



Holger Reibold

Automated Compliance Monitoring

Kontinuierliche Auditfähigkeit
für NIS2, DORA, CRA und EU AI Act

BRAIN-MEDIA.DE

Audit-Checklisten

Die folgenden Audit-Checklisten basieren auf dem Brain-Media Audit Model und sind so gestaltet, dass sie direkt in der Praxis eingesetzt werden können.

B.1 Zugriffskontrollen (IAM & MFA)

Ziel: Sicherstellen, dass Zugriffe kontrolliert, nachvollziehbar und angemessen geschützt sind

Checkliste:

- Sind alle Benutzer eindeutig identifizierbar?
- Sind privilegierte Konten klar definiert und dokumentiert?
- Ist MFA für privilegierte Konten aktiviert?
- Werden neue Benutzerkonten standardisiert angelegt?
- Vergabe von Berechtigungen nach Least-Privilege-Prinzip?
- Erfolgt eine regelmäßige Überprüfung von Benutzerrechten?
- Werden Zugriffe bei Austritt oder Rollenwechsel entzogen?
- Werden ungewöhnliche Login-Aktivitäten erkannt/bewertet?

Bewertung (Score):

- 0 = Keine Struktur
- 1 = Teilweise umgesetzt
- 2 = Vollständig umgesetzt
- 3 = Kontinuierlich überwacht

B.2 Patch- und Schwachstellenmanagement

Ziel: Minimierung technischer Risiken durch zeitnahe Behebung von Schwachstellen

Checkliste:

- Werden regelmäßig Schwachstellenscans durchgeführt?
- Sind Systeme vollständig im Scan erfasst?
- Gibt es definierte SLAs für kritische Schwachstellen?
- Werden kritische Schwachstellen fristgerecht behoben?
- Werden Scan-Ergebnisse priorisiert und dokumentiert?
- Gibt es eine klare Verantwortlichkeit pro System?
- Werden wiederkehrende Schwachstellen analysiert?
- Wird der Patch-Status regelmäßig überprüft?

Bewertung (Score):

- 0 = Kein Prozess
- 1 = Scans ohne Steuerung
- 2 = Strukturierter Prozess mit SLAs
- 3 = Kontinuierliches Monitoring

B.3 KI-Systeme (AI Act Readiness)

Ziel: Sicherstellung der Nachvollziehbarkeit und Kontrolle von KI-Systemen

Checkliste:

- Ist das KI-System als (hoch-)risikorelevant klassifiziert?
- Sind Trainingsdaten dokumentiert und nachvollziehbar?
- Werden Modellversionen und Änderungen protokolliert?
- Ist nachvollziehbar, wie Entscheidungen zustande kommen?
- Werden Eingabedaten auf Qualität und Konsistenz geprüft?
- Gibt es Monitoring für Modellverhalten und Abweichungen?
- Sind Verantwortlichkeiten für das KI-System definiert?
- Werden Änderungen an Modell oder Daten überwacht?

Bewertung (Score):

- 0 = Keine Transparenz
- 1 = Teilweise dokumentiert
- 2 = Strukturierte Kontrolle
- 3 = Kontinuierliches Monitoring & Governance

B.4 Drittanbieter & Lieferkette

Ziel: Transparenz und Kontrolle über externe Abhängigkeiten

Checkliste:

- Sind alle relevanten Drittanbieter erfasst?
- Erfolgt eine Klassifizierung nach Kritikalität?
- Werden Sicherheitsbewertungen regelmäßig durchgeführt?
- Sind Sicherheitsanforderungen vertraglich festgelegt?
- Liegen aktuelle Zertifikate oder Nachweise vor?
- Werden Änderungen oder Vorfälle bei Anbietern überwacht?
- Gibt es klare Verantwortlichkeiten für Drittanbieter?
- Werden Abhängigkeiten dokumentiert und bewertet?

Bewertung (Score):

- 0 = Keine Übersicht
- 1 = Einzelbewertungen
- 2 = Strukturierter Prozess
- 3 = Kontinuierliches Third-Party Monitoring

B.5 Incident Detection & Reporting

Ziel: Sicherstellen, dass Vorfälle erkannt und fristgerecht gemeldet werden

Checkliste:

- Werden sicherheitsrelevante Ereignisse zentral erfasst (z. B. SIEM)?
- Sind Use Cases zur Erkennung definiert?
- Werden Incidents systematisch klassifiziert?
- Gibt es klare Meldefristen und Verantwortlichkeiten?
- Werden regulatorische Meldepflichten eingehalten?
- Sind Incident-Prozesse dokumentiert und getestet?
- Werden Vorfälle vollständig dokumentiert?
- Gibt es regelmäßige Übungen oder Simulationen?

Bewertung (Score):

- 0 = Kein strukturierter Prozess
- 1 = Detection vorhanden, aber unvollständig
- 2 = Strukturierte Prozesse inkl. Reporting
- 3 = Kontinuierliches Monitoring & Testing

B.6 Nutzung in der Praxis

Diese Checklisten können flexibel eingesetzt werden:

- als manuelle Self-Assessments
- als Grundlage für interne Audits
- als Input für KPI- und Score-Systeme
- als Struktur für automatisierte Monitoring-Systeme

In Kombination mit BAM lassen sich die Ergebnisse direkt in strukturierte Daten überführen und kontinuierlich weiterverarbeiten. Damit bilden die Checklisten die Brücke zwischen operativer Umsetzung und systematischer Steuerung.

Mehr zum Thema Automated Compliance Monitoring

Der vollständige Leitfaden „Automated Compliance Monitoring – Kontinuierliche Auditfähigkeit für NIS2, DORA, CRA und EU AI Act“

 [Jetzt bei Amazon bestellen](#)