DIN CEN/TS 18026:2026-05 (D)

Dreistufiger Ansatz für einen Anforderungskatalog für Cybersicherheitsmaßnahmen für Cloud-Dienste; Deutsche Fassung CEN/TS 18026:2024

Inhalt

Seite

Europäisches Vorwort ... 13

Einleitung ... 14

1 Anwendungsbereich ... 19

2 Normative Verweisungen ... 19

3 Begriffe ... 19

4 Organisation der Informationssicherheit ... 45
4.1 OIS-01 Managementsystem für Informationssicherheit ... 45
4.1.1 Ziel ... 45
4.1.2 Anforderungen ... 46
4.2 OIS-02 Aufgabentrennung ... 47
4.2.1 Ziel ... 47
4.2.2 Anforderungen ... 47
4.3 OIS-03 Kontakt mit Behörden und Interessengruppen ... 49
4.3.1 Ziel ... 49
4.3.2 Anforderungen ... 49
4.4 OIS-04 Informationssicherheit im Projektmanagement ... 49
4.4.1 Ziel ... 49
4.4.2 Anforderungen ... 49

5 Informationssicherheitspolitik und -richtlinien ... 50
5.1 ISP-01 Informationssicherheitspolitik ... 50
5.1.1 Ziel ... 50
5.1.2 Anforderungen ... 50
5.2 ISP-02 Themenspezifische Richtlinien und Verfahren ... 52
5.2.1 Ziel ... 52
5.2.2 Anforderungen ... 52
5.3 ISP-03 Ausnahmen ... 54
5.3.1 Ziel ... 54
5.3.2 Anforderungen ... 54

6 Risikomanagement ... 56
6.1 RM-01 Richtlinie zum Risikomanagement ... 56
6.1.1 Ziel ... 56
6.1.2 Anforderungen ... 56
6.2 RM-02 Umsetzung der Risikobeurteilung ... 58
6.2.1 Ziel ... 58
6.2.2 Anforderungen ... 58
6.3 RM-03 Umsetzung der Risikobehandlung ... 59
6.3.1 Ziel ... 59
6.3.2 Anforderungen ... 59

7 Personalwesen ... 60
7.1 HR-01 Personalrichtlinien ... 60
7.1.1 Ziel ... 60
7.1.2 Anforderungen ... 60
7.2 HR-02 Verifizierung der Kompetenz und Vertrauenswürdigkeit ... 62
7.2.1 Ziel ... 62

7.2.2 Anforderungen ... 62
7.3 HR-03 Beschäftigungsbedingungen ... 63
7.3.1 Ziel ... 63
7.3.2 Anforderungen ... 64
7.4 HR-04 Sicherheitssensibilisierung und -schulung ... 65
7.4.1 Ziel ... 65
7.4.2 Anforderungen ... 65
7.5 HR-05 Beendigung oder Änderung der Beschäftigung ... 67
7.5.1 Ziel ... 67
7.5.2 Anforderungen ... 67
7.6 HR-06 Vertraulichkeitsvereinbarungen ... 68
7.6.1 Ziel ... 68
7.6.2 Anforderungen ... 68

8 Asset-Management ... 69
8.1 AM-01 Asset-Inventar ... 69
8.1.1 Ziel ... 69
8.1.2 Anforderungen ... 69
8.2 AM-02 Richtlinie für den zulässigen Gebrauch von und sicheren Umgang mit Assets ... 70
8.2.1 Ziel ... 70
8.2.2 Anforderungen ... 70
8.3 AM-03 Inbetriebnahme und Außerbetriebnahme ... 71
8.3.1 Ziel ... 71
8.3.2 Anforderungen ... 71
8.4 AM-04 Zulässiger Gebrauch von, sicherer Umgang mit und Rückgabe von Assets ... 72
8.4.1 Ziel ... 72
8.4.2 Anforderungen ... 72
8.5 AM-05 Klassifizierung und Kennzeichnung von Assets ... 73
8.5.1 Ziel ... 73
8.5.2 Anforderungen ... 73

9 Physische Sicherheit ... 74
9.1 PS-01 Physische Sicherheitsperimeter ... 74
9.1.1 Ziel ... 74
9.1.2 Anforderungen ... 74
9.2 PS-02 Physische Standort-Zugangssteuerung ... 75
9.2.1 Ziel ... 75
9.2.2 Anforderungen ... 75
9.3 PS-03 Arbeiten in nicht öffentlichen Bereichen ... 77
9.3.1 Ziel ... 77
9.3.2 Anforderungen ... 77
9.4 PS-04 Schutz von Geräten ... 78
9.4.1 Ziel ... 78
9.4.2 Anforderungen ... 78
9.5 PS-05 Schutz vor externen und umweltbedingten Bedrohungen ... 80
9.5.1 Ziel ... 80
9.5.2 Anforderungen ... 80

10 Betriebssicherheit ... 82
10.1 OPS-01 Kapazitätsmanagement – Planung ... 82
10.1.1 Ziel ... 82
10.1.2 Anforderungen ... 82
10.2 OPS-02 Kapazitätsmanagement – Überwachung ... 83
10.2.1 Ziel ... 83
10.2.2 Anforderungen ... 83
10.3 OPS-03 Kapazitätsmanagement – Steuerung von Ressourcen ... 83
10.3.1 Ziel ... 83
10.3.2 Anforderungen ... 84
10.4 OPS-04 Schutz vor Schadsoftware – Richtlinien ... 84

10.4.1 Ziel ... 84
10.4.2 Anforderungen ... 85
10.5 OPS-05 Schutz vor Schadsoftware – Implementierung ... 86
10.5.1 Ziel ... 86
10.5.2 Anforderungen ... 86
10.6 OPS-06 Datensicherung und -wiederherstellung – Richtlinien ... 87
10.6.1 Ziel ... 87
10.6.2 Anforderungen ... 87
10.7 OPS-07 Datensicherung und -wiederherstellung – Überwachung ... 88
10.7.1 Ziel ... 88
10.7.2 Anforderungen ... 88
10.8 OPS-08 Datensicherung und -wiederherstellung – regelmäßige Tests ... 88
10.8.1 Ziel ... 88
10.8.2 Anforderungen ... 89
10.9 OPS-09 Datensicherung und -wiederherstellung – Speicherung ... 89
10.9.1 Ziel ... 89
10.9.2 Anforderungen ... 89
10.10 OPS-10 Protokolle und Überwachung – Richtlinien ... 90
10.10.1 Ziel ... 90
10.10.2 Anforderungen ... 90
10.11 OPS-11 Protokollierung und Überwachung – Verwaltung abgeleiteter Daten ... 92
10.11.1 Ziel ... 92
10.11.2 Anforderungen ... 92
10.12 OPS-12 Protokollierung und Überwachung – Identifizierung von Ereignissen ... 94
10.12.1 Ziel ... 94
10.12.2 Anforderungen ... 94
10.13 OPS-13 Protokollierung und Überwachung – Zugang, Speicherung und Löschung ... 94
10.13.1 Ziel ... 94
10.13.2 Anforderungen ... 94
10.14 OPS-14 Protokollierung und Überwachung – Zuordnung ... 96
10.14.1 Ziel ... 96
10.14.2 Anforderungen ... 96
10.15 OPS-15 Protokollierung und Überwachung – Konfiguration ... 97
10.15.1 Ziel ... 97
10.15.2 Anforderungen ... 97
10.16 OPS-16 Protokollierung und Überwachung – Verfügbarkeit ... 97
10.16.1 Ziel ... 97
10.16.2 Anforderungen ... 97
10.17 OPS-17 Schwachstellen, Störungen und Fehler – Richtlinien ... 98
10.17.1 Ziel ... 98
10.17.2 Anforderungen ... 98
10.18 OPS-18 Verwaltung von Schwachstellen, Störungen und Fehlern – Online-Register ... 99
10.18.1 Ziel ... 99
10.18.2 Anforderungen ... 100
10.19 OPS-19 Verwaltung von Schwachstellen, Störungen und Fehlern – Identifizieren von Schwachstellen ... 102
10.19.1 Ziel ... 102
10.19.2 Anforderungen ... 102
10.20 OPS-20 Umgang mit Schwachstellen, Störungen und Fehlern – Messungen, Analysen und Beurteilungen von Verfahren ... 103
10.20.1 Ziel ... 103
10.20.2 Anforderungen ... 103
10.21 OPS-21 Umgang mit Schwachstellen, Störungen und Fehlern – Systemhärtung ... 104
10.21.1 Ziel ... 104
10.21.2 Anforderungen ... 104
10.22 OPS-22 Trennung von Datensätzen in der Cloud-Infrastruktur ... 104
10.22.1 Ziel ... 104
10.22.2 Anforderungen ... 105

10.23 OPS-23 Uhrensynchronisation 105
10.23.1 Ziel 105
10.23.2 Anforderungen 105

11 Verwaltung der Identifizierungs-, Authentifizierungs- und Zugangssteuerung 106
11.1 IAM-01 Richtlinien für die Zugangssteuerung zu Informationen 106
11.1.1 Ziel 106
11.1.2 Anforderungen 106
11.2 IAM-02 Verwaltung von Identitäten 108
11.2.1 Ziel 108
11.2.2 Anforderungen 108
11.3 IAM-03 Deaktivieren, Reaktivieren und Entfernen von Identitäten 112
11.3.1 Ziel 112
11.3.2 Anforderungen 112
11.4 IAM-04 Verwaltung von Zugangsrechten 113
11.4.1 Ziel 113
11.4.2 Anforderungen 114
11.5 IAM-05 Regelmäßige Überprüfung von Zugangsrechten 115
11.5.1 Ziel 115
11.5.2 Anforderungen 115
11.6 IAM-06 Privilegierte Zugangsrechte 116
11.6.1 Ziel 116
11.6.2 Anforderungen 116
11.7 IAM-07 Authentifizierungsmechanismus 117
11.7.1 Ziel 117
11.7.2 Anforderungen 117
11.8 IAM-08 Schutz und Stärke von Zugangsdaten 120
11.8.1 Ziel 120
11.8.2 Anforderungen 120
11.9 IAM-09 Allgemeine Zugangsbeschränkungen 122
11.9.1 Ziel 122
11.9.2 Anforderungen 122

12 Kryptographie und Schlüsselverwaltung 125
12.1 CKM-01 Richtlinien zur Verwendung von Kryptographie und Schlüsselverwaltung 125
12.1.1 Ziel 125
12.1.2 Anforderungen 125
12.2 CKM-02 Verschlüsselung von Data-in-Motion 126
12.2.1 Ziel 126
12.2.2 Anforderungen 126
12.3 CKM-03 Verschlüsselung von Data-at-Rest 127
12.3.1 Ziel 127
12.3.2 Anforderungen 127
12.4 CKM-04 Sichere Schlüsselverwaltung 127
12.4.1 Ziel 127
12.4.2 Anforderungen 128

13 Kommunikationssicherheit 129
13.1 CS-01 Technische Sicherheitsmaßnahmen 129
13.1.1 Ziel 129
13.1.2 Anforderungen 129
13.2 CS-02 Sicherheitsanforderungen für Verbindungen innerhalb des Netzwerks des CSP 130
13.2.1 Ziel 130
13.2.2 Anforderungen 130
13.3 CS-03 Überwachung von Verbindungen innerhalb des Netzwerks des CSP 132
13.3.1 Ziel 132
13.3.2 Anforderungen 132
13.4 CS-04 Netzwerke für die Administration 133
13.4.1 Ziel 133

13.4.2 Anforderungen 133
13.5 CS-05 Verkehrstrennung in gemeinsam genutzten Netzwerkumgebungen 134
13.5.1 Ziel 134
13.5.2 Anforderungen 134
13.6 CS-06 Dokumentation der Netzwerktopologie 134
13.6.1 Ziel 134
13.6.2 Anforderungen 135
13.7 CS-07 Softwaredefinierte Vernetzung 135
13.7.1 Ziel 135
13.7.2 Anforderungen 136
13.8 CS-08 Richtlinien für die Datenübertragung 136
13.8.1 Ziel 136
13.8.2 Anforderungen 136

14 Portabilität und Interoperabilität 137
14.1 PI-01 Dokumentation und Sicherheit von Ein- und Ausgabeschnittstellen 137
14.1.1 Ziel 137
14.1.2 Anforderungen 137
14.2 PI-02 Vertragliche Vereinbarungen für die Bereitstellung von Daten 138
14.2.1 Ziel 138
14.2.2 Anforderungen 138
14.3 PI-03 Sichere Datenlöschung 140
14.3.1 Ziel 140
14.3.2 Anforderungen 140

15 Änderungs- und Konfigurationsmanagement 141
15.1 CCM-01 Richtlinien für Änderungen an IKT-Systemen 141
15.1.1 Ziel 141
15.1.2 Anforderungen 141
15.2 CCM-02 Risikobeurteilung, Kategorisierung und Priorisierung von Änderungen 142
15.2.1 Ziel 142
15.2.2 Anforderungen 142
15.3 CCM-03 Tests von Änderungen 143
15.3.1 Ziel 143
15.3.2 Anforderungen 143
15.4 CCM-04 Genehmigungen für die Bereitstellung in der Produktionsumgebung 145
15.4.1 Ziel 145
15.4.2 Anforderungen 145
15.5 CCM-05 Durchführen und Protokollieren von Änderungen 145
15.5.1 Ziel 145
15.5.2 Anforderungen 145
15.6 CCM-06 Versionskontrolle 146
15.6.1 Ziel 146
15.6.2 Anforderungen 146

16 Entwicklung von Informationssystemen 147
16.1 DEV-01 Richtlinien für die Entwicklung und Beschaffung von Informationssystemen 147
16.1.1 Ziel 147
16.1.2 Anforderungen 147
16.2 DEV-02 Sicherheit der Entwicklungslieferkette 148
16.2.1 Ziel 148
16.2.2 Anforderungen 148
16.3 DEV-03 Sichere Entwicklungsumgebung 149
16.3.1 Ziel 149
16.3.2 Anforderungen 149
16.4 DEV-04 Trennung von Umgebungen 150
16.4.1 Ziel 150
16.4.2 Anforderungen 150
16.5 DEV-05 Entwicklung von Sicherheitsmerkmalen 151

16.5.1 Ziel 151
16.5.2 Anforderungen 151
16.6 DEV-06 Identifizierung von Schwachstellen des Cloud-Dienstes 152
16.6.1 Ziel 152
16.6.2 Anforderungen 152
16.7 DEV-07 Auslagerung der Entwicklung 153
16.7.1 Ziel 153
16.7.2 Anforderungen 153
16.8 DEV-08 Kontrolle des Austauschs mit Lieferanten von Funktionskomponenten 155
16.8.1 Ziel 155
16.8.2 Anforderungen 155

17 Beschaffungsmanagement 156
17.1 PM-01 Richtlinien und Verfahren für die Kontrolle und Überwachung von Dritten 156
17.1.1 Ziel 156
17.1.2 Anforderungen 156
17.2 PM-02 Risikobeurteilung von Lieferanten 158
17.2.1 Ziel 158
17.2.2 Anforderungen 159
17.3 PM-03 Lieferantenverzeichnis 161
17.3.1 Ziel 161
17.3.2 Anforderungen 161
17.4 PM-04 Überwachung der Einhaltung von Anforderungen 162
17.4.1 Ziel 162
17.4.2 Anforderungen 163
17.5 PM-05 Ausstiegsstrategie 165
17.5.1 Ziel 165
17.5.2 Anforderungen 165

18 Handhabung von Zwischenfällen 166
18.1 IM-01 Richtlinie für die Handhabung von Informationssicherheitsvorfällen 166
18.1.1 Ziel 166
18.1.2 Anforderungen 166
18.2 IM-02 Umgang mit Informationssicherheitsvorfällen 168
18.2.1 Ziel 168
18.2.2 Anforderungen 168
18.3 IM-03 Dokumentation und Berichterstattung über Informationssicherheitsvorfälle 169
18.3.1 Ziel 169
18.3.2 Anforderungen 169
18.4 IM-04 Pflicht des Benutzers zur Meldung von Informationssicherheitsvorfällen 170
18.4.1 Ziel 170
18.4.2 Anforderungen 170
18.5 IM-05 Einbeziehung von CSCs bei Vorfällen 171
18.5.1 Ziel 171
18.5.2 Anforderungen 171
18.6 IM-06 Beurteilung und Lernprozess 172
18.6.1 Ziel 172
18.6.2 Anforderungen 172
18.7 IM-07 Beweissicherung von Vorfällen 173
18.7.1 Ziel 173
18.7.2 Anforderungen 173

19 Aufrechterhaltung der Betriebsfähigkeit 174
19.1 BC-01 Richtlinien zur Aufrechterhaltung der Betriebsfähigkeit und Verantwortung der Leitung 174
19.1.1 Ziel 174
19.1.2 Anforderungen 174
19.2 BC-02 Business-Impact-Analyse 175
19.2.1 Ziel 175

19.2.2 Anforderungen 175
19.3 BC-03 Plan zur Aufrechterhaltung der Betriebsfähigkeit 176
19.3.1 Ziel 176
19.3.2 Anforderungen 177
19.4 BC-04 Tests und Übungen zur Aufrechterhaltung der Betriebsfähigkeit 178
19.4.1 Ziel 178
19.4.2 Anforderungen 178

20 Einhaltung 179
20.1 CO-01 Ermittlung von geltenden Anforderungen an die Einhaltung 179
20.1.1 Ziel 179
20.1.2 Anforderungen 179
20.2 CO-02 Richtlinie für die Planung und Durchführung von Audits 179
20.2.1 Ziel 179
20.2.2 Anforderungen 180
20.3 CO-03 Interne Audits 181
20.3.1 Ziel 181
20.3.2 Anforderungen 181
20.4 CO-04 Beurteilung der Leistung interner Maßnahmen 182
20.4.1 Ziel 182
20.4.2 Anforderungen 182

21 Benutzerdokumentation 182
21.1 DOC-01 Leitfaden und Empfehlungen für CSCs 182
21.1.1 Ziel 182
21.1.2 Anforderungen 182
21.2 DOC-02 Standorte für Datenverarbeitung und -speicherung 185
21.2.1 Ziel 185
21.2.2 Anforderungen 185
21.3 DOC-03 Begründung der angestrebten Evaluierungsstufe 186
21.3.1 Ziel 186
21.3.2 Anforderungen 186

22 Umgang mit Ermittlungsanfragen von staatlichen Stellen 187
22.1 INQ-01 Rechtliche Beurteilung von Ermittlungsanfragen 187
22.1.1 Ziel 187
22.1.2 Anforderungen 187
22.2 INQ-02 Informieren von CSCs über Ermittlungsanfragen 187
22.2.1 Ziel 187
22.2.2 Anforderungen 187
22.3 INQ-03 Voraussetzungen für den Zugang zu oder die Offenlegung von Daten bei Ermittlungsanfragen 188
22.3.1 Ziel 188
22.3.2 Anforderungen 188

23 Produktsicherheit 189
23.1 PSS-01 Fehlerbehandlung und Protokollierungsmechanismen 189
23.1.1 Ziel 189
23.1.2 Anforderungen 189
23.2 PSS-02 Session-Management 190
23.2.1 Ziel 190
23.2.2 Anforderungen 190
23.3 PSS-03 Images für virtuelle Maschinen und Container 191
23.3.1 Ziel 191
23.3.2 Anforderungen 191
23.4 PSS-04 Standortwahl für die Datenverarbeitung und -speicherung 192
23.4.1 Ziel 192
23.4.2 Anforderungen 192

Literaturhinweise 193