Be sure. testo

REVISION ANNEX 11 / AUDIT TRAIL

# Fokus Data Integrity

22.09.2025

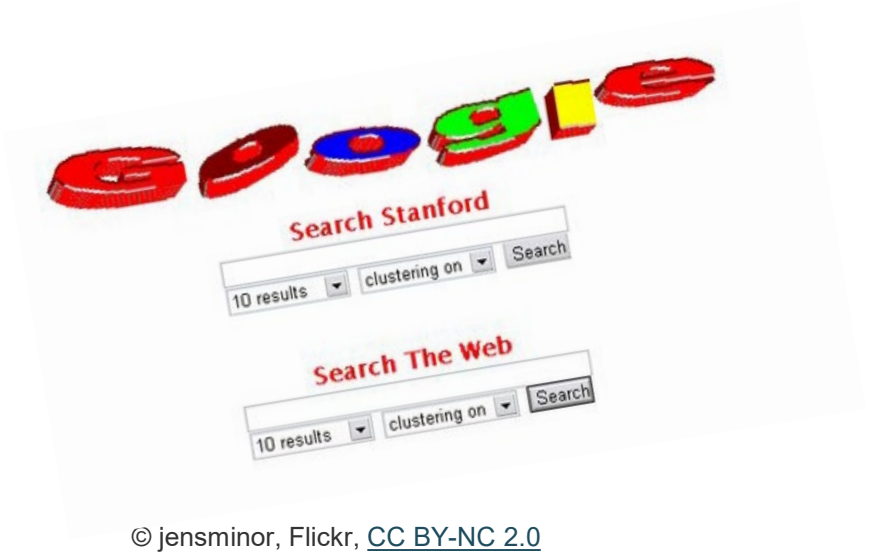
www.testotis.de

# Wie alles begann

Thilo Parg, Wikipedia, CC BY-SA 3.0

1997

1997






Siemens S10
(Quelle Siemens)




# IEEE 802.11

2 MBit/s

3,6 GB > 100,- DM

1997

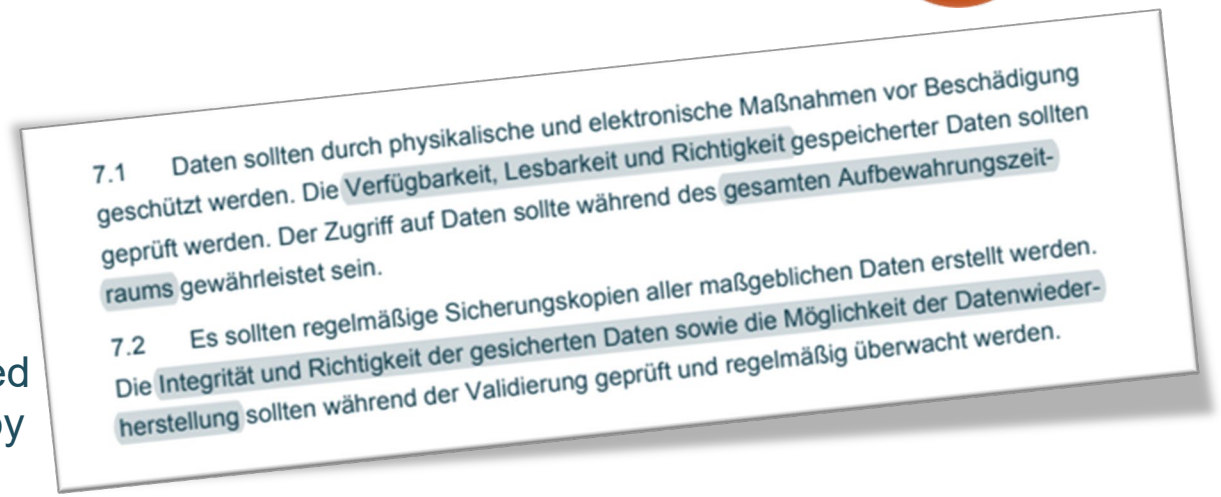
# Und was war noch?

FDA

## 21 CFR Part 11

Wir haben keine E-Records,
Wir machen alles auf
Papier!

# Was sagt der neue Draft des Annex 11?



7.1 Daten sollten durch physikalische und elektronische Maßnahmen vor Beschädigung geschützt werden. Die Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten sollten geprüft werden. Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein.

7.2 Es sollten regelmäßige Sicherungskopien aller maßgeblichen Daten erstellt werden. Die Integrität und Richtigkeit der gesicherten Daten sowie die Möglichkeit der Datenwiederherstellung sollten während der Validierung geprüft und regelmäßig überwacht werden.

It is critically important that data captured, analysed and reported by systems used in GMP activities are trustworthy. As defined by the **ALCOA+** principles, data integrity covers many topics including but not limited to requirements defined in the sections **Handling of Data**, **Identity and Access Management**, **Audit Trails**, **Electronic Signatures**, and **Security**

Quality risk management principles should be used to assess the criticality of data to product quality, patient safety and data integrity, the **vulnerability of data** to deliberate or indeliberate **alteration, deletion or loss**, and the **likelihood of detection of such actions**

# Umgang mit Daten

| Fragestellung | Annex 11 | Revision |
|---|---|---|
| Austausch der Daten zwischen mehreren Systemen | Geeignete Kontrollmaßnahmen für korrekte und sichere Eingabe und Verarbeitung von Daten | Besser validierte Schnittstellen als manueller Übertrag<br><br>Bei manuellem Transfer: Effektive Maßnahme, um sicherzustellen, dass keine zusätzlichen Risiken für die Datenintegrität eingeführt werden |
| Manuelle Dateneingabe | zusätzliche Prüfung auf Richtigkeit der Eingabe<br>- Durch 2. Anwender<br>- validierte elektronische Methode | System soll auf Plausibilität prüfen und Nutzer alarmieren, wenn der Input unplausibel ist |
| Bei Migration in anderes Format/System: | Überprüfung, dass Werte und Bedeutung der Daten nicht verändert wurden<br>(in der Validierung) | Validierter Prozess und sowohl das Empfänger- als auch das Sender-System betrachten |
| Verschlüsselung | - | Wo immer möglich sollten Daten im System verschlüsselt vorliegen |

# Sicherheit

- Physikalische/logische Maßnahmen zur Beschränkung des Zugangs (System und Server)
- Umfang der Sicherheitsmaßnahmen abhängig von der Kritikalität des Systems

**Informationssicherheitsmanagementsystem implementieren**

- ☑ Schulungen zur Sicherheitsbewusstseinsbildung
- ☑ Schutz vor Natur- und technischen Katastrophen
- ☑ Automatische Datenreplikation in 2. Rechenzentrum
- ☑ Getesteter Disaster-Recovery-Plan
- ☑ Netzwerksegmentierung und Firewall-Regeln
- ☑ Regelmäßige Plattformpflege und Patch-Management
- ☑ Kontrolle bidirektionaler Geräte (z. B. USB)
- ☑ Einsatz und Überwachung von Antivirensoftware
- ☑ Regelmäßige Penetrationstests für internetnahe Systeme
- ☑ Verschlüsselter Fernzugriff über sichere Protokolle

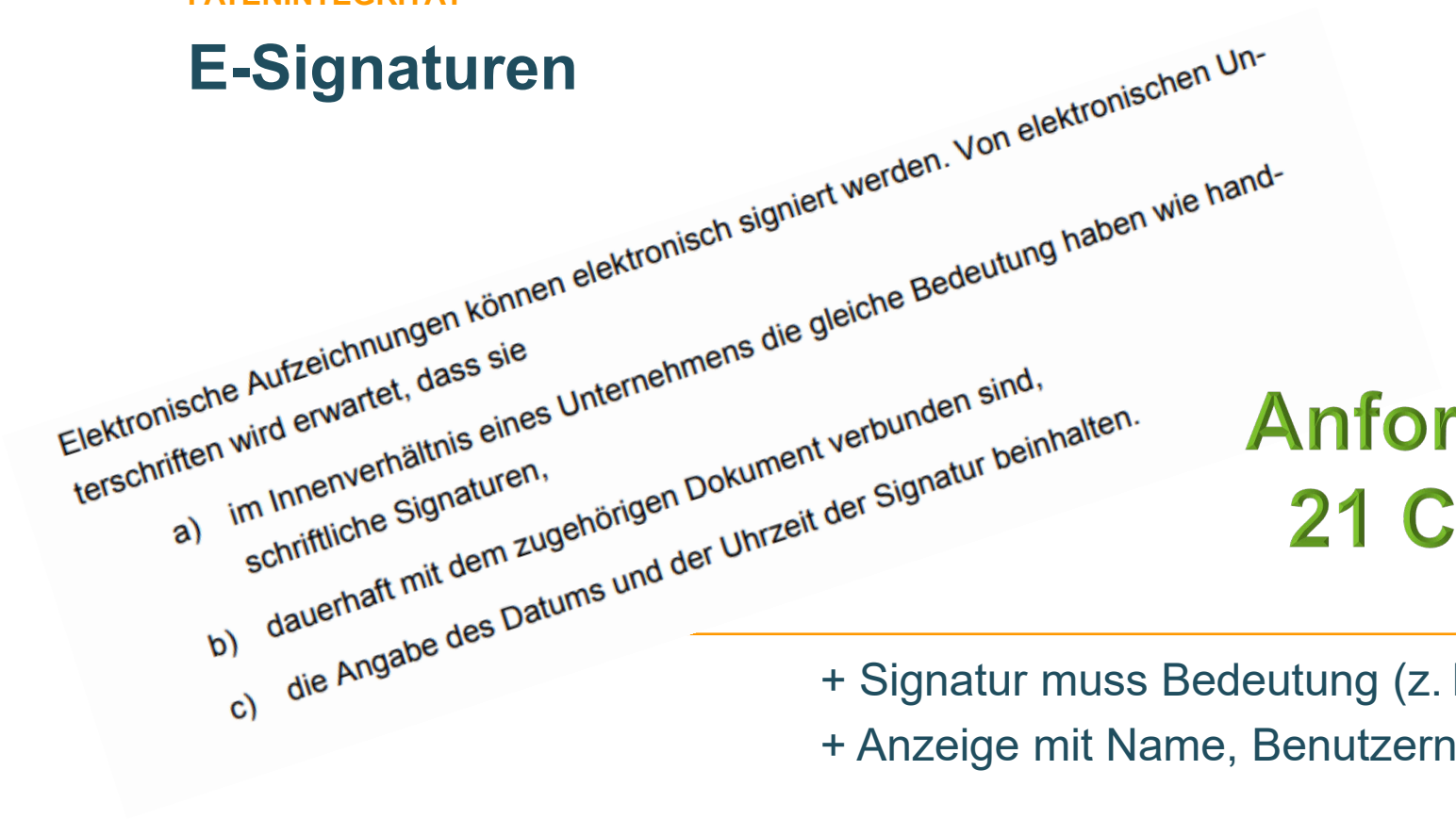
# Identitäts- und Zugriffsmanagement

- Erteilung, Änderung und Entzug von Zugriffsberechtigungen
- Identität des Anwenders/Bearbeiters und Datum und Uhrzeit

+ Eindeutige Benutzerkonten (außer read-only)
+ Zeitnahe Verwaltung von Benutzerrechten
+ Sichere Authentifizierung – Token allein nicht ausreichend
+ Vertrauliche Passwörter – Änderung beim ersten Login
+ Starke Passwortrichtlinien
+ Multifaktor-Authentifizierung (MFA) bei Remote-Zugriff

+ Automatische Sperrung nach Fehlversuchen
+ Inaktivitäts-Logout mit Re-Authentifizierung
+ Protokollierung von Login/Logout inkl. Rolle und Zeitstempel
+ 'Least Privilege' und 'Segregation of Duties'
+ Regelmäßige Reviews der Zugriffsrechte durch Vorgesetzte

# E-Signaturen



Elektronische Aufzeichnungen können elektronisch signiert werden. Von elektronischen Unterschriften wird erwartet, dass sie

a) im Innenverhältnis eines Unternehmens die gleiche Bedeutung haben wie handschriftliche Signaturen,

b) dauerhaft mit dem zugehörigen Dokument verbunden sind,

c) die Angabe des Datums und der Uhrzeit der Signatur beinhalten.

## Anforderung aus 21 CFR Part 11

+ Signatur muss Bedeutung (z. B. Genehmigung) klar darstellen
+ Anzeige mit Name, Benutzername, Rolle, Bedeutung, Zeitstempel

+ Hybride Lösungen müssen Signaturgültigkeit sicherstellen
+ Automatische Erfassung von Datum, Uhrzeit und Zeitzone

# Datensicherung

1. **Regelmäßige Datensicherung** (Daten und Metadaten)
2. **Frequenz und Aufbewahrung**
   - Backup-Intervalle und Aufbewahrungsdauer risikobasiert festlegen
3. **Physische Trennung**
   - Backups müssen physisch vom Originalsystem getrennt gespeichert werden.
4. **Logische Trennung**
   - Backups dürfen nicht im gleichen logischen Netzwerk wie die Originaldaten liegen.
5. **Erweiterter Umfang**
   - Je nach Kritikalität müssen auch Anwendungen und Systemkonfigurationen gesichert werden.
6. **Wiederherstellungstests**
   - Wiederherstellung aus Backup muss getestet und dokumentiert werden.
   - Tests müssen während der Validierung und nach Änderungen am Backup-/Restore-Prozess erfolgen.

# Archivierung

Daten können archiviert werden. Diese Daten sollten auf Verfügbarkeit, Lesbarkeit und Integrität geprüft werden. Sind maßgebliche Änderungen am System erforderlich (z.B. Computer und zugehörige Ausrüstung oder Programme), sollte sichergestellt und getestet werden, ob die Daten weiterhin abrufbar sind.

- 🔒 Schreibschutz nach Abschluss GMP-relevanter Prozesse (read-only)
- ✅ Schutz von Daten, Metadaten & Audit Trails vor Änderungen/Löschung
- 🧪 Integritätsprüfung bei Archivierung (z. B. Checksummen)
- 📦 Backup auch für archivierte Daten (physisch & logisch getrennt)
- 💿 Wenn Langzeitarchivierung auf flüchtigen Medien: validierter Medienwechselprozess
- 🔍 Wiederauffindbarkeit in durchsuchbarem/sortierbarem Format oder Export

# Regulatorische Anforderung

## Annex 11

Basierend auf einer Risikobewertung:

- Aufzeichnung aller GMP-relevanten Änderungen und Löschungen (ein systemgenerierte „Audit Trail).
- Bei Änderungen oder Löschung GMP-relevanter Daten: Grund dokumentieren
- Audit Trail muss verfügbar / allgemein lesbar sein
- Regelmäßige Überprüfung

## 21 CFR Part 11

- Sicherer, computer-generierter Audit Trail mit Zeitstempel
- Aufzeichnung von Datum und Zeit von Eingaben and Aktionen, die E-Records erzeugen, ändern oder löschen
- Änderungen dürfen die vorhergehende Aufzeichnung nicht verschleiern
- Aufberwahrung Solange es für den E-Record notwendig ist
- Verfügbar für Agency Review und kopierbar

# Audit Trail vs. System Log

- **Audit Trail:**
  - Protokolliert Änderungen an GMP-relevanten Daten (Erstellung, Änderung, Löschung)
  - GAMP® 5 2nd Edition: Audit Trail = GMP-relevant
  - Annex 11 Abschnitt 9: Audit Trail für GMP-Daten erforderlich
  - Annex 11 Abschnitt 12.4: Log-Dateien müssen Benutzeridentifikation, Datum und Uhrzeit erfassen

- **System Log:**
  - Erfasst Systemereignisse (z. B. Logins, Systemfehler, technische Prozesse)
  - Nicht GMP-relevant, außer bei Benutzeridentifikation (Abschnitt 12.4)
  - GAMP® 5 2nd Edition: System Log = technische Information
    - Login/Logout-Zeiten
    - Systemstart, Fehlermeldungen
    - Änderungen an Benutzerrollen

# Revision Annex 11

- Pflicht bei manuellen Eingriffen: Audit Trail erforderlich bei **Erstellung, Änderung, Löschung oder Bestätigung** von Daten
- Erfassung von **Wer, Was, Wann, Warum inkl. Rolle, Zeitstempel und Begründung**
- Echtzeit-Erfassung: Änderungen müssen sofort protokolliert werden
- Nicht editierbar und nicht deaktivierbar
- Änderungen an Einstellungen erzeugen selbst Eintrag
- Elektronische Kopie aller Daten inkl. Audit Trail muss verfügbar sein

# Revision Annex 11

## Audit Trail Review

- Effiziente Prüfung: Daten müssen **sortier- und durchsuchbar** sein
- Dokumentierte Prüfverfahren: Wer, Was, Wann, **Umgang mit Abweichungen**
- Unabhängige Prüfung durch Peer Review
- Risiko- und prozessbasierte Prüfung mit **Fokus auf kritische Änderungen**
- Zeitnahe Prüfung, idealerweise vor Chargenfreigabe
- Audit-Trail-Prüfungen müssen der QP zur Freigabe vorliegen

🔍 **Praxisbeispiele:**
- Chargendokumentation: Änderung von Produktionsparametern
- Laborprotokolle: Korrektur von Messergebnissen mit Begründung
- Elektronische Logbücher: Nachverfolgung von Wartungsaktivitäten

## RISIKEN

- Audit Trails sind deaktivierbar oder manipulierbar
- Änderungen werden nicht in Echtzeit / unvollständig erfasst
- 'Warum'-Angaben bei Änderungen fehlen
- Prüfung erfolgt zu spät / gar nicht, z. B. nach Chargenfreigabe
- Audit-Trail-Daten sind nicht durchsuchbar oder exportierbar
- Änderungen an Audit-Trail-Einstellungen bleiben unprotokolliert
- Kritische Änderungen werden nicht risikobasiert priorisiert

Funktionale Risikobewertung und Betrachtung / Testung in der Validierung

Be sure. testo

# Position Paper on Audit Trails and Audit Trail Review

Considerations Aimed at Efficiently Meeting Authorities' Requirements

## Industry Coalition

arevipharma

Boehringer Ingelheim

NOVARTIS

PQE

Rentschler Biopharma

SANOFI

# Risikobasierter Ansatz

Der Ansatz basiert auf regulatorischen Vorgaben (z. B. PIC/S Good Practices) und nutzt **Risikomanagement**, um den Aufwand für die Audit-Trail-Überprüfung zu bestimmen

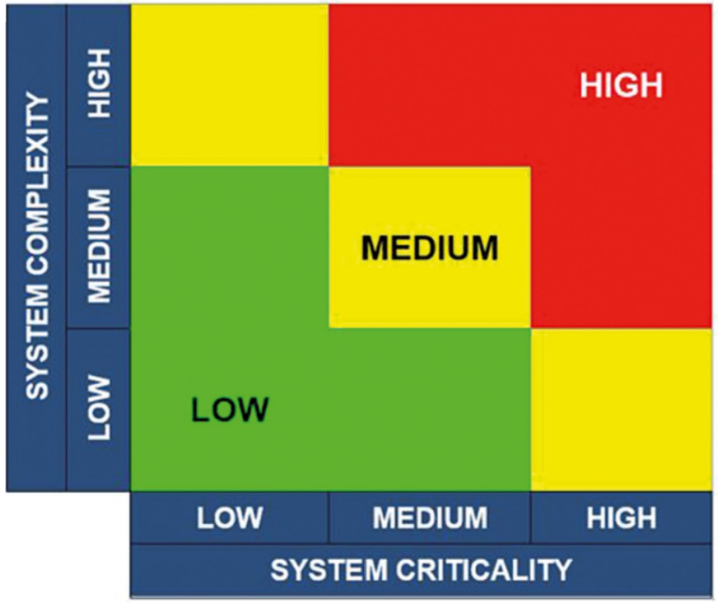
- **Zentrale Bewertungsfaktoren**:
  - **Datenkritikalität**: Wie stark beeinflussen die Daten Entscheidungen und Produktqualität?
  - **Datenrisiko**: Wie wahrscheinlich ist eine Datenmanipulation oder -löschung und wie gut sind solche Änderungen durch Routineprüfungen erkennbar?

- **Systemabhängigkeit**:
  - Der Grad der Datenkonfigurierbarkeit beeinflusst das Risiko.
  - Je komplexer ein System, desto höher der potenzielle Manipulationsspielraum – und desto intensiver sollte die Audit-Trail-Prüfung sein.

# System-Risiko-Level

Kombination aus:

- **Systemkritikalität**: Bedeutung der im System gespeicherten Daten für Patientensicherheit und Produktqualität.
- **Systemkomplexität**: Grad der Konfigurierbarkeit und damit Manipulierbarkeit der Daten



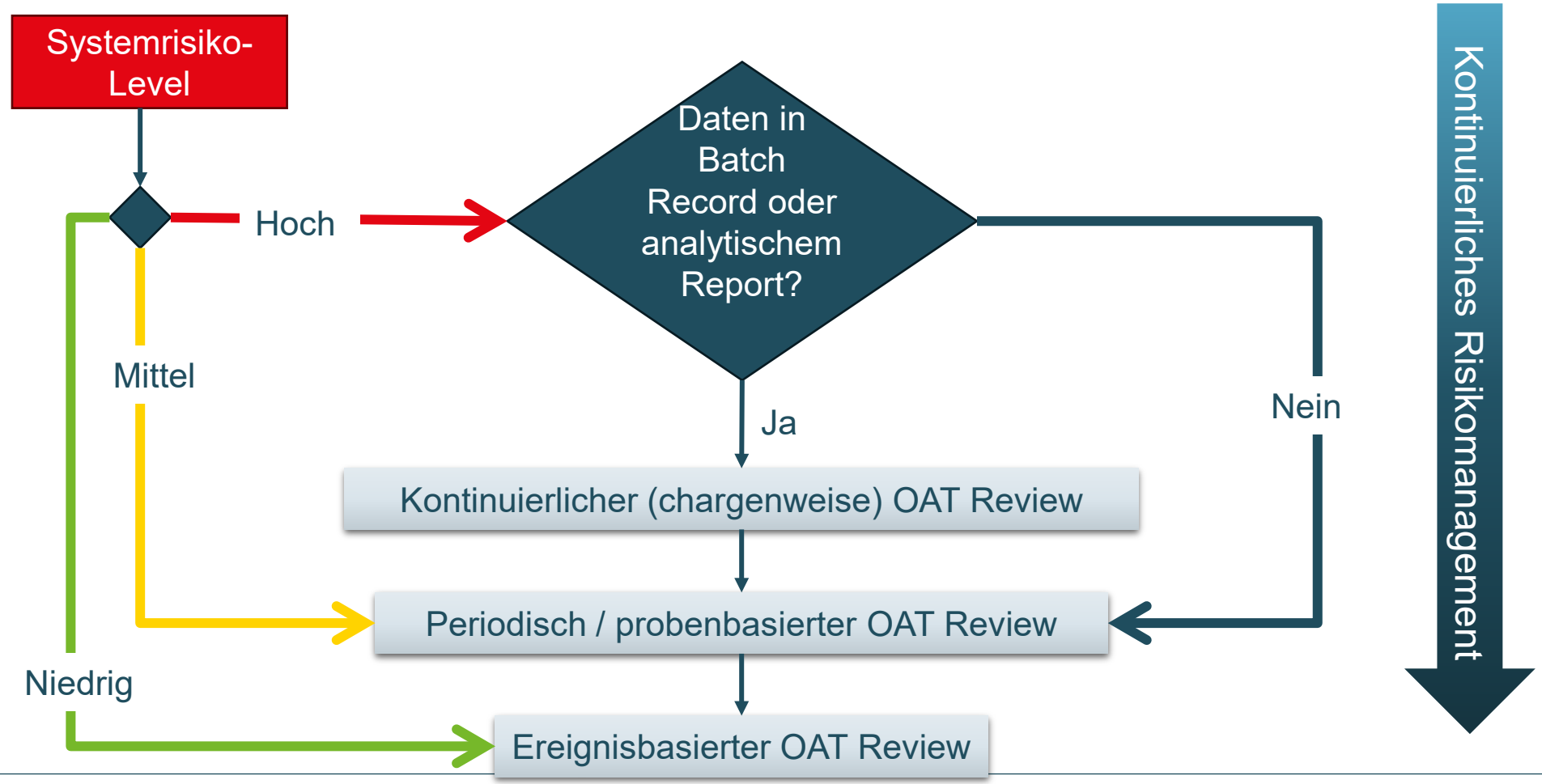

**Programm und Zeitplan** für regelmäßige Audit-Trail-Reviews erstellen: basierend auf Kritikalität und Komplexität des Systems.

# Operativer Audit Trail Review (OAT)

- **Ziel**: Überwachung von Änderungen an produktions- oder prozessrelevanten Daten
- **Typische Inhalte**:
  - Änderungen an Prozess- oder Testparametern
  - Löschung von Prozessdaten (z. B. Injektionen, Ergebnisse)
  - Wiederholte Analysen ohne dokumentierte Begründung
  - Konfiguration von Projekten und Audit Trail-Einstellungen
  - Löschung von Prozessdaten (z. B. Injektionen, Ergebnisse)
  - Auffällige Muster wie wiederholte Analysen ohne dokumentierte Begründung

- **Review-Methode**:
  - Regelmäßige Prüfung auf Auffälligkeiten
  - Dokumentation der Ergebnisse gemäß SOP´, z. B. mit „Keine Auffälligkeiten“ oder Beschreibung der Abweichung
  - Filterung nach Schrittabfolge oder Datenänderung empfohlen
  - Validierte Ausnahmeberichte können zur Unterstützung verwendet werden

# Frequenz / Tiefe Operativer Audit Trail Review



# Vergleich

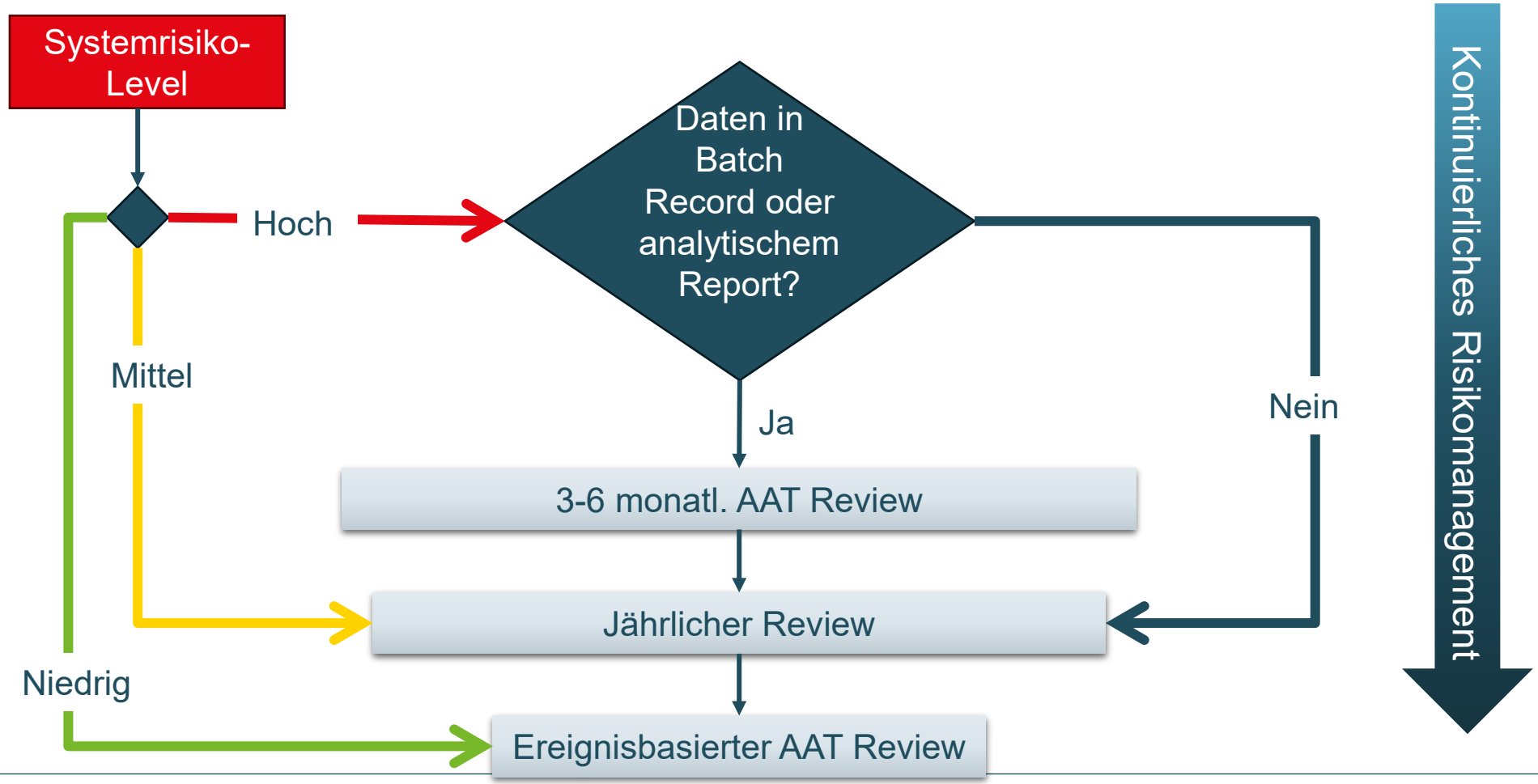
| Kontinuierlicher Audit Trail Review | Ereignisbasierter Audit Trail Review |
|---|---|
| •**Definition**: Regelmäßige, zeitlich festgelegte Überprüfung von Audit Trails – z. B. täglich, wöchentlich oder monatlich<br><br>•**Ziel**: Frühzeitige Erkennung von Unregelmäßigkeiten oder potenziellen Datenintegritätsverletzungen<br>•**Vorteile**:<br>○ Proaktive Kontrolle<br>○ Geeignet für kritische Systeme mit hohem Risiko<br>○ Unterstützt durch Ausnahmeberichte (z. B. validierte Filter für „abnormale“ Aktionen)<br>•**Herausforderungen**:<br>○ Hoher Ressourcenaufwand.<br>○ Notwendigkeit klarer SOPs und Rollenverteilung<br>○ Technische Limitierungen bei Systemen ohne elektronische Signaturen oder getrennte Audit-Trail-Profile | •**Definition**: Anlassbezogene Überprüfung, z. B. bei:<br>○ Abweichungen oder OOS-Ergebnissen<br>○ Reklamationen oder Inspektionsanfragen<br>○ Systemänderungen oder Updates<br>•**Ziel**: Fokussierte Analyse bei konkretem Anlass<br>•**Vorteile**:<br>○ Ressourcenschonend.<br>○ Effizient bei Systemen mit geringem Risiko<br>○ Ermöglicht gezielte Ursachenforschung<br>•**Herausforderungen**:<br>○ Risiko der verspäteten Erkennung von Problemen.<br>○ Abhängigkeit von funktionierenden Eskalationsmechanismen |

# Administrativer Audit Trail Review (AAT)

- **Ziel**: Kontrolle über Systemzugriffe und Benutzerverwaltung.
- **Typische Inhalte**:
  - Liste aktiver Benutzerkonten.
  - Login-Versuche (inkl. fehlgeschlagene).
  - Änderungen an Benutzerrollen und Berechtigungen
  - Änderungen an Systemkonfigurationen

- **Review-Methode**:
  - Regelmäßiger Review durch definierte Rollen (z. B. monatlich)
  - Review durch qualifiziertes Personal mit dokumentierter Schulung.
  - Validierte Ausnahmeberichte zur Unterstützung

# Frequenz Administrativer Audit Trail Review



# Zusammenfassung Vorgehensweise

1. Identifikation des Systems und seiner Funktion
2. Bewertung der Systemkritikalität (z. B. Einfluss auf Produktqualität, Patientensicherheit)
3. Bewertung der Systemkomplexität (z. B. Konfigurierbarkeit, Benutzerrechte)
4. Einstufung des Risikos (niedrig, mittel, hoch)
5. Definition der Audit Trail Review-Frequenz basierend auf dem Risiko
6. Erstellung eines Audit Trail Review-Plans durch die Qualitätseinheit
7. Dokumentation der Review-Ergebnisse gemäß SOP
8. Schulung der verantwortlichen Mitarbeiter
9. Regelmäßige Überprüfung und Anpassung des Review-Plans
10. Sicherstellung der technischen Voraussetzungen (z. B. Filterbarkeit, Exportfunktion)

# Wann kann auf einen Audit Trail verzichtet werden?

- Eine Datenbank, in der man die Daten nicht ändern kann, sondern nur lesen

- Ein weiterleitet (z. B. MES) und das Instrument nur den Messwert erfasst.
  → für das Instrument keine Audit Trail- Funktionalität, **für das MES schon!**

- Eine einfache Steuerung (SPS oder Mikrokontroller)
  → z. B. eine Waschmaschine mit drei vorgegebenen Programmen und einem angeschlossenen Drucker, der die Rohdaten liefert.

# Ist ein fehlender Kommentar (Begründung für eine Änderung) im Audit Trail schon ein Grund für eine Beanstandung bei einer Inspektion?

Wenn das System eine Kommentarfunktion hat und es wurde kein Grund eingetragen: Mangel.

Bei Systemen ohne diese Funktionalität : Workaround
z. B. SOP, wie man die Änderungen oder Löschungen in einem Logbuch dokumentiert.

# Die Bestätigung des Audit Trail Review erfolgt am Bildschirm. Wie überprüft die QP dies bei der Chargenfreigabe bzw. benötigt man das für die Freigabe?

- Audit Trail Review in einer SOP regeln
- Reviewer sollte unabhängig vom Geschäftsprozess sein.
- Der Review wird dokumentiert.
- Der Review kann Bestandteil des Batch Record Review sein.
- Unstimmigkeiten in Audit Trails sind zu untersuchen und zu beheben (Ekalationsprozesse zur Benachrichtigung)
- Bewertung der Abweichungen durch QP
- Danach kann das Produkt freigegeben werden.

# Noch Fragen?

Kundenumfrage zum Thema "digit ale Validierungssoftware"

Link zur Umfrage


**Dr. Susan Spiller**

**Validierungsingenieurin**
**Fachverantwortliche CSV**

Tel.: +49 1512 9236404

E-Mail: sspiller@testotis.de