FINANCE AUDIT

RiMaGo Forum 2026

# DORA – gegen den (Main-?) Stream gebürstet

Welche Art der Resilienz brauchen wir?
Einordnung, Praxisfälle und fachliche Perspektiven

**Prof. Dr. Ralf Kühn**
Wirtschaftsprüfer / CPA ·
Geschäftsführer Finance Audit GmbH Wirtschaftsprüfungsgesellschaft

# Ablauf

FINANCE AUDIT

| | | |
|---|---|---|
| A | **Drei Praxisfälle 2026** | Cyberangriff beim Subdienstleister · Sabotage am Umspannwerk · Hintertür in der Fachsoftware |
| B | **Was die Prüfungspraxis bestätigt** | Feststellungen aus einer aktuellen aufsichtlichen DORA-Vor-Ort-Prüfung – gespiegelt an den Fällen |
| C | **Von Vollständigkeit zu Wirksamkeit** | Regulatorik 2026, eine Steuerungslogik, Evidenzkette und die sechs Prüffelder |
| D | **KI als Beschleuniger** | Deepfakes, Schatten-KI, AI Supply Chains – und Chancen für Codeprüfung, Abwehr und Dokumentation |

FINANCE AUDIT

PRAXISFALL 1

# Vier Stunden in einem realen Notfall 2026

Cyberangriff bei einem IKT-Subdienstleister der Vermögensverwaltung

# Ein realer Fall 2026 …

FINANCE AUDIT

**Ein Institut erhält über einen seiner wichtigsten Dienstleister die erste Information zu einem Sicherheitsvorfall bei einem IKT-Subdienstleister.**

- Unbefugter Zugriff auf Produktivsysteme festgestellt
- Abfluss von Kundendaten kann nicht ausgeschlossen werden
- Rund 300 Kunden zunächst potenziell betroffen
- Kein direkter Vertrag mit dem betroffenen Subdienstleister

**~300** Kunden zunächst potenziell betroffen

**?** unbefugter Zugriff auf Produktivsysteme

**Daten** Abfluss nicht auszuschließen

***Ab diesem Moment wird es etwas „hektischer“ …***

# Dynamik der nächsten Stunden in diesem Fall

FINANCE AUDIT

**07:30** Erstinformation: Cybervorfall beim IKT-Subdienstleister

**09:13** Betroffenheit deutlich größer als zunächst angenommen

**09:30** Weitere Subdienstleister werden sichtbar – kein direkter Vertragsweg

**10:03** Information erreicht Öffentlichkeit und Kunden

**10:30–11:30** Sicherheitsentscheidungen, Ausfälle sowie rechtlicher und öffentlicher Druck

**11:35** Managemententscheidung: Trennung der Verbindungen zum Dienstleister

**Betroffen um 10:03**

**1.404**

Mandate der Vermögensverwaltung

**121,7 Mio. €**

betroffenes Kundenanlagevolumen

**Kernaussage:** Die Lage verändert sich schneller, als Entscheidungen ohne Vorbereitung und Training getroffen werden können.

# Regulatorische Meldepflichten bei unvollständiger Faktenlage

FINANCE AUDIT

**Unvollständige Faktenlage**

### DORA / BaFin: eigene Einstufung und Meldung

- Einstufung nach Art. 18 DORA i. V. m. DelVO (EU) 2024/1772
- Erstmeldung spätestens 4 h nach Einstufung, max. 24 h nach Kenntnis
- Zwischenmeldung spätestens 72 h nach Erstmeldung (Art. 5 Abs. 1 DelVO (EU) 2025/301)

### DSGVO: eigener Bewertungspfad

- Meldung an die Aufsichtsbehörde binnen 72 h (Art. 33 DSGVO)
- Benachrichtigung Betroffener bei hohem Risiko (Art. 34 DSGVO)
- Rollenkette bis zum Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO)

### Weitere Pfade – gesondert prüfen

- Verbund, Versicherer, Strafverfolgung, Kunden
- Nicht automatisch aus den Informationen des Dienstleisters ableitbar
- Eigene Trigger, eigene Fristen, eigene Adressaten

**Kernbotschaft 1:** Mehrere rechtliche Melde- und Informationspfade müssen parallel bewertet werden – mit jeweils eigenen Fristen und Triggern.

**Kernbotschaft 2:** Ein Dienstleister kann melden – die Verantwortung des Finanzunternehmens entfällt dadurch nicht. Jeder Dienstleister verfolgt in dieser Situation sein Eigeninteresse.

# Sicherheit und Verfügbarkeit im Konflikt

FINANCE AUDIT

### Sicherheit erhöhen

Backdoor- und Adminzugänge müssen gesichert bzw. entfernt werden. Die Trennung von Verbindungen reduziert das Sicherheitsrisiko.

### Managemententscheidung unter Zeit- und Fristendruck

Die Entscheidung braucht eine Analyse der Auswirkungen, Fristen, Verantwortlichkeiten/Haftung und des jeweiligen Risikos.

### Verfügbarkeit erhalten

Eine Trennung von Verbindungen beeinträchtigt die Verfügbarkeit geschäftskritischer Prozesse – sofort und für Kunden sichtbar.

**Kernbotschaft:** Eine wirksame Sicherheitsmaßnahme kann gleichzeitig die Verfügbarkeit geschäftskritischer Prozesse beeinträchtigen. Genau deshalb braucht es eine bewusste Managemententscheidung und Transparenz über den „Informationsverbund“.

***DORA-Pflichten im „Maschinenraum“ haben Sinn – bei echten Entscheidungen.***

# Die Trennung wirkt – und erzeugt einen eigenen Ausfall

FINANCE AUDIT

**11:40** Schnittstellen getrennt, Dienstleister-Adminzugänge gesperrt

**11:55** Depot- und Mandatsdaten nicht mehr abrufbar

**12:30** Anrufwelle im Kundenservice, Filialen ohne Auskunft

**14:00** Rebalancing und Orderläufe gestoppt – der Markt läuft weiter

**16:00** Wiederanschaltung erst nach forensischer Freigabe – frühestens in 48 h

## Was konkret ausfällt

- Online-Banking Wertpapierorder: Depot- und Mandatsansicht leer oder veraltet
- Beratung: kein Zugriff auf Reporting und Geeignetheitsdokumentation
- Portfoliomanagement: Keine Umsetzung, Haftung für unterbliebene Dispositionen

## Was die Entscheidung auslöst

- Selbst verursachte Ausfallzeit zählt zur Vorfallsauswirkung (Art. 18 Abs. 1 lit. b DORA i. V. m. Art. 3 Abs. 2 DelVO (EU) 2024/1772)
- Schwelle: > 2 h Ausfall bei IKT-Diensten für kritische oder wichtige Funktionen oder > 24 h Dauer (Art. 9 Abs. 3 DelVO)

**Kernbotschaft:** Die Trennung ist richtig – und trotzdem ein eigener Ausfall. Notbetrieb, Kommunikation, Wiederanschaltkriterien und Entscheidungsbefugnis müssen vorher feststehen.

**Leitfrage:** **Welche Schnittstelle müssen wir morgen trennen – und wissen wir, was dann bei uns ausfällt?**

# Der kritischste Dienstleister war der Bank nicht bekannt – und der Durchgriff ist (sehr) begrenzt

FINANCE AUDIT


## Lieferkettenproblematik in der Praxis – jenseits von Bürokratie

- Kein direkter Vertrags- oder Informationsweg zu Teilen der Leistungskette
- Krisenfähigkeit hängt an Transparenz, Eskalationswegen und realistischen Alternativen

## Praxistipp – oft nicht beachtet

Nicht nur fragen: „Wer ist formal unser Vertragspartner?“

**sondern: „Wovon hängt die Funktion tatsächlich ab?“**

**Kernbotschaft:** Die eigene Handlungsfähigkeit kann von einem Subdienstleister abhängen, zu dem weder ein Vertrags- noch ein Informations- oder Eskalationsweg besteht. Das Wissen ist überall da – aber was machen wir damit?

**Leitfrage: Welche indirekte Abhängigkeit wäre in einer Krise für uns am schwersten zu steuern?**

# Der Angriff scheint technisch – die Gründe sind technisch UND organisatorisch

FINANCE AUDIT

**Technische Schwäche** → **Organisations-lücke** → **Krisendynamik** → **Handlungsfähigkeit?**

## Technisch

Kompromittierter administrativer Zugang und Backdoor-Problematik beim Subdienstleister.

## Organisatorisch

Vertretungslücke, begrenzter Durchgriff, fragmentierte Informationswege, zu viel Bürokratie, zu wenig Handlungskompetenz.

## Managementfolge

Resilienz zeigt sich an Handlungsfähigkeit – nicht nur an technischen Schutzmaßnahmen.

**Kernbotschaft:** Ein technischer Angriff wird oft erst dann zur Krise, wenn technische Schwächen auf organisatorische Lücken in Rollen, Abhängigkeiten, Vertretung, Eskalation und Entscheidung treffen.

**Leitfrage: Welche organisatorische Lücke würde einen technisch beherrschbaren Vorfall bei uns unnötig vergrößern?**

FINANCE AUDIT

PRAXISFALL 2

# 72 Stunden ohne Strom in der Region

Sabotage an einem Umspannwerk – ein realistisches Szenario 2026

*Szenario, angelehnt an den Brandanschlag auf das Berliner Stromnetz vom 03.01.2026 und schon 7 echte ähnliche Fälle allein in Deutschland in diesem Jahr…. Und das dürfte erst der Anfang sein!*

# Die Region fällt aus – das Rechenzentrum läuft

FINANCE AUDIT

**Dienstag, 05:40 Uhr: Brandanschlag auf ein Umspannwerk und dessen Kabeltrasse in der Region des Instituts.**

- Rund 60.000 Haushalte und 3.000 Betriebe ohne Strom
- Netzbetreiber: Wiederversorgung frühestens in 3–4 Tagen
- Hauptstelle, 14 von 22 Geschäftsstellen und SB-Standorte betroffen
- Kernbankverfahren im Rechenzentrum des IT-Dienstleisters verfügbar – das Institut vor Ort trotzdem nur eingeschränkt handlungsfähig

**72 h+** ohne Netzstrom

**14 / 22** Geschäftsstellen ohne Strom

**TK** Festnetz und Mobilfunk brechen ein, lokale IKT-Dienstleister ebenso

**Realer Bezug:** Brandanschlag auf eine Kabelbrücke in Berlin-Lichterfelde am 03.01.2026 – rund 45.000 Haushalte und über 2.200 Betriebe teils bis zum 07.01.2026 ohne Strom; auch Festnetz und Mobilfunk waren betroffen.

Quellen: Stromnetz Berlin GmbH, Pressemitteilung vom 03.01.2026; Bundeszentrale für politische Bildung, 08.01.2026; Wikipedia „Brandanschlag auf das Berliner Stromnetz 2026“. Szenariowerte konstruiert.

# Dynamik der ersten Stunden

FINANCE AUDIT

**05:40** Stromausfall – Notstromaggregat der Hauptstelle startet, USV meist nicht mehr vorhanden, auch Photovoltaik rettet nur ggf.!

**06:15** Alarm- und Zutrittstechnik im Batteriebetrieb, Wachdienst meldet Störungen an mehreren Standorten

**07:30** Mitarbeitende erreichen die Hauptstelle nicht, Mobilfunk zunehmend gestört

**08:00** Geldautomaten und Kartenzahlung im Handel ausgefallen – Bargeldnachfrage steigt

**09:30** Bekennerschreiben im Internet, Staatsschutz ermittelt – Sorge vor Folgeanschlägen

**11:00** Netzbetreiber: Wiederversorgung erst in 72+ Stunden

## Autarkie-Uhr


**Kernaussage:** Nicht die IT fällt aus – die Region fällt insgesamt zu erheblichen Teilen aus, weil die meisten Unternehmen und Privatpersonen noch nicht verstanden haben, sich vorzubereiten. Und damit gleichzeitig Personal, Kommunikation, Bargeldversorgung und physische Sicherheit.

# Physische Ursache – trotzdem mehrere Melde- und Abstimmungspfade

FINANCE AUDIT

## DORA / BaFin – auch ohne Cyberangriff prüfen

- IKT-bezogener Vorfall, soweit die Verfügbarkeit von Netzwerk- und Informationssystemen beeinträchtigt ist (Art. 3 Nr. 8 DORA)
- Schwellen z. B. Dauer > 24 h, Ausfall > 2 h, > 10 % der Kunden (Art. 9 Abs. 1, 3 DelVO (EU) 2024/1772)
- Fristen: Art. 5 DelVO (EU) 2025/301

## Behörden und Krisenstäbe

- Polizei/Staatsschutz: Spurensicherung auch an eigenen Standorten
- Kommunaler Krisenstab und Netzbetreiber: das Institut ist Betroffener, nicht Steuernder
- KRITIS-Dachgesetz (BGBl. 2026 I Nr. 66): Betroffenheit gesondert prüfen

## Verbund, Versicherer, Kunden

- Bargeldlogistik, Verbund und IT-Dienstleister
- Sachversicherung (Betriebsunterbrechung): Obliegenheiten beachten
- Kundeninformation über Kanäle, die ohne Strom funktionieren

**Kernbotschaft 1:** Auch ohne Cyberangriff läuft die DORA-Uhr: Einstufung, Zeitstempel und Meldung müssen ohne stabilen Strom und Mobilfunk funktionieren.

**Kernbotschaft 2:** Diesel, Netzwiederversorgung und Einsatzkräfte werden nach Behördenlage priorisiert – nicht nach dem Notfallhandbuch des Instituts.

# Filialen öffnen – oder schützen?

FINANCE AUDIT

### Versorgung sichern

- Standorte mit Notstrom öffnen
- Bargeld auszahlen, sichtbar präsent sein
- Vertrauen in der Region erhalten

### Managemententscheidung ohne Systeme

Welche Standorte, welche Leistungen, wie lange – mit welchen Offline-Verfahren, Auszahlungsgrenzen und Legitimationsregeln?

### Sicherheit wahren

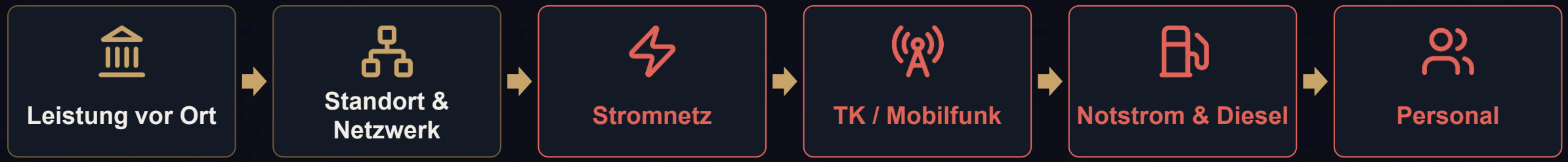
- Alarm- und Zutrittstechnik eingeschränkt
- Bargeldbestände ohne Überwachung
- Personal ohne verlässliche Kommunikation

**Kernbotschaft:** Wer ohne Systeme auszahlt, übernimmt Kredit-, Betrugs- und Identifizierungsrisiken. Das muss vorher entschieden und geübt werden – nicht in der Lage improvisiert.

***Offline-Verfahren entscheiden über die Handlungsfähigkeit – nicht das Rechenzentrum.***

# Die kritischste Abhängigkeit stand in keinem Register

FINANCE AUDIT




*außerhalb jeder Dienstleistersteuerung*

## Regulatorischer Anker

- Art. 26 Abs. 2 DelVO (EU) 2024/1774: weitverbreitete Stromausfälle und physische Angriffe inkl. Terroranschlägen sind Pflichtszenarien
- Art. 25 Abs. 2 DelVO: Tests müssen diese Szenarien abdecken

## Praxistipp

Nicht nur fragen: „Ist das Rechenzentrum georedundant?“

**sondern: „Was funktioniert bei uns vor Ort, wenn die Region 72 Stunden dunkel ist?“**

**Kernbotschaft:** Strom, Diesel und Mobilfunk stehen in keinem Informationsregister – und sind trotzdem Teil der kritischen Abhängigkeit.

**Leitfrage: Welche Leistung könnten wir in unserer Region 72 Stunden ohne Netzstrom noch erbringen?**

# Der Anschlag ist physisch – der Schaden entsteht so richtig erst organisatorisch

FINANCE AUDIT

**Einspeisung ohne Redundanz** → **Begrenzte Autarkie** → **Organisation ohne Strom** → **Handlungsfähigkeit?**

## Physisch / technisch

Einspeisung ohne Redundanz; Notstrom, USV und Telekommunikation nur für Stunden autark.

## Organisatorisch

Alarmierung setzt Mobilfunk voraus, Pläne unterstellen Personal, Offline-Verfahren sind nicht geübt, der Krisenstabsraum liegt im Ausfallgebiet.

## Managementfolge

Resilienz ist Autarkiezeit × Entscheidungsfähigkeit × Übung – nicht nur Redundanz im Rechenzentrum.

**Kernbotschaft:** Die Physik bestimmt die Dauer – die Organisation bestimmt den Schaden.

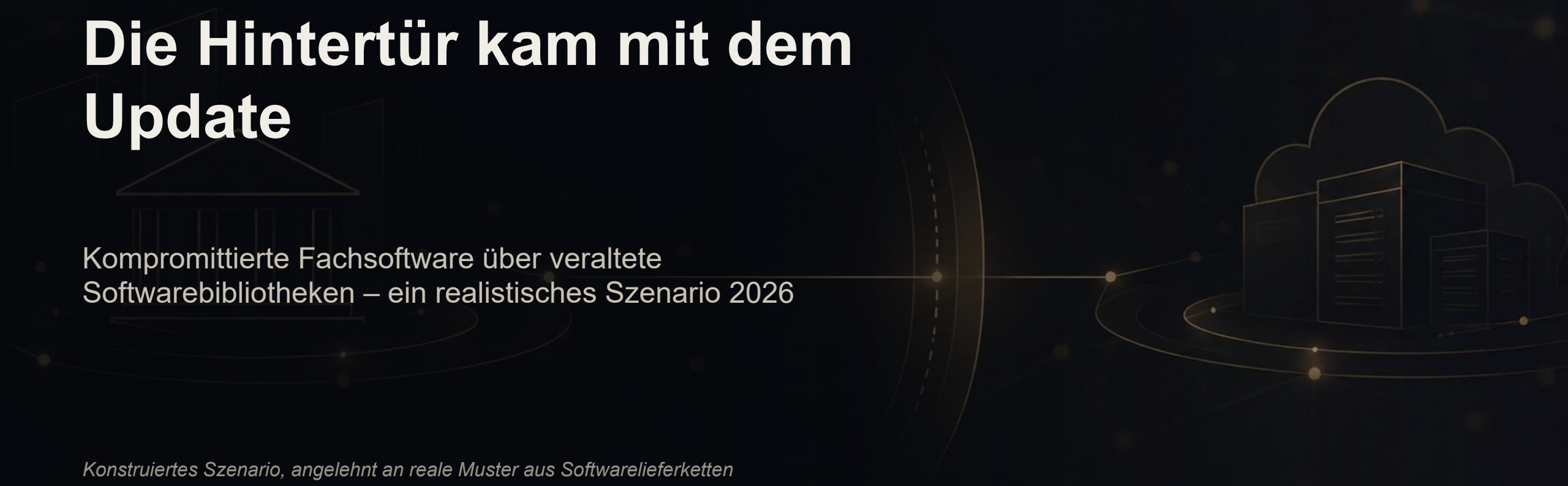
**Leitfrage: Wie viele Stunden sind wir an der Hauptstelle wirklich autark – bei Strom, Kommunikation, Personal und Bargeld?**

FINANCE AUDIT

PRAXISFALL 3

# Die Hintertür kam mit dem Update

Kompromittierte Fachsoftware über veraltete Softwarebibliotheken – ein realistisches Szenario 2026



*Konstruiertes Szenario, angelehnt an reale Muster aus Softwarelieferketten*

# Die Fachanwendung ist geprüft, zertifiziert – und kompromittiert

FINANCE AUDIT

**Ein Institut nutzt eine zugekaufte Fachanwendung eines spezialisierten Softwarehauses – mit Schnittstelle zum Kernbankverfahren.**

- Mehrere hundert Drittbibliotheken, einige seit Jahren ohne Pflege – teils als eigene „Forks“ mit nachgezogenen Korrekturen
- Über eine verwaiste Komponente gelangt eine Hintertür in das reguläre, signierte Update
- Die Hintertür ist seit rund 90 Tagen produktiv aktiv
- Keine Software-Stückliste (SBOM) beim Hersteller

**400+** Drittkomponenten in einem Release

**90 Tage** unentdeckt in Produktion

**~25** Institute mit derselben Version

**Reale Muster:** Log4Shell (CVE-2021-44228, 2021) – Schwachstelle in einer allgegenwärtigen Bibliothek; XZ Utils (CVE-2024-3094, 2024) – gezielt eingeschleuste Hintertür in einer Open-Source-Komponente.

Szenario konstruiert; kein Bezug zu einem konkreten Hersteller.

# Dynamik: Der Angriff beginnt am Tag der Auslieferung

FINANCE AUDIT

| | |
|---|---|
| **Tag −90** | Quartalsupdate mit manipulierter Komponente ausgeliefert – Signatur gültig, Tests grün |
| **06:50** | CERT-Warnung: aktiv ausgenutzte Hintertür in einer verbreiteten Open-Source-Komponente |
| **08:20** | Anfrage beim Hersteller „Sind wir betroffen?“ – Antwort: „Wir prüfen.“ Keine SBOM verfügbar |
| **10:45** | Eigene Logs: ausgehende Verbindungen des Anwendungsservers seit sechs Wochen |
| **12:30** | Hersteller bestätigt Betroffenheit aller Releases seit dem Quartalsupdate – Patch in 5–7 Werktagen |
| **14:00** | Technischer Account mit Schreibrechten zum Kernbankverfahren: Datenabfluss? Manipulation? |

**Kernaussage:** Die Frage „Seit wann?“ ist schwerer als „Was jetzt?“. Ohne Komponenten- und Build-Transparenz lässt sich weder der Beginn noch der Umfang belastbar bestimmen.

# Isolieren – oder weiterarbeiten?

FINANCE AUDIT

### Sicherheit erhöhen

- Anwendung und Schnittstelle trennen
- Technische Accounts neu vergeben
- Systeme forensisch sichern

### Managemententscheidung ohne „saubere“ Version

Notbetrieb manuell? Kompensierende Kontrollen mit Frist und Re-Test? Oder kontrollierter Weiterbetrieb bis zum Patch?

### Verfügbarkeit erhalten

- Antrags- und Kreditbearbeitung steht
- Patch erst in 5–7 Werktagen
- Vorversion enthält dieselbe Komponente

**Kernbotschaft:** „Zurück auf die letzte gute Version“ geht nur, wenn man weiß, welche Version gut ist – dafür braucht es Komponentenlisten, Build-Nachweise und Integritätskontrollen (Art. 16 Abs. 7 DelVO (EU) 2024/1774).

***Kompensierende Kontrollen sind eine befristete Risikoübernahme – keine Lösung.***

# Die gefährlichste Abhängigkeit stand in keinem Vertrag


## Regulatorischer Anker

- Drittbibliotheken nachverfolgen, Versionen überwachen (Art. 10 Abs. 2 lit. d DelVO (EU) 2024/1774)
- Quellcodeprüfung, Paket-Tests, Code-Integrität (Art. 16 Abs. 3, 4, 7 DelVO)
- Vertragliche Unterstützung bei IKT-Vorfällen (Art. 30 Abs. 2 lit. f DORA)

## Praxistipp

Nicht nur fragen: „Ist der Hersteller ISO-27001-zertifiziert?“

**sondern: „Welche Komponenten stecken in Version X – und wer pflegt sie?“**

**Kernbotschaft:** Zertifikate beschreiben den Hersteller – nicht die Komponenten in seinem Produkt.

**Leitfrage: Könnten wir binnen 24 Stunden sagen, ob eine betroffene Bibliothek in unserer Fachsoftware steckt?**

# Die Hintertür war technisch – dass sie 90 Tage blieb, war organisatorisch

FINANCE AUDIT

**Veraltete Komponente** → **Kein Gate im Build** → **Keine Erkennung** → **Handlungsfähigkeit?**

## Technisch

Komponenten ohne Herstellerpflege, Vorabversionen im Produktivpfad, ungeprüfter Bezug von Abhängigkeiten, weitreichender technischer Account.

## Organisatorisch

Freigaben im Code-Review optional, Forks ohne Überwachung, Testsysteme mit Produktivdaten – und eine Dienstleistersteuerung, die Zertifikate prüft statt Komponenten.

## Managementfolge

Transparenz über die Software-Lieferkette ist eine Einkaufs- und Steuerungsentscheidung – nicht nur eine IT-Aufgabe.

**Kernbotschaft:** Nicht die Schwachstelle macht die Krise – sondern dass niemand wusste, wo sie steckt und wer sie behebt.

**Leitfrage: Welche Fachanwendung würden wir heute nicht isolieren können, ohne dass kritische Prozesse stehen?**

# Drei Fälle – ein Muster

FINANCE AUDIT

| | Fall 1: Subdienstleister | Fall 2: Umspannwerk | Fall 3: Software-Lieferkette |
|---|---|---|---|
| **Auslöser** | Cyberangriff beim IKT-Subdienstleister | Sabotage an der Stromversorgung | Hintertür über veraltete Bibliothek im Update |
| **Verborgene Abhängigkeit** | Subdienstleister ohne Vertragsweg | Netz, Telekommunikation, Diesel, Personal | verwaiste Open-Source-Komponente |
| **Zielkonflikt** | Trennen vs. Verfügbarkeit | Öffnen vs. Sicherheit | Isolieren vs. Arbeitsfähigkeit |
| **Meldelogik** | DORA und DSGVO parallel | DORA trotz physischer Ursache | DORA, DSGVO – CRA beim Hersteller |
| **Lehre** | Handlungsfähigkeit vor Papierlage | Autarkie und Offline-Verfahren üben | Komponenten kennen, nicht nur Zertifikate |

**Kernbotschaft:** Drei verschiedene Auslöser – dasselbe Muster: Die kritische Abhängigkeit liegt außerhalb des Vertrags, und die Krise entsteht an der Nahtstelle von Technik, Organisation und Entscheidung.

# Die Fälle sind kein Einzelfall: Was eine DORA-Vor-Ort-Prüfung 2026 konkret feststellt

FINANCE AUDIT

| | | Fall 1 | Fall 2 | Fall 3 | Wirksam-keit |
|---|---|---|---|---|---|
| **Zugriffs- und Berechtigungsmanagement**<br>Servicekonten, Least Privilege, starke Authentifizierung | 🔥 | ● | | ○ | ○ |
| **Sicherheitsüberwachung und Vorfallmanagement**<br>SOC-Bereitschaft, SIEM, Playbooks, Übungen | | ● | ○ | ● | ○ |
| **Sichere Softwareentwicklung**<br>Dependencies, SAST/DAST, Threat Modelling | 🔥 | | | ● | ○ |
| **Schwachstellen- und Patchmanagement**<br>Scanabdeckung, Behebungsfristen, Herabstufungen | | ○ | | ● | ● |
| **Notfallmanagement und Datensicherung**<br>RTO, Notfallpläne, Szenariotests, Restore | | ○ | ● | ○ | ● |
| **Asset-, Architektur- und Datenmanagement**<br>Relationen, Kritikalität, Datenflüsse | | ○ | ● | ● | ○ |
| **Dienstleistersteuerung und physische Sicherheit**<br>Auditrechte, Dienstleistungsgüte, Zutritt | | ● | ● | ○ | |
| **Governance, Risikotoleranz und Reporting**<br>Umsetzungsprüfung, Ausnahmen, Schwellen, GF-Bericht | | ○ | ○ | ○ | ● |

● zahlt direkt ein ○ zahlt mittelbar ein 🔥 Schwerpunktfeststellung

### Lesart

Geprüft wurde ein IKT-Drittdienstleister. Der Maßstab DORA wirkt über die Vertragskette (Art. 28, 30 DORA) auf die Institute zurück.

### Muster

Selten fehlt die Regel. Es fehlen Umsetzungsprüfung, Nachweis und Nachverfolgung.

Quelle: Feststellungen einer aufsichtlichen DORA-Vor-Ort-Prüfung 2026 bei einem IKT-Drittdienstleister – anonymisiert und sinngemäß verdichtet. Maßstabszuordnung: Finance Audit.

# Fall 1 im Spiegel der Prüfung: Zugänge, Erkennung, Reaktion

FINANCE AUDIT

## Im Fall: Adminzugang und Backdoor

Schwerpunktfeststellung

**In der Prüfung festgestellt**

- Service- und Sammelkonten ohne inhaltlichen Review
- Least-Privilege-Prinzip auf zentralen Plattformen nicht eingehalten
- Zugriffe auf Passwörter von Sammelkennungen nicht nachvollziehbar
- Keine durchgängige starke Authentifizierung

**Maßstab:** Art. 9 Abs. 4 lit. c DORA; Art. 20, 21 DelVO (EU) 2024/1774

## Im Fall: Erkennung erst über den Dienstleister (07:30)

**In der Prüfung festgestellt**

- Keine durchgängige SOC-Bereitschaft
- Detektionsregeln automatisch deaktiviert – ohne Risikobewertung
- Sicherheitsrelevante Systeme nicht an das SIEM angebunden
- Alarmbearbeitung und False Positives nicht nachvollziehbar

**Maßstab:** Art. 10 DORA; Art. 23 DelVO (EU) 2024/1774

## Im Fall: Reaktion entlang der Dienstleisterkette

**In der Prüfung festgestellt**

- Incident-Response-Playbooks zu wenig detailliert
- Maßnahmen aus Übungen nicht nachverfolgt
- Dienstleistungsgüte und Auditrechte im RZ-Vertrag nicht verankert
- Vertragserfüllung nicht überprüft

**Maßstab:** Art. 17, Art. 30 Abs. 2, 3 DORA; Art. 22 DelVO (EU) 2024/1774; DelVO (EU) 2025/532

**Einordnung:** Genau die Zugänge, die im Ernstfall getrennt werden müssen, waren in der Prüfung nicht vollständig bekannt, berechtigt und überwacht.

Quelle: Feststellungen einer aufsichtlichen DORA-Vor-Ort-Prüfung 2026 bei einem IKT-Drittdienstleister – anonymisiert und sinngemäß verdichtet. Maßstabszuordnung: Finance Audit.

# Fall 2 im Spiegel der Prüfung: Wiederanlauf, Szenarien, Abhängigkeiten

FINANCE AUDIT

**Im Fall: 72 Stunden ohne Strom – welche Wiederanlaufziele?**

**In der Prüfung festgestellt**

- Wiederanlaufzeiten (RTO) unvollständig erfasst
- Asset-Abhängigkeiten bei der RTO-Definition nicht berücksichtigt
- Sicherungsanforderungen der Dateneigentümer fehlen
- Wiederherstellungstests teils unzureichend

**Maßstab:** Art. 11 Abs. 5, Art. 12 DORA; Art. 24 DelVO (EU) 2024/1774

**Im Fall: Szenario „weitverbreiteter Stromausfall“**

**In der Prüfung festgestellt**

- Notfallpläne fehlen teilweise
- Handlungsanweisungen für den Wiederanlauf nicht detailliert genug
- DORA-relevante Szenarien weder geplant noch getestet
- Risiken aus nicht getesteten Szenarien nicht bewertet

**Maßstab:** Art. 11 Abs. 3, 4, 6 DORA; Art. 25, 26 DelVO (EU) 2024/1774

**Im Fall: Wovon hängen Standort und Leistung ab?**

**In der Prüfung festgestellt**

- Asset-Register ohne Relationen, Attribute und Kritikalität
- Keine Richtlinie mit Sicherheitsanforderungen für Rechenzentren
- Zutritte Externer nicht durchgängig nachvollziehbar
- Kapazitätsüberwachung unzureichend

**Maßstab:** Art. 8 DORA; Art. 4, 5, 9, 18 DelVO (EU) 2024/1774

**Einordnung:** Wer DORA-Szenarien nicht testet und Abhängigkeiten nicht im Asset-Register abbildet, entdeckt die Lücken aus Fall 2 erst im Dunkeln.

Quelle: Feststellungen einer aufsichtlichen DORA-Vor-Ort-Prüfung 2026 bei einem IKT-Drittdienstleister – anonymisiert und sinngemäß verdichtet. Maßstabszuordnung: Finance Audit.

# Fall 3 im Spiegel der Prüfung: Code, Komponenten, Behebung

FINANCE AUDIT

**Im Fall: Veraltete Bibliothek im Release**

Schwerpunktfeststellung

**In der Prüfung festgestellt**

- Produktivsetzungen trotz einer Vielzahl kritischer Dependency-Schwachstellen
- Dependency-Checks unzureichend
- Keine automatisierten Sicherheitstests (SAST/DAST)

**Maßstab:** Art. 25 Abs. 1 DORA; Art. 10 Abs. 2 lit. d, Art. 16 Abs. 2–4 DelVO (EU) 2024/1774

**Im Fall: Manipulation bleibt unbemerkt**

**In der Prüfung festgestellt**

- Unabhängige Sicherheitsfunktion nicht eingebunden
- Threat Modelling lückenhaft
- Vier-Augen-Prinzip in systemnaher Entwicklung unzureichend
- Lokale Administrationsrechte für Entwickler

**Maßstab:** Art. 16 Abs. 1, 7, Art. 21 DelVO (EU) 2024/1774

**Im Fall: Patch erst in 5–7 Werktagen**

**In der Prüfung festgestellt**

- Keine verbindlichen Behebungsfristen
- Herabstufung von Kritikalitäten nicht nachvollziehbar
- Pentest-Befunde nicht versions- und mandantenübergreifend verfolgt
- Kunden-Reporting zu Schwachstellen unzureichend

**Maßstab:** Art. 9 Abs. 4 lit. f, Art. 24 Abs. 5 DORA; Art. 10 Abs. 2 DelVO (EU) 2024/1774

**Einordnung:** Die Prüfung ist schärfer als das Szenario: Produktivsetzung trotz bekannter kritischer Schwachstellen in Drittkomponenten – die Hintertür muss nicht einmal eingeschleust werden.

Quelle: Feststellungen einer aufsichtlichen DORA-Vor-Ort-Prüfung 2026 bei einem IKT-Drittdienstleister – anonymisiert und sinngemäß verdichtet. Maßstabszuordnung: Finance Audit.

FINANCE AUDIT

TEIL C

# Von Vollständigkeit zu Wirksamkeit

Regulatorik 2026, eine Steuerungslogik, Evidenzkette und die sechs Prüffelder

# 2025 war der Ausgangspunkt – 2026/2027 steht Wirksamkeit im Fokus

FINANCE AUDIT

**Kernbotschaft:** 2025 wurde die DORA-Grundlogik weitgehend implementiert. 2026/2027 verlagert sich die Diskussion auf Wirksamkeit – danach auf Effektivität, Effizienz und Automatisierung.

## 2025: Verständnis und Basis schaffen

- Rollen
- Regelwerk
- Kontrollen

## 2026/2027: Wirksamkeit nachweisen

- Prüfpfad
- Nachweis
- Re-Test

**17.01.2025**
DORA anwendbar (Art. 64 DORA)

**30.06.2026**
MaRisk-Novelle, RS 06/2026 (BA)

**01.01.2027**
Umsetzungsfrist der MaRisk-Novelle endet

***Entscheidend ist nicht, ob etwas geregelt ist – sondern ob es im kritischen Moment funktioniert.***

**Leitfrage: Erfüllen wir DORA formal – oder materiell?**

# Vollständigkeit 2025 – Wirksamkeit 2026

FINANCE AUDIT

**Kernbotschaft:** Eine dokumentierte Kontrolle ist erst steuerungsrelevant, wenn Wirkung, Ausnahmen, Maßnahmen und deren Umsetzung nachvollziehbar sind.

**Soll 2025**

- ☑ Richtlinie
- ☑ Rolle
- ☑ Kontrolle

**Ist 2026**

- ? Wirkung belegt?
- ? Ausnahme entschieden?
- ? Re-Test erfolgt?

- 2025: Fokus auf Vollständigkeit von Regelwerk, Rollen und Kontrolllandschaft.
- 2026: Fokus auf die Wirkung von Sicherheitsmaßnahmen und kritischen Kontrollen – inklusive dokumentierter Ausnahmen, Fristen, Verantwortung und Re-Test.
- Risikorelevant wird eine Schwachstelle besonders dort, wo Restrisiko oder Gegenmaßnahmen nicht überzeugend nachgewiesen werden können.

**Leitfrage: Welche Basis erwarten wir bei einer fortbestehenden Schwachstelle, damit die Risikoübernahme verantwortbar ist?**

# Was die Prüfung bemängelt, liegt fast immer zwischen Regel und Nachweis

FINANCE AUDIT

| Regel | Umsetzungs-prüfung | Ausnahme | Risikotoleranz | Reporting | Wirksamkeit |
|---|---|---|---|---|---|
| • Reifegrad der Richtlinien unzureichend<br>• Mindestvorgaben fehlen (z. B. Konfiguration) | • Vorgaben ohne Umsetzungs-prüfung<br>• Doku weicht von Technik ab | • Kein dokumentierter Ausnahmeprozess<br>• Ausnahmen pauschal für alle Geräte | • Keine Toleranz-schwellen für IKT-Risiken<br>• Bewertung nicht nachvollziehbar | • Sicherheitslage unzureichend an GF berichtet<br>• Keine Kennzahlen zur Steuerung | • Wirkung von Schulungen nicht überprüft<br>• Unabhängige Kontrolle kaum eingebunden |

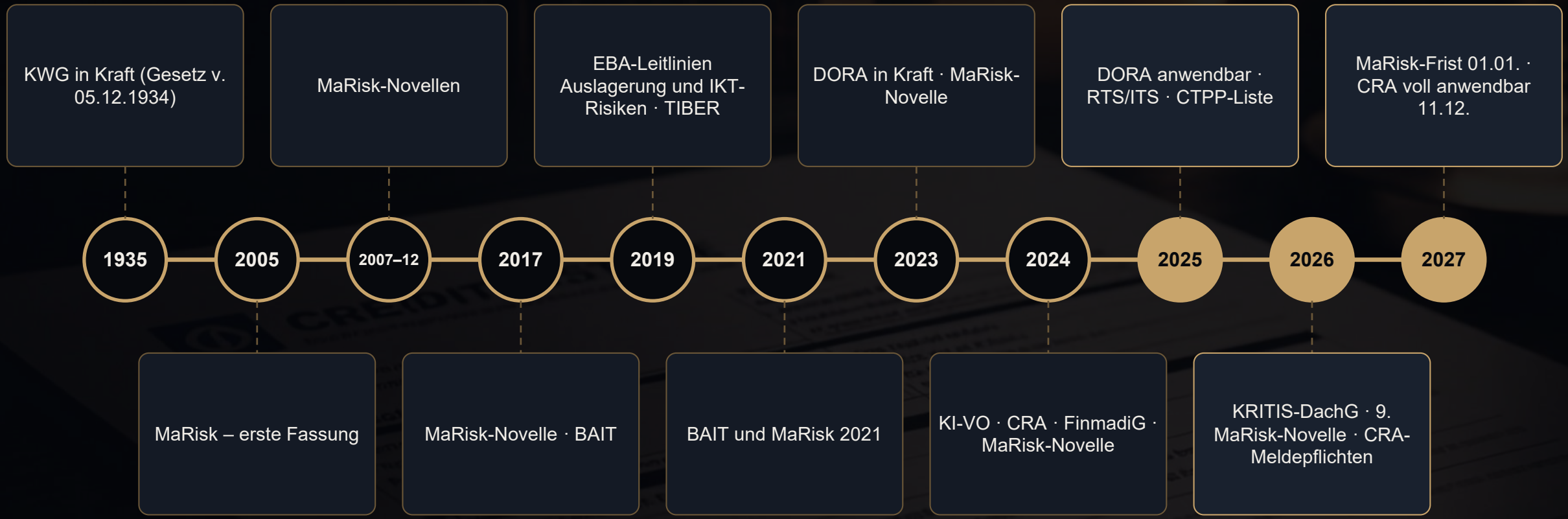
**Kernbotschaft:** Die Aufsicht misst nicht, ob es eine Richtlinie gibt – sondern ob Umsetzung, Ausnahme, Risikoentscheidung und Nachweis zusammenpassen.

**Praxis für den Maßnahmenplan**

Erledigt erst mit dokumentiertem Kontrolldurchlauf – nicht schon mit der Umsetzung.

Quelle: Feststellungen einer aufsichtlichen DORA-Vor-Ort-Prüfung 2026 bei einem IKT-Drittdienstleister – anonymisiert und sinngemäß verdichtet. Maßstabszuordnung: Finance Audit. Maßstab u. a. Art. 5, 6 DORA; Art. 2, 3 DelVO (EU) 2024/1774.

# Chronologie der IKT-Regulatorik




KWG: Reichsgesetz über das Kreditwesen v. 05.12.1934, in Kraft 01.01.1935; Neufassung v. 10.07.1961. KRITIS-DachG v. 11.03.2026 (BGBl. 2026 I Nr. 66). MaRisk RS 06/2026 (BA) v. 30.06.2026. CRA: VO (EU) 2024/2847.

# Ein Rahmen, drei Ebenen – was bedeutet das für den Vorstand?

FINANCE AUDIT

### EU-Rahmen: DORA

Unmittelbar geltende Pflichten; das Leitungsorgan trägt die Verantwortung für den IKT-Risikomanagementrahmen (Art. 5 Abs. 2 DORA).

### Konkretisierung: RTS / ITS

Die Details sind prüfungsrelevant: Schwellen, Fristen, Vertragsinhalte, Testmethodik. „DORA umgesetzt“ allein reicht nicht.

### National: KWG, MaRisk, FinmadiG

BaFin ist zuständige Behörde. MaRisk bleibt Rahmen der Gesamtsteuerung – Doppelungen vermeiden.

### Zentrale Rechtsakte

- DelVO (EU) 2024/1772 – Klassifizierung
- DelVO (EU) 2024/1774 – IKT-Risikomanagement
- DelVO (EU) 2025/301 – Meldeinhalte und -fristen
- DelVO (EU) 2025/532 – Unterauftragsvergabe
- DelVO (EU) 2025/1190 – TLPT
- KI-VO (EU) 2024/1689 · CRA (EU) 2024/2847
- FinmadiG (BGBl. 2024 I Nr. 438): u. a. § 1a Abs. 2 KWG
- MaRisk RS 06/2026 (BA)

**Kernbotschaft:** DORA liefert den unmittelbar geltenden EU-Rahmen, RTS/ITS konkretisieren ihn – KI-VO, CRA, FinmadiG, KWG und MaRisk kommen hinzu.

# DORA, KWG, MaRisk & mehr: Eine Steuerungslogik statt drei Silos

FINANCE AUDIT

**Kernbotschaft:** DORA und bankaufsichtliche Gesamtsteuerung dürfen nicht in getrennten Nachweiswelten laufen – entscheidend ist ein konsistentes Managementbild.


## Konkret

- DORA: Resilienz, IKT-Risikomanagement, Tests, Vorfälle, IKT-Drittparteien
- KWG/MaRisk: Governance, Risikosteuerung, Gesamtverantwortung
- Für das Leitungsorgan zählt ein Bild aus KPI, Risiken, Kontrollen, Maßnahmen und Eskalationen
- BAIT nur noch historische und technische Orientierung

**Leitfrage: Wo erzeugen wir doppelte Nachweise – und wie schaffen wir ein gemeinsames, wirksames Steuerungsbild?**

# Konzentrationsrisiko steuern

**Kernbotschaft:** Die CTPP-Aufsicht erhöht die Transparenz über zentrale IKT-Anbieter. Die eigene Handlungsfähigkeit bleibt in der Verantwortung des Instituts.

## Konkret heißt das

- ESAs haben am 18.11.2025 die erste Liste mit 19 CTPP veröffentlicht (Art. 31 Abs. 9 DORA), u. a. Accenture, AWS, Microsoft, NTT DATA
- National rücken zentrale IKT-Dienstleister in den Fokus
- Ein Vertrag oder die Aufsicht über den Anbieter ersetzt nicht den Nachweis der eigenen Krisenfähigkeit


- **Kritikalität**
- **Substituierbarkeit**
- **Konzentration**
- **Krisenfähigkeit**

**Leitfrage: Bei welcher kritischen Abhängigkeit wäre unsere Handlungsfähigkeit am schwersten aufrecht zu erhalten?**

# Nicht mehr Dokumente schaffen Vertrauen – sondern eine praxistaugliche Evidenzkette

FINANCE AUDIT

**Kernbotschaft:** Prüfungs- und Berichtsfähigkeit entsteht durch einen nachvollziehbaren Zusammenhang von Risiko, Kennzahl, Test, Feststellung, Maßnahme und Re-Test.


**Management-Reporting und Prüfung: Brüche und offene Ausnahmen werden sichtbar**

- Einzelne Dokumente sind kein Wirksamkeitsnachweis – entscheidend ist die Konsistenz von Steuerungsinformation, Testresultat und Maßnahmenstatus, auch themenübergreifend.
- Bei roten Kennzahlen oder wesentlichen Feststellungen müssen Ursache, Restrisiko, Entscheidung, Frist, Verantwortliche und erneute Überprüfung nachvollziehbar sein.
- Die Evidenzkette stärkt Berichtsfähigkeit und Prüfungssicherheit – vor allem aber effektives Handeln in der Praxis.

**Leitfrage: Welche Evidenzen wollen wir – wann, von wem und warum?**

# TOP-IKT-Risiken: Szenarien priorisieren, nicht Schlagworte sammeln

FINANCE AUDIT

**Kernbotschaft:** Priorisieren Sie Risiken danach, ob sie mehrere kritische Prozesse gleichzeitig treffen – und ob Entscheidungen und Evidenzen dafür vorbereitet sind.


## Diskussionsrahmen

- Kategorien: Infrastruktur- und Versorgungsstörungen, Social Hacking, Lieferkettenrisiken, hybride Bedrohungslagen, schwer steuerbare Software-Abhängigkeiten
- Ziel: Debatte über Mehrfachbelastung kritischer Prozesse, Entscheidungsfähigkeit und fehlende Evidenz
- Die Einordnung ist institutsindividuell vorzunehmen

**Leitfrage: Welches Szenario könnte mehrere kritische Prozesse gleichzeitig belasten – und welche Evidenz oder Entscheidung fehlt dafür?**

# DORA-Prüfungen: Wirksamkeit in sechs Feldern

FINANCE AUDIT

Nicht die Papierlage ist entscheidend, sondern eine nachweisbar wirksame Steuerung.


**In allen sechs Feldern zählen: klare Verantwortlichkeit · belastbare Evidenz · nachvollziehbare Reaktion auf Abweichungen**

**Leitfrage: In welchem der sechs Felder wäre Wirksamkeit für uns am schwersten durchgängig nachzuweisen?**

# Governance, KPI und Risikotoleranzschwellen müssen Entscheidungen auslösen

FINANCE AUDIT

**Kernbotschaft:** Kennzahlen, Rollen und Schwellen schaffen nur dann Steuerung, wenn sie zu Risikoakzeptanz oder Maßnahmen führen.

## ROLLEN

- 1st / 2nd Line
- Leitungsorgan

## KPI / KRI


## ENTSCHEIDUNGSBAUM


KPI und KRI sollen Trends und Schwellen sichtbar machen – nicht nur Berichte erzeugen.

Risikotoleranz braucht klare Schwellen, dokumentierte Entscheidungsrechte und belastbare Eskalationswege.

Bei roten Kennzahlen müssen Ursache, Restrisiko, Entscheidung, Verantwortlichkeit, Frist und Re-Test nachvollziehbar sein.

**Leitfrage: Welche Kennzahl muss zwingend eine Entscheidung oder Eskalation auslösen – ohne echten Steuerungsimpuls ist jede Kennzahl nur “Bullshit”?**

# Asset- und Architekturtransparenz entscheidet über Steuerbarkeit

FINANCE AUDIT

**Kernbotschaft:** Wer kritische Funktionen nicht bis zu Prozess, Asset und Anbieter nachvollziehen kann, kann Abhängigkeiten, Auswirkungen und Krisenoptionen nur eingeschränkt steuern.

**Kritische Funktion** → **Geschäftsprozess** → **IKT-Asset / Applikation** → **Anbieter / Unterauftragnehmer**

*Welche Funktion?* — *Welcher Prozess?* — *Welches Asset?* — *Welcher Anbieter?*

Was wie lästige Fleißarbeit wirkt, kann – richtig gemacht – die entscheidende Hilfe im Notfall sein.

Verknüpfungen zeigen, welche kritischen Prozesse durch ein Asset oder einen Anbieter gleichzeitig betroffen wären.

Transparenz ist kein Inventar-Selbstzweck: Sie ermöglicht Impact-Analyse und handlungsfähige Entscheidungen.

**Leitfrage: Können wir für eine kritische Funktion in kurzer Zeit nachvollziehen, welche Prozesse, Assets und Anbieter gleichzeitig betroffen sind?**

# Schutzbedarf und Bedrohung bestimmen die Kontrollintensität

FINANCE AUDIT

**Kernbotschaft:** Kontrollen müssen am Schutzbedarf und an der Bedrohungslage ausgerichtet sein – ein einheitlicher Kontrollkatalog mit „Alibifunktion“ reicht nicht aus.


- Die entscheidende Frage ist, ob Kontrollen risikoadäquat sind – nicht, ob eine technische Maßnahmenliste vollständig ist.
- Bedrohungsbild und Schutzbedarf bestimmen Tiefe, Häufigkeit und Nachweis von Kontrollen.
- Schutzbedarf macht sichtbar, welche Dimension bei einer Funktion besonders kritisch ist.

FINANCE AUDIT

TEIL D

# KI als Beschleuniger

Geschwindigkeit, Glaubwürdigkeit und Skalierung – und wo KI die DORA-Umsetzung stärkt

# KI verändert Geschwindigkeit, Glaubwürdigkeit und Skalierung von Angriffen

FINANCE AUDIT

**Kernbotschaft:** KI verstärkt vor allem bekannte Cyberrisiken. Neu ist weniger die Angriffskategorie als die Geschwindigkeit, Qualität und Skalierbarkeit, mit der Angriffe vorbereitet und durchgeführt werden.

## Geschwindigkeit

Analyse, Angriffsvorbereitung und Anpassung werden schneller.

## Glaubwürdigkeit

Social Engineering wird sprachlich, visuell und akustisch überzeugender.

## Skalierung

Angriffe und Varianten lassen sich mit geringerem Aufwand breiter ausrollen.

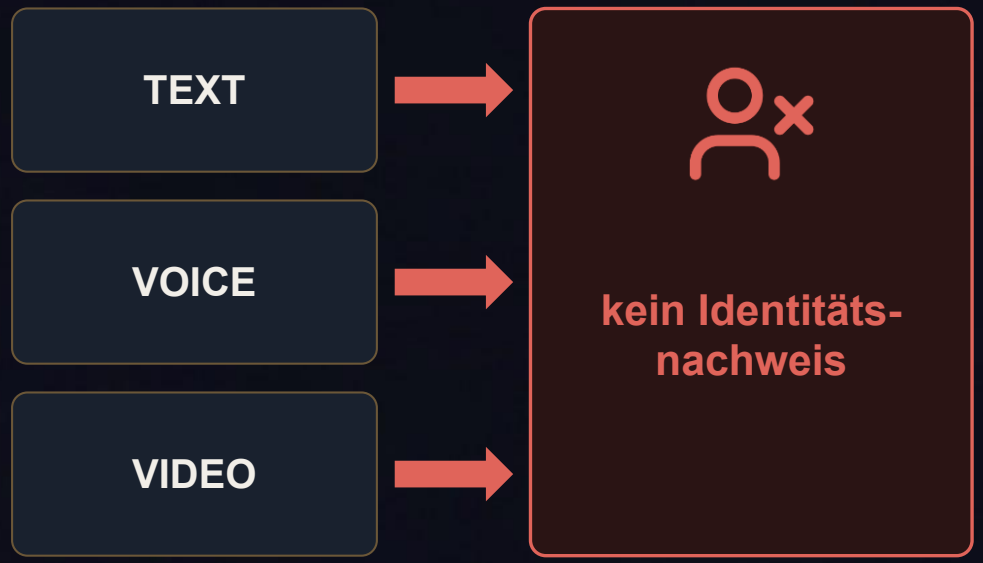
**Operativer Handlungsdruck: nicht nur „Haben wir Kontrollen?“ – sondern „Sind sie schnell genug?“**

**Leitfrage: Welche unserer heutigen Reaktionszeiten wären unter KI-beschleunigter Angriffsdynamik zu langsam?**

# Wenn Stimme und Bild des Vorstands kein Identitätsbeweis mehr sind

FINANCE AUDIT

**Kernbotschaft:** Generative KI und Deepfakes schwächen vertraute Identitätssignale. Für kritische Freigaben muss Identität prozessual und über einen unabhängigen zweiten Kanal abgesichert werden.




**Bekannte Führungsperson → 2. Kanal | definierter Freigabeprozess**

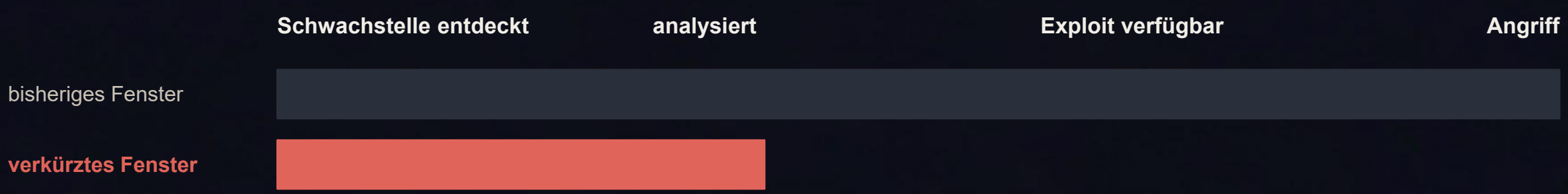
- Stimme, Bild und korrekt formulierte Nachricht können glaubwürdig manipuliert werden.
- Spear-Phishing, Vishing und CEO-Fraud gewinnen an Qualität und Personalisierung.
- Kritische Anweisungen brauchen unabhängige Verifikation – Vertrauen allein reicht nicht.

**Leitfrage:** **Bei welcher kritischen Handlung brauchen wir zwingend einen zweiten, unabhängigen Bestätigungskanal?**

# Die Zeit zwischen Schwachstelle und Ausnutzung schrumpft

FINANCE AUDIT

**Kernbotschaft:** Wenn KI Schwachstellen schneller findet und Exploits schneller erzeugt, wird Patch-Governance von einer technischen Routine zu einer Frage von Reaktionskapazität, Priorisierung und Risikotoleranz.




## Priorisieren

Exponierte Systeme, Drittsoftware und Open Source zuerst.

## Kapazität

Patch und Change für mehr Frequenz und Volumen auslegen.

## Ausnahmen

Risikoentscheidung, Kompensation, Frist und Re-Test.

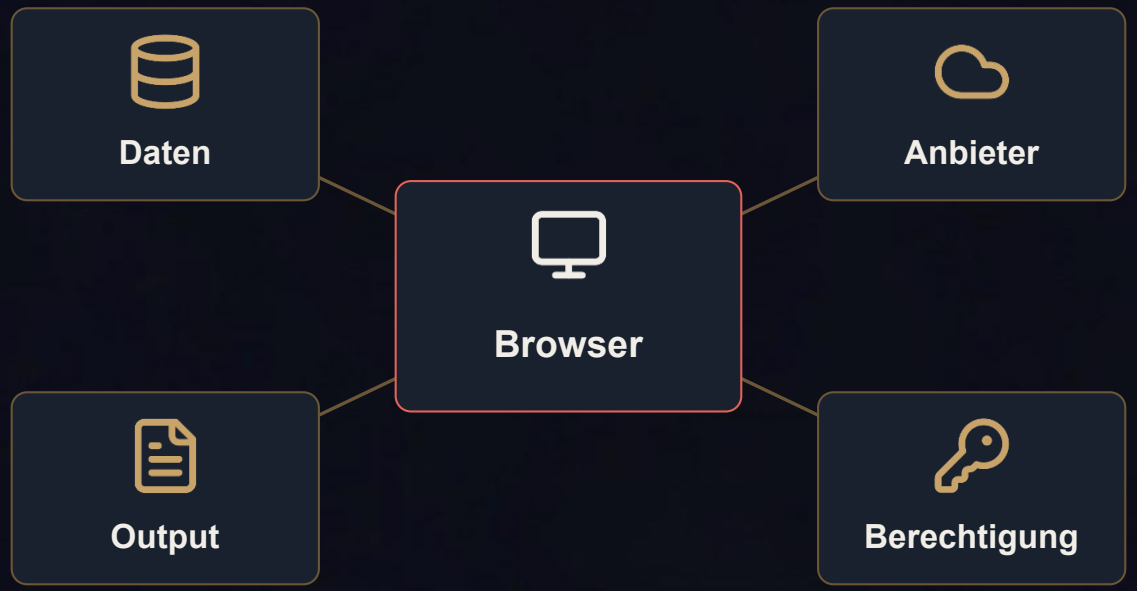
**Managementhebel: Priorisierung · Kompetenz der Mitarbeitenden · Provider-SLA · Bezug Praxisfall 3**

**Leitfrage: Sind Patch-, Change- und Provider-Zeiten auf ein deutlich kürzeres Ausnutzungsfenster ausgelegt – und sind unsere Mitarbeitenden dafür fit?**

# Schatten-KI kann bereits im Browser der Mitarbeitenden liegen

FINANCE AUDIT

**Kernbotschaft:** Webbasierte GenAI-Dienste funktionieren ohne Installation. Das Risiko entsteht aus Daten, Anbieterwahl, Berechtigungen und unkontrollierter Nutzung.




**Governance-Rahmen: freigegeben · geregelt · überwacht**

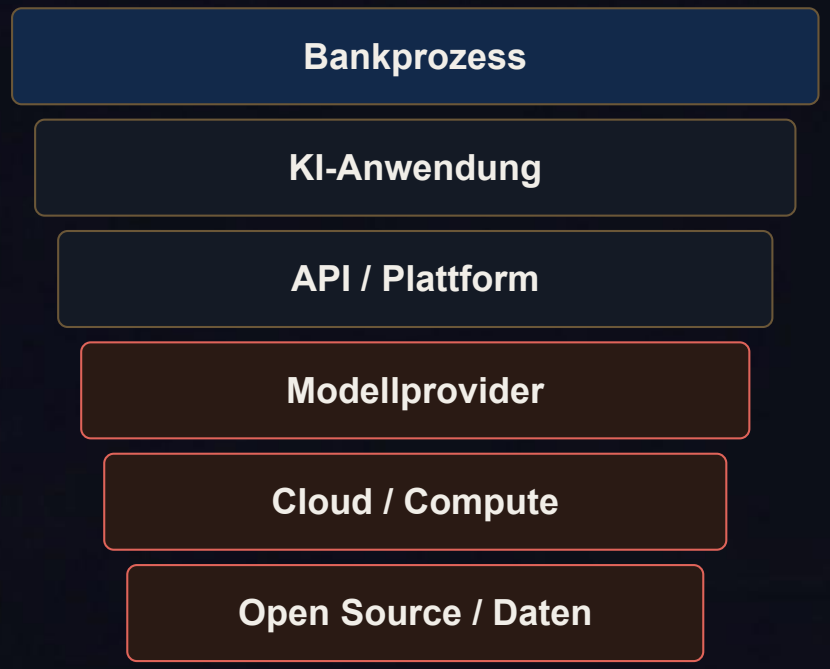
- Nicht freigegebene KI-Nutzung kann vertrauliche Daten in externe Verarbeitungswege bringen.
- Unklare Anbieter-, Speicher- und Modellabhängigkeiten erschweren Steuerung und Nachweis.
- Freigegebene Werkzeuge, klare Nutzungsregeln, Datenklassifikation und Awareness schaffen einen steuerbaren Rahmen.

**Leitfrage: Wie erkennen und steuern wir nicht freigegebene KI-Nutzung, bevor sensible Daten oder kritische Entscheidungen betroffen sind?**

# AI Supply Chains schaffen neue Konzentrationsrisiken

FINANCE AUDIT

**Kernbotschaft:** KI-Funktionalität hängt oft von mehreren externen Ebenen ab – Cloud, Modell, API, Daten- und Softwarekomponenten. Dadurch entstehen neue indirekte Abhängigkeiten.




**Prüffragen**

- **Kritikalität**
- **Konzentration**
- **Substituierbarkeit**
- **Krisenfähigkeit**

- Eine KI-Anwendung ist oft nur die sichtbare Oberfläche einer mehrstufigen Lieferkette.
- Für kritische Nutzung zählen Substituierbarkeit, Subdienstleister, Patch-Bereitschaft und Ausfallfolgen.
- Die DORA-Verantwortung für IKT-Drittparteien bleibt beim Institut.
- Und auch hier: Vieles konzentriert sich auf wenige, meist nicht europäische Anbieter.

**Leitfrage: Welche KI- oder IKT-Abhängigkeit könnte mehrere kritische Prozesse gleichzeitig treffen, obwohl wir keinen direkten Steuerungsweg zum eigentlichen Anbieter haben?**

# Chance 1: KI-gestützte Codeprüfung in Entwicklung und Änderungsprozess

FINANCE AUDIT

**Kernbotschaft:** KI kann Prüftiefe und Abdeckung im Code- und Change-Prozess erhöhen. Freigabeentscheidung und Verantwortung für sichere Entwicklung bleiben beim Institut.


## Chancen

- Abdeckung: Vorprüfung jeder Änderung statt Stichprobe – auch bei hoher Change-Frequenz.
- Altsysteme und Open Source: Auffälligkeiten in übernommenem Code werden früher sichtbar.
- Entlastung: Standardbefunde vorsortiert – Fachkapazität geht an die kritischen Stellen.

## Regulatorische Leitplanken

- Kein Deployment allein auf KI-Votum – Quellcodeintegrität, Tests und Testdaten bleiben geregelt.
- Alt-IT bleibt eigenständig zu bewerten; die KI-Prüfung ersetzt diese Bewertung nicht.
- Ein externer KI-Dienst im Entwicklungsprozess ist IKT-Dienstleistung: Vertrag, Risikoanalyse, Register.

**Praxisbezug:** Fall 3 und Prüfungspraxis – Produktivsetzung trotz kritischer Dependency-Schwachstellen, keine automatisierten Sicherheitstests.

**Leitfrage: Wo lassen wir KI-gestützte Codeprüfung zu – und wo bleibt die Freigabe zwingend menschlich?**

Maßstab: Art. 8 Abs. 3 und 7, Art. 28 ff. DORA; Art. 16 DelVO (EU) 2024/1774; Art. 4 KI-VO (EU) 2024/1689.

# Chance 2: KI in Erkennung und Abwehr – schneller sehen, schneller priorisieren

FINANCE AUDIT

**Kernbotschaft:** Dieselbe Technologie, die Angriffe beschleunigt, verkürzt auch die Zeit bis zur Erkennung. Der Anspruch an Schwellenwerte, Tests und Nachweis bleibt unberührt.


## Chancen

- Anomalien in großen Log- und Netzdatenmengen werden früher und mit weniger Vorwissen erkennbar.
- Korrelation und Priorisierung senken Fehlalarme und verkürzen die Triage bis zur Entscheidung.
- Vorfilterung stützt die Erkennung außerhalb der Geschäftszeiten – der wunde Punkt vieler Häuser.

## Regulatorische Leitplanken

- Erkennungsmechanismen sind regelmäßig zu testen – auch das KI-gestützte Verfahren.
- Kontrollebenen, Alarmschwellen und -kriterien bleiben festzulegen und zu dokumentieren.
- Ausreichende Ressourcen zur Überwachung bleiben vorzuhalten – KI ersetzt keine Personalausstattung.

**Praxisbezug:** Fall 1 und Prüfungspraxis – Erstinformation erst über den Dienstleister, keine durchgängige SOC-Bereitschaft, deaktivierte Regeln.

**Leitfrage: Welchen Nachweis verlangen wir, dass eine KI-gestützte Erkennung tatsächlich wirkt – und wer testet sie?**

Maßstab: Art. 10 Abs. 1–3, Art. 25 DORA; Art. 23 DelVO (EU) 2024/1774.

# Chance 3: KI in Dokumentation und Nachweisführung der DORA-Umsetzung

FINANCE AUDIT

**Kernbotschaft:** Ein erheblicher Teil des DORA-Aufwands ist Dokumentations- und Konsistenzarbeit. Dort ist der Entlastungseffekt am größten – solange Prüfung und Freigabe beim Institut bleiben.

**Inventare, Verträge, Richtlinien** → **KI-Entwurf und Konsistenzabgleich** → **Fachliche Prüfung** → **Freigabe und Prüfspur**

## Chancen

- Entwürfe und Aktualisierungen von Richtlinien, Verfahren und Berichten entstehen schneller.
- Brüche zwischen Asset-Inventar, Prozesslandkarte, Vertragsdaten und Register werden früher sichtbar.
- Gap-Abgleiche gegen die RTS-Anforderungen werden wiederholbar statt einmalig.

## Regulatorische Leitplanken

- Die Letztverantwortung des Leitungsorgans für den IKT-Risikomanagementrahmen bleibt unteilbar.
- Die jährliche Überprüfung des Rahmens und der Bericht darüber bleiben eigenständige Pflicht.
- Bankgeheimnis und personenbezogene Daten nur in freigegebenen Verarbeitungswegen.

**Praxisbezug:** Prüfungspraxis – Asset-Register ohne Relationen, Dokumentation weicht von der technischen Umsetzung ab.

**Leitfrage: Welche Dokumentation dürfte KI entwerfen – und wer verantwortet sie gegenüber Prüfern und Aufsicht?**

Maßstab: Art. 5 Abs. 2, Art. 6 Abs. 5, Art. 8 Abs. 1, 4–6, Art. 28 Abs. 3 DORA; Art. 28, 32 DSGVO.

FINANCE
AUDIT

# Vielen Dank.


## Prof. Dr. Ralf Kühn

Geschäftsführer · Finance Audit GmbH

Wirtschaftsprüfungsgesellschaft · Steuerberatungsgesellschaft

Wirtschaftsprüfer / CPA / Steuerberater

ralf.kuehn@finance-audit.de · Tel. 0157 56556673


**Qualifikationen & Kernkompetenzen**

CISA · CIA · Datenschutzbeauftragter und -auditor ·
Externe Beauftragtenfunktionen Datenschutz, Informationssicherheit in mehreren Banken, Sparkassen, Versicherungen und Instituten

www.finance-audit.de