

Inhaltsverzeichnis

1	Einführung	9
1.1	Hintergrund	9
1.2	Zweck	9
1.3	Geltungsbereich	10
1.4	Struktur des Leitfadens	11
1.5	Kernkonzepte	11
1.5.1	Risikomanagement-Verfahren	11
1.5.2	Datensteuerungs-Grundsätze	11
1.5.3	Daten-Lebenszyklus	11
1.5.4	Kernkonzepte zusammengefasst durch ALCOA und ALCOA+	12
1.5.5	Kritisches Denken	13
1.5.6	Lebenszyklus eines GxP-computergestützten Systems	14
1.5.7	Zusammenfassung der Kernkonzepte	15
1.6	Kernbegriffe	16
2	Regulatorischer Fokus	17
2.1	Einführung	17
2.2	Datenintegritäts-Anforderungen	17
2.2.1	Verhaltensorientierte Schritte	18
2.2.2	Vorgehensbezogene Schritte	19
2.2.3	Technische Schritte	20
3	Rahmenwerk für Datensteuerungs-Grundsätze	23
3.1	Einführung	23
3.2	Übersicht	23
3.3	Elemente des Datensteuerungs-Grundsätze-Rahmenwerks	25
3.3.1	Geltungsbereich und Ziele	26
3.3.2	Führungs- und Managementverantwortlichkeiten	27
3.3.3	Organisation und Dateneignerschaft	28
3.3.4	Kern-Leistungsindikatoren	28
3.3.5	Rollen und Zuständigkeiten	29
3.3.6	Grundsätze und Standards	31
3.3.7	Sensibilisierung und Schulung	31
3.3.8	Techniken und Werkzeuge	31
3.3.9	Strategische Planung und Datenintegritäts-Programm	32
3.3.10	Daten-Lebenszyklus und Datenmanagement	32
3.4	Menschliche Faktoren in der Datenintegrität	33
3.5	Datenintegritäts-Reifemodell	34
4	Daten-Lebenszyklus	35
4.1	Einführung	35
4.2	Datenerzeugung	36
4.3	Datenverarbeitung	37
4.4	Datenprüfung, -berichterstattung und -nutzung	39
4.4.1	Datenprüfung	39
4.4.2	Audit-Trail-Prüfung	40
4.4.3	Daten-Berichterstattung	40
4.4.4	Datenverteilung	41
4.5	Datenaufbewahrung und Rückspielung	41
4.5.1	Allgemeine Anforderungen	41
4.5.2	Sicherung und Wiedereinspielung	44
4.5.3	Archivierung	44

4.6	Datenvernichtung	45
5	Qualitätsrisiko-Management	47
5.1	Einführung	47
5.2	Prozessrisiko-Bewertung	47
5.3	Qualitätsrisiko-Management-Ansatz	47
5.4	Produkt- und Prozess-Zusammenhang	49
	<u>Management-Anhänge</u>	
6	Anhang M1 – Unternehmens-Datenintegritäts-Programm	51
6.1	Einführung	51
6.2	Wird ein Unternehmens-Datenintegritäts-Programm benötigt?	51
6.3	Indikatoren für den Programmumfang und den Aufwand	52
6.3.1	Eigenbewertung	53
6.3.2	Regulatorische Inspektion	54
6.3.3	Aufwand und Ressourcen	54
6.4	Implementierungsbetrachtungen	54
6.4.1	Sponsor	55
6.4.2	Führungskräfte-Verantwortlichkeit	55
6.4.3	Wissensaustausch und Schulung	56
6.4.4	Verhaltensorientierte Faktoren	56
6.5	Schlüssel zum Erfolg	57
6.5.1	Technische Kontrollen	58
6.5.2	Periodische Prüfungen	59
7	Anhang M2 – Datenintegritäts-Reifemodell	61
7.1	Reifemodell	61
7.2	Datenintegritäts-Reifegrad-Charakterisierung	65
8	Anhang M3 – Menschliche Faktoren	75
8.1	Einführung	75
8.2	Unternehmenskultur und lokale Kulturen	75
8.2.1	Unternehmenskultur	75
8.2.2	Lokale geografische Kulturen	75
8.2.3	Kulturelle Unterschiede	76
8.3	Klassifizierung von Vorfällen	77
8.4	Menschliche Fehler	77
8.5	Datenfälschung und Betrug	78
8.5.1	Profitorientierte Fälschung	78
8.5.2	Reduzierung des Betrugs	78
8.6	Unvoreingenommenheit	79
8.7	Verhaltensorientierte Kontrollen	80
8.7.1	Kenntnis wirksamer Kontrollen	80
8.7.2	Unternehmens-Datenintegritäts-Schulungsprogramm	80
8.7.3	Improvisation	82
9	Anhang M4 – Daten-Audit-Trail und Audit-Trail-Prüfung	83
9.1	Einführung	83
9.2	Regulatorischer Hintergrund	84
9.3	Einsatz und Nutzung von Audit-Trails	85
9.4	Audit-Trail-Prüfung	87
9.5	Technische Aspekte und Systemgestaltung	88
10	Anhang M5 – Datenaudit und periodische Prüfung	89
10.1	Einführung	89

10.2	Auditierung der Datenintegrität	89
10.3	Periodische Prüfung	90
10.4	Andere Prüfungen	91
10.5	Dokumentierung des Prüfungsprozesses	91
11	Anhang M6 – Inspektionsbereitschaft	93
11.1	Allgemeine Vorgehensweisen	93
11.1.1	Besondere Anforderungen	93
11.1.2	Rechtsaspekte	94
11.1.3	Zugang zu Computersystemen	94
11.2	Wichtige Informationen für behördliche Inspektionen	95
11.2.1	Prozesseigner und Systemeigner	95
11.2.2	Prozesseigner	95
11.2.3	Systemeigner	96
11.2.4	Überwachung	96
11.2.5	Personalbereitschaft, Schulungsaufzeichnungen und Vorgehensweisen	97
11.2.6	Interne Datenintegritäts-Untersuchungen	97
12	Anhang M7 – Integration der Datenintegrität in bestehende Dokumenten-Management-Prozesse	99
12.1	Einführung	99
12.2	Aufzeichnungserstellung	100
12.3	Aktive Aufzeichnungen	100
12.4	Semi-aktive Aufzeichnungen	100
12.5	Inaktive Aufzeichnungen	100
12.5.1	Vernichtung	100
	<u>Entwicklungs-Anhänge</u>	
13	Anhang D1 – Anwenderanforderungen (Lasten)	101
13.1	Einführung	101
13.2	Geschäftsprozess	101
13.3	Allgemeine Datenintegritäts-Anforderungen (Lasten)	102
13.3.1	Technische Anforderungen (Lasten)	103
13.3.2	Vorgehensbezogene Anforderungen (Lasten)	104
14	Anhang D2 – Prozess-Zuordnung und Schnittstellen	107
14.1	Einführung	107
14.2	Prozess-Flussdiagramme	107
14.3	Datenfluss-Diagramme	110
14.4	Wie viel wird benötigt?	111
15	Anhang D3 – Risiko-Kontrollmaßnahmen für Aufzeichnungen, Daten und elektronische Unterschriften	113
15.1	Einführung	113
15.2	Aufzeichnungs- und Daten-Kontrollen	113
15.3	Kontrollen für elektronische Unterschriften	113
15.4	Implementierung von Aufzeichnungs- und Daten-Kontrollen	115
15.5	Strenge der Kontrollen	118
16	Anhang D4 – Datenintegritäts-Probleme bezogen auf die Systemarchitektur	121
16.1	Daten liegen auf einer lokalen Festplatte	121
16.2	Intern verwaltete zentrale Datenbank	122
16.3	Intern verwaltete verteilte Daten	123
16.3.1	Lokal eindeutige Daten global zugreifbar	123
16.3.2	Global nachgebildete Daten	123

16.4	Ausgelagerte verwaltete Dienstleistungen	123
16.4.1	Intern verwaltet mit Cloud-Speicherung (Infrastruktur als Dienstleistung (IaaS))	124
16.4.2	Intern verwaltete Applikation mit cloud-basierter Plattform (PaaS)	125
16.4.3	Software als Dienstleistung (SaaS)	125

17 Anhang D5 – Datenintegrität für Endanwender-Applikationen 127

17.1	Einführung	127
17.2	Datenintegrität für Tabellenkalkulationen	127
17.2.1	Tabellenkalkulationen, die einfache Dokumente sind	128
17.2.2	Tabellenkalkulationen als Vorlagen	128
17.2.3	Tabellenkalkulationen für den Einzelfall	129
17.2.4	Tabellenkalkulationen als Datenbanken	129
17.3	Datenintegrität für PC-Datenbanken	130
17.3.1	Anwenderentwickelte und -verwaltete Werkzeuge	130
17.3.2	Zentral verwaltete PC-Datenbanken	130
17.4	Datenintegrität für statistische Werkzeuge	130

Betriebs-Anhänge

18 Anhang O1 – Aufbewahrung, Archivierung und Migration 133

18.1	Einführung	133
18.2	Aufbewahrungs-Optionen	133
18.3	Schutz von Aufzeichnungen	134
18.4	Aufzeichnungsalterung und Risiko	134
18.5	Archivierung	135
18.5.1	Sicherung	135
18.6	Hybride Situationen und Archive	136
18.7	Audit-Trail-Betrachtungen	137
18.8	Alternative Systeme	137
18.9	Umwandeln von einem elektronischen in ein alternatives Format oder alternative Medien-Hybride	138
18.9.1	Betrachtungen zur Konvertierung	139
18.9.2	Ändern von Speicherorten ohne Formatänderung	139
18.9.3	Risikobewertung für die Konvertierung	139

19 Anhang O2 – Papieraufzeichnungen und Hybrid-Situationen 143

19.1	Papieraufzeichnungen	143
19.1.1	Einführung	143
19.1.2	Übersicht	143
19.1.3	Management	143
19.1.4	Nutzung	144
19.2	Hybride Situationen	145
19.2.1	Einführung	145
19.2.2	Kontrollen zur Handhabung hybrider Situationen	145
19.2.3	Praktische Schwierigkeiten mit Hybrid-Situationen	146
19.3	Einsatz von Formularen zur Durchsetzung von Vorgehensweisen	148

Allgemeine Anhänge

20 Anhang G1 – Literaturstellen 149

21 Anhang G2 – Glossar 153

21.1	Akronyme und Abkürzungen	153
21.2	Definitionen	155