

Quellen, Methodik und Prüfung

Quellenregister, Claim-Evidence-Matrix und Recherchemethodik der sechs Fachleitfäden

Vollständiges Quellenregister, eine 46 Aussagen umfassende Claim-Evidence-Matrix und die Recherche- und Prüfmethodik hinter den sechs Fachleitfäden — für die Nachprüfung jeder einzelnen tragenden Aussage.

Fassung 1.0 · Stand 25. September 2026 · Adressaten: Fachprüfer, wissenschaftliche Beiräte, Redaktionen und Verantwortliche für die externe Begutachtung.

Dokumenttyp: Beleg- und Methodikanhang. Ein Quellenverweis ist weder Gütesiegel noch Beleg für jede folgende Empfehlung; Normvolltexte sind gegebenenfalls lizenziert selbst zu beschaffen, sie werden hier nicht mitervielfältigt.

Steckbrief

Merkmal	Wert
Dokumenttyp	Beleg- und Methodikanhang; strukturierte Quellen- und Dokumentenarbeit, kein externes Peer Review
Zielgruppe	Fachprüfer, wissenschaftliche Beiräte, Redaktionen
Recherche- und Rechtsstand	25. September 2026
Umfang	7.941 Wörter, 31 Seiten
Belege	0 Literatureinträge, 0 Quellenadressen
Gliederung	13 nummerierte Abschnitte, 2 Tabellen

Inhalt

Quellenregister und Fundstellen	7
Q01 · Autonomous AI agents are hacking online retailers for \$25 a company	7
Q02 · Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3	7
Q03 · Guide to Operational Technology (OT) Security, SP 800-82 Rev. 4, Initial Public Draft	7
Q04 · The NIST Cybersecurity Framework (CSF) 2.0	7
Q05 · Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, SP 800-61 Rev. 3	8
Q06 · Zero Trust Architecture, SP 800-207	8
Q07 · Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, SP 800-160 Vol. 2 Rev. 1	8
Q08 · OT Backup Quick Start Guide, SP 1339	8
Q09 · Software and AI Agent Identity and Authorization	8
Q10 · Back to the Future: Why Agentic AI Needs a Strong Identity Foundation	9
Q11 · Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, AI 100-2e2025	9
Q12 · AI Risk Management Framework (AI RMF)	9
Q13 · Best Current Practice for OAuth 2.0 Security, RFC 9700	9
Q14 · OAuth 2.0 Token Exchange, RFC 8693	10
Q15 · OAuth 2.0 Token Revocation, RFC 7009	10
Q16 · FHIR R5, Security, Version 5.0.0	10
Q17 · Healthcare and Public Health Cybersecurity Performance Goals	10
Q18 · Electronic Health Records and Downtime Procedures	10
Q19 · Cybersecurity Vulnerabilities in Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication	11
Q20 · Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US	11
Q21 · Anatomy of a Cyberattack: Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime	11
Q22 · MDCG 2019-16 rev. 1: Guidance on Cybersecurity for medical devices	12
Q23 · IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices — Part 1	12
Q24 · IEC 62443-3-2:2020: Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design	12
Q25 · ISO 10218-1:2025: Robotics — Safety requirements — Part 1: Industrial robots	12
Q26 · ISO 10218-2:2025: Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells	13
Q27 · ATT&CK for ICS: Loss of Safety, T0880	13
Q28 · Triton Safety Instrumented System Attack, C0030	13
Q29 · BSI-Gesetz (BSIG 2025), aktuelle bereitgestellte Fassung	13
Q30 · SGB V § 391 — IT-Sicherheit in Krankenhäusern	13
Q31 · Betriebssicherheitsverordnung § 3 — Gefährdungsbeurteilung	14
Q32 · Betriebsverfassungsgesetz § 87 — Mitbestimmungsrechte	14
Q33 · AI Act — Application timeline and implementation	14
Q34 · AI Omnibus enters into force	14

Q35 · Machinery — Machinery Regulation	15
Q36 · Cyber Resilience Act — Implementation	15
Q37 · Cyber Resilience Act — Reporting obligations	15
Q38 · Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung	15
Q39 · AI Act, Verordnung (EU) 2024/1689 — konsolidierte Fassung vom 27.07.2026	16
Q40 · Verordnung (EU) 2023/1230 — Maschinenverordnung	16
Q41 · Verordnung (EU) 2024/2847 — Cyber Resilience Act	16
Q42 · BSI-Standard 200-4: Business Continuity Management	16

Claim–Evidence-Matrix 17

C01 · BERICHTETER_BEFUND	17
C02 · BERICHTETER_BEFUND	17
C03 · BERICHTETER_BEFUND	17
C04 · FINALE_LEITLINIE	17
C05 · QUELLENSTATUS	17
C06 · EIGENE_SYNTHESE	17
C07 · EIGENES_MODELL	18
C08 · EMPIRISCHE_STUDIE	18
C09 · ABSTRACT_ERFAHRUNGSBERICHT	18
C10 · GERAETESPEZIFISCHE_BEHOERDENMITTEILUNG	18
C11 · SPEZIFIKATION	18
C12 · EIGENE_SYNTHESE	18
C13 · EIGENE_SYNTHESE	19
C14 · NORMTEXT_GELESEN	19
C15 · NORMMETADATEN	19
C16 · NORMMETADATEN	19
C17 · NORMMETADATEN	19
C18 · TAXONOMIE_HISTORISCHER_FALL	19
C19 · EIGENE_SYNTHESE	19
C20 · EIGENE_SYNTHESE	20
C21 · NORMTEXT_GELESEN	20
C22 · EIGENE_SYNTHESE	20
C23 · PROJEKT_FACHBEITRAG	20
C24 · SPEZIFIKATION	20
C25 · SPEZIFIKATION_UND_ABLEITUNG	20
C26 · TAXONOMIE_UND_ABLEITUNG	21
C27 · EIGENE_SYNTHESE	21
C28 · EIGENE_SYNTHESE	21
C29 · EIGENE_SYNTHESE	21
C30 · NORMTEXT_GELESEN	21

C31 · NORMTEXT_GELESEN	21
C32 · AMTLICHE_UMSETZUNGSINFORMATION	22
C33 · AMTLICHE_UMSETZUNGSINFORMATION	22
C34 · AMTLICHE_UMSETZUNGSINFORMATION	22
C35 · AMTLICHE_UMSETZUNGSINFORMATION	22
C36 · NORM_NACHSCHLAGEAUFTRAG	22
C37 · NORMTEXT_GELESEN	22
C38 · EIGENE_ORGANISATIONSEMPFEHLUNG	23
C39 · FINALE_LEITLINIE_UND_ABLEITUNG	23
C40 · EIGENE_EVIDENZGRENZE	23
C41 · EIGENE_SYNTHESE	23
C42 · MATHEMATISCHE_ABLEITUNG	23
C43 · MATHEMATISCHE_ABLEITUNG	23
C44 · EIGENE_PRUEFMETHODIK	24
C45 · EIGENE_PRUEFMETHODIK	24
C46 · EIGENE_PRUEFMETHODIK	24
Methodik, Recherche und Quellenkritik	24
1. Ausgangsmaterial und Provenienz	24
2. Recherchetyp und bewusste Grenzen	24
3. Tatsächliche Recherchepfade	25
4. Zugriffsklassen und Aussageumfang	25
5. PDF-Auswertung und proprietäre Inhalte	26
6. Trennung von Beobachtung und Übertragung	26
7. Eigenleistung der Leitfäden	26
8. Welche Prüfung vor verbindlicher Verwendung fehlt	26
9. Aktualisierung und Änderungskontrolle	27
Korrekturen, Grenzen und Freigabestatus	27
1. Verhältnis zum bisherigen Master	27
2. Nicht abgedeckte vertiefte Fachgebiete	28
3. Freigabegates	28
4. Freigabeprotokoll für den Empfänger	28
12 Rechtliche Hinweise	30
12.1 Keine Beratung	30
12.2 Keine Zusicherung, keine Konformitätsaussage	30
12.3 Rechtsstand	30
12.4 Haftung	30
12.5 Verweise auf fremde Inhalte	30
12.6 Marken und Produktbezeichnungen	30

12.7 Urheberrecht und Nutzung	30
12.8 Keine personenbezogenen Daten	31
12.9 Unabhängigkeit	31
12.10 Anwendbares Recht	31

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Quellen, Methodik und Prüfung*. Fassung 1.0, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus vier Markdown-Quellen des Leitfaden-Pakets zusammengesetzt und gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung. Gesetzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält keine Abbildungen.

Quellenregister und Fundstellen

Stand: 25.09.2026. Q bezeichnet externe Quellen; K eigene Kontrollen; E Nachweise; P Prüfungen. Ein Quellenverweis ist weder Gütesiegel noch Beleg für jede folgende Empfehlung. Zugriffstiefe und Schlussgrenzen gehören zur Quellenangabe. Die vollständigen Quellen werden nicht mitervielfältigt. Normvolltexte sind gegebenenfalls lizenziert zu beschaffen.

Q01 · Autonomous AI agents are hacking online retailers for \$25 a company

Urheber: Eyal Sela / Gambit Security **Datum / Version:** 2026-09-22 **Typ:** Anbieteruntersuchung / Interimsbericht
URL: <<https://gambit.security/blog-posts/autonomous-ai-agents-online-retailers-25-a-company>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Web-Volltext und relevante Abschnitte gelesen.

Fundstelle: Executive Summary; Methodology; Cost; Data Exfiltration / Cleanup.

Trägt: Berichtete Kampagne, beobachtete Automatisierung, Kostenbasis und Kollateralschaden.

Grenzen: Keine unabhängige Prüfung der Rohlogs durch FluxLane. Einzelne Agentenaussagen laut Bericht nicht unabhängig bestätigt. Keine Klinik-/Robotikfallstudie.

Q02 · Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3

Urheber: Keith Stouffer et al. / NIST **Datum / Version:** 2023-09-28 **Typ:** Finale technische Behördenleitlinie **URL:** <<https://csrc.nist.gov/pubs/sp/800/82/r3/final>> **DOI:** 10.6028/NIST.SP.800-82r3 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Landingpage und relevante PDF-Abschnitte gelesen; PDF-Stichprobe visuell geprüft.

Fundstelle: §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138.

Trägt: OT-spezifische Abhängigkeiten, Safety, Architektur, Fernzugriff und Betriebsresilienz.

Grenzen: Freiwillige US-Leitlinie, kein deutscher Konformitätsnachweis. Der Leitfaden ergänzt eigene Überlegungen; Kapitelverweise sind keine wörtlichen Normanforderungen.

Q03 · Guide to Operational Technology (OT) Security, SP 800-82 Rev. 4, Initial Public Draft

Urheber: NIST **Datum / Version:** 2026-09-21 **Typ:** Entwurf **URL:** <<https://csrc.nist.gov/pubs/sp/800/82/r4/ipd>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Landingpage einschließlich Entwurfsstatus gelesen.

Fundstelle: Status / Announcement / Abstract; Kommentierungsfrist 30.11.2026.

Trägt: Ausblick auf Überarbeitung der OT-Leitlinie.

Grenzen: Nicht final und keine ersetzende verbindliche Grundlage. Inhaltlicher Horizont, nicht Abnahmekriterium.

Q04 · The NIST Cybersecurity Framework (CSF) 2.0

Urheber: NIST **Datum / Version:** 2024-02-26 **Typ:** Finales Rahmenwerk **URL:** <<https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>> **DOI:** 10.6028/NIST.CSWP.29
Abruf-/Prüfdatum: 2026-09-25

Zugriffstiefe: Offizielle Publikationsseite und Beschreibung gelesen.

Fundstelle: Abstract; Funktionen GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER.

Trägt: Organisationsweite Strukturierung von Cyberrisiken.

Grenzen: Rahmenwerk mit Ergebnissen, keine universelle Implementierungsvorschrift und keine eigene Zertifizierung dieses Pakets.

Q05 · Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, SP 800-61 Rev. 3

Urheber: NIST **Datum / Version:** 2025-04-03 **Typ:** Finale technische Behördenleitlinie **URL:** <<https://csrc.nist.gov/pubs/sp/800/61/r3/final>> **DOI:** 10.6028/NIST.SP.800-61r3 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Publikationsseite / Abstract gelesen.

Fundstelle: Abstract; Integration von Incident Response in CSF 2.0.

Trägt: Incident Response als Teil des laufenden Risikomanagements.

Grenzen: Konkrete Abläufe und Formulare dieses Pakets sind eigene Ableitungen, kein vollständig nacherzählter Standard.

Q06 · Zero Trust Architecture, SP 800-207

Urheber: Scott Rose; Oliver Borchert; Stu Mitchell; Sean Connelly / NIST **Datum / Version:** 2020-08 **Typ:** Finale technische Behördenleitlinie **URL:** <<https://csrc.nist.gov/pubs/sp/800/207/final>> **DOI:** 10.6028/NIST.SP.800-207 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Publikationsseite / Abstract gelesen.

Fundstelle: Abstract; ressourcenbezogenes Vertrauen und getrennte Authentisierung/Autorisierung.

Trägt: Keine implizite Autorisierung allein aus Netzposition oder Zugehörigkeit.

Grenzen: Zero Trust garantiert weder Prozesssicherheit noch korrekte Daten. Die vorgeschlagene Agentenarchitektur ist eigene Synthese.

Q07 · Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, SP 800-160 Vol. 2 Rev. 1

Urheber: NIST **Datum / Version:** 2021-12 **Typ:** Finale technische Behördenleitlinie **URL:** <<https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>> **DOI:** 10.6028/NIST.SP.800-160v2r1 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Publikationsseite / Abstract gelesen.

Fundstelle: Abstract; cyber resiliency engineering.

Trägt: Resilienz als Systemeigenschaft und Engineering-Aufgabe.

Grenzen: Keine empirische Validierung der in diesem Paket vorgeschlagenen Architektur.

Q08 · OT Backup Quick Start Guide, SP 1339

Urheber: NIST **Datum / Version:** 2026-06-17 **Typ:** Finale technische Behördenleitlinie **URL:** <<https://csrc.nist.gov/pubs/sp/1339/final>> **DOI:** 10.6028/NIST.SP.1339 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Publikationsseite / Beschreibung gelesen.

Fundstelle: Abstract; Backup und Recovery für OT.

Trägt: Getestete Wiederherstellung und Einbettung von Backups in den Betrieb.

Grenzen: Ein Backup- oder Hashnachweis ist kein Beweis fachlicher Datenrichtigkeit. Konkrete Recovery-Gates sind eigene Ableitungen.

Q09 · Software and AI Agent Identity and Authorization

Urheber: NIST NCCoE **Datum / Version:** Projektstand abgerufen 2026-09-25 **Typ:**

Forschungs-/Standardisierungsprojekt **URL:**

<<https://www.nccoe.nist.gov/projects/software-and-ai-agent-identity-and-authorization>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Projektseite gelesen.

Fundstelle: Project overview; Identity and Authorization.

Trägt: Laufende Arbeit an Identitäten und Berechtigungen autonomer Softwareakteure.

Grenzen: Projektseite ist kein verabschiedeter Standard und keine gesetzliche Pflicht.

Q10 · Back to the Future: Why Agentic AI Needs a Strong Identity Foundation

Urheber: NIST Cybersecurity Insights **Datum / Version:** 2026-08-27 **Typ:** Behördlicher Fachbeitrag **URL:**

<<https://www.nist.gov/blogs/cybersecurity-insights/back-future-why-agentic-ai-needs-strong-identity-foundation>>

DOI: Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext gelesen.

Fundstelle: Agent identities; credentials; authorization; consent fatigue.

Trägt: Eigenständige Agentenidentitäten, Delegation und Grenzen dauerhafter Zugangsdaten.

Grenzen: Fachbeitrag, keine Norm. Zustimmungsermüdung ist hier qualitativ behandelt, nicht als populationsweite Effektgröße.

Q11 · Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, AI 100-2e2025

Urheber: Apostol Vassilev et al. / NIST **Datum / Version:** 2025-03 **Typ:** Finale technische Taxonomie **URL:**

<<https://csrc.nist.gov/pubs/ai/100/2/e2025/final>> **DOI:** 10.6028/NIST.AI.100-2e2025 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Publikationsseite / Abstract einschließlich Erratahinweis gelesen.

Fundstelle: Abstract; Attack goals, capabilities and knowledge; Errata.

Trägt: Einordnung von Angriffen auf KI über Ziele, Fähigkeiten und Lebenszyklus.

Grenzen: Taxonomie belegt keine Häufigkeit; keine Aussage, dass jede beschriebene Angriffsklasse im betrachteten System praktisch funktioniert.

Q12 · AI Risk Management Framework (AI RMF)

Urheber: NIST **Datum / Version:** Rahmenwerk 1.0 (2023); Webstand abgerufen 2026-09-25 **Typ:** Freiwilliges

KI-Risikomanagementrahmenwerk **URL:** <<https://www.nist.gov/itl/ai-risk-management-framework>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Überblicksseite gelesen.

Fundstelle: Overview; AI RMF 1.0.

Trägt: Lebenszyklusorientiertes Management von KI-Risiken.

Grenzen: Kein Medizinprodukte- oder Maschinen-Sicherheitsnachweis; Anwendung ersetzt keine Risikobeurteilung des Gesamtsystems.

Q13 · Best Current Practice for OAuth 2.0 Security, RFC 9700

Urheber: T. Lodderstedt et al. / IETF **Datum / Version:** 2025-01 **Typ:** IETF Best Current Practice **URL:**

<<https://www.rfc-editor.org/rfc/rfc9700.html>> **DOI:** 10.17487/RFC9700 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: RFC-Webvolltext / relevante Abschnitte gelesen.

Fundstelle: § 2 Best Practices; § 4 Threats and Mitigations.

Trägt: Aktuelle OAuth-Sicherheitsgrundsätze und Beschränkung von Tokenmissbrauch.

Grenzen: OAuth ist eine technische Grundlage, kein fertiges Agenten- oder Safety-Berechtigungsmodell.

Q14 · OAuth 2.0 Token Exchange, RFC 8693

Urheber: M. Jones et al. / IETF **Datum / Version:** 2020-01 **Typ:** IETF Proposed Standard **URL:** <<https://www.rfc-editor.org/rfc/rfc8693.html>> **DOI:** 10.17487/RFC8693 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: RFC-Webvolltext / Delegationsabschnitte gelesen.

Fundstelle: § 1.1 Delegation vs. Impersonation; § 4.1 act claim.

Trägt: Unterscheidung zwischen Stellvertretung und Weitergabe delegierter Autorität.

Grenzen: Token Exchange allein begrenzt keine physische Wirkung und erzeugt keine vollständige Verantwortlichkeitskette.

Q15 · OAuth 2.0 Token Revocation, RFC 7009

Urheber: T. Lodderstedt et al. / IETF **Datum / Version:** 2013-08 **Typ:** IETF Proposed Standard **URL:** <<https://www.rfc-editor.org/rfc/rfc7009.html>> **DOI:** 10.17487/RFC7009 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: RFC-Webvolltext / Widerrufsabschnitte gelesen.

Fundstelle: § 2.1–2.2 Revocation Request / Response; § 3 Implementation Note.

Trägt: Widerruf von Tokens und praktische Implementierungsbedingungen.

Grenzen: Ein Tokenwiderruf hebt bereits ausgeführte oder autonom weiterlaufende Maschinenaktionen nicht auf. Diese Folgerung ist eigene Systemanalyse.

Q16 · FHIR R5, Security, Version 5.0.0

Urheber: HL7 International **Datum / Version:** R5 (2023); abgerufen 2026-09-25 **Typ:** Technische Spezifikationsdokumentation **URL:** <<https://hl7.org/fhir/R5/security.html>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext / Abschnitte 6.1.0.1–6.1.0.5 gelesen.

Fundstelle: General Considerations; Authentication; Authorization/Access Control; Audit Log.

Trägt: FHIR setzt eine geeignete Sicherheitsarchitektur voraus; Schnittstellenstandard ist kein Sicherheitsprodukt.

Grenzen: Release R5 ausdrücklich gewählt; keine Behauptung, alle Kliniken nutzten R5 oder die Seite sei in jedem Verweis aktuell. OAuth-Draftverweis dort wird hier durch RFC 9700 ergänzt.

Q17 · Healthcare and Public Health Cybersecurity Performance Goals

Urheber: US HHS **Datum / Version:** abgerufen 2026-09-25 **Typ:** Freiwillige sektorale Behördenempfehlungen **URL:** <<https://hhs cyber.hhs.gov/cybersecurity-performance-goals.html>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext und konkrete Zielabschnitte gelesen.

Fundstelle: Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection.

Trägt: US-Referenz für grundlegende und weitergehende Gesundheits-Cybersicherheit.

Grenzen: Freiwillige US-Empfehlungen, keine unmittelbar geltenden deutschen Klinikpflichten.

Q18 · Electronic Health Records and Downtime Procedures

Urheber: US HHS ASPR TRACIE **Datum / Version:** abgerufen 2026-09-25 **Typ:** Behördliche Ressourcensammlung
URL: <<https://asprtracie.hhs.gov/technical-resources/66/electronic-health-records-and-downtime-procedures/0>>
DOI: Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Sammlung und Einträge gelesen.

Fundstelle: Downtime Procedures; Recovery; referenzierte Fallberichte.

Trägt: Recherchezugang zu klinischen Ausfall- und Wiederanlaufverfahren.

Grenzen: Sammlung ist keine einzelne Studie. Ergebnisse zugrunde liegender Studien müssen separat bewertet werden.

Q19 · Cybersecurity Vulnerabilities in Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication

Urheber: US FDA **Datum / Version:** 2025-01-30; maßgebliches Update 2025-07-02 **Typ:** Behördliche produktspezifische Sicherheitsmitteilung **URL:** <<https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webvolltext einschließlich zeitlich jüngster Ergänzung gelesen.

Fundstelle: July 2, 2025 Update; Recommendations for Health Care Providers and Facilities.

Trägt: Konkreter Monitorfall; Korrektur entfernt Netzwerkfunktion und lässt lokale Überwachung.

Grenzen: Historische Mitteilung; kein Beleg für erfolgten Patientenschaden. Kein allgemeiner Auftrag, Medizintechnik vom Netz zu trennen. Juli-Update geht älterem Text zur fehlenden Korrektur vor.

Q20 · Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Urheber: Christian Dameff et al. **Datum / Version:** 2023-05-08 **Typ:** Empirische Primärstudie / retrospektive Beobachtungsstudie **URL:** <<https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585>> **DOI:** 10.1001/jamanetworkopen.2023.12270 **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Web-Volltext, Methoden, Ergebnisse und Limitationen gelesen.

Fundstelle: JAMA Network Open 6(5):e2312270; Methods; Results; Limitations.

Trägt: Beobachtete Zusammenhänge zwischen regionalem Ransomwareereignis und Belastung angrenzender Notaufnahmen.

Grenzen: Assoziation, keine randomisierte Kausalidentifikation; begrenzte regionale Übertragbarkeit; keine Studie über KI-Angriffe.

Q21 · Anatomy of a Cyberattack: Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime

Urheber: Goodwin et al. **Datum / Version:** 2022 **Typ:** Primärer Erfahrungsbericht **URL:** <<https://pubmed.ncbi.nlm.nih.gov/35188951/>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: PubMed-Abstract / Metadaten gelesen; Volltext nicht ausgewertet.

Fundstelle: American Journal of Clinical Pathology 157(5):653–663; Abstract.

Trägt: Dokumentierter Erfahrungsbericht eines 25-tägigen Labor-IT-Ausfalls.

Grenzen: Nur Abstractzugriff; keine Detailbehauptungen über Interventionseffekt, Kennzahlen oder Volltextmethodik.

Q22 · MDCG 2019-16 rev. 1: Guidance on Cybersecurity for medical devices

Urheber: Medical Device Coordination Group / Europäische Kommission **Datum / Version:** 2020-07 (Rev. 1) **Typ:** Nicht verbindliche regulatorische Leitlinie **URL:** <https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Relevante PDF-Abschnitte gelesen; Inhaltsverzeichnis und Annex IV visuell geprüft.

Fundstelle: Abschnitte zu Design / Post-market; Annex IV, gedruckte S. 46.

Trägt: Wechselseitige Beziehung zwischen Cyberrisikomanagement und Safety-Risikomanagement bei Medizinprodukten.

Grenzen: Leitlinie ist ausdrücklich nicht rechtsverbindlich; kein Ersatz für MDR/IVDR oder den Normvolltext.

Q23 · IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices — Part 1

Urheber: IEC **Datum / Version:** 2021-09-21 **Typ:** Internationale Norm **URL:** <<https://webstore.iec.ch/en/publication/34263>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Metadaten und öffentliches Abstract; Normvolltext nicht zugänglich.

Fundstelle: Abstract / Scope; edition 2.0.

Trägt: Verantwortung und Risikomanagement beim Anschluss an Gesundheits-IT, Sicherheit, Wirksamkeit und Informationssicherheit.

Grenzen: Keine Klausel- oder Konformitätsprüfung. Normbeschaffung und Anwendungsprüfung erforderlich.

Q24 · IEC 62443-3-2:2020: Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design

Urheber: IEC **Datum / Version:** 2020 **Typ:** Internationale Norm **URL:** <<https://webstore.iec.ch/en/publication/30727>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Metadaten und öffentliches Abstract; Normvolltext nicht zugänglich.

Fundstelle: Abstract; system under consideration, zones and conduits.

Trägt: Risikobasierte Zerlegung industrieller Systeme in Zonen und Kommunikationspfade.

Grenzen: Kein frei behaupteter Security Level oder Nachweis normgerechter Umsetzung. Funktionale Safety gesondert prüfen.

Q25 · ISO 10218-1:2025: Robotics — Safety requirements — Part 1: Industrial robots

Urheber: ISO **Datum / Version:** 2025-02 **Typ:** Internationale Norm **URL:** <<https://www.iso.org/standard/73933.html>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Metadaten / Scope gelesen; Normvolltext nicht geprüft.

Fundstelle: Abstract / Scope; edition 3.

Trägt: Abgrenzung Anforderungen an Industrieroboter.

Grenzen: Ausgabestand allein belegt keine EU-Harmonisierung und keinen individuellen Konformitätsstatus.

Q26 · ISO 10218-2:2025: Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells

Urheber: ISO **Datum / Version:** 2025-02 **Typ:** Internationale Norm **URL:**

<<https://www.iso.org/standard/73934.html>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizielle Metadaten / Scope gelesen; Normvolltext nicht geprüft.

Fundstelle: Abstract / Scope; edition 2; ausdrückliche Ausschlüsse.

Trägt: Integration von Industrieroboteranwendungen und Zellen; begrenzter Geltungsbereich.

Grenzen: Nicht pauschal auf OP-Roboter, Pflegerobotik oder öffentliche Servicerobotik übertragbar. Normvolltext und Produktscope prüfen.

Q27 · ATT&CK for ICS: Loss of Safety, T0880

Urheber: MITRE **Datum / Version:** abgerufen 2026-09-25 **Typ:** Primäre Taxonomie / kuratierte Wissensbasis **URL:**

<<https://attack.mitre.org/techniques/T0880/>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Eintrag gelesen.

Fundstelle: Description; Mitigations; References.

Trägt: Begriff des Verlusts von Safety und Schutzebenen.

Grenzen: Taxonomie belegt keine Angriffsquote und keine lückenlose Historie.

Q28 · Triton Safety Instrumented System Attack, C0030

Urheber: MITRE **Datum / Version:** abgerufen 2026-09-25 **Typ:** Kuratierte historische Kampagnenbeschreibung **URL:**

<<https://attack.mitre.org/campaigns/C0030/>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Eintrag und Einordnung gelesen.

Fundstelle: Campaign description; techniques; references.

Trägt: Dokumentierter historischer Angriff auf eine industrielle Safety-Umgebung.

Grenzen: Kontextquelle; keine eigene forensische Verifikation; keine agentische KI-Kampagne.

Q29 · BSI-Gesetz (BSIG 2025), aktuelle bereitgestellte Fassung

Urheber: Bundesrepublik Deutschland / Gesetze im Internet **Datum / Version:** Gesetz 2025; Änderungsstand im Abruf 2026 **Typ:** Gesetz **URL:** <https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Bereitgestellter Volltext; §§ 28, 30–32, 38–39 und Änderungsvermerk gelesen.

Fundstelle: § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung.

Trägt: Differenzierte Einrichtungs-, Risiko-, Melde- und Leitungsanforderungen.

Grenzen: Keine automatische Einstufung eines konkreten Unternehmens. Gesetze-im-Internet-Fassung enthält Bearbeitungshinweise; Einzelfall und Spezialregeln separat prüfen.

Q30 · SGB V § 391 — IT-Sicherheit in Krankenhäusern

Urheber: Bundesrepublik Deutschland / Gesetze im Internet **Datum / Version:** aktuelle Fassung abgerufen

2026-09-25 **Typ:** Gesetz **URL:** <https://www.gesetze-im-internet.de/sgb_5/_391.html> **DOI:** Kein DOI in diesem

Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Vollständiger Paragraph gelesen.

Fundstelle: Absätze 1–5; besonders Abs. 5.

Trägt: Krankenhausspezifische IT-Sicherheit auch außerhalb der identischen KRITIS-Pflichtenkonstellation.

Grenzen: Keine Gleichsetzung aller Krankenhäuser mit Betreibern kritischer Anlagen; Abgrenzung nach Abs. 5 beachten.

Q31 · Betriebssicherheitsverordnung § 3 — Gefährdungsbeurteilung

Urheber: Bundesrepublik Deutschland / Gesetze im Internet **Datum / Version:** aktuelle Fassung abgerufen 2026-09-25 **Typ:** Rechtsverordnung **URL:** <https://www.gesetze-im-internet.de/betrsv_2015/__3.html> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Paragraph vollständig gelesen.

Fundstelle: Abs. 1–3 sowie Aktualisierung / Dokumentation.

Trägt: Betriebsbezogene Gefährdungsbeurteilung; CE-Kennzeichnung ersetzt Arbeitgeberpflichten nicht.

Grenzen: Konkrete Prüfpflichten und befähigte Personen aus weiteren Vorschriften und Anlagenscope ableiten, nicht allein aus diesem Paragraphen.

Q32 · Betriebsverfassungsgesetz § 87 — Mitbestimmungsrechte

Urheber: Bundesrepublik Deutschland / Gesetze im Internet **Datum / Version:** aktuelle Fassung abgerufen 2026-09-25 **Typ:** Gesetz **URL:** <https://www.gesetze-im-internet.de/betrvg/__87.html> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Paragraph gelesen.

Fundstelle: Abs. 1 Nr. 6 und 7.

Trägt: Mitbestimmungsprüfung bei technischer Beschäftigtenüberwachung und Gesundheitsschutz.

Grenzen: Betriebliche Anwendbarkeit und gesetzliche/tarifliche Vorrangregelungen prüfen; öffentliche und kirchliche Träger können anderen Vertretungsregeln unterliegen.

Q33 · AI Act — Application timeline and implementation

Urheber: Europäische Kommission, DG CONNECT **Datum / Version:** Webupdate 2026-08-03 **Typ:** Amtliche Erläuterung geltenden/gestuften EU-Rechts **URL:** <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Aktuelle Webseite einschließlich Omnibus- und Fristenabschnitt gelesen.

Fundstelle: Application timeline; How has the Commission simplified the implementation of the AI Act?.

Trägt: Kommission nennt 02.12.2027 für Anhang-III-Hochrisikoregeln und 02.08.2028 für produktintegrierte Hochrisiko-KI.

Grenzen: Amtliche Erläuterung ersetzt nicht konsolidierten Normtext. Dessen Abruf war technisch blockiert; rechtsverbindliche Subsumtion bleibt Freigabeaufgabe.

Q34 · AI Omnibus enters into force

Urheber: Europäische Kommission, DG CONNECT **Datum / Version:** 2026-07-27 **Typ:** Amtliche Mitteilung **URL:** <<https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext gelesen.

Fundstelle: Entry into force / transition periods.

Trägt: Bestätigung der 2026 geänderten AI-Act-Zeitachse.

Grenzen: Keine vollständige Normkommentierung; für Übergangs-/Bestandsfälle Q39 im Volltext nachprüfen.

Q35 · Machinery — Machinery Regulation

Urheber: Europäische Kommission, DG GROW **Datum / Version:** abgerufen 2026-09-25 **Typ:** Amtliche sektorale Rechtsübersicht **URL:**

<https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext / Anwendungsdatum gelesen.

Fundstelle: Machinery Regulation; mandatory application date.

Trägt: Grundsätzliche Anwendung der Maschinenverordnung ab 20.01.2027; Übergang von Maschinenrichtlinie.

Grenzen: Kein individueller Bescheid; Produktscope, Umbau und aktuelle konsolidierte Anhänge Q40 separat prüfen.

Q36 · Cyber Resilience Act — Implementation

Urheber: Europäische Kommission, DG CONNECT **Datum / Version:** Webupdate 2026-07-27 **Typ:** Amtliche Rechtsübersicht **URL:** <<https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>>

DOI: Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext / Zeitachse gelesen.

Fundstelle: Implementation timeline.

Trägt: Hauptanwendung 11.12.2027; vorgezogene Berichtspflichten 11.09.2026.

Grenzen: Produkt- und Rollenprüfung erforderlich; nicht jeder Betreiber ist Hersteller.

Q37 · Cyber Resilience Act — Reporting obligations

Urheber: Europäische Kommission, DG CONNECT **Datum / Version:** Webupdate 2026-09-11 **Typ:** Amtliche Rechtsübersicht **URL:** <<https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Webtext vollständig gelesen.

Fundstelle: What are the main rules?; Where should manufacturers submit their notifications?.

Trägt: Herstellerberichte 24/72 Stunden; unterschiedliche Abschlussfristen; SRP; abweichender Beginn für Open-Source-Stewards.

Grenzen: Aktiv ausgenutzte Schwachstelle und schwerwiegender Vorfall unterscheiden. Kein Ersatz für Einzelfallprüfung des CRA.

Q38 · Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung

Urheber: Europäische Union **Datum / Version:** 2016; aktuelle Fassung vor Anwendung prüfen **Typ:** EU-Verordnung / Nachschlagequelle **URL:** <<https://eur-lex.europa.eu/eli/reg/2016/679/oj/deu>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Direkter Web-Volltextabruf technisch blockiert; nicht als neu volltextverifiziert ausgewiesen.

Fundstelle: Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff..

Trägt: Nachschlagepfad für Datenschutz, Datensicherheit, Betroffenenrisiko und Meldepflichten.

Grenzen: Artikelzuordnung dient der rechtlichen Prüfung. Redaktionell bekannte Regelungsinhalte werden nicht als vollständig neu geprüfte konsolidierte Rechtsberatung ausgegeben.

Q39 · AI Act, Verordnung (EU) 2024/1689 — konsolidierte Fassung vom 27.07.2026

Urheber: Europäische Union **Datum / Version:** 2026-07-27 **Typ:** EU-Verordnung / Nachschlagequelle **URL:** <<https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng>> **DOI:** Kein DOI in diesem Register angegeben.
Abruf-/Prüfdatum: 2026-09-25

Zugriffstiefe: Abruf technisch blockiert; aktuelle Zeitachse über Q33/Q34 geprüft.

Fundstelle: Art. 6, 9–15, 26, 113; Anhänge I/III; Änderungsverordnung EU 2026/1744.

Trägt: Normpfad für Rollen, Risiko-Einstufung, Aufsicht und Übergang.

Grenzen: Keine Behauptung, der konsolidierte Volltext sei in dieser Recherche geprüft worden. Geänderte Detailvorschriften vor konkreter Nutzung juristisch lesen.

Q40 · Verordnung (EU) 2023/1230 — Maschinenverordnung

Urheber: Europäische Union **Datum / Version:** 2023; konsolidierte Fassung vor Anwendung prüfen **Typ:** EU-Verordnung / Nachschlagequelle **URL:** <<https://eur-lex.europa.eu/eli/reg/2023/1230/oj/deu>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Volltextabruf technisch blockiert; Datum/Überblick über Q35 geprüft.

Fundstelle: Anwendungs-/Übergangsbestimmungen; Anhang III insbesondere 1.1.9 und 1.2.1 als Prüfsuchstellen.

Trägt: Normpfad zum Schutz sicherheitsrelevanter Software und Steuerungssysteme.

Grenzen: Fundstellen sind Suchaufträge für die aktuelle Volltextprüfung, kein behaupteter vollständiger Nachweis sämtlicher Anforderungen.

Q41 · Verordnung (EU) 2024/2847 — Cyber Resilience Act

Urheber: Europäische Union **Datum / Version:** 2024; Anwendungsstufen bis 2027 **Typ:** EU-Verordnung / Nachschlagequelle **URL:** <<https://eur-lex.europa.eu/eli/reg/2024/2847/oj/deu>> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Volltextabruf technisch blockiert; aktuelle Übersicht und Berichtspflichten Q36/Q37 gelesen.

Fundstelle: Art. 2 Scope; Art. 14–16 Meldung; Art. 24 Software-Stewards; Art. 71 Fristen.

Trägt: Normpfad zur produktspezifischen und rollenabhängigen Prüfung.

Grenzen: Ausnahmen, unter anderem sektoral regulierte Produkte, müssen am aktuellen Normtext einzeln bestätigt werden.

Q42 · BSI-Standard 200-4: Business Continuity Management

Urheber: BSI **Datum / Version:** 2023-06-14 **Typ:** Finaler BSI-Standard / Nachschlagequelle **URL:** <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.html> **DOI:** Kein DOI in diesem Register angegeben. **Abruf-/Prüfdatum:** 2026-09-25

Zugriffstiefe: Offizieller Suchindex mit Titel/Datum/Abstract; direkter Abruf 403.

Fundstelle: Standard 200-4; Hilfsmittel zu Business Impact Analyse, Vorsorge, Übungen.

Trägt: Deutsche BCMS-Referenz und Beschaffungs-/Nachschlagepfad.

Grenzen: Keine vorgetäuschte Volltext- oder Kapitelprüfung. Eigene BCM-Vorlagen dieses Pakets sind nicht die offiziellen BSI-Vorlagen.

Claim–Evidence–Matrix

46 tragende Aussagen · Stand 25. September 2026. Diese Matrix trennt berichtete Beobachtung, normative Aussage, amtliche Umsetzungshilfe und eigene Ableitung. Quellenbezug ist keine Konformitätsbescheinigung. Eigene mathematische Beispiele sind ausdrücklich nicht aus einem Leitfaden abgelesene Messwerte.

C01 · BERICHTETER_BEFUND

Gambit beschreibt eine agentengestützte Kampagne gegen Onlinehändler; der Bericht ist vorläufig.

Fundstelle in dieser Ausgabe: L01 §3 **Quellen:** Q01 **Nachschlagestellen:** Executive Summary; Methodology; Cost; Data Exfiltration / Cleanup **Aussagegrenze:** Anbieterbericht; keine unabhängige Rohdatenprüfung durch FluxLane.

Konsequenz für die Anwendung: Als Anlass verwenden, nicht als Beweis für Klinik-/Roboterkompromittierung.

C02 · BERICHTETER_BEFUND

Die 25,46 US-Dollar sind durchschnittliche Modellkosten eines abgeschlossenen Scans, kein belegter Preis erfolgreicher Kompromittierung.

Fundstelle in dieser Ausgabe: L01 §3 **Quellen:** Q01 **Nachschlagestellen:** Executive Summary; Methodology; Cost; Data Exfiltration / Cleanup **Aussagegrenze:** Nicht Gesamtkosten des Angreifers; nicht auf andere Zielklassen übertragbar.

Konsequenz für die Anwendung: Keine Wirtschaftlichkeitsrechnung für den eigenen Betrieb daraus ableiten.

C03 · BERICHTETER_BEFUND

Der beschriebene Tabellenverlust verdeutlicht möglichen unbeabsichtigten Schaden automatisierter Aktionen.

Fundstelle in dieser Ausgabe: L01 §3 **Quellen:** Q01 **Nachschlagestellen:** Executive Summary; Methodology; Cost; Data Exfiltration / Cleanup **Aussagegrenze:** 180 Tabellen laut Anbieter; keine eigene forensische Bestätigung.

Konsequenz für die Anwendung: Auch Fehlhandlungen normaler und defensiver Agenten in Risikoanalyse aufnehmen.

C04 · FINALE_LEITLINIE

OT-Sicherheit muss physische Prozesse, Zuverlässigkeit und Safety berücksichtigen.

Fundstelle in dieser Ausgabe: L01 §§1,6; L03 §§1,5 **Quellen:** Q02 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 **Aussagegrenze:** US-Leitlinie; kein lokaler Sicherheitsnachweis. **Konsequenz für die Anwendung:** Wirkungskette statt ausschließlich IT-Asset betrachten.

C05 · QUELLENSTATUS

SP 800-82 Rev. 3 ist eine finale Leitlinie; Rev. 4 liegt zum Stichtag als Initial Public Draft vor.

Fundstelle in dieser Ausgabe: L01; Quellenregister **Quellen:** Q02, Q03 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 | Status / Announcement / Abstract; Kommentierungsfrist 30.11.2026 **Aussagegrenze:** Ein Entwurf ist nicht als finaler Maßstab oder deutsche Pflicht auszugeben. **Konsequenz für die Anwendung:** Ausgabe und Status im lokalen Standardregister festhalten.

C06 · EIGENE_SYNTHESE

Handlungsvollmacht und Leistungsabhängigkeit sind zusätzliche Prüfsichten, keine neu gesetzlich vorgeschriebenen Graphprodukte.

Fundstelle in dieser Ausgabe: L01 §7 **Quellen:** Q02, Q06, Q09 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 | Abstract; ressourcenbezogenes

Vertrauen und getrennte Authentisierung/Autorisierung | Project overview; Identity and Authorization

Aussagegrenze: Eigene Zusammenführung etablierter Konzepte; keine Neuheits- oder Patentbehauptung.

Konsequenz für die Anwendung: Graphen am lokalen Daten- und Befehlsfluss aufbauen.

C07 · EIGENES_MODELL

Das formale Autorisierungsmodell in L01 ordnet Prüfbedingungen, beweist aber keine Systemkorrektheit.

Fundstelle in dieser Ausgabe: L01 §9 **Quellen:** Q06, Q13, Q14 **Nachschlagestellen:** Abstract; ressourcenbezogenes Vertrauen und getrennte Authentisierung/Autorisierung | § 2 Best Practices; § 4 Threats and Mitigations | § 1.1

Delegation vs. Impersonation; § 4.1 act claim **Aussagegrenze:** Formalisierung ist Entwurfsmodell ohne maschinellen Beweis und ohne Vollständigkeitsgarantie. **Konsequenz für die Anwendung:** Invarianten konkret implementieren und testen.

C08 · EMPIRISCHE_STUDIE

Die JAMA-Studie untersucht Versorgungsbelastungen an benachbarten Notaufnahmen während eines Ransomwareereignisses.

Fundstelle in dieser Ausgabe: L02 §14 **Quellen:** Q20 **Nachschlagestellen:** JAMA Network Open 6(5):e2312270; Methods; Results; Limitations **Aussagegrenze:** Retrospektiver Zusammenhang; kein allgemeiner Kausalnachweis für KI, Mortalität oder jede Region. **Konsequenz für die Anwendung:** Regionale Abhängigkeiten und Ausweichkapazität prüfen.

C09 · ABSTRACT_ERFAHRUNGSBERICHT

Der publizierte Laborbericht behandelt einen länger dauernden IT-Ausfall und Ersatzabläufe.

Fundstelle in dieser Ausgabe: L02 §§7,17 **Quellen:** Q21 **Nachschlagestellen:** American Journal of Clinical Pathology 157(5):653–663; Abstract **Aussagegrenze:** Hier Abstract gelesen, nicht vollständige Methoden-/Ergebnisprüfung. **Konsequenz für die Anwendung:** Keine konkreten Leistungswerte universell übernehmen.

C10 · GERAETESPEZIFISCHE_BEHOERDENMITTEILUNG

Die FDA beschreibt für bestimmte Contec/Epsimed-Monitore Cyberprobleme und eine Netzwerkentfernung durch eine konkrete Korrektur.

Fundstelle in dieser Ausgabe: L02 §9 **Quellen:** Q19 **Nachschlagestellen:** July 2, 2025 Update; Recommendations for Health Care Providers and Facilities **Aussagegrenze:** Modell- und mitteilungsspezifisch; Stand der Mitteilung ist nicht heutiger Status aller Geräte. **Konsequenz für die Anwendung:** Herstellerangaben und eigene Alarm-/Personalabhängigkeiten prüfen; nicht pauschal trennen.

C11 · SPEZIFIKATION

FHIR stellt selbst keine vollständige Sicherheitslösung bereit.

Fundstelle in dieser Ausgabe: L02 §10 **Quellen:** Q16 **Nachschlagestellen:** General Considerations; Authentication; Authorization/Access Control; Audit Log **Aussagegrenze:** R5-Sicherheitsabschnitt; Implementierung muss Authentifizierung, Autorisierung und Audit ergänzen. **Konsequenz für die Anwendung:** Interoperabilitätsabnahme getrennt von Sicherheits- und Prozessabnahme durchführen.

C12 · EIGENE_SYNTHESE

Patientenidentität, Auftragsbindung und Version sind Bestandteile einer end-to-end Integritätsprüfung.

Fundstelle in dieser Ausgabe: L02 §§4–7 **Quellen:** Q16, Q17, Q22 **Nachschlagestellen:** General Considerations; Authentication; Authorization/Access Control; Audit Log | Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection | Abschnitte zu Design / Post-market; Annex IV, gedruckte S. 46

Aussagegrenze: Konkrete Prüfkontrollen eigene Anwendungssynthese, keine behauptete Einzelklausel.

Konsequenz für die Anwendung: K09–K13 und F02/F05 lokal umsetzen.

C13 · EIGENE_SYNTHESE

Klinischer Mindestbetrieb braucht Kapazität, Personal, Kommunikation und eine zeitliche Grenze.

Fundstelle in dieser Ausgabe: L02 §§11–13 **Quellen:** Q17, Q18, Q21 **Nachschlagestellen:** Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection | Downtime Procedures; Recovery; referenzierte Fallberichte | American Journal of Clinical Pathology 157(5):653–663; Abstract **Aussagegrenze:** Minimum Viable Hospital ist keine hier nachgewiesene normierte Betriebsart. **Konsequenz für die Anwendung:** F08 mit realer Schichtbesetzung und Durchgängigkeit prüfen.

C14 · NORMTEXT_GELESEN

§391 SGB V betrifft IT-Sicherheitsvorkehrungen von Krankenhäusern einschließlich Awareness und Angemessenheit; Abs.5 grenzt bereits als kritische Anlagen verpflichtete Betreiber ab.

Fundstelle in dieser Ausgabe: L02 §2; L05 §5 **Quellen:** Q30 **Nachschlagestellen:** Absätze 1–5; besonders Abs. 5

Aussagegrenze: Keine Aussage, dass jedes Krankenhaus dieselben KRITIS-/BSIG-Zusatzpflichten hat. **Konsequenz für die Anwendung:** Rollen und Anwendungsbereiche einzeln dokumentieren.

C15 · NORMMETADATEN

IEC 80001-1:2021 betrifft das Risikomanagement verbundener Gesundheits-IT-Systeme.

Fundstelle in dieser Ausgabe: L02 §2 **Quellen:** Q23 **Nachschlagestellen:** Abstract / Scope; edition 2.0

Aussagegrenze: Nur öffentliche Metadaten/Scope; Normvolltext nicht ausgewertet. **Konsequenz für die Anwendung:** Aktuelle einschlägige Norm beschaffen und Fachanwendung prüfen.

C16 · NORMMETADATEN

IEC 62443-3-2:2020 behandelt Risikobeurteilung sowie Zonen und Kommunikationsverbindungen.

Fundstelle in dieser Ausgabe: L03 §6 **Quellen:** Q24 **Nachschlagestellen:** Abstract; system under consideration, zones and conduits **Aussagegrenze:** Keine SL-Zuordnung oder Konformität aus öffentlichem Abstract. **Konsequenz für die Anwendung:** Lokale Zonierung und Vertrauensübergänge evidenzbasiert ableiten.

C17 · NORMMETADATEN

ISO 10218-1 und -2 liegen in Ausgaben 2025 für industrielle Robotik beziehungsweise Anwendungen vor.

Fundstelle in dieser Ausgabe: L03 §18 **Quellen:** Q25, Q26 **Nachschlagestellen:** Abstract / Scope; edition 3 | Abstract / Scope; edition 2; ausdrückliche Ausschlüsse **Aussagegrenze:** Scope-Ausschlüsse beachten; kein pauschaler Transfer auf medizinische oder öffentliche Robotik; Harmonisierung nicht hier nachgewiesen. **Konsequenz für die Anwendung:** Relevante Normvolltexte und Konformitätsweg fachlich prüfen.

C18 · TAXONOMIE_HISTORISCHER_FALL

MITRE dokumentiert Loss of Safety und den historischen Triton-Angriff als industriellen Kontext.

Fundstelle in dieser Ausgabe: L03 §§5,8 **Quellen:** Q27, Q28 **Nachschlagestellen:** Description; Mitigations; References | Campaign description; techniques; references **Aussagegrenze:** Kuratiertes Wissen; keine Primärforsik durch FluxLane und kein AI-Agent-Angriff. **Konsequenz für die Anwendung:** Safety-Pfade und gemeinsame Ursachen prüfen, keine Häufigkeit daraus ableiten.

C19 · EIGENE_SYNTHESE

Ein allgemeines Policy-Gateway ist nicht automatisch eine sicherheitsgerichtete Schutzfunktion.

Fundstelle in dieser Ausgabe: L03 §8; L04 §5 **Quellen:** Q02, Q24, Q25, Q26 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 | Abstract; system under consideration, zones and conduits | Abstract / Scope; edition 3 | Abstract / Scope; edition 2; ausdrückliche Ausschlüsse **Aussagegrenze:** Konkrete technische Unabhängigkeit und erforderliche Sicherheitseigenschaften sind lokal nachzuweisen. **Konsequenz für die Anwendung:** Safety-Verantwortung und Security-Policy getrennt abnehmen.

C20 · EIGENE_SYNTHESE

Stoppen, Netzwerkisolieren und Energieabschalten sind unterschiedliche Eingriffe.

Fundstelle in dieser Ausgabe: L03 §15; L06 §10 **Quellen:** Q02 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 **Aussagegrenze:** Keine universelle Stoppreihenfolge oder sichere Abschaltzeit. **Konsequenz für die Anwendung:** Gefährdungsbeurteilung und Betriebsarten bestimmen die Reaktion.

C21 · NORMTEXT_GELESEN

Eine CE-Kennzeichnung ersetzt nicht die nach §3 BetrSichV erforderliche betriebliche Gefährdungsbeurteilung.

Fundstelle in dieser Ausgabe: L03 §18; L05 §4 **Quellen:** Q31 **Nachschlagestellen:** Abs. 1–3 sowie Aktualisierung / Dokumentation **Aussagegrenze:** Die konkret geltende Betreiberrolle und Arbeitsmittelsituation bleiben zu prüfen. **Konsequenz für die Anwendung:** Betrieblichen Nachweis neben Produktunterlagen führen.

C22 · EIGENE_SYNTHESE

Produktqualität und Chargenfreigabe sind von der technischen Wiederfreigabe zu unterscheiden.

Fundstelle in dieser Ausgabe: L03 §§10,16 **Quellen:** Q02, Q07, Q08 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 | Abstract; cyber resiliency engineering | Abstract; Backup und Recovery für OT **Aussagegrenze:** Abgeleitete Betriebsregel, keine pauschale branchenspezifische Qualitätsvorschrift. **Konsequenz für die Anwendung:** Produkt- und Prozessdaten separat rekonstruieren und fachlich entscheiden.

C23 · PROJEKT_FACHBEITRAG

NIST behandelt eigenständige Agentenidentitäten, begrenzte Rechte und Delegation als Sicherheitsaufgabe.

Fundstelle in dieser Ausgabe: L04 §§3,4 **Quellen:** Q09, Q10 **Nachschlagestellen:** Project overview; Identity and Authorization | Agent identities; credentials; authorization; consent fatigue **Aussagegrenze:** Projekt/Fachbeitrag, keine finale neue Pflichtnorm. **Konsequenz für die Anwendung:** Getrennte technische Identität und verantwortliche menschliche Rolle dokumentieren.

C24 · SPEZIFIKATION

OAuth-Sicherheitspraktiken, Tokenexchange und Widerruf sind unterschiedliche Spezifikationsgegenstände.

Fundstelle in dieser Ausgabe: L04 §§4,10 **Quellen:** Q13, Q14, Q15 **Nachschlagestellen:** § 2 Best Practices; § 4 Threats and Mitigations | § 1.1 Delegation vs. Impersonation; § 4.1 act claim | § 2.1–2.2 Revocation Request / Response; § 3 Implementation Note **Aussagegrenze:** Protokollkonformität garantiert nicht fachlich richtige Anwendung oder Safety. **Konsequenz für die Anwendung:** Passende Implementierung, Sender-/Ressourcenbindung und Negativtests prüfen.

C25 · SPEZIFIKATION_UND_ABLEITUNG

Tokenwiderrief darf nicht mit Rücknahme schon ausgelöster physischer oder fachlicher Wirkung gleichgesetzt werden.

Fundstelle in dieser Ausgabe: L04 §10; L06 §6 **Quellen:** Q15, Q02 **Nachschlagestellen:** § 2.1–2.2 Revocation Request / Response; § 3 Implementation Note | §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 **Aussagegrenze:** RFC7009 regelt Tokens, nicht sämtliche Jobs, Caches und Aktoren. **Konsequenz für die Anwendung:** Effektiven Zeitpunkt und Restwirkungen an den Endpunkten testen.

C26 · TAXONOMIE_UND_ABLEITUNG

Prompt Injection, manipulierte Quelldaten und Modellfehler benötigen unterscheidbare Analysen.

Fundstelle in dieser Ausgabe: L04 §9 **Quellen:** Q11, Q12 **Nachschlagestellen:** Abstract; Attack goals, capabilities and knowledge; Errata | Overview; AI RMF 1.0 **Aussagegrenze:** Nicht jede falsche Ausgabe ist Prompt Injection; die Taxonomie ist kein lokaler Detektor. **Konsequenz für die Anwendung:** Untrusted input nicht zur Autorisierungsquelle machen.

C27 · EIGENE_SYNTHESE

Prüfung und Ausführung müssen an den maßgeblichen aktuellen Zustand gebunden sein.

Fundstelle in dieser Ausgabe: L04 §11 **Quellen:** Q06, Q13, Q14 **Nachschlagestellen:** Abstract; ressourcenbezogenes Vertrauen und getrennte Authentisierung/Autorisierung | § 2 Best Practices; § 4 Threats and Mitigations | § 1.1 Delegation vs. Impersonation; § 4.1 act claim **Aussagegrenze:** Kein Protokoll garantiert ohne Anwendungsgestaltung die Vermeidung aller Zeitfensterfehler. **Konsequenz für die Anwendung:** Version, Auftrag, Wiederholung und Warteschlange testen.

C28 · EIGENE_SYNTHESE

Defensive Agenten benötigen begrenzte, nebenwirkungsgeprüfte Reaktionsmandate.

Fundstelle in dieser Ausgabe: L04 §14; L06 §10 **Quellen:** Q05, Q07, Q10 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 | Abstract; cyber resiliency engineering | Agent identities; credentials; authorization; consent fatigue **Aussagegrenze:** Empfehlung, keine bewiesene optimale Automatisierungsquote. **Konsequenz für die Anwendung:** F09 einschließlich Rücknahme, Vertretung und Gegenproben.

C29 · EIGENE_SYNTHESE

Menschliche Freigabe trägt nur mit Information, Kompetenz, Zeit und tatsächlicher Entscheidungsbefugnis.

Fundstelle in dieser Ausgabe: L04 §13 **Quellen:** Q10, Q12 **Nachschlagestellen:** Agent identities; credentials; authorization; consent fatigue | Overview; AI RMF 1.0 **Aussagegrenze:** Keine Garantie durch bloßes Human-in-the-Loop-Label. **Konsequenz für die Anwendung:** Freigabearbeit und Ausnahmezustände realistisch testen.

C30 · NORMTEXT_GELESEN

BSIG §§28,30,31,32,38 und 39 betreffen unterschiedliche Anwendungs-, Risiko-, Melde-, Leitungs- und Nachweisaspekte.

Fundstelle in dieser Ausgabe: L05 §§4,5,7 **Quellen:** Q29 **Nachschlagestellen:** § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung **Aussagegrenze:** Pflichten hängen von Rolle und Anwendungsbereich ab; kein universelles Krankenhaus- oder Unternehmenspaket. **Konsequenz für die Anwendung:** F06 und gesonderte Meldeentscheidung je Rechtsregime.

C31 · NORMTEXT_GELESEN

BSIG §32 sieht bei einschlägigen erheblichen Vorfällen gestufte Meldungen mit 24-/72-Stunden-Schritten und einem Folgebericht vor.

Fundstelle in dieser Ausgabe: L05 §7; F13 **Quellen:** Q29 **Nachschlagestellen:** § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung **Aussagegrenze:** Fristauslöser,

Inhalt, Zeitpunkt des Folgeberichts und Fortdauer müssen am Normtext geprüft werden. **Konsequenz für die Anwendung:** Kenntnisstand und jede Pflichtuhr getrennt dokumentieren; Frist ist keine Warteempfehlung.

C32 · AMTLICHE_UMSETZUNGSINFORMATION

Die Kommission nennt für die geänderte AI-Act-Zeitachse 2.12.2027 für bestimmte Hochrisikofälle und 2.8.2028 für produktintegrierte Hochrisikosysteme.

Fundstelle in dieser Ausgabe: L05 §6 **Quellen:** Q33, Q34, Q39 **Nachschlagestellen:** Application timeline; How has the Commission simplified the implementation of the AI Act? | Entry into force / transition periods | Art. 6, 9–15, 26, 113; Anhänge I/III; Änderungsverordnung EU 2026/1744 **Aussagegrenze:** Kommissionsseiten gelesen; konsolidierter Normvolltext technisch blockiert. Keine Verschiebung sämtlicher AI-Act-Pflichten. **Konsequenz für die Anwendung:** Konkrete Rolle, Systemkategorie und Übergangsbestimmung vor Anwendung rechtsfachlich prüfen.

C33 · AMTLICHE_UMSETZUNGSINFORMATION

Die Maschinenverordnung gilt nach Kommissionsdarstellung grundsätzlich ab 20.1.2027.

Fundstelle in dieser Ausgabe: L03 §18; L05 §6 **Quellen:** Q35, Q40 **Nachschlagestellen:** Machinery Regulation; mandatory application date | Anwendungs-/Übergangsbestimmungen; Anhang III insbesondere 1.1.9 und 1.2.1 als Prüfsuchstellen **Aussagegrenze:** Normvolltext hier technisch blockiert; Einzelfall- und Übergangsvorschriften nicht vollständig geprüft. **Konsequenz für die Anwendung:** Keine ungeprüfte Klauselparaphrase als abschließende Rechtsberatung verwenden.

C34 · AMTLICHE_UMSETZUNGSINFORMATION

CRA-Hauptpflichten und Meldepflichten haben unterschiedliche Anwendungsdaten.

Fundstelle in dieser Ausgabe: L05 §§6,7 **Quellen:** Q36, Q37, Q41 **Nachschlagestellen:** Implementation timeline | What are the main rules?; Where should manufacturers submit their notifications? | Art. 2 Scope; Art. 14–16 Meldung; Art. 24 Software-Stewards; Art. 71 Fristen **Aussagegrenze:** Hauptanwendung 11.12.2027; Hersteller-Meldepflichten seit 11.9.2026; Produkt-/Rollenausnahmen prüfen. **Konsequenz für die Anwendung:** Herstellerrolle und Ereignisart bestimmen; nicht jeden Betreiber als meldepflichtigen Hersteller behandeln.

C35 · AMTLICHE_UMSETZUNGSINFORMATION

CRA-Abschlussmeldungen unterscheiden aktiv ausgenutzte Schwachstellen von schweren Sicherheitsvorfällen.

Fundstelle in dieser Ausgabe: L05 §7; F13 **Quellen:** Q37 **Nachschlagestellen:** What are the main rules?; Where should manufacturers submit their notifications? **Aussagegrenze:** 24/72-Stunden-Schritte sowie 14 Tage nach verfügbarer Korrektur bzw. ein Monat nach 72-Stunden-Meldung laut amtlicher Übersicht; konkrete Anwendung prüfen. **Konsequenz für die Anwendung:** Kein einheitliches Schlussberichtsdatum für alle Ereignistypen.

C36 · NORM_NACHSCHLAGEAUFTRAG

DSGVO-Prüfung betrifft insbesondere Zweck, Rechtsgrundlage, besondere Daten, Sicherheitsmaßnahmen, Datenschutzvorfälle und gegebenenfalls Folgenabschätzung.

Fundstelle in dieser Ausgabe: L05 §§7,8 **Quellen:** Q38 **Nachschlagestellen:** Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff. **Aussagegrenze:** Direkter Normabruf war blockiert; einschlägige Artikel vor verbindlicher Anwendung aktuell rechtsfachlich gegenprüfen. **Konsequenz für die Anwendung:** Kein pauschales 72-Stunden-Schema für alle Cyberereignisse oder alle Beteiligten.

C37 · NORMTEXT_GELESEN

Technische Beschäftigtenüberwachung kann Beteiligungsrechte nach §87 BetrVG auslösen.

Fundstelle in dieser Ausgabe: L05 §9 **Quellen:** Q32 **Nachschlagestellen:** Abs. 1 Nr. 6 und 7 **Aussagegrenze:** Anwendbarkeit und parallele Personalvertretungs- oder kirchliche Regeln lokal prüfen. **Konsequenz für die**

Anwendung: Überwachungskonzept früh datenschutz- und beteiligungsrechtlich prüfen.

C38 · EIGENE_ORGANISATIONSEMPFEHLUNG

Ein gemeinsames Cyber-Physical-Gremium kann Zuständigkeitslücken schließen, ersetzt aber keine gesetzlichen Organe oder Fachrollen.

Fundstelle in dieser Ausgabe: L05 §§10,11 **Quellen:** Q04, Q05, Q29 **Nachschlagestellen:** Abstract; Funktionen GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER | Abstract; Integration von Incident Response in CSF 2.0 | § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung **Aussagegrenze:** Kein allgemein vorgeschriebenes neues Gremium und keine Beschäftigungsprognose. **Konsequenz für die Anwendung:** Mandat, Entscheidung, Vertretung und Eskalation statt nur Titel festlegen.

C39 · FINALE_LEITLINIE_UND_ABLEITUNG

Resilienz umfasst Wiederherstellung und Anpassung; ein einzelnes Backup beweist keine betriebliche Wiederanlauffähigkeit.

Fundstelle in dieser Ausgabe: L06 §§12–14 **Quellen:** Q05, Q07, Q08 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 | Abstract; cyber resiliency engineering | Abstract; Backup und Recovery für OT **Aussagegrenze:** Konkrete Abhängigkeiten, Zielzeiten und Leistungsfähigkeit sind lokal zu erheben. **Konsequenz für die Anwendung:** Isolierte Sicherungen, Engineering-Stände, Schlüssel und Bootstrappfade prüfen.

C40 · EIGENE_EVIDENZGRENZE

Hashgleichheit belegt Unverändertheit relativ zu einem Referenzwert, nicht die fachliche Richtigkeit oder Schadsoftwarefreiheit.

Fundstelle in dieser Ausgabe: L01 §14; L06 §13 **Quellen:** Q07, Q08 **Nachschlagestellen:** Abstract; cyber resiliency engineering | Abstract; Backup und Recovery für OT **Aussagegrenze:** Technische Ableitung; ein kompromittierter Referenzwert bietet keine unabhängige Sicherheit. **Konsequenz für die Anwendung:** Validierungszeitraum und Vertrauen in Referenz, Daten und Schlüssel separat begründen.

C41 · EIGENE_SYNTHESE

Wiederhergestellte Daten und im Notbetrieb entstandene Vorgänge brauchen einen nachvollziehbaren Abgleich.

Fundstelle in dieser Ausgabe: L02 §15; L03 §16; L06 §15 **Quellen:** Q08, Q18, Q21 **Nachschlagestellen:** Abstract; Backup und Recovery für OT | Downtime Procedures; Recovery; referenzierte Fallberichte | American Journal of Clinical Pathology 157(5):653–663; Abstract **Aussagegrenze:** Keine universelle Merge-Regel für klinische oder industrielle Konflikte. **Konsequenz für die Anwendung:** F11 mit Fachverantwortung, Duplikaten, Korrekturen und offenen Konflikten.

C42 · MATHEMATISCHE_ABLEITUNG

Null Fehler in 100 unabhängigen vergleichbaren Versuchen ergeben keine Fehlerwahrscheinlichkeit von null.

Fundstelle in dieser Ausgabe: L06 §7 **Quellen:** Q05 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 **Aussagegrenze:** Die konkrete Binomialrechnung ist eigene Mathematik; Q05 ist nur Prüfkontext, nicht Quelle der Formel. Unabhängigkeitsannahme oft nicht erfüllt. **Konsequenz für die Anwendung:** Stichprobe, Testverteilung und Restunsicherheit offenlegen.

C43 · MATHEMATISCHE_ABLEITUNG

Hohe Sensitivität und Spezifität verhindern bei seltenen Ereignissen nicht automatisch viele Fehlalarme.

Fundstelle in dieser Ausgabe: L06 §7 **Quellen:** Q05 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 **Aussagegrenze:** Das Zahlenbeispiel ist hypothetische Bayes-Rechnung, keine Produktmessung

und kein empirischer Wert aus Q05. **Konsequenz für die Anwendung:** Grundrate und Fehlalarmfolgen in der Bewertung ausweisen.

C44 · EIGENE_PRUEFMETHODIK

Tabletop, technischer Test und End-to-End-Betriebsprobe tragen unterschiedliche Nachweise.

Fundstelle in dieser Ausgabe: L06 §8 **Quellen:** Q05, Q17, Q18 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 | Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection | Downtime Procedures; Recovery; referenzierte Fallberichte **Aussagegrenze:** Keines dieser Verfahren ersetzt alle anderen oder eine unabhängige fachliche Bewertung. **Konsequenz für die Anwendung:** F15 muss Testart, Scope, Status und Evidenz eindeutig enthalten.

C45 · EIGENE_PRUEFMETHODIK

Der Kontrollkatalog ist ein eigener Prüfraum, keine vollständige Normkonformitätsmatrix.

Fundstelle in dieser Ausgabe: L01 §16; Kontrollkatalog **Quellen:** Q02, Q04, Q05, Q17, Q24 **Nachschlagestellen:** §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138 | Abstract; Funktionen GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER | Abstract; Integration von Incident Response in CSF 2.0 | Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection | Abstract; system under consideration, zones and conduits **Aussagegrenze:** Kontrollen sind quellenbegründete Synthese, ihre Wirksamkeit wurde nicht lokal getestet. **Konsequenz für die Anwendung:** 60 Kontrollen auf Anwendbarkeit prüfen, positive und negative Tests durchführen.

C46 · EIGENE_PRUEFMETHODIK

Eine technische Qualitätskontrolle des Dokuments ist keine externe Begutachtung und keine Betriebsfreigabe.

Fundstelle in dieser Ausgabe: L05 §18; L06 §§1,19 **Quellen:** Q05 **Nachschlagestellen:** Abstract; Integration von Incident Response in CSF 2.0 **Aussagegrenze:** Die Unterscheidung ist methodische Abgrenzung, nicht ein vom NIST erteiltes Gütesiegel. **Konsequenz für die Anwendung:** Externe klinische, juristische und Safety-Prüfung sowie lokale Tests separat ausweisen.

Methodik, Recherche und Quellenkritik

Redaktions- und Recherchestichtag: 25. September 2026. **Gegenstand:** fachliche Leitfäden als Anhang zur FluxLane-Serie über Cyber-Physical AI Security. **Prüfstatus:** strukturierte Quellen- und Dokumentenarbeit; keine empirische Sicherheitsprüfung einer Organisation, kein externes Peer Review und keine Rechtsberatung im konkreten Einzelfall.

1. Ausgangsmaterial und Provenienz

Das Ausgangsarchiv heißt FluxLane_Master_CyberPhysical_AI_Security_v1.0_2026-09-25.zip. Seine 27 Archivmitglieder waren lesbar; der ZIP-Integritätstest ergab keinen defekten Eintrag. Der am tatsächlichen Archiv ermittelte SHA-256-Wert lautet:

2a2b83e9185f114e2c72722429d4fca6544390471921ff8685c9169c9661f0fa

Das Archiv wurde zur Auswertung entpackt, aber nicht verändert und nicht als zweite Kopie in diesen Anhang aufgenommen. Es ist redaktionelles Ausgangsmaterial, keine externe wissenschaftliche Quelle. Die neue Ausgabe übernimmt die Leitfragen, nicht uneingeschränkt jede frühere Formulierung. Die zentrale methodische Änderung ist der Wechsel von einem journalistischen Themenmaster zu einem anwendbaren Nachweis- und Entscheidungsrahmen.

2. Recherchetyp und bewusste Grenzen

Die Auswahl ist eine strukturierte, zweckgerichtete und integrative Dokumentenanalyse. Gesucht wurden tragende Grundlagen für sechs Fragen: Systemwirkung; klinische Sicherheit; industrielle Safety und OT; Agentenidentität und Autorisierung; rechtliche Zuständigkeit; Prüfung und Wiederanlauf. Die Arbeit erhebt keinen Anspruch, sämtliche Forschung zu Cybersecurity, KI, Medizintechnik und Robotik vollständig zusammenzufassen.

Ein systematisches Review wäre anders anzulegen: mit vorab registriertem Suchprotokoll, festgelegten Datenbanken, reproduzierbaren vollständigen Trefferlisten, doppeltem Screening, bewerteten Ausschlussgründen und gegebenenfalls einer formalen Bewertung des Verzerrungsrisikos jeder Studie. Solche Schritte wurden hier nicht durchgeführt. Deshalb enthält der Anhang weder erfundene Trefferzahlen noch ein nachträglich konstruiertes PRISMA-Diagramm.

Die Stärke der vorliegenden Methode ist die gezielte Verbindung verschiedener Beweisfunktionen. Ihre Grenze liegt unter anderem in der selektiven Quellenbasis, der fehlenden lokalen Empirie und den eingeschränkten Normvolltextzugängen. Die technische Konzeptbildung wird deshalb nicht als empirisch bewiesene Überlegenheit einer Architektur ausgegeben.

3. Tatsächliche Recherchefade

Die Recherche ging vom Gambit-Originalbericht zu NISTs OT-, Incident-, Resilienz- und Agentenidentitätsarbeiten. Für Krankenhäuser wurden HHS/ASPR, die FDA, HL7, MDCG sowie die Primärstudie von Dameff und Kollegen und ein Labor-Erfahrungsbericht herangezogen. Für industrielle Anwendung und Scope wurden IEC- und ISO-Katalogangaben sowie MITREs Industrie-Taxonomie und historischer Triton-Kontext geprüft. Für Deutschland und die EU wurden das aktuelle BSIG, §391 SGB V, §3 BetrSichV, §87 BetrVG und die Kommissionsinformationen zu AI Act, Maschinenverordnung und CRA ausgewertet.

Zu den tatsächlich bearbeiteten Suchthemen gehörten „Gambit autonomous AI agents online retailers cost“, „NIST OT security revision 4 draft 2026“, „agent identity authorization NIST“, „hospital cyber downtime patient safety“, „Contec Epsimed patient monitor FDA“, „FHIR R5 security“, „BSIG 2025 §32“, „SGB V §391“, „AI Act implementation timeline 2026“, „CRA reporting obligations“ sowie die aktuellen Normausgaben. Diese Themenliste dokumentiert den Researchweg, behauptet aber keine vollständige maschinenlesbare Liste jeder einzelnen Suchanfrage.

Maßgeblich war die jeweilige Primärquelle beziehungsweise die für die Aussage verantwortliche Stelle. Mehrere Medienberichte über dieselbe Gambit-Untersuchung wurden nicht als mehrere unabhängige Befunde gewertet. Nicht einschlägige Suchergebnisse wurden nicht als Evidenz übernommen.

4. Zugriffsklassen und Aussageumfang

Das Quellenregister führt bei jedem Eintrag Autor/Herausgeber, Titel, Ausgabe oder Datum, Adresse, Dokumentart, tatsächlich verwendeten Zugriff, Nachschlagestellen, Verwendungszweck und Grenzen. „Geprüfte Quelle“ darf nur zusammen mit dieser Zugriffsklasse verwendet werden.

Volltext oder relevante Abschnitte: Diese Quellen erlauben die im Register eingegrenzte sachliche Auswertung. Auch ein gelesener Volltext kann methodische Grenzen besitzen; das gilt insbesondere für Anbieterberichte und Beobachtungsstudien.

Landingpage, Abstract oder Metadaten: Hier werden nur Ausgabe, Scope und öffentlich beschriebene Inhalte verwendet. Das trifft insbesondere auf proprietäre Normen, einzelne Behörden-Landingpages und den Labor-Erfahrungsbericht zu. Die Arbeit darf daraus weder ungelesene Detailklauseln zitieren noch Wirksamkeitswerte erfinden.

Technisch eingeschränkter Abruf: Einzelne EUR-Lex-Volltexte waren durch technische Abrufhindernisse nicht zuverlässig auswertbar. Für AI Act, Maschinenverordnung und CRA wurden deshalb ausdrücklich die aktuellen amtlichen Kommissionsdarstellungen verwendet; der Normvolltextcheck bleibt ein eigenständiger Punkt. Auch weitere Zugriffe auf Datenschutz-/BSI-Seiten waren teilweise mit Zugriffssperren beziehungsweise Abruffehlern verbunden. Ein Abruffehler ist kein inhaltlicher Befund über die Rechtslage. Beim BSI-Standard 200-4 bleiben daher

die öffentlich sichtbaren Metadaten von einer nicht behaupteten Volltextprüfung getrennt.

Die betroffenen Nachschlageeinträge Q38–Q41 werden nicht als frisch vollständig verifizierte Normtexte bezeichnet. Sie sind weiterhin wertvolle Fundstellen für den Leser, aber nicht Grundlage einer uneingeschränkten Volltextprüfbehauptung.

5. PDF-Auswertung und proprietäre Inhalte

Die einschlägigen Abschnitte von NIST SP 800-82 Rev.3 und der MDCG-Cybersecurity-Leitlinie wurden zusätzlich anhand der PDF-Darstellung stichprobenartig geprüft. Gedruckte Seitenzahlen und technische PDF-Seitenindizes wurden unterschieden. Diese Sichtprüfung ist keine Prüfung jedes Zeichens sämtlicher externer PDFs.

Es werden keine proprietären Normvolltexte, fremden Artikelvolltexte oder Schriftdateien verteilt. Der Anhang enthält eigene Analyse, kurze paraphrasierte Einordnungen sowie bibliografische Angaben und Quelladressen. Der Empfänger muss kostenpflichtige Normen gegebenenfalls selbst rechtmäßig beschaffen.

6. Trennung von Beobachtung und Übertragung

Der aktuelle Gambit-Fall trägt nur die in L01 begrenzte Einstiegsaussage. Weder Erfolgswahrscheinlichkeit noch Angriffskosten werden auf Kliniken oder Industrie hochgerechnet. Die drei Fallstudien sind eigene, klar gekennzeichnete Lehrkonstruktionen. Sie zeigen mögliche Prüfungspfade und erwartete Testeigenschaften, nicht nachgewiesene reale Vorfälle.

Die empirische Krankenhausstudie wird mit Design- und Übertragungsgrenzen verwendet. Ein regionaler retrospektiver Zusammenhang beweist weder eine universelle Kausalwirkung noch eine bestimmte Mortalitätsfolge. Die FDA-Mitteilung bleibt auf ihren Gerätescope und Mitteilungsstand begrenzt. NIST-Projekte und Blogs werden von finalen NIST-Leitlinien unterschieden. Die mathematischen Prüfbeispiele sind selbst hergeleitet und nicht aus einer Produktmessung entnommen.

7. Eigenleistung der Leitfäden

Die Eigenleistung besteht in der Zusammenführung zu einer nachvollziehbaren Kette:

Leistung → Abhängigkeit → Handlungsvollmacht → mögliche Wirkung → Kontrolle → Nachweis → Gegenprobe → Restunsicherheit → Entscheidung.

Die Kontrollschicht, das Handlungsvollmachtsregister und die organisatorischen Vorschläge sind eigene Anwendungssynthesen auf vorhandener Grundlage. Es wird weder behauptet, dass Zero Trust erstmals kontextbezogene Autorisierung entdeckt, noch dass das Paket eine neue Sicherheitsnorm oder eine universell überlegene Architektur begründet. Ein einfacher Softwarefilter wird nicht zur Safety-zertifizierten Schutzfunktion umbenannt.

Die 60 Kontrollen operationalisieren diese Synthese. Die 16 Formulare machen sie dokumentierbar. Die 46 Claim–Evidence-Einträge sichern tragende Aussagen ab und kennzeichnen ihre Beweisgrenzen. Das ersetzt nicht die Überprüfung zusätzlicher, lokal relevanter Regeln, Gefahren und Lieferantenanforderungen.

8. Welche Prüfung vor verbindlicher Verwendung fehlt

Vor einer organisationsintern verbindlichen Verwendung sind Systemgrenze, Betriebsverhältnisse, Datenflüsse, Rechtsrollen, einschlägige Normvolltexte, klinische oder industrielle Sicherheitsanforderungen und konkrete Notbetriebsfähigkeit zu erheben. Die Positiv- und Negativtests sind in einer autorisierten sicheren Umgebung durchzuführen. Verbliebene Risiken müssen die befugten Stellen ausdrücklich und gegebenenfalls nur befristet entscheiden.

Vor Veröffentlichung als fachlich freigegebener Anhang sollen mindestens redaktionelle Quellenprüfung und unabhängige fachliche Begutachtung erfolgen. Je nach Einsatz sind klinische Leitung/Medizintechnik, OT-/Safety-Fachkunde sowie juristische und datenschutzrechtliche Bewertung beteiligt. Die bereits durchgeführte Dateiprüfung ist davon getrennt. Sie besagt weder, dass ein Krankenhaus getestet wurde, noch dass ein Ausschuss

die Inhalte angenommen hat.

9. Aktualisierung und Änderungskontrolle

Eine neue Version wird ausgelöst, wenn sich tragende Rechtsfristen, Normausgaben, Source-Status oder wesentliche Fakten des Einstiegsfalls ändern. Lokal lösen auch neue Modelle, Werkzeuge, Rechte, Lieferantenverbindungen oder Betriebsmodi eine Neubewertung aus. Das bedeutet nicht, dass bei jeder redaktionellen Änderung sämtliche 60 Kontrollen neu geprüft werden müssen; der betroffene Nachweisscope wird begründet.

Für jede Änderung werden Anlass, betroffene Aussagen, Quellen, Kontrollen und Freigabeentscheidungen erfasst. Ein späterer Renderer darf diese Aktualisierung nicht still durchführen. Sachänderungen und reine Satzkorrekturen werden getrennt versioniert. Die im Paket enthaltenen SHA-256-Werte unterstützen die Erkennung von Dateiveränderungen, beweisen aber nicht die fachliche Wahrheit der Inhalte.

Korrekturen, Grenzen und Freigabestatus

1. Verhältnis zum bisherigen Master

Dieser Anhang ergänzt und präzisiert den journalistischen Master. Der ältere Master bleibt als Ausgangsfassung unverändert. Bei Widersprüchen sind die hier dokumentierten Einschränkungen für die Leitfadenfassung maßgeblich; eine redaktionelle Veröffentlichung der alten Artikel muss diese Stellen separat nachziehen.

Thema	Präzisierung dieser Ausgabe	Beleg / Arbeitsort
Gambit-Kosten	Durchschnittliche Scan-Modellkosten, nicht erfolgreicher Hack für 25 Dollar	Q01; L01 §3
Autonomie des Angriffs	Agentengestützte Arbeit mit menschlichem Operator, nicht nachgewiesen vollständig menschenlos	Q01; L01 §3
Herkunft	Chinesischsprachige Steuerung ist keine belegte Nationalität oder staatliche Zuordnung	Q01; L01 §3
Krankenhaus-/Roboterübernahme	Durch den E-Commerce-Fall nicht belegt; Beispiele dieses Pakets sind konstruiert	L01; Fallstudien
OT-Leitlinie	SP 800-82 Rev.3 final, Rev.4 zum Stichtag Entwurf	Q02/Q03
Krankenhauspflichten	§391 SGB V ausdrücklich berücksichtigt; nicht pauschal jede Klinik als KRITIS eingestuft	Q29/Q30; L02/L05
AI-Act-Zeichse	Aktuelle Kommissionsinformationen berücksichtigen die 2026 geänderten Hochrisiko-Fristen; Normvolltextprüfung bleibt ausgewiesen	Q33/Q34/Q39; L05 §6
CRA	Melde- und Hauptpflichten haben unterschiedliche Daten; Hersteller-/Betreiberrollen unterscheiden	Q36/Q37/Q41
Maschinenrecht	Hauptanwendungsdatum genannt; ungelesene Normklauseln nicht als geprüft präsentiert	Q35/Q40
Agenten-Gateway	Policy-/Autorisierungsprüfung nicht mit nachgewiesener sicherheitsgerichteter Schutzfunktion gleichgesetzt	L03 §8; L04 §5
Zero Trust	Kontext und Autorisierung sind bereits Gegenstand etablierter Ansätze; keine erfundene Neuheit	Q06; L04
Not-Aus	Kein globales Trennrezept; sicherer Übergang ist anlagen-/leistungsabhängig	L02 §§11–13; L03 §15
Lokaler Medizinbetrieb	Verlust zentraler Alarmierung/Kommunikation und zusätzlicher Personalbedarf werden geprüft	Q19; L02 §9
Tokenwiderruf	Ende eines Tokens ist nicht automatisch Ende angenommener Jobs oder physischer Wirkung	Q15; L04 §10
Known Good State	Begründet validierter Referenzzustand mit offenen Annahmen, kein absolut sauberer Zeitpunkt	L01 §14; L06 §13
Hashwerte	Dateiintegrität relativ zum Referenzwert, keine fachliche Richtigkeit oder Schadsoftwarefreiheit	L06 §11/13

Thema	Präzisierung dieser Ausgabe	Beleg / Arbeitsort
Wiederanlauf	Keine universelle Reihenfolge; Abhängigkeitszyklen und Wiederherstellungsstart gesondert prüfen	L06 §12
RTO/RPO	Lokale Zielwerte mit Leistung, Umfang und Messpunkt; keine universellen Beispielzeiten als Vorgabe	L01/L06; F08/F10
Neue Rollen	Aufgaben- und Kompetenzmodell, keine belegte quantitative Jobprognose	L05 §12
Gremium	Organisationsvorschlag, keine allgemein vorgeschriebene neue Aufsichtsinstanz	L05 §11
Prüfscore	Keine automatische Gesamtfreigabe durch Durchschnittswerte; kritische Gegenbefunde bleiben sichtbar	L05 §17; L06 §16

2. Nicht abgedeckte vertiefte Fachgebiete

Die Arbeit ersetzt keine klinischen Therapie- oder Diagnoseleitlinien, keine gerätespezifische Gebrauchsanweisung, keine anlagenspezifische Gefährdungsbeurteilung und keine vollständige Konformitätsbewertung. Sie enthält keine Auslegung eines bestimmten Sicherheitsintegritäts- oder Performance-Levels, keine detaillierte Auslegung eines medizinischen Alarmkonzepts und keine Anleitung zur Veränderung produktiver Safety-Steuerungen.

Nicht vollständig geprüft sind sämtliche sektorspezifischen Betreiber-, Melde-, Haftungs- und Beschäftigtenvertretungsregeln einer konkreten Organisation. Medizinprodukte, kritische Anlagen, Datenschutzrollen, AI-Act-Rollen und CRA-Rollen benötigen jeweils eine eigene Einstufung. Spezialgebiete wie Luftfahrt, Straßenverkehr, Kerntechnik oder militärische Systeme liegen außerhalb der sektoralen Detailtiefe dieses Anhangs.

Das Modell ersetzt auch keine empirische Validierung von KI-Leistung, Robustheit, Bias oder klinischem Nutzen. Ein Agent kann angemessen begrenzte Rechte besitzen und dennoch schlechte Vorschläge machen. Umgekehrt kann ein Modell im fachlichen Test leistungsfähig sein, aber unzulässig weitreichende Werkzeuge erhalten. Beide Prüfungen bleiben erforderlich, sofern sie zur Anwendung gehören.

3. Freigabegates

Gate	Was erforderlich ist	Status dieses Pakets
G-DOK	Vorhandene Dateien, gültige interne IDs, lesbare Register, konsistente Status, Archivintegrität	Gemäß separat erzeugtem QC-Bericht
G-QUELLE	Tragende Aussagen mit konkreten Fundstellen und offengelegtem Zugriff	Vorbereitet; eingeschränkte Normabrufe ausdrücklich offen
G-FACH	Unabhängige klinische/technische/Safety-Begutachtung des vorgesehenen Anwendungsumfangs	NICHT_DURCHGEFUEHRT
G-RECHT	Aktuelle Normvolltexte und tatsächliche Rollen/Übergangsregeln im Einzelfall beurteilt	NICHT_DURCHGEFUEHRT
G-LOKAL	Betrieb erhoben, Kontrollen umgesetzt, Tests und Ersatzbetrieb tatsächlich ausgeführt	NICHT_DURCHGEFUEHRT
G-PDF	Satz, Links, Tabellen, Verzeichnisse, Lesbarkeit und Zugänglichkeit der PDF-Ausgaben geprüft	NICHT_ERSTELLT; Aufgabe von Claude Code und anschließender Sichtprüfung
G-PUBLISHER	Redaktionell und fachlich verantwortliche Veröffentlichungsfreigabe	AUSSTEHEND

Eine Freigabe des Quelldateipakets ist keine Freigabe für unkontrollierte produktive Veränderungen. Der Status darf durch optische Gestaltung nicht aufgewertet werden. Insbesondere sind „zertifiziert“, „klinisch validiert“, „rechtssicher“, „wissenschaftlich begutachtet“ und „vollständig normkonform“ ohne die entsprechenden tatsächlichen Nachweise unzulässige Kennzeichnungen.

4. Freigabeprotokoll für den Empfänger

Das Protokoll sollte Auftrag, Zielpublikum, eingeschlossene Bände, Version, geprüfte Quellen, beteiligte Fachprüfer, offene Befunde, beschlossene Korrekturen und erlaubte Nutzung benennen. Dissens wird mit Begründung

festgehalten. Wird nur ein Teilbereich freigegeben, müssen Inhaltsverzeichnis, Titel und Vorwort den begrenzten Scope wiedergeben.

Für lokale Betriebsentscheidungen ist F16 zu verwenden. Für die redaktionelle Veröffentlichung sind die vorhandene FluxLane-Governance und der echte Laufzettel maßgeblich. Dieser Anhang baut keinen konkurrierenden Veröffentlichungsworkflow auf und erteilt keine automatische Publikationsfreigabe.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.