

Prüfung, Übung, Incident Response und Recovery

Leitfaden für Prüfer, Krisenstäbe, Sicherheitsbetrieb und Wiederanlaufverantwortliche

Fachlicher Leitfaden zur Cyber-Physical-AI-Security.

Fassung 1.0 · Stand 25. September 2026 · Adressaten: Interne und externe Prüfer, SOC, Incident Response, Krisenleitung, Business Continuity Management, klinisches Risikomanagement, OT, Medizintechnik und Qualitätsmanagement.

Dokumenttyp: Prüf- und Verfahrensleitfaden; keine realen Tests an einer Nutzeranlage durchgeführt

Die Fallstudien in diesem Leitfaden-Paket sind ausdrücklich konstruierte Prüfbeispiele; eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden.

Steckbrief

Merkmal	Wert
Dokumenttyp	Prüf- und Verfahrensleitfaden; keine realen Tests an einer Nutzeranlage durchgeführt
Zielgruppe	Interne und externe Prüfer, SOC, Incident Response, Krisenleitung, Business Continuity Management, klinisches Risikomanagement, OT, Medizintechnik und Qualitätsmanagement.
Recherche- und Rechtsstand	25. September 2026
Umfang	3.416 Wörter, 13 Seiten
Belege	0 Literatureinträge, 8 Quellenadressen
Gliederung	20 nummerierte Abschnitte, 0 Tabellen

Inhalt

1. Was eine Prüfung beweisen kann – und was nicht	4
2. Prüfauftrag und Unabhängigkeit	4
3. Nachweiskette vom Risiko bis zur Entscheidung	4
4. Bestands- und Dokumentenprüfung	4
5. Technische Tests mit Positiv- und Negativfällen	5
6. Zeitverhalten und Rücknahme von Handlungsvollmacht	5
7. Statistik ohne Scheinsicherheit	5
8. Tabletop, technische Übung und Vollprozessprobe	6
9. Erkennen, klassifizieren und stabilisieren	6
10. Eingrenzung mit dokumentierter Nebenwirkung	6
11. Beweissicherung ohne Vorrang vor unmittelbarem Schutz	7
12. Wiederherstellungsplanung und Abhängigkeitszyklen	7
13. Referenzzustand, Kontaminationsverdacht und fachliches Vertrauen	7
14. Technischer und fachlicher Wiederanlauf	8
15. Reconciliation: zwei Ereigniswelten zusammenführen	8
16. Freigabegates mit überprüfbaren Kriterien	8
17. Melde- und Kommunikationsnachweise	9
18. Nachbereitung und Wirksamkeitskontrolle	9
19. Mindestinhalt eines Prüfberichts	9
20. Arbeitsunterlagen und Ergebnis	9
Literatur und Quellenstatus	10
12 Rechtliche Hinweise	12
12.1 Keine Beratung	12
12.2 Keine Zusicherung, keine Konformitätsaussage	12
12.3 Rechtsstand	12
12.4 Haftung	12
12.5 Verweise auf fremde Inhalte	12
12.6 Marken und Produktbezeichnungen	12
12.7 Urheberrecht und Nutzung	12
12.8 Keine personenbezogenen Daten	13
12.9 Unabhängigkeit	13
12.10 Anwendbares Recht	13

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): *Prüfung, Übung, Incident Response und Recovery – Leitfaden für Prüfer, Krisenstäbe, Sicherheitsbetrieb und Wiederanlaufverantwortliche*. Fassung 1.0, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Gesetzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält keine Abbildungen.

1. Was eine Prüfung beweisen kann – und was nicht

Ein positiver Test zeigt, dass ein definiertes System unter dokumentierten Bedingungen das erwartete Verhalten gezeigt hat. Er beweist nicht die Abwesenheit sämtlicher unbekannter Schwachstellen. Eine gute Prüfung macht deshalb ihren Scope sichtbar: Komponenten, Konfiguration, Daten, Rollen, Belastung, Umgebungsbedingungen, Störungsfälle und ausdrücklich ausgeschlossene Bereiche.

Verifikation fragt, ob eine festgelegte Anforderung umgesetzt ist. **Validierung** fragt, ob Anforderung und Umsetzung für den beabsichtigten Betrieb geeignet sind. Ein Gateway kann eine Access-Control-Regel korrekt durchsetzen und dennoch ungeeignet sein, wenn seine Verzögerung einen kritischen Prozess beeinträchtigt. Ein Wiederanlauf kann technisch gelingen und fachlich unvollständig sein, wenn die während des Ausfalls entstandenen Informationen nicht abgeglichen wurden.

Die Prüfung muss daher mindestens vier Nachweisarten verbinden: Konfiguration beziehungsweise Dokumentation, beobachtetes technisches Verhalten, fachlich bestätigte Prozesswirkung und organisatorische Ausführbarkeit. Die Wiederherstellung einer Anwendung wird erst dann als Betriebsnachweis anerkannt, wenn die relevante Leistung im freigegebenen Umfang wieder erbracht werden kann. NIST ordnet Incident Response und Resilienz in ein laufendes Risikomanagement ein; die detaillierten Prüfverfahren dieses Bandes sind darauf aufbauende eigene Arbeitsmethoden. [Q05; Q07]

2. Prüfauftrag und Unabhängigkeit

Der Auftrag beschreibt, wer was gegen welche Anforderungen prüft und welche Entscheidung das Ergebnis tragen soll. Eine Softwarevorführung, ein internes Audit und eine normative Konformitätsbewertung sind unterschiedliche Leistungen. Die Bezeichnung „Audit“ darf den begrenzten Prüfgegenstand nicht verdecken.

Für sicherheitskritische Freigaben wird eine angemessene Unabhängigkeit zwischen Umsetzung und Bewertung vorgesehen. Das bedeutet nicht zwangsläufig ein externes Unternehmen für jeden Test. Es bedeutet, dass Interessenkonflikte, Kompetenz und Entscheidungsspielraum transparent sind. Die Person, die ein kritisches Ergebnis verantwortet, muss einen Mangel dokumentieren können, ohne dass das Projektteam ihn durch bloße Statusänderung beseitigt.

Die Prüfstelle benötigt Informationen über bekannte Einschränkungen. Nicht beantwortete Fragen werden als offen geführt. Ein fehlender Zugriff auf die Produktionsumgebung kann aus Sicherheitsgründen angemessen sein; er begrenzt aber die Aussage über deren tatsächliche Konfiguration. Solche Grenzen sind in der Schlussfolgerung zu erhalten.

3. Nachweiskette vom Risiko bis zur Entscheidung

Die Arbeitskette lautet: Verlustszenario → Anforderung → Kontrolle → Nachweis → Test → Befund → Korrektur → Freigabe. Jede Verbindung besitzt eine Kennung. Die Kontrollsammlung verwendet K01 bis K60, Nachweise erhalten E-Kennungen, Prüfungen P-Kennungen. Das Beispielregister zeigt dieses Prinzip mit synthetischen Daten; es behauptet keine real durchgeführte Prüfung.

Eine Anforderung ohne Risiko- oder Pflichtenbezug kann unnötigen Aufwand erzeugen. Eine Kontrolle ohne Nachweis kann reine Absicht bleiben. Ein Test ohne vorher festgelegtes erwartetes Ergebnis kann nachträglich beliebig interpretiert werden. Eine Freigabe ohne klare Einschränkungen kann über den tatsächlich geprüften Umfang hinauswirken.

Die Schlussfolgerung wird deshalb als kurzer Nachweisfall formuliert. Sie nennt die behauptete Eigenschaft, die sie stützenden Evidenzen, die geprüften Gegenfälle und die verbleibenden Annahmen. Ein Beispiel: „Der Planungsagent kann im geprüften Stand keine Therapieeinträge freigeben. Belegt durch die Rollenprüfung E-17 und die Negativtests P-08/P-09. Nicht geprüft wurde ein separat betriebenes Altsystem; dessen Integration ist nicht Teil dieser Freigabe.“ Diese Begrenzung macht den Nachweis belastbarer, nicht schwächer.

4. Bestands- und Dokumentenprüfung

Die Dokumentenprüfung beginnt mit Systemgrenze, Verantwortlichkeiten, Datenflüssen, Berechtigungen, Herstellerbedingungen und Betriebsmodi. Die Prüfer gleichen Dokumente untereinander ab. Ein Netzwerkdiagramm, das keinen Fernzugang zeigt, widerspricht beispielsweise einem Wartungsvertrag mit ständigem Remote-Service. Ein Ablaufplan, der lokale Bedienung voraussetzt, ist unvollständig, wenn die benötigten Anmeldedaten nur über den ausgefallenen zentralen Dienst bereitgestellt werden.

Wichtig ist der Versionsbezug. Eine aktuelle Policy kann zu einer älteren produktiven Konfiguration gehören. Ein Prüfbericht kann sich auf eine Modellversion ohne später hinzugefügtes Tool beziehen. Dokumente werden daher nicht allein nach Aktualisierungsdatum bewertet, sondern nach ihrem Bezug zum tatsächlich freizugebenden Stand.

Stichproben werden risikobezogen ausgewählt und begründet. Besonders relevante Konten, gemeinsame Dienste, Notfallzugänge, Schutzfunktionen und selten verwendete Wiederherstellungswege gehören typischerweise in die Auswahl. Der Prüfer dokumentiert, welche Population untersucht wurde und weshalb bestimmte Fälle ausgewählt wurden. Eine bequeme Auswahl der besten dokumentierten Systeme darf nicht als repräsentative Gesamtprüfung ausgegeben werden.

5. Technische Tests mit Positiv- und Negativfällen

Zu jeder kritischen Berechtigungsregel gehört mindestens ein zulässiger Referenzfall und ein unzulässiger Gegenfall. Der Referenzfall zeigt, dass die notwendige Leistung erhalten bleibt. Der Gegenfall zeigt, dass eine konkrete Grenze durchgesetzt wird. Zusätzlich werden veraltete Zustände, fehlende Angaben, abgelaufene Rechte, Unterdelegation und alternative Zugriffspfade untersucht.

Der Test beobachtet die Wirkung an der maßgeblichen Grenze. Eine abgelehnte Meldung im Agentenfrontend genügt nicht, wenn ein nachgelagerter Dienst den Auftrag trotzdem ausführt. Umgekehrt kann eine API formal Erfolg melden, obwohl die Handlung nur angenommen, aber noch nicht umgesetzt wurde. Deshalb wird zwischen Anfrage, Annahme, Ausführung, Wirkung und Rückmeldung unterschieden.

Bei physischer Wirkung beginnen Prüfungen in isolierten Modellen oder Testumgebungen. Reale Tests benötigen freigegebenen Scope, Verantwortliche, Schutzmaßnahmen, Abbruchkriterien und Rückbau. Penetrationstests, Störungsinjektionen oder Netztrennungen werden nicht ohne Genehmigung an Kliniken oder produktiven Anlagen durchgeführt. Dieser Leitfaden ist kein Auftrag zu solchen Eingriffen.

6. Zeitverhalten und Rücknahme von Handlungsvollmacht

Ein Widerrufstest misst nicht nur die Zeit, bis ein Konto im Verzeichnis als gesperrt erscheint. Er untersucht die Zeit bis zur tatsächlichen Begrenzung neuer unzulässiger Wirkung. Zu betrachten sind Entscheidung, Verteilung, Caches, lokale Ausführung, Warteschlangen und bereits begonnene Handlungen. [Q15, technische Widerrufsgrundlage; eigene Wirkungsanalyse]

Ein analytisches Zeitmodell kann lauten:

$$T_{\text{gesamt}} = T_{\text{erkennen}} + T_{\text{entscheiden}} + T_{\text{durchsetzen}} + T_{\text{betriebsreaktion}}.$$

Dieses Modell ist eine eigene Prüfhilfe. Für eine zeitkritische Gefährdung reicht es nur, wenn die Summe unter den festgelegten Annahmen zur verfügbaren Reaktionszeit passt. Sind einzelne Zeiten unbekannt oder länger als die Zeit bis zu einer möglichen gefährlichen Wirkung, darf die Schutzwirkung nicht allein auf dieses Verfahren gestützt werden. Eine geeignete lokale Begrenzung oder ein anderer sicherer Entwurf ist dann erforderlich.

Gemessen werden nicht nur Mittelwerte. Ausreißer, Teilausfälle, Zeitbasisfehler und Wiederverbindungen können entscheidend sein. Die maximal beobachtete Zeit ist außerdem kein mathematischer Beweis eines absoluten Maximums. Ihre Aussage hängt von Testumfang und Modell der Umgebung ab. Der Bericht muss diese Grenze benennen.

7. Statistik ohne Scheinsicherheit

Nehmen wir als rein mathematisches Beispiel an, ein klar definierter Test werde 100-mal unter unabhängigen, gleich verteilten Bedingungen durchgeführt und zeige keinen Fehler. Für eine angenommene konstante

Fehlerwahrscheinlichkeit p ist die Wahrscheinlichkeit von null Fehlern $(1-p)^{100}$. Eine einseitige 95-Prozent-Obergrenze aus diesem Modell ergibt sich aus $(1-p)^{100} = 0,05$, also $p = 1 - 0,05^{(1/100)}$, ungefähr 2,95 Prozent.

Das Beispiel zeigt, weshalb „hundert Tests bestanden“ nicht „praktisch kein Risiko“ bedeutet. Es ist aber **kein** Verfahren, mit dem sich aus beliebigen Agententests unmittelbar eine reale Angriffsquote bestimmen ließe. Tests können korreliert sein, dieselben Vorlagen verwenden oder gerade die nicht untersuchten Angriffswege verfehlen. Ein anpassungsfähiger Angreifer verletzt zudem häufig die einfache Modellannahme einer konstanten zufälligen Ereignisverteilung.

Für Detektoren ist auch die Grundhäufigkeit relevant. Unter rein hypothetischen Annahmen von 0,1 Prozent Angriffen, 95 Prozent Erkennung und 99 Prozent Spezifität entstehen in 10.000 Ereignissen rechnerisch 9,5 richtige und 99,9 falsche Alarmer. Der Anteil tatsächlicher Angriffe an allen Alarmen läge damit nur bei rund 8,7 Prozent. Das ist kein Messwert einer realen Klinik oder eines SOC, sondern eine Herleitung, warum isolierte Prozentangaben zur Modellgüte ohne Grundgesamtheit irreführend sein können.

Die praktische Konsequenz lautet: Testklassen, Nenner, Verteilung, Fehlerarten und nicht abgedeckte Situationen müssen im Bericht stehen. Eine Produktkennzahl darf nicht ohne Prüfung ihrer Erhebungsbedingungen in eine Betriebsfreigabe übersetzt werden.

8. Tabletop, technische Übung und Vollprozessprobe

Eine Tabletop-Übung prüft Entscheidungen und Zusammenarbeit anhand eines beschriebenen Ereignisses. Sie kann Zuständigkeitslücken, Kommunikationsprobleme und unklare Prioritäten sichtbar machen. Sie beweist nicht, dass Backups wiederherstellbar oder technische Sperren wirksam sind.

Eine technische Übung prüft ausgewählte Komponenten oder Abläufe unter kontrollierten Bedingungen. Sie kann Widerruf, Schnittstellensperre oder Restore zeigen, aber möglicherweise noch nicht die tatsächliche klinische oder industrielle Leistung. Eine Vollprozessprobe verbindet die technischen Schritte mit fachlicher Arbeit, Schichtwechsel, Ersatzkommunikation und späterem Abgleich. Die Methoden ergänzen sich.

Der Übungsplan benennt Ziele und bewusst ausgeschlossene Handlungen. Beispielsweise wird eine Netzisolation nur simuliert, während das Auffinden und Nutzen von Notfalldokumenten real geprüft wird. Beobachter dokumentieren nicht nur, ob eine Entscheidung getroffen wurde, sondern auf welcher Informationsgrundlage und mit welcher Verzögerung. Dadurch wird erkennbar, ob ein richtiger Ausgang auf belastbaren Verfahren oder bloß auf Zufall und persönlichem Wissen beruhte.

9. Erkennen, klassifizieren und stabilisieren

Im realen Ereignis steht zunächst die Erhaltung beziehungsweise Herstellung eines vertretbaren Zustands im Vordergrund. Eine klinische oder industrielle Gefährdung muss nicht auf die vollständige Attribution eines Angreifers warten. Zugleich darf eine technische Auffälligkeit nicht automatisch zum unkontrollierten Ausschalten kritischer Funktionen führen.

Die Erstaufnahme trennt bestätigte Beobachtung, plausible Hypothese und offene Frage. „Ungewöhnliche Anmeldung gesehen“ ist eine Beobachtung. „Angreifer kontrolliert die gesamte Anlage“ wäre ohne weitere Evidenz eine Hypothese. Diese Trennung verhindert überzogene Maßnahmen und erleichtert spätere Korrekturen.

Die koordinierende Incident-Rolle holt den betroffenen Fachbetrieb früh hinzu. Gemeinsam werden mögliche unmittelbare Wirkungen, zulässige Eingrenzungen und die nächsten Informationsbedarfe bestimmt. Bei hoher Unsicherheit kann ein begrenzter, reversibler Schritt angemessen sein, sofern er den Betrieb nicht gefährdet. Die konkrete Handlung folgt dem vorab genehmigten Reaktionsmandat und der Lage, nicht einer starren allgemeinen Eskalationstreppe. [Q05; Q02, § 6.4]

10. Eingrenzung mit dokumentierter Nebenwirkung

Jede Eingrenzungsoption wird mit Ziel und möglicher Nebenwirkung beschrieben. Das Sperren neuer Delegationen betrifft zukünftige Agentenbefugnisse. Ein Tokenwiderruf kann bestehende Sitzungen je nach Implementierung unterschiedlich erreichen. Eine Netzisolation kann gemeinsame Dienste unterbrechen. Das Stoppen eines Prozesses kann Restenergie, Zwischenprodukte oder personelle Ersatzaufgaben hinterlassen.

Die Entscheidung berücksichtigt daher Bedrohung, Betriebszustand, zeitliche Dringlichkeit, Umkehrbarkeit und verfügbare Beobachtung. Die Organisation darf weitergehende Maßnahmen vorab autorisieren, aber nur mit klarer Reichweite und bekannten Bedingungen. Ein Verteidigungsagent, der aus unzuverlässiger Klassifikation eigenständig jede Schutzmaßnahme auswählen darf, wäre selbst ein unzureichend begrenzter Akteur.

Nach der Maßnahme wird deren Wirkung bestätigt. Ein administrativ abgeschalteter Zugang ist erst dann wirksam eingegrenzt, wenn die relevanten nachgelagerten Pfade entsprechend reagieren. Ebenso muss ein vermeintlicher lokaler Betriebsmodus durch Beobachtung bestätigt werden. Die Dokumentation erfasst, welche Funktionen erhalten, eingeschränkt oder unbekannt sind.

11. Beweissicherung ohne Vorrang vor unmittelbarem Schutz

Protokolle, Konfigurationen und Zeitstände können für Ursachenanalyse, Meldepflichten und spätere Verfahren wesentlich sein. Sie werden im erforderlichen Umfang gesichert, sofern dies mit den prioritären Schutz- und Betriebsmaßnahmen vereinbar ist. Die Sicherung darf keine akute Gefährdung verlängern, nur um ein forensisch vollständigeres Bild zu erhalten.

Ein Evidenzdatensatz enthält Quelle, Erhebungszeit, Erheber, Methode, Speicherort, Integritätsmerkmal, Zugriffsberechtigung und bekannte Einschränkungen. Werden Dateien exportiert, wird ihr Bezug zum Ursprung dokumentiert. Ein Hash unterstützt die Kontrolle, ob die gesicherte Datei später verändert wurde. Er beweist nicht, dass die ursprüngliche Quelle wahrheitsgemäß oder vollständig war.

Für personenbezogene und vertrauliche Daten gelten Zweck- und Zugriffsbeschränkungen auch im Incident. Es wird nicht vorsorglich alles an alle Beteiligten verteilt. Externe Unterstützer erhalten den notwendigen Umfang über geeignete Wege. Die Entscheidung über Aufbewahrung und Weitergabe ist mit den einschlägigen rechtlichen Anforderungen zu verbinden. [Q38, Prüfsuchstellen; Q05, übergreifende Incident-Grundlage]

12. Wiederherstellungsplanung und Abhängigkeitszyklen

Eine universelle Reihenfolge „erst Identität, dann Netzwerk, dann Anwendung“ kann in der Praxis an Zyklen scheitern. Der Identitätsdienst benötigt möglicherweise Namensauflösung, Zeit und Speicher; diese wiederum können von Identität und Managementzugriffen abhängen. Der Recovery-Plan muss deshalb auch seinen eigenen Startpunkt erklären.

Benötigt wird eine vorbereitete, begrenzte Wiederherstellungsumgebung mit bekannten Zugängen, erforderlicher Dokumentation und geeigneten Vertrauensankern. Notfallzugänge sind verwahrt, zugänglich und überprüfbar, aber nicht als dauerhaft offene Hintertüren eingerichtet. Die für Recovery benötigten Informationen dürfen nicht ausschließlich in der Umgebung liegen, die wiederhergestellt werden soll.

Für jede wesentliche Leistung entsteht ein Wiederaufbaupaket: technische Artefakte, Konfigurationen, Schlüsselverfahren, Abhängigkeiten, Fachbedingungen, Prüfungen und Freigaben. NIST SP 1339 bietet eine aktuelle OT-Backup-Grundlage; die hier vorgeschlagene Paketstruktur ergänzt sie um fachliche Wirkungs- und Abgleichanforderungen. [Q08]

13. Referenzzustand, Kontaminationsverdacht und fachliches Vertrauen

Ein zeitlich altes Backup ist nicht automatisch vertrauenswürdig, und ein neues Backup ist nicht automatisch kompromittiert. Die Auswahl berücksichtigt vermuteten Ereignisbeginn, beobachtete Änderungen, Herkunft, Integritätsprüfung und mögliche bereits vorher bestehende Fehler. Der Recovery-Bericht unterscheidet tatsächliche Befunde und Annahmen.

Ein geeigneter Referenzzustand ist **begründet validiert**, nicht absolut als fehlerfrei bewiesen. Für Software kann dies vertrauenswürdige Herkunft, Konfigurationsprüfung und Tests bedeuten. Für Patientendaten kommen Identität, fachlicher Kontext und Korrekturstände hinzu. Für die Fertigung sind Parameter, Material, Werkzeuge und Qualitätsbezug relevant. Die verschiedenen Vertrauensdimensionen dürfen nicht durch einen einzigen grünen Status ersetzt werden.

Ist ein Teil des Datenbestands unklar, wird seine Verwendung begrenzt oder mit sichtbaren Bedingungen versehen. Die Organisation dokumentiert, welche Informationen vor erneuter entscheidungsrelevanter Nutzung bestätigt werden müssen. Eine pauschale Erklärung „Daten wieder da“ wäre für diesen Zweck unzureichend.

14. Technischer und fachlicher Wiederanlauf

Der technische Wiederanlauf beginnt in der freigegebenen Umgebung und folgt dem konkreten Abhängigkeitsplan. Identitäten, Geheimnisse und Berechtigungen werden nach dem Verdachtsumfang behandelt. Kritische externe Verbindungen werden nicht unbesehen übernommen. Änderungen gegenüber dem früheren Stand werden dokumentiert, damit spätere Abweichungen nicht mit dem ursprünglichen Angriff verwechselt werden.

Der fachliche Wiederanlauf prüft die tatsächlich erbrachte Leistung. In der Klinik umfasst dies beispielsweise die Zuordnung und Erreichbarkeit relevanter Informationen sowie den Umgang mit Ersatzdokumentation. In der Industrie umfasst es den realen Anlagenzustand, erforderliche Schutzfunktionen und Produktqualität. Die Freigabe erfordert die dafür zuständigen Fachrollen; das SOC kann diese Bewertung nicht allein ersetzen.

Eine gestufte Wiederaufnahme kann Risiken begrenzen. Zunächst werden ausgewählte Funktionen, dann weitere Verbindungen und schließlich erweiterte Agentenbefugnisse zugelassen. Die Stufung ist ein Vorschlag, kein universelles zwingendes Verfahren. Ihre Kriterien, Beobachtungen und Rücknahmemöglichkeiten müssen zur konkreten Leistung passen. [Q02, § 6.5; Q05]

15. Reconciliation: zwei Ereigniswelten zusammenführen

Während des Ausfalls entstehen weiterhin reale Ereignisse. Patienten werden aufgenommen, Behandlungen dokumentiert, Werkstücke bearbeitet, Chargen bewegt oder technische Zustände verändert. Eine Wiederherstellung auf einen früheren Datenstand bildet diese Ereignisse nicht automatisch ab. Der anschließende Abgleich ist daher ein eigenständiger Betriebsprozess.

Das Abgleichregister enthält Ereigniszeit, Erfassungszeit, Quelle, Identität beziehungsweise Produktbezug, fachlichen Inhalt, Konfliktstatus und verantwortliche Freigabe. Informationen werden nicht still überschrieben. Eine spätere Erfassung wird als solche erkennbar gehalten. Dubletten und widersprüchliche Angaben werden fachlich entschieden und mit Entscheidungshistorie versehen.

Der noch offene Abgleich kann als Arbeitsbestand gemessen werden. Eine reine Anzahl sagt jedoch wenig, wenn ein einziger offener Punkt besonders kritisch ist. Deshalb wird zusätzlich seine Bedeutung für weitere Entscheidungen bewertet. Eine Wiederfreigabe kann bestimmte offene unkritische Abgleiche zulassen, sofern sie eindeutig abgegrenzt sind. Kritische ungeklärte Identitäten, Aufträge oder Qualitätszustände dürfen nicht hinter einem niedrigen Restprozentsatz verborgen werden.

16. Freigabegates mit überprüfbaren Kriterien

Die Wiederaufnahme unterscheidet mindestens **Security-Eingrenzung, technische Funktionsprüfung, fachliche Betriebsfähigkeit, erforderliche Schutzfunktionen** und **Daten-/Produktintegrität**. Nicht jede Anwendung benötigt dieselbe Form jeder Prüfung; die Anwendbarkeit wird begründet. Für jede relevante Prüfung existiert ein benannter Verantwortlicher.

Ein Gate kann erfüllt, unter klaren Bedingungen erfüllt oder nicht erfüllt sein. Eine Bedingung enthält betroffenen Scope, zulässige Nutzung, Ersatzkontrolle, Überwachung und spätesten Überprüfungspunkt. „Restrisiko akzeptiert“ ohne diese Angaben ist nicht hinreichend. Eine gemeinsame Freigabe darf keine fachliche Ablehnung unsichtbar machen.

Sperrgründe betreffen insbesondere eine nicht verstandene letzte Schutzfunktion, nicht nachvollziehbare kritische Berechtigungen, ungeklärte entscheidungsrelevante Datenintegrität oder ein nicht beherrschtes Wiederanlaufverhalten. Sie sperren die betroffene Funktion oder Betriebsart; daraus ist nicht automatisch eine universelle Stilllegungsanweisung für das gesamte Unternehmen abzuleiten. Die betriebliche Entscheidung bleibt an Fachlage und Schutzbedarf gebunden.

17. Melde- und Kommunikationsnachweise

Die Meldeprüfung läuft parallel zur technischen und fachlichen Bewältigung. Für jede potenzielle Pflicht werden Kenntnisstand, auslösender Sachverhalt, Bewertender, Entscheidung, Frist und Empfänger erfasst. Die unterschiedlichen gesetzlichen Verfahren werden nicht in einem einzigen Feld „gemeldet“ zusammengefasst. Band 5 enthält die aktuelle Rechts- und Fristenorientierung. [Q29, § 32; Q37; Q38]

Kommunikation an Beschäftigte und betroffene externe Stellen muss den tatsächlich geltenden Betriebsmodus erklären. Eine technische Entwarnung ist nicht gleichbedeutend mit vollständiger fachlicher Normalisierung. Offene Datenabgleiche oder eingeschränkte Leistungen bleiben sichtbar. Auch eine Aussage „kein Datenabfluss nachgewiesen“ darf nicht zu „nachweislich kein Datenabfluss“ umformuliert werden.

Die Kommunikation dokumentiert Fassungen und Zeitpunkte. Dadurch lässt sich später nachvollziehen, welche Informationen bei einer Entscheidung vorlagen. Das schützt vor nachträglicher Vermischung früherer Unsicherheit mit späterem Wissen.

18. Nachbereitung und Wirksamkeitskontrolle

Die Nachbereitung fragt nicht nur, welches technische Loch geschlossen wurde. Sie untersucht, warum der Pfad erreichbar war, welche Annahme falsch war, welche Kontrolle nicht wirkte und welche Gegenmaßnahme selbst Probleme erzeugte. Änderungen werden mit Verantwortlichen, Fristen und erneuter Prüfung verknüpft.

Ein Maßnahmenpunkt gilt nicht deshalb als erledigt, weil eine neue Richtlinie veröffentlicht wurde. Er benötigt einen passenden Wirksamkeitsnachweis. Wurde ein fehlender Ersatzkommunikationsweg festgestellt, muss dieser unter den relevanten Ausfallbedingungen geprüft werden. Wurde ein zu breites Agentenmandat erkannt, ist ein erneuter Negativtest erforderlich.

Die Erkenntnisse fließen in Inventar, Wirkungsketten, Beschaffung, Schulung und Übungen ein. Das Ziel ist eine verbesserte Fähigkeit unter realen Bedingungen, nicht nur eine größere Dokumentensammlung. Neue Erkenntnisse können auch zeigen, dass eine geplante autonome Funktion enger bleiben muss als ursprünglich vorgesehen.

19. Mindestinhalt eines Prüfberichts

Ein vollständiger Bericht enthält Auftrag und Scope, Systemstand, Prüfkriterien, Methodik, Daten- und Stichprobengrundlage, durchgeführte Prüfungen, Ergebnisse, Gegenbelege, offene Punkte, Risikoeinordnung und Entscheidungsvorschlag. Er benennt, welche Aussagen auf Dokumenten, welche auf Testbeobachtung und welche auf fachlicher Bewertung beruhen.

Für jeden Befund werden Reproduktionsbedingungen, Bedeutung, betroffene Funktion und geeignete Abhilfe festgehalten. Ergebnisse werden nicht durch pauschale Aussagen wie „Best Practice eingehalten“ ersetzt. Ein kritischer Befund kann eine Teilfreigabe verhindern, auch wenn andere Kontrollen positiv sind. Ein Gesamtprozentsatz allein ist daher kein angemessener Abschluss.

Der Bericht muss lesbar sein, ohne dass der Prüfer informelles Projektwissen mitbringt. Alle Nachweise sind über eindeutige Kennungen und Speicherorte auffindbar. Die Bibliografie verweist auf externe Grundlagen; das Evidenzregister verweist auf die lokalen Tatsachen. Beides erfüllt unterschiedliche Aufgaben und darf nicht miteinander verwechselt werden.

20. Arbeitsunterlagen und Ergebnis

Die Kontrollen **K49–K60** bilden den Schwerpunkt. Verwendet werden **F05 Nachweisfall**, **F08 Betriebsmodi**, **F09 Reaktionsmandat**, **F10 Wiederanlauf**, **F11 Ereignisabgleich**, **F13 Meldeentscheidungen**, **F15 Prüfprotokoll** und **F16 Ausschussentscheidung**. Die drei ausgearbeiteten Fallstudien liefern Übungsabläufe und Gegenfragen; sie sind keine Berichte realer Klinik- oder Anlagenvorfälle.

Ergebnis: Eine belastbare Prüfung endet nicht mit „System wieder online“. Sie endet mit einer begründeten Aussage darüber, welche Leistung unter welchen Bedingungen wieder zulässig ist, welche Unsicherheit bleibt und welcher konkrete Nachweis die Entscheidung trägt.

<!-- GENERATED_LOCAL_BIBLIOGRAPHY -->

Literatur und Quellenstatus

Die folgenden Angaben gehören zu diesem Band. Das vollständige Quellenregister erläutert Verwendungszweck und Zugriff. Quellenstatus und Grenzen sind bei jeder Weiterverwendung zu erhalten. Die Q-Nummern im Text beziehen sich auf diese Einträge; Fundstellen bezeichnen die externe Quelle, nicht eine erfundene PDF-Seite dieses Bandes.

Q02 – Keith Stouffer et al. / NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3. 2023-09-28. DOI: 10.6028/NIST.SP.800-82r3. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

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. Zugriff: Landingpage und relevante PDF-Abschnitte gelesen; PDF-Stichprobe visuell geprüft. Grenze: Freiwillige US-Leitlinie, kein deutscher Konformitätsnachweis. Der Leitfaden ergänzt eigene Überlegungen; Kapitelverweise sind keine wörtlichen Normanforderungen.

Q05 – NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, SP 800-61 Rev. 3. 2025-04-03. DOI: 10.6028/NIST.SP.800-61r3. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Integration von Incident Response in CSF 2.0. Zugriff: Publikationsseite / Abstract gelesen. Grenze: Konkrete Abläufe und Formulare dieses Pakets sind eigene Ableitungen, kein vollständig nacherzählter Standard.

Q07 – NIST. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, SP 800-160 Vol. 2 Rev. 1. 2021-12. DOI: 10.6028/NIST.SP.800-160v2r1. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; cyber resiliency engineering. Zugriff: Publikationsseite / Abstract gelesen. Grenze: Keine empirische Validierung der in diesem Paket vorgeschlagenen Architektur.

Q08 – NIST. OT Backup Quick Start Guide, SP 1339. 2026-06-17. DOI: 10.6028/NIST.SP.1339. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Backup und Recovery für OT. Zugriff: Publikationsseite / Beschreibung gelesen. Grenze: Ein Backup- oder Hashnachweis ist kein Beweis fachlicher Datenrichtigkeit. Konkrete Recovery-Gates sind eigene Ableitungen.

Q15 – T. Lodderstedt et al. / IETF. OAuth 2.0 Token Revocation, RFC 7009. 2013-08. DOI: 10.17487/RFC7009. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 2.1–2.2 Revocation Request / Response; § 3 Implementation Note. Zugriff: RFC-Webvolltext / Widerrufsabschnitte gelesen. Grenze: Ein Tokenwiderruf hebt bereits ausgeführte oder autonom weiterlaufende Maschinenaktionen nicht auf. Diese Folgerung ist eigene Systemanalyse.

Q29 – Bundesrepublik Deutschland / Gesetze im Internet. BSI-Gesetz (BSIG 2025), aktuelle bereitgestellte Fassung. Gesetz 2025; Änderungsstand im Abruf 2026. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung. Zugriff: Bereitgestellter Volltext; §§ 28, 30–32, 38–39 und Änderungsvermerk gelesen. Grenze: Keine automatische Einstufung eines konkreten Unternehmens. Gesetze-im-Internet-Fassung enthält Bearbeitungshinweise; Einzelfall und Spezialregeln separat prüfen.

Q37 — Europäische Kommission, DG CONNECT. Cyber Resilience Act — Reporting obligations. Webupdate 2026-09-11. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: What are the main rules?; Where should manufacturers submit their notifications?. Zugriff: Webtext vollständig gelesen. Grenze: Aktiv ausgenutzte Schwachstelle und schwerwiegender Vorfall unterscheiden. Kein Ersatz für Einzelfallprüfung des CRA.

Q38 — Europäische Union. Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung. 2016; aktuelle Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff.. Zugriff: Direkter Web-Volltextabruf technisch blockiert; nicht als neu volltextverifiziert ausgewiesen. Grenze: Artikelzuordnung dient der rechtlichen Prüfung. Redaktionell bekannte Regelungsinhalte werden nicht als vollständig neu geprüfte konsolidierte Rechtsberatung ausgegeben.

Arbeitsmittel: Kontrollkatalog, Formularbuch, Fallstudien und Claim–Evidence-Matrix.

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.