Checkliste:

IT-Risiken für Reinraum-Monitoringsysteme

06 | 2026

BRIEM
messen. überwachen.

Als Hersteller von Reinraum-Monitoringsystemen liegen uns die langfristige Betriebssicherheit unserer Systeme und damit auch die Sicherheit der Herstellprozesse unserer Kunden besonders am Herzen.

Unter dem Leitgedanken **„Heute schon an morgen denken“** möchten wir Ihnen mit dieser Checkliste praktische Hinweise und konkrete Fragestellungen an die Hand geben, um IT-Risiken frühzeitig zu erkennen und wirksam zu reduzieren.

Im Fokus stehen dabei nicht nur Cyberangriffe, sondern allgemein Risiken rund um:

- Systemverfügbarkeit
- Datenverlust
- Infrastruktur- und Serverausfälle
- Externe Dienstleister
- Datenintegrität
- Business Continuity Management (BCM)

Reinraum-Monitoringsysteme liefern GMP-relevante Messdaten, Alarmierungen, Audit-Trails und Chargenreports und sind damit Bestandteil des Qualitätssicherungssystems.

Ohne valide und nachvollziehbare Umgebungsdaten kann nicht sicher nachgewiesen werden. IT-Risiken werden damit unmittelbar zu Qualitäts-, Compliance- und Versorgungsrisiken.

Diese Checkliste soll Sie dabei unterstützen, gemeinsam mit IT, Qualitätssicherung, Herstellleitung und Dienstleistern praktische Maßnahmen zur Risikoreduzierung umzusetzen und die langfristige Betriebssicherheit zu erhöhen.

Bedeutung von Validierung und strukturiertem Risikomanagement

Im Unterschied zu einfachen technischen Überwachungssystemen unterliegen validierte Systeme besonderen regulatorischen Anforderungen.

Jede Änderung an der Systemumgebung – beispielsweise Softwareupdates, Servermigrationen oder Änderungen der IT-Infrastruktur– kann Einfluss auf den validierten Zustand des Systems haben und muss daher kontrolliert bewertet, dokumentiert und gegebenenfalls qualifiziert werden.

IT-Risiken betreffen damit nicht nur die technische Verfügbarkeit eines Systems, sondern unmittelbar auch die GMP-Compliance.

Empfohlener Vorgehensablauf

Die Absicherung eines Reinraum-Monitoringsystems erfordert einen strukturierten und wiederkehrenden Prozess zur Identifikation, Bewertung und Minimierung potenzieller Risiken.

Diese Checkliste unterstützt insbesondere den folgenden Vorgehensablauf:

A. Durchführung einer Risikoanalyse
Im ersten Schritt sollten mögliche Risiken und Schwachstellen systematisch identifiziert und bewertet werden.

Dabei sollten sowohl technische als auch organisatorische Risiken betrachtet werden, beispielsweise: Serverausfall, Netzwerkausfall, Stromausfall, Ransomware, Verfügbarkeit IT-Support usw.
Diese Checkliste dient hierbei als strukturierte Hilfestellung zur systematischen Risikoerfassung.

B. Erstellung eines Notfallplans
Auf Basis der Risikoanalyse sollte ein umfassender Notfallplan erstellt werden. Dieser sollte zentrale Fragestellungen auf Basis der Checkliste beinhalten. Ziel ist es, die Verfügbarkeit GMP-relevanter Funktionen und Daten auch im Störungsfall sicherzustellen.

C. Definition von SOPs und Schulung der Mitarbeiter
Die festgelegten Prozesse und Maßnahmen sollten in geeigneten SOPs dokumentiert werden.
Zusätzlich sollten alle beteiligten Mitarbeiter regelmäßig geschult werden, insbesondere hinsichtlich:

- → Verhalten im Störungsfall
- → Eskalationswege / Verantwortlichkeiten
- → Dokumentationsanforderungen

D. Regelmäßige Überprüfung und Aktualisierung
Risiken, IT-Infrastrukturen und regulatorische Anforderungen verändern sich kontinuierlich.

Daher sollten Risikoanalyse, Notfallkonzepte, SOPs und technische Schutzmaßnahmen regelmäßig überprüft, getestet und aktualisiert werden z.B. nach Änderungen an Hard- oder Software, Infrastrukturänderungen, oder beim Wechsel externer Dienstleister.

1. Systemübersicht & Verantwortlichkeiten

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Liegt der Apotheke eine aktuelle Systemübersicht vor?	Prüfen und ggf. bei BRIEM Systemtopologie anfordern?	Verantwortliche für die Herstellung		
Sind Verantwortlichkeiten definiert? ☐ Systemverantwortlicher (Nutzer) ☐ Ansprechpartner IT ☐ Ansprechpartner Haustechnik	Verantwortlichkeiten definieren Verantwortlichkeiten kommunizieren.	Verantwortliche für die Herstellung		
Gibt es eine Übersicht mit Ansprechpartner bei Störungen? ☐ Systemverantwortlicher (Nutzer) ☐ Ansprechpartner IT ☐ Ansprechpartner Haustechnik ☐ Support BRIEM (support@briem.de - +49 7022 60 92 -75)	Kontaktliste pflegen / Verantwortlichkeiten definieren	Verantwortliche für die Herstellung		
Gibt es eine Übersicht der Schnittstellen? Gibt es Schnittstellen zu anderen Systemen? (z.B. GLT)	Erstellung einer Übersicht	Verantwortliche für die Herstellung		

2. Verfügbarkeit & Betriebssicherheit

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Gibt es eine USV? Welche Teile sind an der USV angeschlossen (Server, Schaltschrank?)	Mit IT / Haustechnik besprechen	IT / Haustechnik		

Wie lange läuft das System bei Stromausfall weiter?	Autonomie prüfen	IT / Haustechnik		
Gibt es Redundanzen für kritische Komponenten?	Server- und Netzwerkredundanz prüfen	IT		
Wurde geprüft ob kritische Komponenten auf Lager gelegt werden sollten?	Kritische Komponenten prüfen / auf Lager legen.	Haustechnik (Rücksprache mit BRIEM)		
Werden Serverzustände überwacht?	Systemmonitoring installieren / aktivieren	IT		
Wird die Anlage regelmäßig gemäß Herstellerempfehlung gewartet?	Prüfung ob Wartungsvertrag (inklusive Support) vorliegt.	Systemverantwortlicher		
Werden Alarmierungen regelmäßig getestet?	Alarmtests durchführen (Ampel, SMS, E-Mail, ...)	IT		

3. Backup & Wiederherstellung

Prüffrage	Maßnahme	Ansprechpartner	Notizen	Status
Ist ein Backup eingerichtet?	Backup-Konzept dokumentieren	IT		
Wie häufig werden Backups durchgeführt?	Backup-Intervall definieren	IT		
Welche Daten werden gesichert?	BRIEM Datenbank oder kompletter Server	IT		
Wo werden Backups gespeichert? Gibt es Backups, die nicht über das Netzwerk erreichbar sind?	Speicherorte dokumentieren. Schutz vor Verschlüsselung sicherstellen	IT		
Wird die Wiederherstellung getestet?	Restore-Test durchführen und dokumentieren	IT		
Können komplette Systeme wiederhergestellt werden?	Desaster-Recovery testen	IT		

4. Benutzer & Zugriffsschutz

Prüffrage	Maßnahme	Ansprechpartner	Notizen	Status
Haben alle Nutzer eigene Benutzerkonten?	Keine Sammelaccounts verwenden	Systemverantwortlicher		
Ist der Zugang zum Monitoring-Server physisch geschützt?	Zugangskonzept prüfen	IT / Systemverantwortlicher		
Gibt es Rollen- und Rechtekonzepte?	Rechte prüfen und minimieren	Systemverantwortlicher		
Werden Standardpasswörter geändert?	Herstellerzugänge prüfen	Systemverantwortlicher		
Werden Passwörter sicher verwaltet?	Passwortregeln im Monitoringsystem überprüfen und ggf. anpassen. Active-Directory Anbindung des BRIEM-Systems prüfen.	Systemverantwortlicher		
Werden ehemalige Mitarbeiter deaktiviert?	Offboarding-Prozess definieren	Systemverantwortlicher		

5. Netzwerk & Infrastruktur

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Ist das Monitoringsystem vom restlichen Netz getrennt? (VLAN)	Netzwerksegmentierung umsetzen	IT		
Sind unnötige Netzwerkports deaktiviert? (Gerne schicken wir unsere Anforderungen an Netzwerk Ports zu.)	Sicherheitsprüfung durchführen	IT		
Ist ein Fernzugriff für BRIEM eingerichtet?	Mit IT prüfen	IT		
Werden Netzwerkänderungen im GMP Umfeld dokumentiert?	Change-Management durchführen	IT		

6. Software, Updates & Konfiguration

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Werden Betriebssystem Updates von der IT installiert?	Patchprozess definieren	IT		
Werden Updates vor Einsatz bewertet?	GMP-Auswirkungen prüfen	IT / QS		
Werden Konfigurationsänderungen dokumentiert?	Änderungsprotokoll führen	IT / QS		
Gibt es Schutz vor Schadsoftware auf dem Monitoring Server?	Virenschutz/MDR einsetzen	IT		
Sind Virenschutzprogramme aktuell?	Automatische Aktualisierung prüfen	IT		
Befinden sich alle Softwarekomponenten im aktiven Support-Zeitraum?	Prüfung Information über Supportzeitraum von BRIEM	System-verantwort-licher		
Ist sichergestellt, dass Software vor Ende des Support-Zeitraums aktualisiert wird?	Prüfung mit Systemverantwort-lichen, Einkauf etc.	System-verantwort-licher		

7. Notfallmanagement / Business Continuity Management (BCM)

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Gibt es einen IT-Notfallplan / BCM-Konzept für die Apotheke?	SOP erstellen	IT / QS		
Ist definiert, wann Herstellung gestoppt werden muss?	GMP-Kriterien festlegen	QS		
Wie sehen Ersatzmaßnahmen aus? - Können Messwerte manuell dokumentiert werden? (z.B. mittels mobilem Partikel-zähler)	Übergangsprozess definieren	QS		
Sind kritische Prozesse identifiziert?	z.B. Herstellung und Alarmierung	QS /		
Gibt es Wiederanlaufpläne?	Reihenfolge definieren	IT / QS		
Ist dokumentiert, wie Systeme nach Aus-fall freigegeben werden?	Requalifizierung definieren	QS		

8. Dienstleister

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Gibt es Wartungsverträge?	Verantwortlichkeiten prüfen	Einkauf / IT		
Sind Fernzugriffe geregelt?	Zugriffskontrolle definieren	IT / Dienst-leister		
Werden Serviceeinsätze dokumentiert?	Protokollierung sicherstellen	IT / QS		

9. Mitarbeiterschulung

Prüffrage	Maßnahme	Ansprech-partner	Notizen	Status
Wissen Mitarbeiter, wie Störungen gemeldet werden?	Meldeweg definieren	IT		
Wissen Mitarbeiter, wie sie sich bei Systemausfällen verhalten?	Notfalltraining durchführen	IT / QS		
Werden typische Fehlerquellen erklärt?	Praxisbeispiele verwenden	IT / QS		

IT-Risiken lassen sich nicht vollständig vermeiden.

Durch klare Prozesse, regelmäßige Prüfungen und eine strukturierte Zusammenarbeit zwischen Apotheke, Qualitätssicherung, IT und Dienstleistern können Risiken reduziert werden.

Diese Checkliste soll dabei unterstützen, Risiken frühzeitig sichtbar zu machen und praktische Maßnahmen zur Verbesserung der Betriebssicherheit umzusetzen.

Diese Checkliste wurde mit größtmöglicher Sorgfalt erstellt und dient ausschließlich als allgemeine Orientierungshilfe zur Identifikation und Reduzierung möglicher IT- und Betriebsrisiken im Umfeld von Reinraum-Monitoringsystemen. Sie erhebt keinen Anspruch auf Vollständigkeit und kann eine individuelle Risikoanalyse, Validierung, Qualifizierung sowie Bewertung der konkreten System- und Infrastrukturbedingungen vor Ort nicht ersetzen.

Die Verantwortung für die Auswahl, Umsetzung, Prüfung und regelmäßige Überwachung geeigneter technischer, organisatorischer und regulatorischer Maßnahmen verbleibt beim Betreiber. Insbesondere sind die jeweils geltenden gesetzlichen, normativen und GMP-relevanten Anforderungen eigenverantwortlich zu berücksichtigen.

Eine Haftung für Schäden oder sonstige Folgen, die direkt oder indirekt aus der Nutzung dieser Checkliste entstehen, ist ausgeschlossen. Dies gilt auch für die Vollständigkeit, Aktualität und Richtigkeit der enthaltenen Informationen.

Bei Fragen rund um Ihr Reinraum-Monitoring System unterstützen wir Sie gerne.

BRIEM Steuerungstechnik GmbH
Lauterstraße 23
D-72622 Nürtingen
Telefon +49 (0) 7022 60 92-0
info@briem.de
Eingetragen am Amtsgericht Stuttgart HRB 224325

Autor:
Matthias Alber
Key Account Manager
E-Mail: matthias.alber@briem.de

BRIEM ist Ihr kompetenter Partner für anspruchsvolle Messtechnik und Überwachungslösungen in Reinräumen und Lagerräumen. Als Full-Service-Anbieter begleiten wir unsere Kunden von der Konzeptionierung und Fachplanung über die Umsetzung vor Ort bis hin zur Wartung und Instandhaltung.

Von unseren Standorten Nürtingen, Berlin und Hagen aus betreuen wir Kunden in ganz Europa.