General Principles of Software Validation	473
23.1.3	Regulatory Requirements Summary	473
23.2	Organising the Test Suite Execution	473
23.2.1	Planning the Test Suite Execution	473
23.2.2	Have a Known Location for Collating and Reviewing Test Results	474
23.2.3	Test Script Execution Status Board	474
23.3	Executing a Test Script	475
23.3.1	All is Well or Are There Problems?	475
23.3.2	Read the Test Script	476
23.3.3	Preparation for Testing	477
23.3.4	Sign into the Test Script	477
23.3.5	Execute the Individual Test Procedures and Document the Testing	478
23.3.6	Documented Evidence to Support Testing	478
23.3.7	Collating Documented Evidence	480
23.3.8	Has the Test Passed or Failed?	480
23.3.9	Documenting and Handling Unexpected Results	480
23.3.10	Check the Test Execution Log	481
23.3.11	Tester Completes the Test Summary Log and Signs the Test Script	481
23.3.12	Update the Test Script Execution Status	481
23.4	Reviewing the Completed Test Script	481
23.4.1	Role of the Reviewer	481
23.4.2	Correcting Any Mistakes	482
23.4.3	Resolving Any Disagreements	482
23.4.4	Approving the Test Script Execution and Update the Test Script Execution Status	482
23.4.5	Enter the Test Script Result into the PQ Section of the Validation Summary Report	482
	References	483
Chapter 24	User Training and System Documentation	484
24.1	What Do the Regulators Require? Part 1	484
24.1.1	EU GMP Annex 11	484
24.1.2	FDA 21 CFR 11	484
24.1.3	FDA 21 CFR 211 GMP	485
24.1.4	FDA 21 CFR 58 GLP	485
24.1.5	Regulatory Requirements Summary	485
24.2	Personnel and Training Records	485
24.2.1	Personnel Involved in a CDS Validation Project	485
24.2.2	User Training Records	486

24.3	URS Requirements Define CDS Procedures	487
24.3.1	Proactive Use of Requirements for Procedures	487
24.3.2	Challenge Existing SOPs with CDS Procedural Requirements	487
24.3.3	Confirm Accuracy of CDS Procedures in the UAT Phase	488
24.4	System Documentation from the Supplier	488
24.5	Standard Operating Procedures (SOPs) for a CDS	489
24.5.1	SOPs for a CDS in Relation to a Company Data Governance Framework	489
24.5.2	Good Chromatographic Practices	491
24.5.3	Good Chromatographic Integration Practices	492
24.5.4	Good Analytical Data Review Practices	493
24.5.5	Laboratory Deviations and Laboratory Investigations SOPs	493
24.5.6	Training for Data Integrity SOPs	494
24.5.7	SOP for Laboratory Administration of the CDS	494
24.6	Managing Custom Calculations, Fields and Reports	495
24.6.1	Development Environment	495
24.6.2	Control of Custom Calculations and Fields	495
24.6.3	Control of Custom Reports	496
24.6.4	Control Changes of Verified Custom Calculations and Reports	496
24.7	Second Person Review of CDS Data and Records	496
24.7.1	Importance of the Second Person Review	497
24.7.2	What Do the Regulators Require? Part 2	497
24.7.3	Scope of the Second Person Review	499
24.7.4	A CDS Interfaced with a LIMS	499
24.7.5	Second Person Review in Practice	501
24.7.6	Using the CDS Features to Aid Second Person Review	504
24.7.7	How Should the Second Person Review be documented?	504
24.8	Administrative and Procedural Controls Required for 21 CFR 11 Compliance	507
24.8.1	Verifying the Identity of Individuals	508
24.8.2	Use of Electronic Signatures with Non Repudiation	509
24.8.3	Uniqueness of Electronic Signatures	509
24.8.4	Password Management	509
24.8.5	Change Control and Configuration Management	510

24.8.6	Date and Time Stamps	510
24.8.7	Backup and Recovery SOP	510
24.8.8	Defining E-Records for the CDS	511
24.8.9	Security and Access Control	511
24.8.10	Remote Access	511
	Acknowledgements	512
	References	512
Chapter 25	IT Support for a CDS	513
25.1	What Do the Regulators Want?	513
25.1.1	FDA GMP 21 CFR 211	513
25.1.2	21 CFR 11	514
25.1.3	EU GMP Annex 11	514
25.1.4	PIC/S Guidance	515
25.1.5	FDA Perspective on Time Stamps	516
25.1.6	Regulatory Requirements Summary	516
25.2	IT Department Quality Management System	517
25.2.1	Overview of the IT QMS	517
25.2.2	Associated QMS Procedures and Work Instructions	517
25.3	Service Level Agreement	520
25.4	Backup and Recovery	521
25.4.1	Business Rationale: How Important are Your Data?	521
25.4.2	What is Backup and Recovery?	522
25.4.3	Roles and Responsibilities	522
25.4.4	Hardware to Help Data Security and Integrity	523
25.4.5	Options to Consider for Backup	524
25.4.6	Main Backup Activities	525
25.4.7	Hot or Cold Backups?	526
25.4.8	Cold Backups	526
25.4.9	Hot Backups	527
25.4.10	Management of Magnetic Media	527
25.4.11	Restoring Data from Tape	528
25.4.12	Validation of Backup	529
25.5	Time and Date Stamps	529
25.5.1	Time Stamps for Standalone CDS Systems	529
25.5.2	Time Stamps for Networked CDS Systems	530
	References	530
Chapter 26	System Description	532
26.1	What Do The Regulators Want?	532
26.1.1	EU GMP Annex 11	532

26.1.2	OECD Application of GLP Principles to Computerised Systems	532
26.1.3	OECD 17: Guidance on the Application of GLP Principles to Computerised Systems	533
26.1.4	PIC/S Guidance	533
26.1.5	Regulatory Requirements Summary	534
26.2	Turning Regulations into Practice	534
26.2.1	Single Document or Multiple Documents?	534
26.2.2	Outline for a System Description	534
26.2.3	Keeping Current: Updating the System Description	535
26.3	Key Sections of the System Description	536
26.3.1	Introduction	536
26.3.2	System Scope	536
26.3.3	Definition of Electronic Records	538
26.4	Do Not be Stupid	538
	References	538
Chapter 27	Defining Electronic Records and Raw Data for a CDS	540
27.1	What Do the Regulators Want?	540
27.1.1	US GLP 21 CFR 58 – Raw Data	540
27.1.2	21 CFR 11 – Electronic Records	541
27.1.3	US GMP 21 CFR 211 – Complete Data	541
27.1.4	EU GMP Chapter 4 on Documentation – Raw Data	541
27.1.5	Regulatory Requirements Summary	542
27.2	Contributions to the E-Records Debate	542
27.2.1	Furman, Tetzlaff and Layloff	542
27.2.2	BARQA Paper on Raw Data	542
27.2.3	How Raw are Your Data? – 1	543
27.2.4	How Raw are Your Data? – 2	543
27.2.5	FDA Part 11 Scope and Application Guidance for Industry	544
27.2.6	FDA Level 2 Guidance on Records and Reports	546
27.2.7	EU GMP Chapter 4 – A Requirement to Define GMP Raw Data	548
27.2.8	GLP Raw Data Definition and Interpretation	549
27.2.9	Swiss AGIT GLP Electronic Raw Data Guidance	550
27.2.10	Compliance Policy Guide 7346.832	552
27.2.11	GAMP Good Practice Guide for Validation of Laboratory Computerised Systems	552

27.2.12	FDA Draft Guidance on Data Integrity and cGMP Compliance	553
27.2.13	Summarising the Regulations and Guidance	554
27.2.14	Dead as a Dodo: Raw Data are Paper	555
27.3	Defining the Electronic Records for Your System	555
27.3.1	Static and Dynamic Data	555
27.3.2	Data Acquisition Phase	555
27.3.3	Integration, Calculation and Reporting Phase	557
27.3.4	Traceability for Data Integrity	558
27.3.5	Common Elements of Raw Data and Complete Data	558
27.3.6	Controlled Chromatograph with Separate Data System	560
	References	560
Chapter 28	Writing the Validation Summary Report	562
28.1	What Do the Regulators Want?	562
28.1.1	PIC/S Guidance	562
28.1.2	General Principles of Software Validation	563
28.1.3	Regulatory Requirements Summary	563
28.2	Map the Validation Plan to the Validation Summary Report	563
28.3	Content of the Validation Summary Report	564
28.4	Writing the Validation Summary Report	564
28.4.1	How to Summarise the Work	564
28.4.2	How to Summarise PQ Testing	566
28.4.3	PQ Test Execution Notes	566
28.4.4	Deviations and Departures from the Validation Plan	567
28.4.5	Validation Package	567
28.4.6	Releasing the System	568
28.4.7	Going Live! Sit Back and Relax?	568
	References	568
Chapter 29	Integration in a Regulated Environment	569
29.1	What Do the Regulators Want?	569
29.1.1	US GMP 21 CFR 211 – Laboratory Controls	569
29.1.2	United States and European Pharmacopoeias	570
29.1.3	FDA Guidance for Industry Bioanalytical Methods Validation	570

29.1.4	EMA Guidance on Bioanalytical Methods Validation	570
29.1.5	Regulatory Summary	571
29.2	Why Control Chromatographic Integration?	571
29.2.1	Extracts from FDA Warning Letters	571
29.2.2	Approaches to Controlling Chromatographic Integration	572
29.3	Back to Integration Basics	573
29.4	How Can Manual Integration Result in Falsification?	576
29.4.1	Uncovering Manipulation	577
29.4.2	What is Missing?	577
29.4.3	Why is there No Definition of Manual Integration?	578
29.5	Scope of an SOP on Chromatographic Integration	578
29.5.1	Integration Process Flow and Decision Tree	579
29.5.2	Manual Intervention <i>versus</i> Manual Integration	581
29.6	The Four Eyes Principle Applied to Chromatographic Integration	582
29.6.1	The Primary Objective is Automatic Integration	582
29.6.2	The Secondary Objective is Manual Intervention	582
29.6.3	When All Else Fails – Manual Integration	582
29.6.4	Methods that Quantify Both Active Ingredient and Impurities	583
29.6.5	Procedure and Training for Integration Consistency and Data Integrity	583
29.6.6	Second Person Review of Integration	584
	References	584
Chapter 30	User Account Management	586
30.1	What Do the Regulators Require?	586
30.1.1	FDA GMP 21 CFR 211	586
30.1.2	FDA 21 CFR 11	586
30.1.3	FDA Guidance: Computerised Systems in Clinical Investigations	587
30.1.4	EU GMP Annex 11	587
30.1.5	MHRA Data Integrity Guidance	587
30.1.6	FDA Guidance on Data Integrity and cGMP Compliance	588
30.1.7	WHO Guidance on Good Data and Record Management Practices	589
30.1.8	Regulatory Summary	589

30.2	Principles of User Account Management	590
30.2.1	Prerequisites for User Account Management	590
30.2.2	Administration by IT	591
30.2.3	Authorised User	591
30.2.4	Individual User Accounts	591
30.2.5	Cumulative List of Users	592
30.2.6	Staff Security Awareness	592
30.2.7	Regular Review of Accounts	593
30.3	User Account Management in Practice	593
30.3.1	Process Workflow	593
30.3.2	Creation of a New User Account	594
30.3.3	Modification of an Existing User Account	594
30.3.4	Disabling a User Account	595
30.3.5	Maintaining a Cumulative List of Users	595
30.3.6	Periodic Review or Audit of User Accounts	595
30.4	Password Management	596
30.4.1	Technical Implementation and Enforcement	596
30.4.2	Password Paradox	596
30.4.3	Forgotten Password?	597
	References	597
Chapter 31	Incident and Problem Management	598
31.1	What Do the Regulators Want?	598
31.1.1	EU GMP Annex 11	598
31.1.2	OECD Guidance 17 for Computerised Systems	598
31.1.3	Regulatory Requirements Summary	599
31.2	Incidents and Problems	600
31.2.1	What is an Incident?	600
31.2.2	What is a Problem?	600
31.2.3	Incident <i>Versus</i> Problem	600
31.3	Coordination of Incident and Problem Management	601
31.3.1	Automation of the Process	601
31.3.2	Help Desk Staff	602
31.4	Incident Management	602
31.4.1	Incident Management Workflow	602
31.4.2	Procedure for Incident Management	603
31.4.3	Periodic Review of Incidents	604
31.5	Problem Management	604
31.5.1	Problem Management Workflow	604
31.5.2	Procedure for Problem Management	605
31.5.3	Problem Management and Regulatory Compliance	607
31.6	Linking Incident and Problem Management with Change Management	607
	References	607

Chapter 32	Change Control and Configuration Management	608
32.1	What Do the Regulators Want?	608
32.1.1	EU GMP Annex 11	608
32.1.2	FDA GMP 21 CFR 211	608
32.1.3	OECD Guidance No. 17 on Computerised Systems	609
32.1.4	FDA Guidance: General Principles of Software Validation	609
32.1.5	PIC/S Guidance for GXP Systems	610
32.1.6	Regulatory Requirements Summary	611
32.2	Scope of Changes to a CDS	612
32.2.1	Definition of Terms	612
32.2.2	Separate Infrastructure from Application Changes	615
32.2.3	Triggers for Change	616
32.2.4	Is it a Change or Normal Operation?	616
32.3	Change Control	617
32.3.1	The Basic Process	617
32.3.2	Types of Change	620
32.3.3	Roles and Responsibilities	621
32.4	Some Typical CDS Changes	621
32.4.1	Scope of Changes to the CDS	621
32.4.2	Regression Testing After a Change	623
32.5	Configuration Management for a CDS	623
32.5.1	Defining the Detail of Configuration Items	624
32.5.2	Defining the System Baseline Configuration	624
32.5.3	Linking Configuration Management with Change Control	625
32.5.4	Re-Baselining the System Configuration	625
32.6	Automating the Change Control Process	625
32.6.1	Does the Service Desk Software Need to be Validated?	626
32.6.2	IT Personnel Must Have GXP Awareness Training	626
32.6.3	Service Management Software as a SaaS Solution	626
	References	626
Chapter 33	Periodic Review of the CDS	628
33.1	What Do the Regulators Want?	628
33.1.1	EU GMP Annex 11	628
33.1.2	PIC/S Guidance on Computerised Systems in GXP Environments	629

33.1.3	ICH Q7 GMP for Active Pharmaceutical Ingredients	630
33.1.4	WHO Guidance on Good Data and Record Management Practices	630
33.1.5	Compliance Policy Guide Section 130.300	630
33.1.6	Regulatory Requirements Summary	631
33.2	Rationale for a Periodic Review	632
33.2.1	What's in a Name?	632
33.2.2	Who Performs the Review?	632
33.2.3	How Often Should the Review Occur?	633
33.2.4	Skills and Training of the Auditor	634
33.3	Overview of the Periodic Review Process	635
33.3.1	Objectives of a Periodic Review	635
33.3.2	Planning a Periodic Review	635
33.3.3	Who is Involved and What Do They Do?	636
33.3.4	Schedule for a Review	637
33.3.5	Scope of the Review	637
33.3.6	Reporting the Periodic Review and Follow-Up	639
33.4	Conducting a Periodic Review	640
33.4.1	Preparation for a Periodic Review	640
33.4.2	Defining the System Scope	641
33.4.3	Types of Periodic Review	643
33.4.4	Are Computerised Systems Designed to Help Periodic Reviews?	645
33.4.5	Conducting the Periodic Review	646
33.4.6	A Picture is Worth a Thousand Words	647
33.4.7	Death by Checklist?	647
33.4.8	Options for Checklists: Working Smarter Not Harder	648
33.5	Data Integrity Audit of a CDS	649
33.5.1	Data Integrity at the System Level	649
33.5.2	Data Integrity Audit at the Data Level	652
33.5.3	Data Integrity and an Interfaced CDS	652
33.5.4	Reporting the Audit	655
	References	655
Chapter 34	CDS Records Retention	657
34.1	What Do the Regulators Want?	657
34.1.1	EU GMP Annex 11	657
34.1.2	GLP Regulations: 21 CFR 58	657
34.1.3	US GMP Regulations: 21 CFR 211	658
34.1.4	US Medical Device GMP Regulations: 21 CFR 820	659

34.1.5	21 CFR 11 Requirements	659
34.1.6	FDA Guidance on Data Integrity	659
34.1.7	EU GMP Chapter 4 Documentation	659
34.1.8	FDA Guidance for Industry Part 11 – Scope and Application Guidance	660
34.1.9	FDA Inspection of Pharmaceutical Quality Control Laboratories	661
34.1.10	OECD GLP Regulations	661
34.1.11	OECD GLP Guidance on Establishment and Control of GLP Archives	662
34.1.12	OECD GLP Guidance on Application of GLP to Computerised Systems	662
34.1.13	Regulatory Requirements Summary	662
34.2	CDS Data File Formats and Standards	663
34.2.1	Current CDS Data Standards	663
34.2.2	Progress towards a Universal CDS Data File Format	664
34.3	Options for Electronic Records Retention and Archive	665
34.3.1	Backup is Not Archive (Unless You Are the FDA)	665
34.3.2	Organising CDS Electronic Records to Archive	666
34.3.3	Options for Electronic Archive	666
34.3.4	Can I Read the Records?	667
34.3.5	Impact of a Changed CDS File Format	668
34.3.6	Selection of Off-Line Archive Media	669
34.3.7	Changing CDS – What Are The Archive Options?	669
34.3.8	Overview of Some Options	669
34.3.9	Assessment of Option Feasibility	670
34.4	OECD Guidance for Developing an Electronic Archive	670
34.4.1	Definitions	670
34.4.2	Roles and Responsibilities	671
34.4.3	Archive Facilities	672
34.4.4	Archiving Electronic Records	672
	References	674
Chapter 35	CDS System Retirement	676
35.1	What Do the Regulators Want?	676
35.1.1	OECD GLP Guidance 17	676
35.1.2	GMP Regulations	676
35.1.3	Business Rationale for System Retirement	676

<i>Contents</i>	xliii
35.2 Generic Process for System Retirement	677
35.2.1 Notification of System Retirement	677
35.2.2 Involvement of Quality Assurance and IT	678
35.2.3 Cessation of Work	678
35.2.4 Shutdown of the System	679
35.2.5 Documenting Retirement and Disposal	679
35.3 Case Study of System Retirement	680
Reference	681
Chapter 36 CDS Data Migration	682
36.1 What Do the Regulators Want?	682
36.1.1 EU GMP Annex 11	682
36.1.2 EU GMP Chapter 4 on Documentation	683
36.1.3 FDA 21 CFR 11 and the Part 11 Scope and Application Guidance for Industry	683
36.1.4 OECD Guidance 17 Application of GLP Principles to Computerised Systems	683
36.1.5 Regulatory Requirements Summary	684
36.2 Business Rationale for Data Migration	684
36.3 Drivers for Data Migration and System Retirement	685
36.3.1 Internal Drivers	685
36.3.2 External Drivers	685
36.3.3 Data Migration Options	686
36.3.4 Data Migration Between Different Applications	686
36.3.5 Data Migration Within an Application	687
36.3.6 Validation of Within Application Data Migration	687
36.4 Generic Data Migration and System Retirement Process	687
36.4.1 Roles of the Process Owner and Senior Management	689
36.4.2 Step 1: Inventory of the System	689
36.4.3 Step 2: Carry Out a Risk Assessment	689
36.4.4 Step 3: Write the Retirement Plan	689
36.4.5 Step 4: Detailed Information Gathering	690
36.4.6 Step 5: System Decommissioning and Data Migration Plan	690
36.4.7 Step 6: Execute Work and Document Activities	690
36.4.8 Step 7: Write Retirement and Migration Report	690
36.5 Case Study of Data Migration	691
36.5.1 Design of the Overall Validation Project	691

36.5.2	Overview of the Mass Spectrometry Systems	692
36.5.3	Data Acquisition and Processing Software Applications	692
36.5.4	Computing Environments	692
36.5.5	Differences Between the Two CDS Systems	693
36.5.6	Data Migration Strategy	694
36.5.7	Supplier Supplied Data Conversion Utilities	694
36.5.8	Limitation of the Data Conversion Utilities	694
36.5.9	Data Migration Options	695
36.5.10	Evolution of the Data Migration Design	695
36.5.11	Design of the Overall Data Migration and System Retirement	696
36.6	Data Migration: Key Results	696
36.6.1	Retention Time	696
36.6.2	Instrument Control Parameters	697
36.6.3	Integration Algorithms and Calculated Results	698
36.6.4	History Logs	699
36.6.5	Data Migration Summary	700
	References	700
Chapter 37	Retrospective Validation	701
37.1	What Do the Regulators Want?	701
37.1.1	EU GMP Annex 11	701
37.1.2	EMA Annex 11 Questions and Answers	701
37.1.3	PIC/S Guidance	702
37.1.4	Regulatory Requirements Summary	703
37.2	Literature References to Retrospective CDS Validation	703
37.3	Gap and Plan for Retrospective Validation	703
37.3.1	Stage 1: Collect Existing Documentation and Review for Coverage	703
37.3.2	Phase 2: Review Existing Documents for Adequacy	705
37.3.3	Phase 3: Write the Gap and Plan Report	706
	References	707
	Glossary and Abbreviations	708
	Subject Index	717