DORA in der Praxis

Praxiserfahrungen, Prüfungsimplikationen und Handlungsfelder für die Finanzbranche

Prof. Dr. Aykut Bußian
Felix Kramer
Matthias Oßmann

Ihre Referenten heute

Prof. Dr. Aykut Bußian

Partner, Wirtschaftsprüfer
Financial Services IT & Controls Assurance
Tel. 0152-0186 8 197
aykut.bussian@bdo.de

Felix Kramer

Partner
IT & Controls Assurance
Tel. 089 76906-232
felix.kramer@bdo.de

Matthias Oßmann

Partner
Financial Services
Tel. 069 95941-386
matthias.ossmann@bdo.de

Agenda

01 IDW EPS 528 & DORA

02 Operational Resilience

03 Incident Reporting

04 Outsourcing

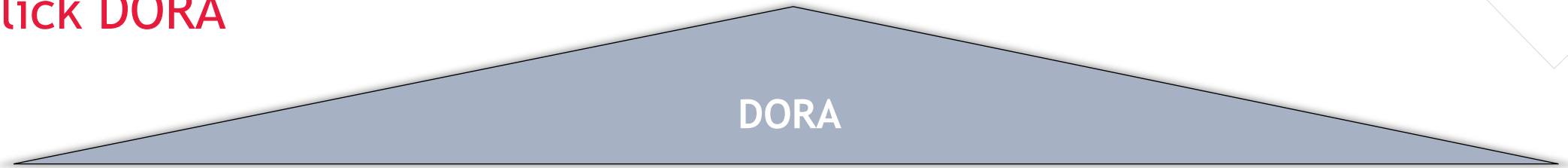
05 Testing

DORA in der Praxis

Praxiserfahrungen,
Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

EPS 528 & DORA

Überblick DORA



	IKT Risiko-management Artikel 5-16	Meldung von IKT-Vorfällen Artikel 17-23	Resilienztests Artikel 24-27	Drittparteienrisiko Artikel 28-44	Informations-austausch Artikel 45	Überwachungs-rahmen Artikel 46-64
Level 1						
Level 2 & Level 3	▸ RTS zur Festlegung des IKT-Risiko-managementrahmens ▸ Richtlinien zur Schätzung der aggregierten Kosten/Verluste, die durch größere IKT-bezogene Vorfälle verursacht werden	▸ RTS zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen ▸ RTS zur Spezifizierung der Meldung schwer-wiegender IKT-bezogener Vorfälle ▸ ITS zur Festlegung der Einzelheiten der Bericht-erstattung über größere IKT-bezogene Vorfälle	▸ RTS für Tests, die sich an realen Bedrohungen orientieren	▸ RTS zur Spezifizierung der Leitlinie für vertragliche Vereinbarungen mit IKT-Dienstleistern ▸ RTS zur Festlegung der Aspekte, die bei der Vergabe von Unteraufträgen für kritische IKT-Dienstleistungen zu bestimmen und bewerten sind ▸ ITS für die Anwendung auf Standardvorlagen des Informationsregisters		▸ Richtlinien für die Zusammenarbeit zwischen den ESAs und den CAs hinsichtlich der DORA-Aufsicht ▸ RTS zur Harmonisierung der Aufsichtsbedingungen ▸ RTS zur Festlegung der Kriterien der Zusammensetzung des gemeinsamen Untersuchungsteams

DORA in der Jahresabschlussprüfung

Überblick IDW EPS 528: „Aufsichtliche DORA-Prüfung im Rahmen der Abschlussprüfung"

Rahmenbedingungen & Zeitplan

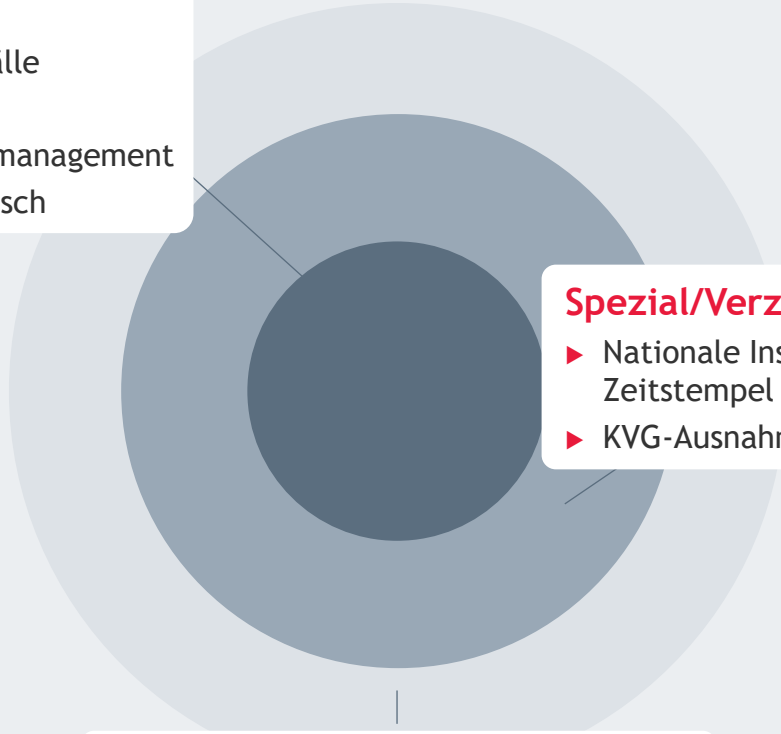
- Grundlage: IDW EPS 528; Erweiterung der Jahresabschlussprüfung
- Start: Für Geschäftsjahre beginnend nach dem 31.12.2024
- Vorzeitige Anwendung zulässig

Abgrenzungen & Proportionalität

- Out-of-Scope: TLPT (Art. 26/27) unterliegt direkter Aufsicht; Art. 16 (vereinf. Rahmen) für best. KVGs ungeprüft

In Scope

- Risikomanagement
- IKT-bezogene Vorfälle
- Testing
- Drittparteienrisikomanagement
- Informationsaustausch



Spezial/Verzögert

- Nationale Institute mit Zeitstempel 2027
- KVG-Ausnahmen

Out of Scope

TLPT (Art. 26/27) -> Bankenaufsicht

Prüfungsmaßstab & Methodik

Der qualitative Sprung

Problem: GoA
Fokus: Historische Finanzdaten

Methodik-Shift: IDW EPS 528
Hebel: ISAE 3000

Prüfungsziel:Wirksamkeit
Prüfung von Design + Implementierung & Operating Effectiveness

Prüfungstiefe: 360°
Org. + Pers. + Tech. + Externe

1. Das methodische Problem

- Integrität und Verfügbarkeit der unterliegenden IT-Infrastruktur wird nur insoweit betrachtet, sofern (direkter) Einfluss auf die Rechnungslegung
- Risiken mit geringer Eintrittswahrscheinlichkeit, aber existentialbedrohendem Schadensausmaß (z.B. Advanced Persistent Threats), werden methodisch oft nur unzureichend abgebildet

2. Der inhaltliche Maßstab

- Ziel: Beurteilung von Angemessenheit UND Wirksamkeit (End-to-End Governance)
- Objekt: Organisatorische, personelle & technische Vorkehrungen
- Schutzziele: Integrität, Vertraulichkeit, Authentizität, Verfügbarkeit
- Erweiterung: Expliziter Einbezug externer IKT-Ressourcen

Der Grundsatz der Verhältnismäßigkeit gem. EPS 528

Indikatoren steuern die Prüfungsintensität

Größe & Business | Risikogehalt

Komplexität | Organisation

Ziel: Risikoorientierte Steuerung der Prüfungsintensität & Walkthroughs.

Soll-Objekt
Wurde die Regulatorik korrekt in interne Richtlinien übersetzt?

Design
Sind die Prozesse geeignet, die Risiken zu mitigieren?

Wirksamkeit
Werden die Vorgaben im laufenden Betrieb tatsächlich eingehalten?

Der Grundsatz der Verhältnismäßigkeit gem. EPS 528

Fallbeispiel

Typ	Kategorie	Bank A	Bank B	Bank C
Indikator	Geschäftsmodell			
Indikator	Organisation			
Indikator	Infrastruktur			
Indikator	Risikogehalt			
Prüfungsumfang	*IKT-Risikomanagement*			
Prüfungsumfang	*Vereinfachter IKT-Rahmen*			
Prüfungsumfang	*Incident-Management*			
Prüfungsumfang	*Resilienz-Testing*			
Prüfungsumfang	*Drittparteimanagement*			
Prüfungsumfang	*Cyberbedrohungsinformationen*			

Prüfung Soll-Objekt und Angemessenheit

Regulatorischer Rahmen
DORA (Art. 5-45)
Abstrakte Anforderungen

1. Ziel der Soll-Objekts-Beurteilung

- Verantwortung: Die gesetzlichen Vertreter (Geschäftsleitung) müssen nachweisen, dass sie die DORA-Anforderungen (Art. 5-45) korrekt in interne Vorgaben übersetzt haben.
- Zielsetzung: Sicherstellung der Schutzziele Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit (CIA+A) für kritische Prozesse & Daten.
- Manifestation: Das "Soll-Objekt" ist nicht das Gesetz, sondern die interne Konkretisierung in Strategien, Richtlinien und gelebten Prozessen.

2. Der Prüfungsansatz

- Vorgehen: Aufnahme eines umfassenden Bildes der Aufbau- und Ablauforganisation.
- Methodik: Abgleich der internen Regelungen gegen die regulatorischen Anforderungen (Gap-Analyse).

Prüfung Soll-Objekt und Angemessenheit

1. Governance & Strategie (Der Rahmen)

2. Architektur & Assets (Das Objekt)

3. Drittparteirisiko (Die Erweiterung)

4. Monitoring & Reporting (Der Nachweis)

Angemessenheitsprüfung

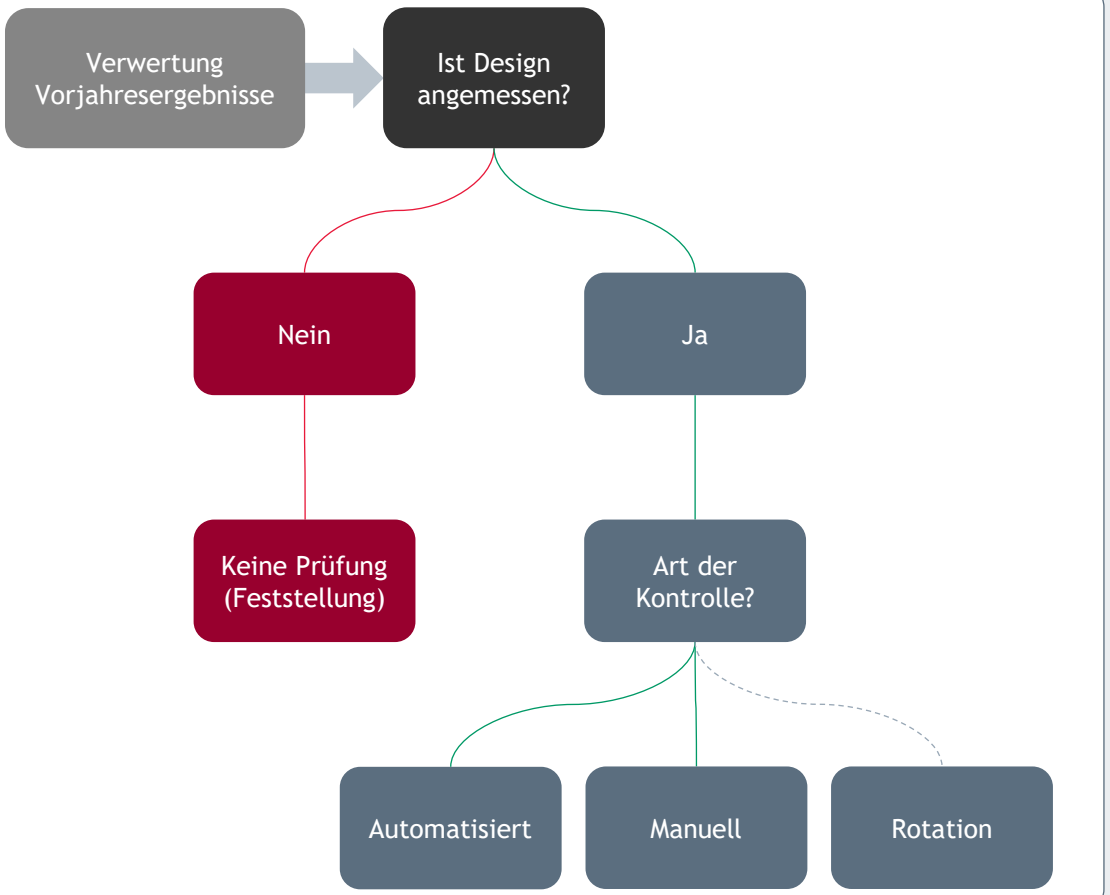
1. Zielsetzung der Angemessenheitsprüfung

- Kernfrage: Wurden die regulatorischen Vorgaben (Soll-Objekt) korrekt in konkrete Prozesse, Regelungen und Verfahren übersetzt?
- Prüfungsurteil: Beurteilung, ob die implementierten Maßnahmen geeignet sind, die DORA-Anforderungen dauerhaft zu erfüllen.

2. Durchführung

- Der Prüfer gewinnt Prüfungsnachweise nicht nur durch bloßes Lesen, sondern durch einen Mix aus fünf Prüfungshandlungen, um die tatsächliche Implementierung zu verifizieren.

Wirksamkeitsprüfung



1. Die "Gatekeeper"-Regel

- Voraussetzung: Eine Wirksamkeitsprüfung erfolgt nur, wenn die vorangegangene Angemessenheitsprüfung (Design) positiv war.
- Konsequenz: Ist das Design mangelhaft (nicht angemessen), entfällt der Wirksamkeitstest. Der Mangel wird direkt berichtet.

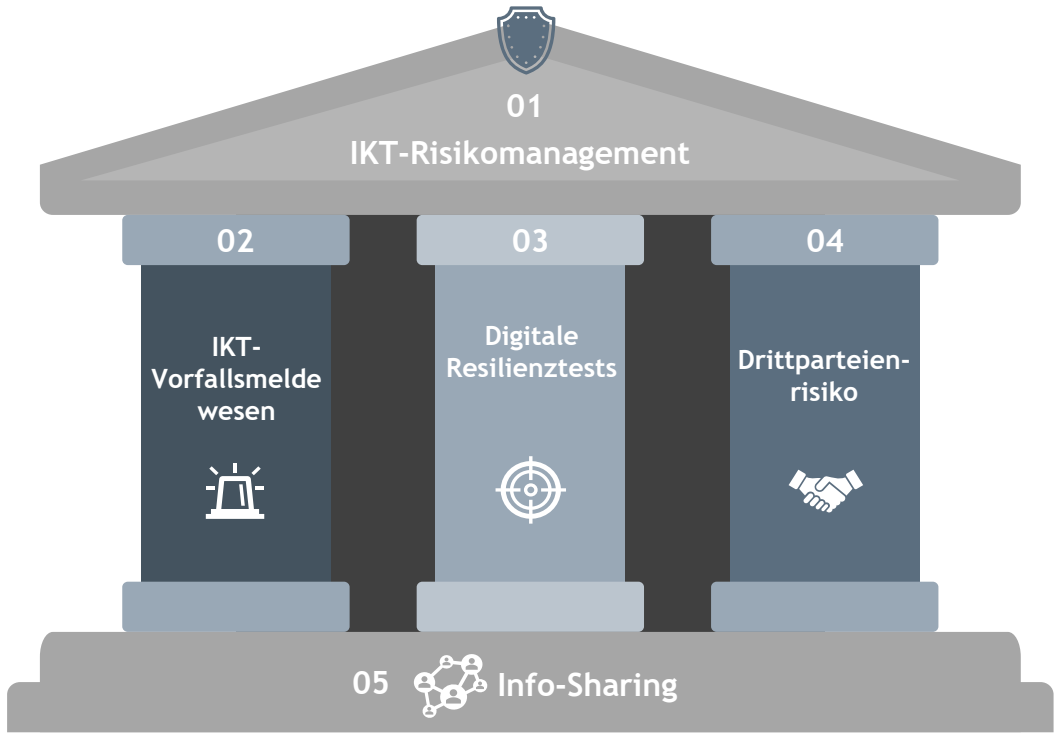
2. Prüfungsstrategie & Umfang

- Automatisierte Kontrollen: Hier genügt in der Regel ein "Test of One" (einmaliger Durchlauf), da das System deterministisch arbeitet (Dual Purpose Test).
- Manuelle Prozesse: Hier ist eine Auswahl von Elementen (Stichprobe) zwingend erforderlich. Umfang richtet sich nach Risikofaktoren (Proportionalität).
- Rotations-Prinzip: Bei unveränderten Rahmenbedingungen und mangelfreier Historie können Ergebnisse aus Vorjahren genutzt werden (max. 2 Jahre alt).

3. Feedback-Schleife

- Eine hohe Fehlerquote in der Wirksamkeit kann rückwirkend das Urteil zur Angemessenheit (Design) in Frage stellen

Wirksamkeitsprüfung



Säule	Thema	Wirksamkeits-Check
Risikomanagement		
Vorfallsmeldewesen		
Resilienztests		
Drittparteienrisiko		
Info-Sharing		

DORA in der Praxis

Praxiserfahrungen,
Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

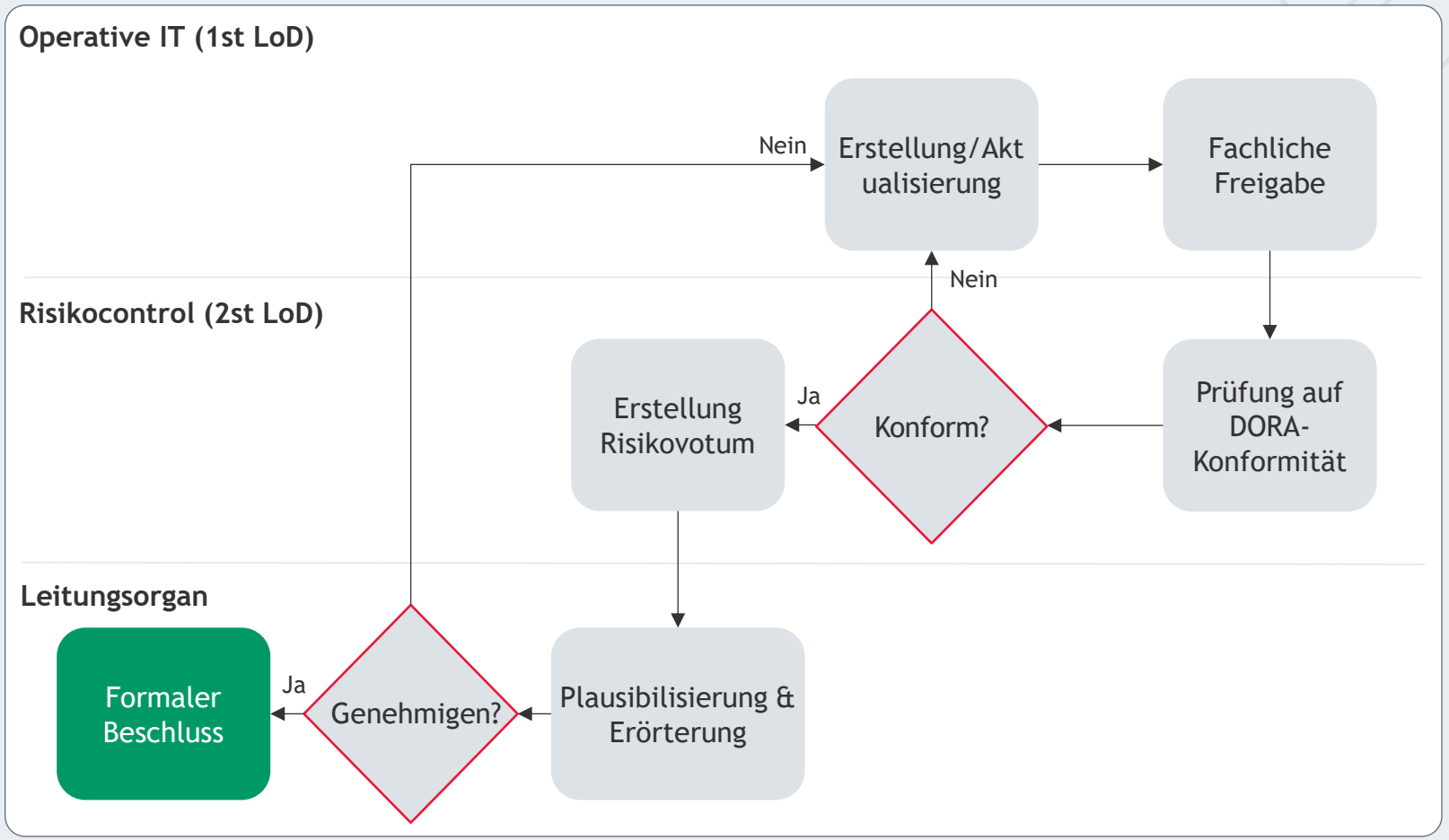
Operational Resilience

Governance

Die neue operative Tiefe

Pflichten des Leitungsorgans

- Von der Kenntnisnahme zur Genehmigungspflicht
- Quantifizierung der Risikotoleranz
- Direkte Budgetsteuerung
- Aktive Steuerung



Herausforderungen

des IKT-Risikomanagementrahmens

Zwingende Institutionalisierung der Kontrollfunktion (Art. 6 Abs. 4):

- Übergang von der bloßen Benennung eines Beauftragten (ISB) zu einer strukturell unabhängigen Kontrollfunktion (2nd Line) mit erweitertem Mandat

Quantifizierung der Risikotoleranz (Art. 6 Abs. 8):

- Abkehr von qualitativen Risikoappetit-Beschreibungen ("Gering/Mittel") hin zu harten Metriken für die Auswirkungstoleranz (Impact Tolerance, z.B. "Max. 2h Downtime")

Verhärtung des Überprüfungszyklus (Art. 6 Abs. 5):

- Ersetzung des unbestimmten Rechtsbegriffs "regelmäßig" durch eine fixe jährliche Review-Pflicht des gesamten Frameworks sowie zwingende Ad-hoc-Reviews bei Vorfällen.

Formalisierter Mängel-Prozess (Art. 6 Abs. 7):

- Einführung eines gesetzlich zwingenden Follow-up-Verfahrens für Revisionsfeststellungen; Mängelbehebung ist nicht mehr Ermessenssache des Managements, sondern prozessual gebunden

Das erweiterte Asset- & Metrik-Universum (Art. 6)

Datenintegrität (Max. zulässiger Datenverlust)	Verfügbarkeit (Max. Ausfallzeit)	Vertraulichkeit (Klassifizierungs-Schema & Access-Level)	Muss mit Geschäftsstrategie synchronisiert sein
Digitale Assets: Software, Code-Respositories, Algorithmen	Physische Infrastruktur: Rechenzentrum, Stromversorgung, Sensible Räume	Legacy-Systeme: Altsysteme	Externe Ressourcen: Cloud-Instanzen & SaaS

Netzwerk-Segmentierung & Isolierung
IAM (Identity & Access Management) & Starke Authentifizierung
Verschlüsselung (Data at Rest / in Transit)
Automatisierte Schwachstellen-Scans (Patch Management)

Wiederherstellungsfähigkeit

Kernanforderung DORA

BIA als zwingender Architektur-Treiber (Art. 11 Abs. 5):

- Die Business Impact Analyse (BIA) ist keine reine Dokumentation mehr. IKT-Systeme müssen "in voller Übereinstimmung" mit der BIA konzipiert sein (z.B. Redundanz). Passt die Architektur nicht zur BIA, ist das ein Compliance-Verstoß

Erweiterter Test-Scope: "Live Switchover" (Art. 11 Abs. 6):

- Verschärfung der Testpflicht. Gefordert sind Szenarien für Cyberangriffe und die tatsächliche Umstellung von Primär- auf Redundanz-Systeme (keine reine "Papierübung")

Durchgriff auf Drittdienstleister (Art. 11 Abs. 4):

- BCM-Pläne müssen explizit ausgelagerte Funktionen abdecken. Der Finanzdienstleister muss sicherstellen (und testen!), dass der Notfallplan auch funktioniert, wenn AWS, FI oder Atruvia betroffen sind

Monetarisierung von Vorfällen (Art. 11 Abs. 10):

- Neu: Pflicht zur Bezifferung der Kosten und Verluste durch IKT-Vorfälle (Aggregierte Meldung an Aufsicht). BCM wird zur kaufmännischen Rechengröße

DORA in der Praxis

Praxiserfahrungen,
Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

Incident Reporting

Standardisierung der Incident-Behandlung

Art. 17
Incident Management

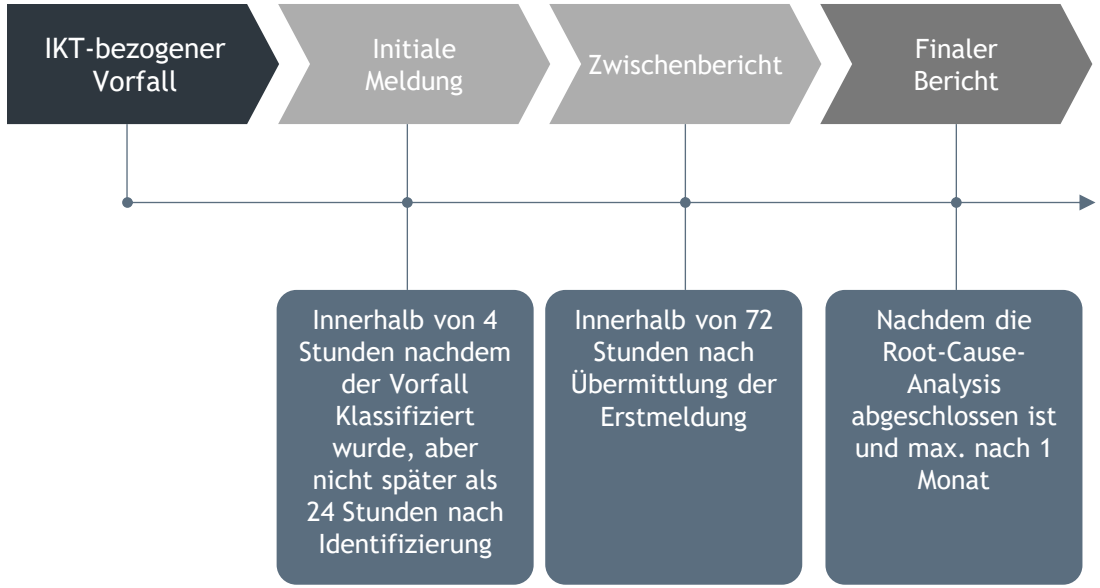
- Holistischer Ansatz: Etablierung eines integrierten Prozesses zur Überwachung, Protokollierung und Nachverfolgung aller IKT-Vorfälle.
- Lernende Organisation: Verpflichtende Ursachenanalyse und Ableitung von Maßnahmen zur Verhinderung von Wiederholungen

Art. 18
Klassifizierung

- Harmonisierte Kriterien: Bewertung der Schwere anhand von Dauer, Datenverlust, betroffenen Kunden und geografischer Ausbreitung (gemäß RTS der ESAs).
- Cyberbedrohungen: Separate Klassifizierung von "erheblichen Cyberbedrohungen" (potenzielle Gefahr ohne Eintritt).

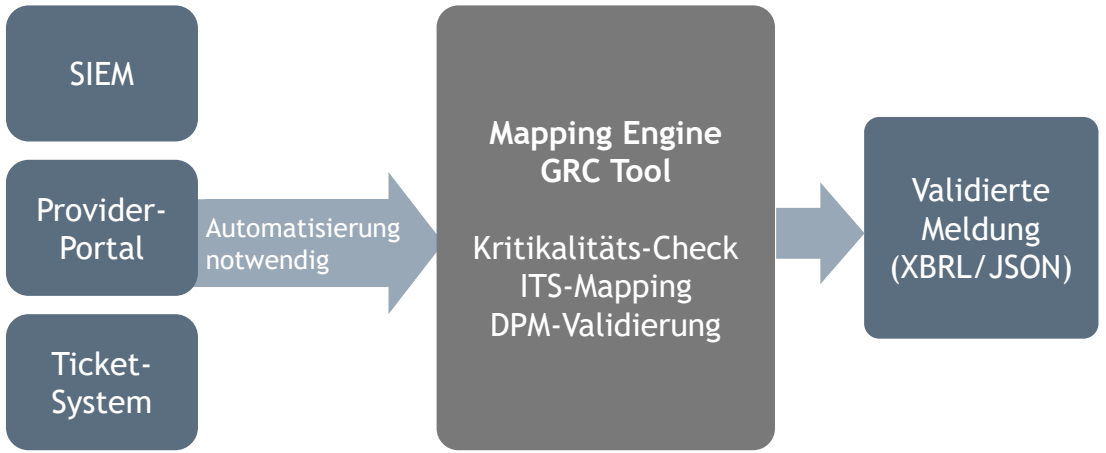
Art. 19
Meldewesen

- 3-Phasen-Meldung: Meldepflicht für schwerwiegende Vorfälle an die Aufsicht (Initial / Update / Final) mit strikten Fristen.
- Kundenkommunikation: Informationspflicht bei finanziellen Auswirkungen oder notwendigen Schutzmaßnahmen für den Kunden.



Herausforderungen der Incident-Behandlung

Daten, Systeme und Dritte



Analyse & Forensik

- **Langwierige Root Cause Analysis (RCA):** Für die Abschlussmeldung ist eine vollständige Ursachenanalyse nötig. Bei komplexen Hacks dauert die Forensik oft länger als die Monatsfrist, was zu Fristverletzungen führen kann.

Datenmodell & Integration (Der technische Überbau)

- **ITS-Datenmodell-Anpassung:** Umsetzung verlangt tiefgreifende Anpassungen der GRC-Systeme an neue Taxonomien.
- **Silo-Überwindung:** Technische Konsolidierung in zentraler GRC-Plattform ist zwingend, um eine ganzheitliche Sicht für die Meldung zu generieren.
- **Automatisierungs-Zwang:** Um die 4-Stunden-Frist zu halten, muss die Kategorisierung technisch (teil-)automatisiert erfolgen.

Abhängigkeit von der Lieferkette (Dritte)

- **Fristen-Domino:** Die Bank kann ihre 4-Stunden-Frist nur halten, wenn der IT-Dienstleister schnell meldet. Abhängigkeit verlagert sich in die Lieferkette.
- **Vertrags-Gap:** Bestandsverträge müssen technisch und juristisch angepasst werden, um die Meldefristen vom Dienstleister einzufordern.
- **Register-Komplexität (RoI)**: Das Informationsregister muss um neue Datenspalten erweitert werden und technisch mit dem Auslagerungs-Management-Tool synchronisiert sein.

Herausforderungen der Incidentbehandlung

Prozess, Fristen und Klassifizierung

Der "Speed-Trap" (Meldefristen vs. Qualität)

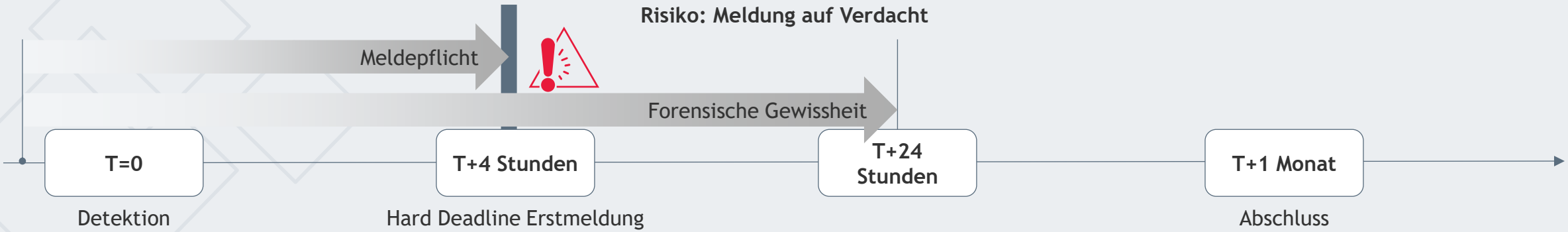
- 4-Stunden-Ultimatum: Die Pflicht zur Erstmeldung binnen 4 Stunden nach Klassifizierung (max. 24h nach Entdeckung) erzeugt extremen Stress.
- Problem: Konflikt zwischen Geschwindigkeit und Datenqualität. Die Meldung muss erfolgen, bevor eine vollständige Analyse vorliegt
- Zwang zum 24/7-Betrieb: Die Fristen gelten rund um die Uhr. Kleinere Institute müssen ihre Organisation auf einen belastbaren 24/7-Betrieb umstellen
- Bürokratisierung durch Taktung: 72h-Zwischenmeldungen binden Ressourcen, die eigentlich für die operative Behebung des Vorfalls ("Löschen") benötigt würden.

Ambiguität & Übermeldung (Klassifizierung)

- Interpretationsrisiko "Kritikalität": Die Definition "kritischer Dienste" bleibt trotz EBF-Kritik schwammig.
- Rationales Übermelden (Minor Incident Overflow): Aus Angst vor Sanktionen neigen Institute dazu, lieber zu viel ("Schwerwiegend") zu melden.
- Retrospektive Kumulation: Die Pflicht, wiederholte kleine Vorfälle über 6 Monate zu kumulieren, erfordert eine komplexe statistische Analyse historischer Daten.

Regulatorische Triage (Koordination)

- Meldepflicht-Dschungel: Ein Vorfall kann gleichzeitig DORA, NIS2 und DSGVO betreffen. Die interne Triage-Logik muss entscheiden: Welche Behörde? Welche Frist ist die kürzeste?.



DORA in der Praxis

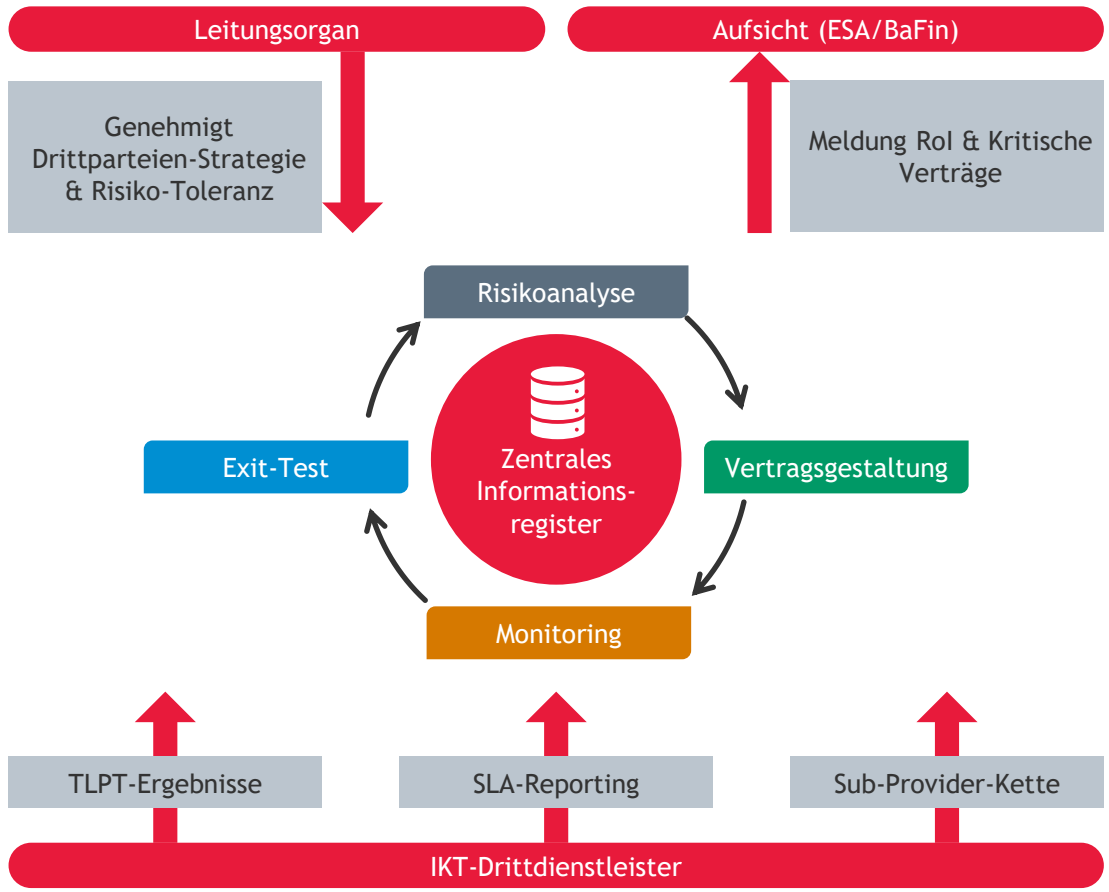
Praxiserfahrungen,
Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

Outsourcing

Drittparteienrisiko DORA vs. xAIT

Vom Prinzip zur harten Evidenz

- **Zwingende Konzentrationsanalyse (Art. 29):** Die Risikobewertung vor Vertragsabschluss wird erweitert: Neben dem Einzelrisiko muss zwingend das Konzentrationsrisiko (Vendor Lock-in) und das Risiko durch Sub-Dienstleister (Ketten-Auslagerung) bewertet werden.
- **Standardisiertes Meldewesen (Art. 28 Abs. 3 & 9):** Die interne Vertragsübersicht wird durch das Informationsregister (RoI) nach ITS-Standard ersetzt. Es besteht eine aktive Meldepflicht neuer kritischer Auslagerungen sowie des gesamten Registers an die Aufsicht.
- **Vertragliche Durchgriffsrechte (Art. 30):** Verträge müssen präzise SLAs, garantierte Unterstützung bei Vorfällen (kostenfrei/definiert) und die verpflichtende Teilnahme an Threat-Led Penetration Tests (TLPT) beinhalten.
- **Operative Testpflicht für Exit-Strategien (Art. 28 Abs. 8):** Exit-Pläne dürfen keine theoretischen Konzepte bleiben; ihre Wirksamkeit (Datenmigration, Wechsel) muss regelmäßig getestet werden.
- **Insolvenzfester Datenzugriff:** Vertragliche Sicherstellung, dass Daten auch bei Geschäftsaufgabe des Dienstleisters in einem lesbaren Format zurückgeholt werden können.



Herausforderungen Drittparteienrisiko

Die Implementierungsanalyse

Komplexität des Informationsregisters (RoI - ITS Standard):

- Jeden IKT-Service mit LEI-Codes, genauen Funktionsbeschreibungen und Verknüpfung kritischer Funktionen zu mappen.
- Branchen-Realität: Stammdaten sind oft unsauber. Die Abgrenzung ist schwierig: Ist der BiPRO-Service (Versicherung) ein IKT-Dienst? Ist der Reuters-Feed (KVG) ein IKT-Dienst?

Intransparenz der Sub-Outsourcing-Kette (N-th Party):

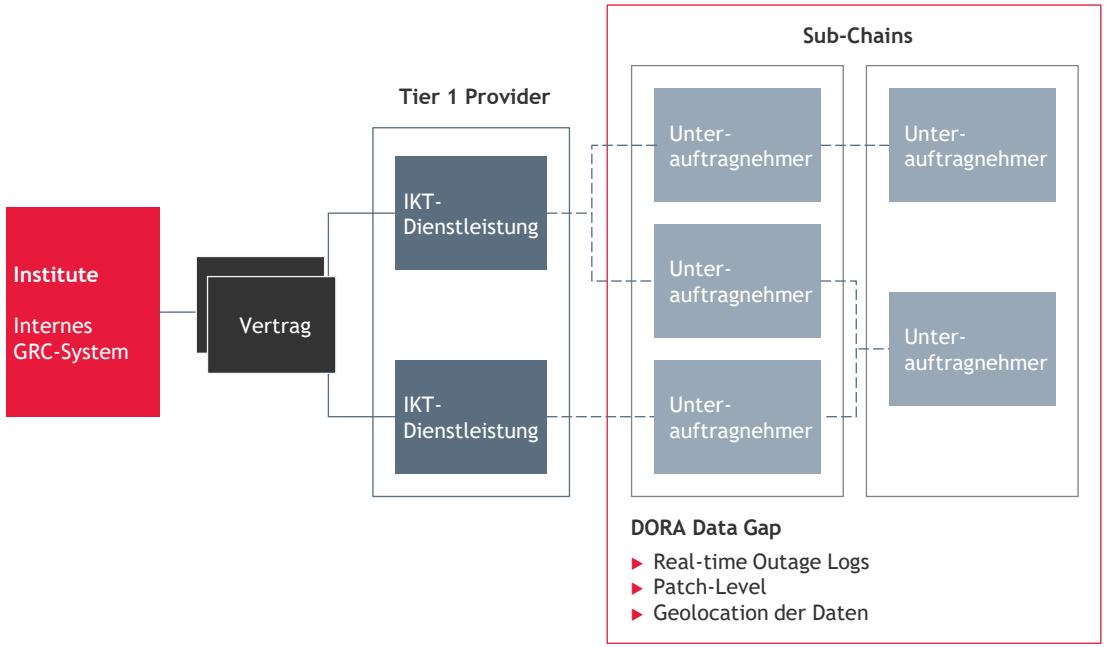
- Pflicht zur Überwachung der gesamten Kette.
- Branchen-Realität: Bei SaaS-Lösungen (z.B. Salesforce, ServiceNow, Aladdin) ist die darunterliegende Infrastruktur (Hosting, Wartung) oft dynamisch und intransparent.

Fehlende Testumgebungen für Exit-Strategien:

- Pflicht zum Test des Exits.
- Branchen-Realität: Für Monolithen existieren oft keine parallelen "Standby-Systeme" anderer Hersteller. Ein Exit-Test (Migration auf System B) ist technisch nicht leistbar. Der "Test" degeneriert zur reinen Papierübung

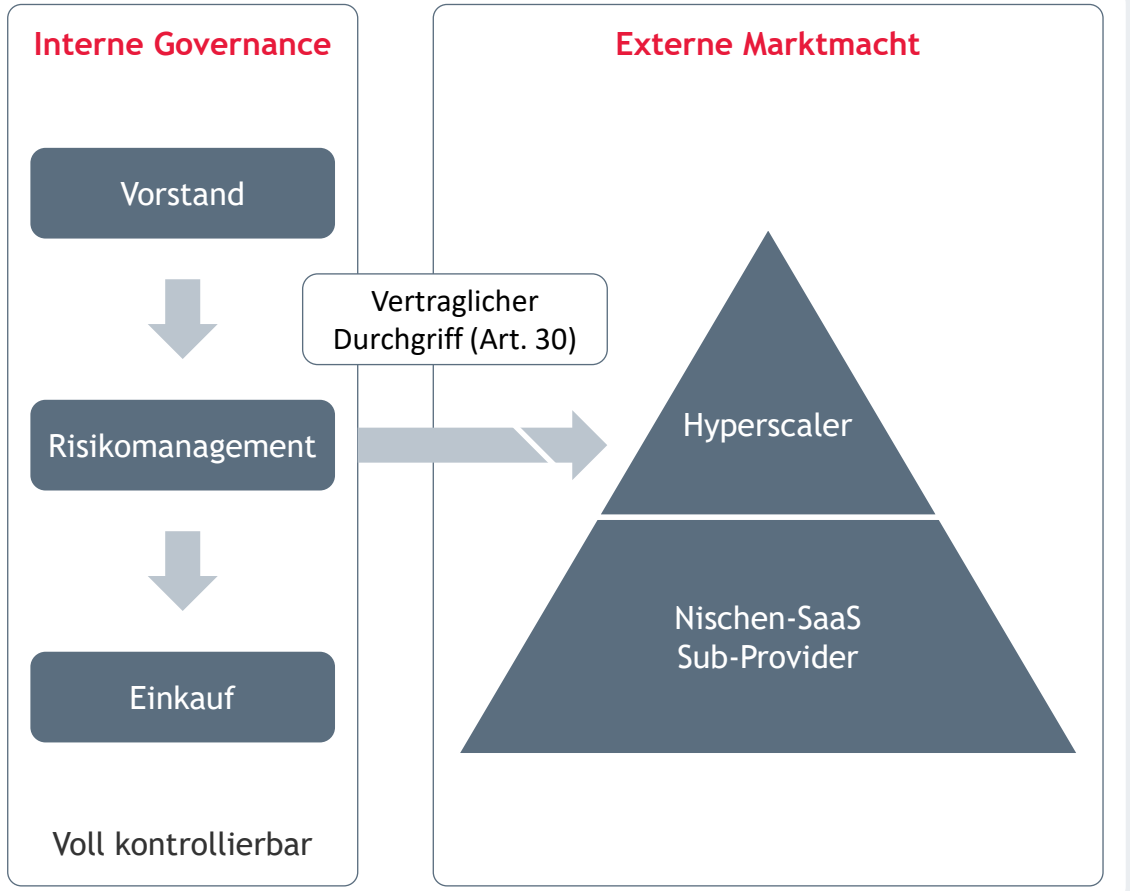
TLPT in Multi-Tenant Umgebungen:

- Branchen-Realität: Cloud-Provider und SaaS-Anbieter verweigern oft individuelle Penetration Tests (Red Teaming), da diese die Stabilität für andere Mandanten gefährden könnten.



Herausforderungen Drittparteienrisiko

Die Governance-GAP



Asymmetrie der Verantwortlichkeit (Art. 28):

- Das Finanzunternehmen trägt die volle regulatorische Endverantwortung.
- Branchen-Realität: Gegenüber globalen Oligopolisten oder monopolistischen Zentral-Dienstleistern (Verbund-Rechenzentren) besteht faktisch oft keine Durchsetzungsmacht für individuelle DORA-Klauseln. Die Governance läuft ins Leere ("Take it or leave it").

Ressourcen-Engpass "Re-Papering":

- Notwendigkeit der Nachverhandlung von Bestandsverträgen zur Inklusion der Art. 30 Pflichten (TLPT, Audit-Rechte).
- Branchen-Realität: Bei Versicherern betrifft dies tausende fragmentierte Partnerschaften (Makler, Assistance); bei Banken komplexe Altverträge. Die Rechts- und Einkaufsabteilungen sind kapazitiv nicht in der Lage, diese Masse in der Frist individuell zu verhandeln.

Silo-Problematik in der 2nd Line:

- Drittparteienrisikomanagement erfordert eine synchrone Risikobewertung durch ISB (Sicherheit), Legal (Vertrag), Business Owner (Leistung) und Risk (Konzentration).
- Branchen-Realität: In vielen Häusern agieren diese Funktionen in Silos. Es fehlt ein integrierter Workflow, der "Schatten-IT-Beschaffung" am Einkauf vorbei wirksam verhindert.

DORA in der Praxis

Praxiserfahrungen,
Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

Testing

Testingprozess nach DORA

Methode	Fokus/Ziel	Herausforderung / Merhwert (Value Add)
Vulnerability Scan	Automatische Suche nach bekannten technischen Schwachstellen	**Herausforderung**: Hohe False-Positive-Rate; findet nur „bekannte“ Lücken, keine Logikfehler
Source Code Review	Analyse des Programm-Codes auf Sicherheitslücken und Backdoors vor Kompilierung	**Mehrwert**: Findet tiefe Designfehler früh **Herausforderung**: Bei Legacy oft unmöglich; bei SaaS verweigert.
End-to-End Test	Prüfung einer kompletten Geschäftstransaktion über alle Systemgrenzen hinweg	**Mehrwert**: Testet die Schnittstellen-Resilienz **Herausforderung**: Erfordert synchrone Testumgebungen über mehrere Provider hinweg
Szenariobasierter Test	Simulation eines realen Vorfalls statt Checklisten-Abarbeitung	**Mehrwert**: Prüft die Reaktionsfähigkeit der Organisation, nicht nur die Technik **Herausforderung**: Erfordert Business-Know-How für realistische Szenarien

- **Integrales Rahmenwerk (Art. 24):** Verpflichtung zur Etablierung eines umfassenden Testprogramms als fester Bestandteil des IKT-Risikomanagements; Durchführung muss risikobasiert erfolgen (Fokus auf sich entwickelnde Bedrohungslandschaften und Kritikalität der Assets).
- **Erweiterte Methodik-Breite (Art. 25):** Abkehr vom reinen "Vulnerability Scan"; gefordert ist ein breites Portfolio an Testarten, explizit inklusive Quellcodeprüfungen (soweit durchführbar), End-to-End-Tests über Systemgrenzen hinweg und szenariobasierten Tests.
- **Jährliche Frequenz & Unabhängigkeit:** Zwingende Prüfung aller IKT-Systeme, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich. Durchführung durch unabhängige Parteien (intern/extern) unter strikter Vermeidung von Interessenkonflikten (Segregation of Duties).
- **Verbindliche Remediation & Validierung:** Formalisierter Prozess zur Priorisierung und Behebung von Schwachstellen ("Remediation“). Kritisch: Die Behebung gilt erst als abgeschlossen nach erfolgreicher interner Validierung (Re-Test).

Herausforderungen der Testing-Anforderungen

Der „Remediation-Stau“

1. Programmatische Verwaltungslast (Art. 24): DORA fordert den Übergang von punktuellen Tests zu einem "umfassenden Programm".

- **Herausforderung:** Die Orchestrierung verschiedenster Testarten für alle kritischen Assets in einem integralen Risikomanagement-Rahmenwerk erfordert massive administrative Ressourcen.

2. Der Validierungs-Engpass (Remediation): Pflicht zur Priorisierung, Behebung und internen Validierung aller Mängel.

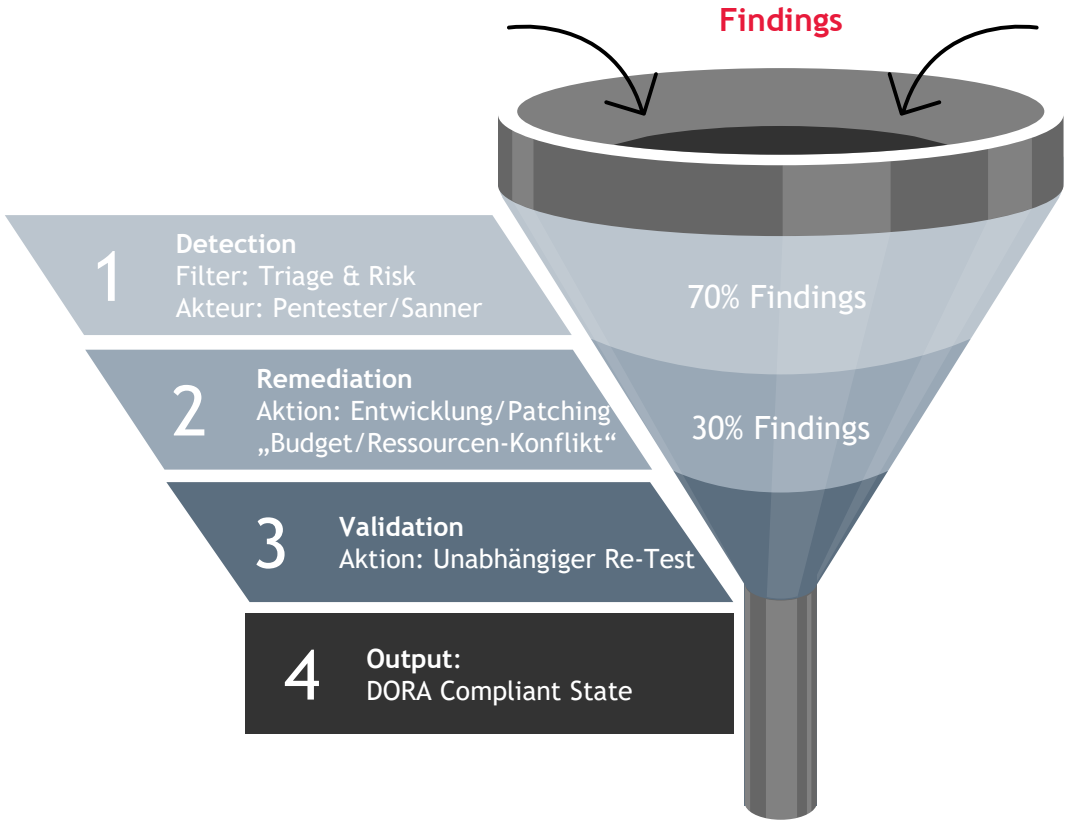
- **Herausforderung:** "Testing ist einfach, Fixing ist schwer." In der Praxis führt die erhöhte Testfrequenz (jährlich) zu einem Anstau von Findings. Die geforderte Validierung (Re-Test) bindet Ressourcen

3. Organisatorische Unabhängigkeit (SoD): Interne Tester dürfen keine Interessenkonflikte haben.

- **Branchen-Realität:** In vielen IT-Abteilungen testen Entwickler ihren eigenen Code oder Admins ihre eigene Konfiguration. Die Etablierung einer wirklich unabhängigen internen Instanz (2nd Line Testing) erfordert oft Personalaufbau oder teuren externen Einkaufen.

4. Jährliche Frequenz-Dichte: Pflichttests für alle kritischen Systeme mindestens jährlich.

- **Herausforderung:** Dies erzeugt eine saisonale "Test-Welle", die IT-Change-Fenster blockiert.



Testingprozess nach DORA

1. End-to-End Tests in hybriden Architekturen:

- Art. 25 fordert "End-to-End-Tests".
- **Branchen-Realität:** Ein Geschäftsprozess läuft über: App (Cloud) -> API-Gateway-> Kernbankensystem (Host) -> Marktdatenprovider (Extern).
- **Herausforderung:** Einen E2E-Test technisch zu orchestrieren, wenn Teilsysteme (SaaS) nicht kontrollierbar sind, ist extrem komplex.

2. Quellcodeprüfung (Source Code Review):

- Gefordert "soweit durchführbar".
- Branchen-Realität:
- Legacy: Spaghetti-Code aus den 90ern ist oft nicht mehr statisch analysierbar.
- SaaS/Proprietär: Anbieter legen ihren Quellcode nicht offen ("Blackbox"). Hier müssen kompensierende Verfahren (Zertifikate) etabliert werden.

3. Testdaten-Management (GDPR-Konflikt):

- Tests benötigen realistische Daten für "Leistungstests" und "Szenariobasierte Tests".
- **Herausforderung:** Die Anonymisierung komplexer relationaler Datenbanken (Integritätserhalt) für Testumgebungen ist aufwendig. Die Nutzung von Prod-Daten ist datenschutzrechtlich riskant.

Die „Machbarkeits-Heatmap“

	Vulnerability -Scan	Source Code Review	E2E-Test	Penetration Test
Eigene Entwicklung				
Legacy Host		Tooling fehlt oft	Testdaten-Silos	
SaaS/3rd Party	Nur Public Interface	Zugriff verweigert		Nur mit Erlaubnis

4. Szenariobasierte Tests (Über den Standard hinaus):

- Abkehr vom reinen "Checklisten-Test" hin zu Szenarien.
- **Herausforderung:** Entwicklung realistischer Business-Szenarien (z.B. "Ausfall Clearing-Stelle") erfordert tiefes Fachwissen, das in der reinen IT-Security oft fehlt.

And it goes on…

System-Garantie statt Datencheck

Prüfung der technischen “Überlebensfähigkeit” steht im Zentrum

Fokus auf Prozesse

Nicht (nur) Existenz von Abwehrmaßnahmen, sondern auch Reaktionsgeschwindigkeit

Haftung endet nicht am Werkstor

Verantwortlichkeit für gesamte digitale Lieferkette

Gatekeeper-Prinzip

Ordnungsgemäßes Design ist starker noch als bei IKS-Prüfung Voraussetzung für Wirksamkeitsprüfung

„Assume Breach“ statt Festung

Sicherheit misst sich nicht mehr an der Abwehrquote, sondern u.a. an der Wiederherstellungszeit (RTO)

.

Mögliche Zielkonflikte

Hochverfügbarkeit und Datenkonsistenz müssen in Einklang gebracht werden.

DORA in der Praxis

Praxiserfahrungen, Prüfungsimplikationen und
Handlungsfelder für die Finanzbranche

Wir freuen uns auf Ihre Fragen und Anmerkungen

Prof. Dr. Aykut Bußian
Felix Kramer
Matthias Oßmann