BAM-Beispiele

(JSON)

Nachfolgend finden Sie fünf vollständige Beispiel-Controls auf Basis des Brain-Media Audit Model. Die Beispiele zeigen, wie sich regulatorische Anforderungen in strukturierte, maschinenlesbare und auditfähige Objekte überführen lassen. Sie dienen als Referenz für die praktische Umsetzung in Monitoring-, Audit- und KaaS-Kontexten.

A.1 Zugriffskontrolle – Multi-Faktor-Authentifizierung


```
{
  "id": "BAM-ACCESS-001",
  "framework": ["ISO27001", "NIS-2", "DORA"],
  "domain": "Access Control",
  "requirement": "Privilegierte und administrative Zugriffe müssen besonders geschützt werden.",
  "risk": "Unbefugter Zugriff auf kritische Systeme führt zu Sicherheitsvorfällen, Datenverlust oder Manipulation.",
  "control": "Multi-Faktor-Authentifizierung für alle privilegierten und administrativen Konten implementieren.",
  "evidence": [
    "MFA-Konfigurationsnachweise aus dem Identity Provider",
    "Liste privilegierter Konten",
    "Authentifizierungsprotokolle"
  ],
  "audit_questions": [
    "Ist für alle administrativen Konten Multi-Faktor-Authentifizierung aktiviert?",
    "Werden neu angelegte privilegierte Konten automatisch der MFA-Pflicht unterworfen?"
  ],
  "score_model": {
```

```
    "0": "Keine MFA für privilegierte Konten",
    "1": "Teilweise aktiviert",
    "2": "Für alle privilegierten Konten aktiviert",
    "3": "Kontinuierlich überwacht und bei Abweichungen automatisiert eskaliert"
  },
  "mappings": {
    "nis-2": ["Art. 21"],
    "dora": ["ICT Risk Management"],
    "iso27001": ["Annex A - Access Control"]
  },
  "tags": ["MFA", "Access Control", "IAM", "Privileged Access", "Identity Security"]
}
```

A.2 Patch- und Schwachstellenmanagement

```
{
  "id": "BAM-VULN-002",
  "framework": ["ISO27001", "NIS-2", "CRA", "DORA"],
  "domain": "Vulnerability Management",
  "requirement": "Bekannte Schwachstellen müssen identifiziert, bewertet und fristgerecht behandelt werden.",
  "risk": "Offene Schwachstellen können ausgenutzt werden und zu Kompromittierung, Ausfall oder regulatorischen Verstößen führen.",
  "control": "Regelmäßige Schwachstellenscans durchführen und kritische Schwachstellen innerhalb definierter Fristen beheben.",
  "evidence": [
```

```
    "Berichte aus Vulnerability Scannern",
    "Patch-Status aus Endpoint-Management-Systemen",
    "Ticket- und Eskalationshistorie"
  ],
  "audit_questions": [
    "Werden kritische Schwachstellen innerhalb definierter SLAs behoben?",
    "Werden Scan-Ergebnisse regelmäßig ausgewertet und priorisiert?"
  ],
  "score_model": {
    "0": "Kein strukturierter Schwachstellenprozess",
    "1": "Scans vorhanden, aber keine verbindlichen Fristen",
    "2": "Scans und Behebung nach definierten SLAs",
    "3": "Kontinuierliches Monitoring mit Trendanalyse und Eskalation"
  },
  "mappings": {
    "nis-2": ["Art. 21"],
    "dora": ["ICT Risk Monitoring"],
    "cra": ["Vulnerability Handling"],
    "iso27001": ["Technical Vulnerability Management"]
  },
  "tags": ["Vulnerability", "Patching", "Exposure Management", "Security Operations", "CRA"]
}
```

A.3 Hochrisiko-KI-System – Monitoring


```
{
  "id": "BAM-AI-003",
  "framework": ["AI Act", "ISO27001", "NIS-2"],
  "domain": "AI Monitoring",
  "requirement": "Hochrisiko-KI-Systeme müssen kontinuierlich
überwacht, dokumentiert und kontrolliert betrieben werden.",
  "risk": "Fehlentscheidungen, Bias, Datenprobleme oder man-
gelnde Transparenz führen zu regulatorischen Verstößen und ope-
rativen Schäden.",
  "control": "Monitoring für Modellverhalten, Datenqualität,
Nutzungskontext und Änderungen an Modellversionen etablieren.",
  "evidence": [
    "Logs zu Modellentscheidungen",
    "Dokumentation von Trainings- und Eingabedaten",
    "Versionshistorie des Modells",
    "Freigabe- und Änderungsprotokolle"
  ],
  "audit_questions": [
    "Werden Änderungen an Modellen und Datenquellen kontinuier-
lich überwacht?",
    "Ist nachvollziehbar, mit welcher Modellversion eine Ent-
scheidung getroffen wurde?",
    "Werden ungewöhnliche Muster oder Abweichungen im Modellver-
halten erkannt?"
  ],
  "score_model": {
    "0": "Kein strukturiertes Monitoring des KI-Systems",
    "1": "Einzelne Dokumentation vorhanden",
```

```
    "2": "Strukturierte Überwachung und Nachvollziehbarkeit ge-
geben",

    "3": "Kontinuierliches Monitoring mit Governance, Eskalation
und Audit-Trail"

  },

  "mappings": {

    "ai_act": ["High-Risk AI Monitoring", "Post-Market Monitor-
ing"],

    "nis-2": ["Risk Monitoring"],

    "iso27001": ["Logging and Monitoring"]

  },

  "tags": ["AI Act", "High-Risk AI", "Model Monitoring", "Data
Quality", "AI Governance"]

}
```

A.4 Drittanbieter- und Lie erkettenüberwachung

```
{

  "id": "BAM-TPRM-004",

  "framework": ["NIS-2", "DORA", "CRA", "ISO27001"],

  "domain": "Third Party Risk Management",

  "requirement": "Risiken durch Drittanbieter und Lieferanten
müssen bewertet, dokumentiert und regelmäßig überwacht werden.",

  "risk": "Schwachstellen oder Ausfälle bei Dienstleistern wir-
ken sich direkt auf Sicherheit, Verfügbarkeit und Compliance der
eigenen Organisation aus.",

  "control": "Kritische Drittanbieter klassifizieren, regelmäßig
bewerten und relevante Sicherheitsinformationen laufend überwa-
chen.",

  "evidence": [

    "Lieferantenklassifizierung",
```

```
    "Sicherheitsfragebögen",
    "Zertifikate und Auditberichte",
    "Vertragsklauseln zu Sicherheit und Meldepflichten"
  ],
  "audit_questions": [
    "Werden kritische Drittanbieter regelmäßig bewertet?",
    "Sind Sicherheitsanforderungen vertraglich festgelegt?",
    "Werden relevante Änderungen oder Vorfälle bei Dienstleis-
tern laufend berücksichtigt?"
  ],
  "score_model": {
    "0": "Keine strukturierte Drittanbieterbewertung",
    "1": "Einmalige Bewertung ohne laufende Überwachung",
    "2": "Regelmäßige Bewertung und Dokumentation vorhanden",
    "3": "Kontinuierliches Third-Party Monitoring mit Eskalation
und Abhängigkeitsanalyse"
  },
  "mappings": {
    "nis-2": ["Supply Chain Security"],
    "dora": ["Third Party ICT Risk"],
    "cra": ["Supply Chain Obligations"],
    "iso27001": ["Supplier Relationships"]
  },
  "tags": ["Third Party", "Supply Chain", "Vendor Risk", "TPRM",
"Contract Security"]
}
```

A.5 Incident Detection & Reporting


```
{
  "id": "BAM-INC-005",
  "framework": ["NIS-2", "DORA", "AI Act", "ISO27001"],
  "domain": "Incident Management",
  "requirement": "Sicherheitsvorfälle müssen erkannt, bewertet und innerhalb regulatorischer Fristen gemeldet werden.",
  "risk": "Verzögerte oder unvollständige Erkennung und Meldung von Vorfällen führt zu erhöhtem Schaden und regulatorischen Sanktionen.",
  "control": "Incident Detection, Klassifizierung und Reporting mit definierten Fristen und Verantwortlichkeiten etablieren.",
  "evidence": [
    "SIEM- oder EDR-Logs",
    "Incident-Tickets",
    "Meldeprotokolle",
    "Eskalations- und Kommunikationsnachweise"
  ],
  "audit_questions": [
    "Werden sicherheitsrelevante Vorfälle rechtzeitig erkannt?",
    "Werden meldepflichtige Incidents korrekt klassifiziert und fristgerecht gemeldet?",
    "Sind Rollen, Fristen und Eskalationswege dokumentiert und nachweisbar?"
  ],
  "score_model": {
    "0": "Kein strukturierter Incident-Prozess",
    "1": "Detection vorhanden, aber Reporting unklar oder un-vollständig",
```

```
    "2": "Erkennung, Klassifizierung und Meldung strukturiert
umgesetzt",
    "3": "Kontinuierlich überwacht, getestet und mit Fristen-
steuerung verknüpft"
  },
  "mappings": {
    "nis-2": ["Incident Notification"],
    "dora": ["ICT Incident Reporting"],
    "ai_act": ["Serious Incident Handling"],
    "iso27001": ["Information Security Incident Management"]
  },
  "tags": ["Incident Response", "Detection", "Reporting",
"SIEM", "Regulatory Notification"]
}
```

Mehr zum Thema Automated Compliance Monitoring

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