

Inhaltsverzeichnis

1. Vorwort des VOI	9
2. Vorwort des TÜViT	13
3. Was ist neu?	15
4. Einführung	19
4.1. Fachliche Ausgangslage	20
4.2. Definitionen / Abgrenzungen	21
4.2.1. Dokument	21
4.2.2. Digitales Dokument	21
4.2.3. IT-System	22
4.2.4. Lösung	22
4.2.5. Betreiber der Lösung	22
4.2.6. Beweistauglichkeit der Lösung	23
4.2.7. Rechts- und Revisionssicherheit	24
4.2.8. Die 10 Merksätze des VOI für eine ordnungs- gemäße Aufbewahrung digitaler Dokumente.	25
4.2.9. Verfahrensdokumentation als regulatorische Grundanforderung	29
4.2.10. Prüfobjekte	30
4.2.11. Geschlechtsbezogener Sprachgebrauch	30
5. Methodik der PK-DML	31
5.1. Definition von Kernkriterien	31
5.1.1. Ordnungsmäßigkeit	31
5.1.2. Vollständigkeit	32
5.1.3. Unveränderbarkeit	32
5.1.4. Verfügbarkeit	33
5.1.5. Nachvollziehbarkeit	33

5.2. Erstellung einer Verfahrensdokumentation auf Basis der Prüfkriterien.	34
5.3. Trennung von Anwendungsfeldern	36
6. Überblick über die Bewertungsbereiche.	37
6.1. Allgemeine Beschreibung des Einsatzgebietes.	38
6.2. Fachliche und sachlogische Lösung.	38
6.3. Technische Lösung	39
6.4. Informationssicherheit.	39
6.5. Technischer Betrieb	39
6.6. Langzeitverfügbarkeit und Migration	39
6.7. Qualifikation der Beschäftigten	40
6.8. Tests	40
6.9. Outsourcing.	40
6.10. Beschreibung des Internen Kontrollsystems (IKS). ...	41
7. Bewertungskriterien	43
7.1. Allgemeine Beschreibung des Einsatzgebiets.	43
7.1.1. Darstellung der Organisation.	43
7.1.2. Standort	44
7.1.3. Aufbauorganisation	44
7.2. Fachliche und sachlogische Lösung.	45
7.2.1. Rahmen, Aufgabenstellung und Richtlinien.	45
7.2.2. Organisationsbeschreibung	45
7.2.3. Dokumentenbestände.	46
7.2.4. Digitalisierung und Übernahme von Papierdokumenten	47
7.2.5. Vernichtung von Papier- und sonstigen Originaldokumenten	47
7.2.6. Übernahme elektronisch eingehender Dokumente	48
7.2.7. Behandlung von elektronisch signierten Dokumenten	49

7.2.8. Behandlung von E-Mails	51
7.2.9. Übernahme von digitalen Massendaten	53
7.2.10. Indexieren	54
7.2.11. Archivieren	55
7.2.12. Recherche und Zugriff	56
7.2.13. Check-in / Check-out	56
7.2.14. Bearbeiten und Versionieren	57
7.2.15. Weiterleiten	57
7.2.16. Reproduktion	58
7.2.17. Löschen	58
7.3. Technische Systemlösung	61
7.3.1. Grafische Systemdarstellung	61
7.3.2. Speichersysteme	61
7.3.3. Erfassungssysteme	62
7.3.4. Ausgabesysteme	62
7.3.5. Virtualisierung	63
7.3.6. Server-Hardware	63
7.3.7. Client-Hardware	64
7.3.8. Server-Software	64
7.3.9. Client-Software	65
7.3.10. Spezialfall: Individualsoftware	65
7.3.11. Schnittstellen	66
7.3.12. Beschreibung der Netzwerk-Architektur	66
7.3.13. Cloud-Management	67
7.3.14. Elektronische Signaturen, Siegel und Zeitstempel	67
7.4. Informationssicherheit	68
7.4.1. Allgemeines Informationssicherheitskonzept	68
7.4.2. Spezifische Anforderungen an das Informationssicherheitskonzept	68
7.4.3. Backup-Konzept	69
7.4.4. Benutzerverwaltung und Berechtigungskonzept ..	69

7.4.5. Zutrittskontrollen	70
7.4.6. Zugangs- und Zugriffskontrollen	70
7.4.7. Transaktions-, Integritäts- und Konsistenzsicherung	71
7.4.8. Protokollierung	71
7.4.9. Ausfallsicherheit	72
7.4.10. Datenschutz und Kontrollmaßnahmen	72
7.5. Technischer Betrieb	74
7.5.1. Zuständigkeiten	74
7.5.2. Bauliche Voraussetzungen	75
7.5.3. Betriebsbedingungen Hardware	75
7.5.4. Betriebsbedingungen Software	75
7.5.5. Datensicherung	76
7.5.6. Umgang mit Speichermedien	76
7.5.7. Überwachung des ordnungsgemäßen Betriebes ...	77
7.5.8. Verantwortung für Wartung und Störungsbehebung	77
7.5.9. Präventive Wartung	77
7.5.10. Dokumentation der Wartungsprozesse	78
7.5.11. Störungsbehebung	78
7.5.12. Restart	79
7.5.13. Recovery	79
7.5.14. Aktualisierung der Hardware	79
7.5.15. Aktualisierung der Software	80
7.6. Langzeitverfügbarkeit und Migration	81
7.6.1. Konzept zur Langzeitverfügbarkeit	82
7.6.2. Migrationskonzept	82
7.6.3. Kontrolle	83
7.6.4. Durchführung einer Migration	83
7.7. Qualifikation der Beschäftigten	84
7.7.1. Rollen	84
7.7.2. Erforderliche Kenntnisse	84

7.7.3. Verantwortlichkeiten	85
7.7.4. Qualifizierungsmaßnahmen	85
7.7.5. Dokumentation der Qualifikationen und Maßnahmen	86
7.8. Tests	87
7.8.1. Testkonzept	87
7.8.2. Testpläne und Testvorgaben	87
7.8.3. Testprotokolle	88
7.9. Outsourcing	89
7.9.1. Leistungen und Verantwortlichkeiten	89
7.9.2. Verfahrensdokumentation	90
7.9.3. Schnittstellen	90
7.9.4. Kontrolle	91
7.10. Internes Kontrollsystem (IKS)	92
7.10.1. Beschreibung der IKS-Methodik	92
7.10.2. Nachvollziehbarkeit der Kontrollen	93
7.10.3. Dokumentation der organisatorischen Kontrollmaßnahmen	93
7.10.4. Dokumentation der technischen Kontrollmaßnahmen	94
7.10.5. Verfahrensdokumentation	95
7.10.6. Kontrolle und Auswertung des IKS	95
7.10.7. Zuordnung von Verantwortlichkeiten	95
8. Prüfung und Zertifizierung	97
8.1. Einleitung	97
8.2. Prüf- und Zertifizierungsoptionen	98
8.2.1. Prüfung einer Gesamtlösung	98
8.2.2. Teilzertifizierungen	98
8.3. Zertifizierung, Zertifikatsgültigkeit und Re-Zertifizierung	100

8.4. Zuständigkeiten	103
8.4.1. Lenkungskreis	103
8.4.2. Arbeitskreis	103
8.4.3. Zertifizierungsstelle	104
9. Allgemeines	105
9.1. Geltungsbereich des Kriterienwerkes	105
9.2. Zuständigkeiten und Anschriften	105
9.2.1. Zertifizierungsstelle der TÜViT	105
9.2.2. Zertifizierungsstelle des VOI (VOI-CERT)	105
9.2.3. Arbeitskreis	106
9.3. Haftungsausschluss	107
10. Glossar	109
11. Anhang	127
11.1. Weitere qualitätssichernde Verfahren mit Berührungspunkten zur PK-DML	127
11.1.1. Inhaltliche Zuordnung der PK-DML-Struktur zur ISO 9001:2008.	139
11.1.2. Inhaltliche Zuordnung zur 27001	139