Webinar

DORA – Viel Lärm um nichts?!

17.10.2023

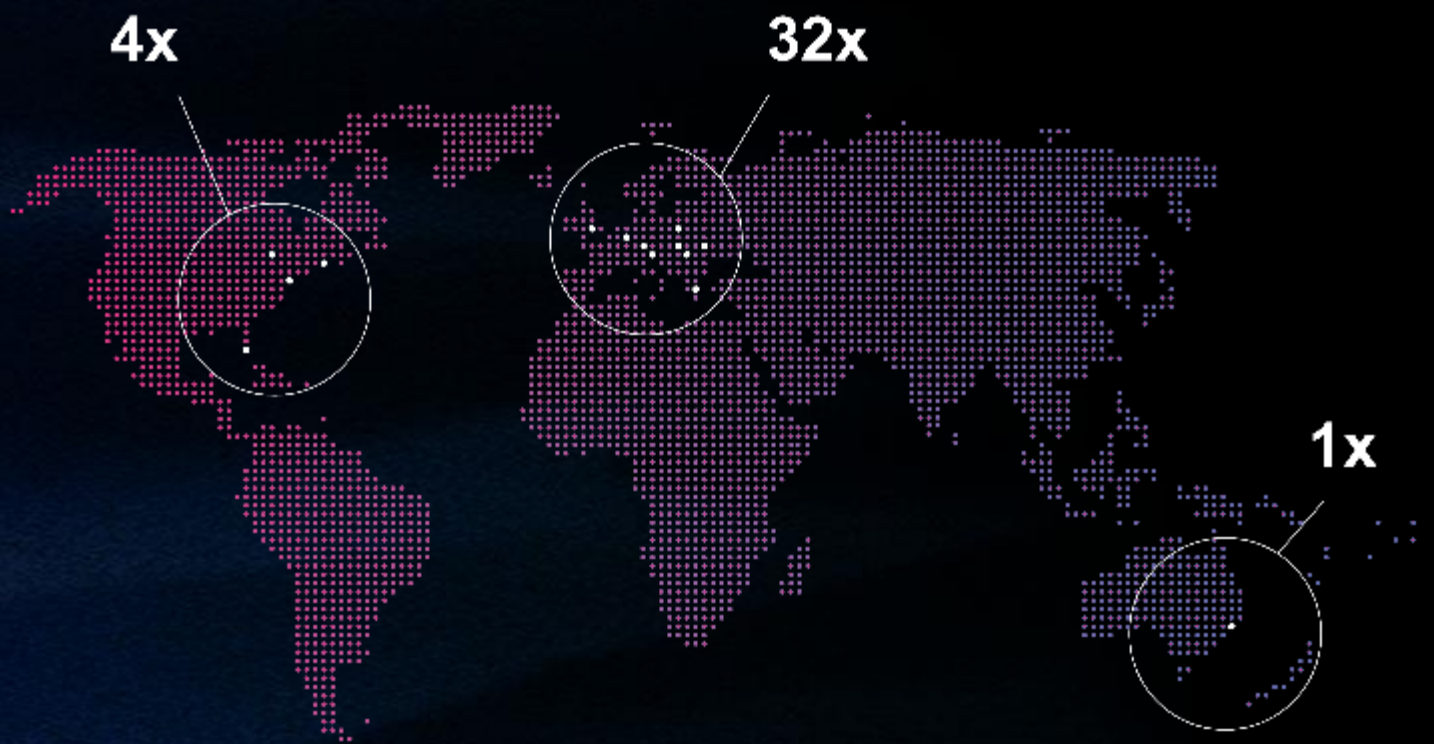
X1F in Zahlen

37
INTERNATIONALE STANDORTE IN 12 LÄNDERN:
GER, AUT, CH, GBR, POL, HUN, ROU, GRE, SRB, USA, CAN, AUS

145+ m €
UMSATZ 2022

1000+
HOCHQUALIFIZIERTE MITARBEITER:INNEN

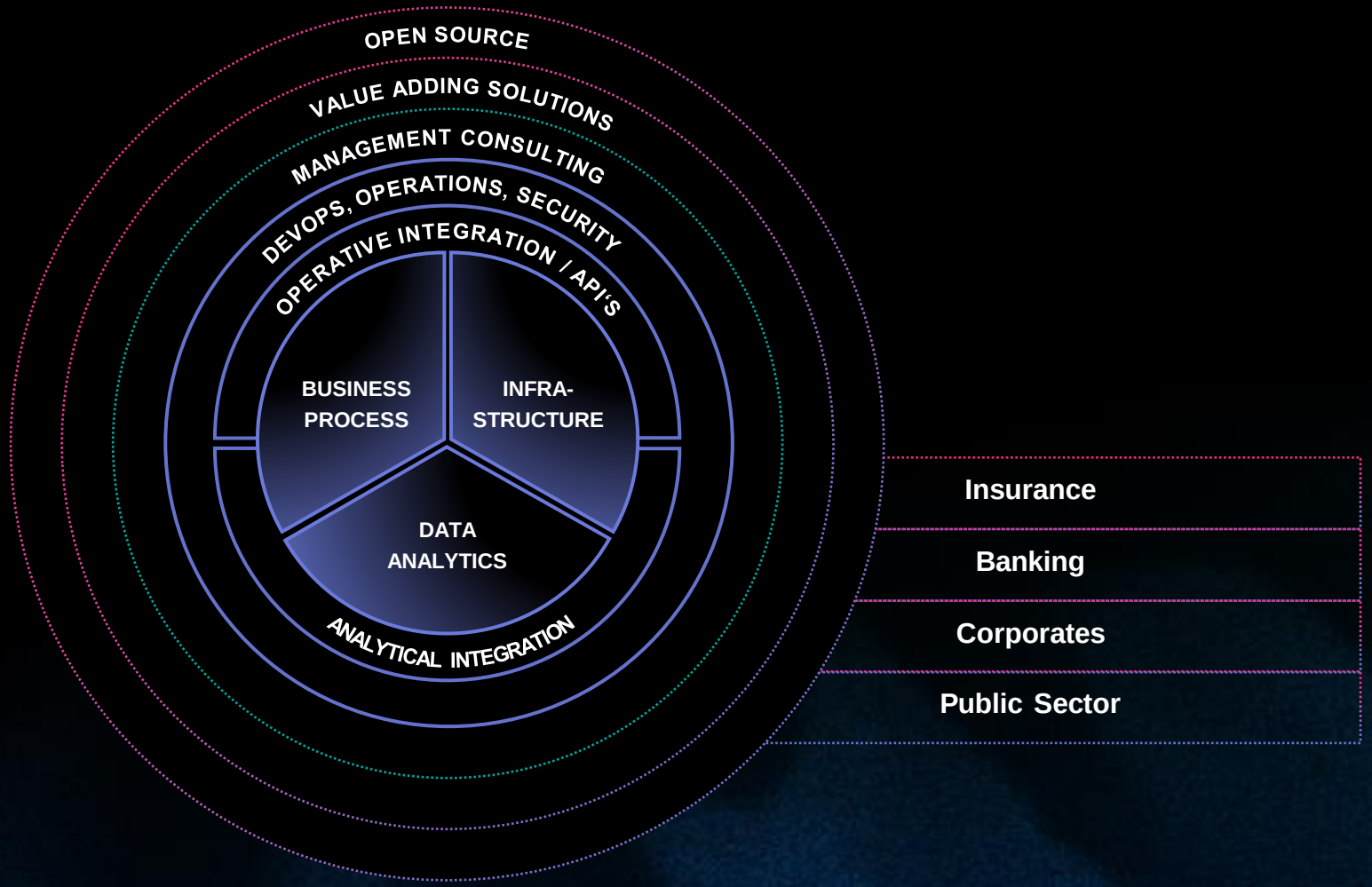
365+
AKTIVE KUNDEN



Übersicht der Gruppe und ihrer Services

X1F

Mit unseren plattformorientierten Services bedienen wir die fachlichen und technologischen Anforderungen verschiedener Branchen.



Ihre heutigen Referent:innen

Pia Streicher
Senior Consultant IT-Security
bei ADWEKO Consulting GmbH

Carolin Neumeir
Teamlead Compliance & Security Consulting
bei matrix technology GmbH

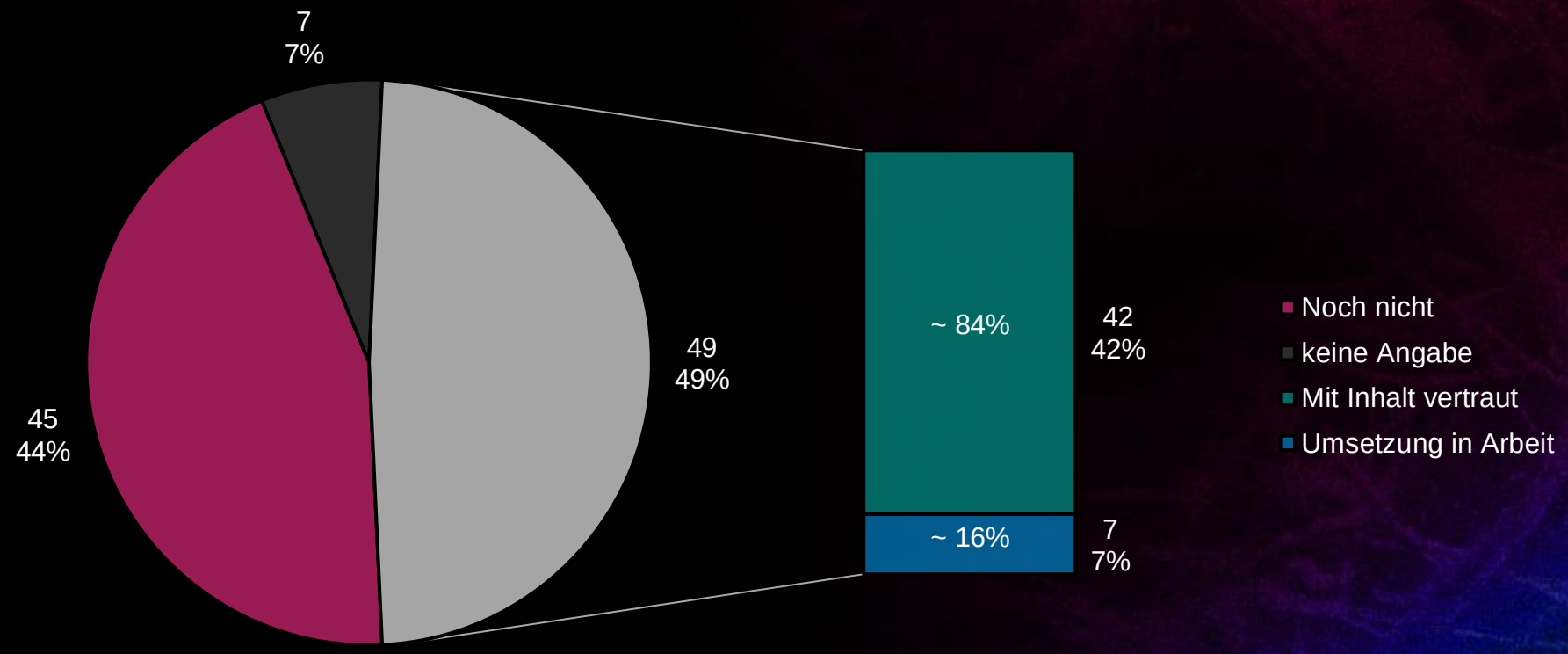
Johannes Rieder
Compliance Consultant
bei matrix technology GmbH

Jan Pawel Pasieka
Penetration Tester
bei e2 Security GmbH

1. **Regulatorische Grundlagen und Einstieg in DORA**
2. Auslagerungsmanagement und Providersteuerung
3. PenTesting im Kontext von DORA
4. Risikoorientierte Herangehensweise
5. Q&A

Ergebnisse Anmeldeumfrage

Haben Sie sich schon mit DORA auseinandergesetzt?



Steigende übergreifende Risiken erfordern eine höhere Widerstandsfähigkeit

Mit der steigenden Nutzung digitaler Dienstleistungen wachsen Cyberrisiken auf Institutsebene, aber auch branchenweit.

Zunehmende Nutzung **digitaler Dienstleistungen** auch in der Finanzbranche. Zum Beispiel: Microsoft Teams & SharePoint, DeepL, Tools für Governance, Risk & Compliance oder das Auslagerungsmanagement.

Zunehmende Digitalisierung

Häufig nutzen Finanzunternehmen **ähnliche oder gleiche Dienstleistungen von einem Anbieter**, wodurch die Abhängigkeit zu Dienstleistern und anderen Instituten wächst. Das erhöht auch die Anfälligkeit für Cyberrisiken.

Steigende Abhängigkeit & Risikoexposition

Regulatorisch wird dies bisher eher auf **nationaler Ebene** adressiert, was zu **unterschiedlichen, teils nicht ausreichenden** Anforderungen für den heutigen Stand der Technik führt.

Mangelnde Konvergenz

Die Auswirkungen dieser Grundsituation betreffen nicht nur einzelne Institute, sondern **wirken sich auf das gesamte europäische Finanzsystem aus**.

Wachsende systemische Risiken

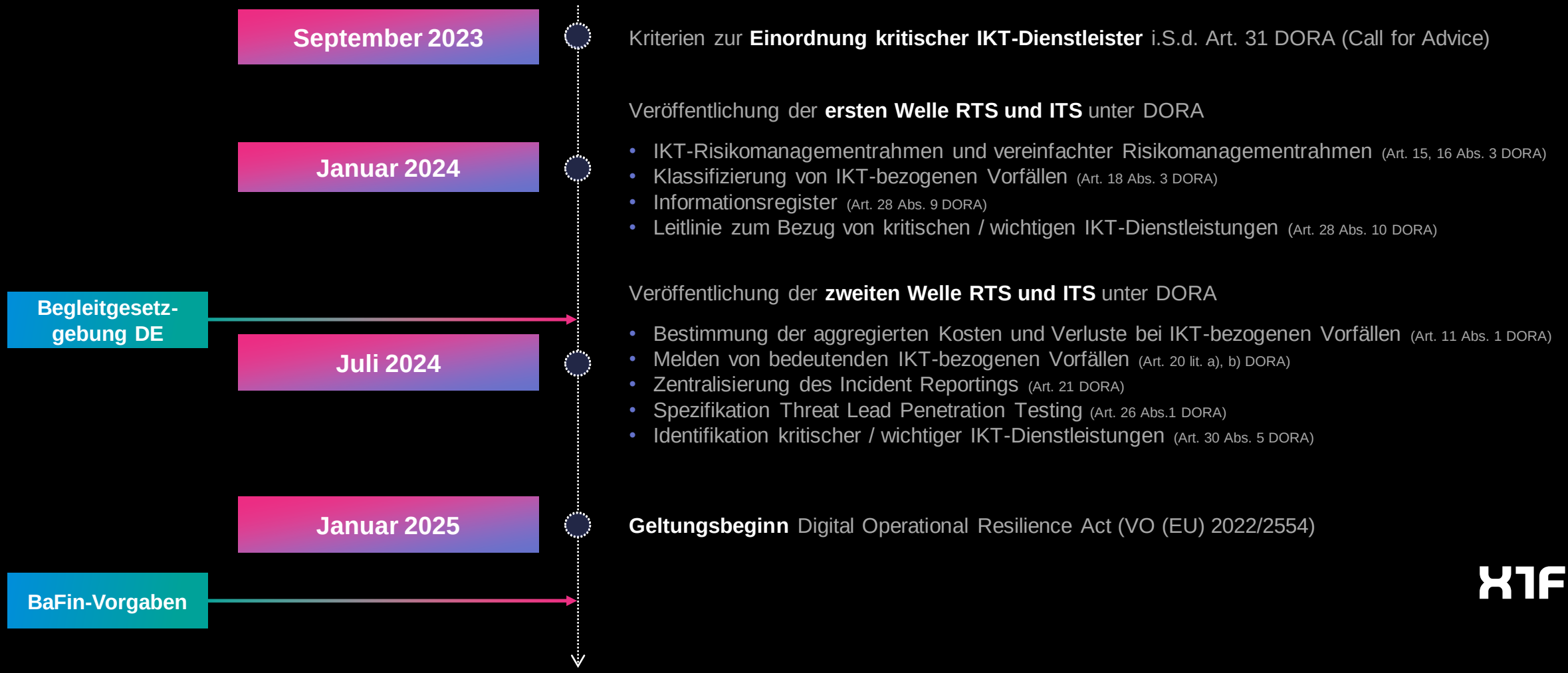
Maßnahme: Steigerung der digitalen operationalen Widerstandsfähigkeit von Finanzunternehmen und dem Finanzsystem

Durch die Entwicklung einer europäischen Vorgabe, zur

- **Verringerung** der aufsichtsrechtlichen Unterschiede
- Senkung von **Konzentrationsrisiken**
- **Einbettung** der Themen rund um Informations- und Kommunikationstechnologien (IKT) in das Risikomanagement
- Steigerung der **Resilienz**

DORA - Timeline

Bis zum Geltungsbeginn des DORA im Januar 2025 stehen noch einige Rechtsakte auf Level 2-Ebene aus.



Themenschwerpunkte DORA

Regulatorisch ist DORA als europäische Verordnung einzuordnen, die also **unmittelbar** in den Mitgliedstaaten der EU gilt und sich thematisch den folgenden Schwerpunkten widmet.

DORA stellt vor allem die **Zusammenhänge** zwischen oft einzeln betrachteten Themengebieten in den Fokus und regt so dazu an, **Schnittstellen zwischen Prozessen und Inhalten** aktiver zu gestalten.

Thematisch widmet der Rechtsakt sich dabei vor allem folgenden Themen:

- Informationsaustausch
- Risikomanagement
- Incident Management
- Testmanagement
- Auslagerungsmanagement/ Providersteuerung

1. Regulatorische Grundlagen und Einstieg in DORA
2. **Auslagerungsmanagement und Providersteuerung**
3. PenTesting im Kontext von DORA
4. Risikoorientierte Herangehensweise
5. Q&A

IKT-Dienstleister nach DORA

Definition von IKT-Dienstleistungen

IKT-Dienstleistungen voraussichtlich **weiter aufgefasst** als in bisheriger Regulatorik

Beispiele: Isolierter Bezug von Softwarelizenzen, PMO, Consulting

Kritische Dienstleister

Zeichnen sich im Falle von Betriebsstörungen durch **systemische Auswirkungen** aus.

Kritische Dienstleister werden zukünftig **überwacht, nicht beaufsichtigt.**

- ESA veröffentlicht Kriterien und Liste von Dienstleistern (nach Art. 31)

nicht zu verwechseln mit „kritischen Funktionen“!

Gruppeninterne Dienstleister

Für gruppeninterne Dienstleister findet ein Großteil der Regelungen auch Anwendung

- **Auslegung** durch RTS zu Art. 28 und Art. 30

Weitere Aspekte

Grundsatz der **Verhältnismäßigkeit** (Art. 4) gilt, zusätzlich Ausnahmen für Kleinstunternehmen

Spezialfälle: Dienstleister aus Drittländern, Unterauftragsnehmer

Neue Pflichten

Risikomanagement

- Strategie zum Umgang mit **IKT-Konzentrationsrisiken**
  → insb. Betrachtung anhand der gesamten supply chain
- Intensivere Betrachtung der **Prozessabhängigkeiten**
- Höhere Bedeutung des Managements von **IKT-Drittparteienrisiken**
  → anhand eigener spezifischer Risiken anpassen und verbessern
- Erweiterte **Due Diligence**

Neuerung Relevanz

Vertragsgestaltung

- **Mindestinhalte** für Vertragsgestaltung, darunter z. B. umfassende Auditrechte
- **Kündigungspflicht** bei schwerwiegenden Verstößen oder mangelhaftem Risikomanagement
- Vertragsgestaltung für **gruppeninterne** Dienstleister auch betroffen

Neuerung Relevanz

Informationsregister

- **Keine Unterscheidung** zwischen Auslagerung und (sonstigem) Fremdbezug
  → Handlungsbedarf v.a. im Fremdbezug
- Pflicht zur Führung von **zwei Registern** (nach XAIT und nach DORA) (?)
- Neue **Pflichtinformationen**, nachgelagerte Pflichten (z. B. Archivierung)

Neuerung Relevanz

Aktive Steuerung

- Dienstleister werden nur **überwacht**
  → keine Pflichtentbindung möglich
- **Meldepflichten** können (nach wie vor) nicht an Dienstleister abgegeben werden
- **Durchführen von Audits**
  - mit qualifiziertem Personal
  - anhand von anerkannten Standards
  - mit festgelegtem Rhythmus

Neuerung Relevanz

Tipps für die Praxis – gut vorbereitet auf DORA

- Neuerungen bereits jetzt in **Neuverträgen** berücksichtigen, erweiterte Informationen für Register erfassen
  → Vertragsinhalte, Zurückgreifen auf Standardvertragsklauseln, Beachtung möglicher Konzentrationsrisiken
- Veröffentlichungen der **technischen Regulierungsstandards (RTS)** der ESA verfolgen (einschließlich der Erwägungsgründe!)
  → insb. zu Artikel 28 (first batch) und Artikel 30 (second batch)
- Dienstleister risikoorientiert in **Cluster** zusammenfassen, daraus „Minimalverträge“ und unterschiedliche Steuerung ableiten
  → Gruppierung beispielsweise anhand der assoziierten Risiken, des Schutzbedarfs oder der betroffenen Prozesse
- **Zertifizierungen** und Prüfstandards bei der Dienstleisterauswahl stärker berücksichtigen
  → z. B. ISO 27001, ISO 9001 oder ISAE 3402
- Erweiterte **Dienstleister-Definition** beachten und analysieren, welche Dienstleister durch DORA neu dazukommen
  → z. B. Pflicht zum Einsatz von externen Testern zur Durchführung von bedrohungsorientierten Penetrationstests (TLPT)

1. Regulatorische Grundlagen und Einstieg in DORA
2. Auslagerungsmanagement und Providersteuerung
3. **PenTesting im Kontext von DORA**
4. Risikoorientierte Herangehensweise
5. Q&A

Testen der digitalen operationalen Resilienz (Kapitel IV)

Anforderung

- Die Fähigkeiten und Funktionen im Rahmen des IKT-Risikomanagements müssen in regelmäßigen Abständen überprüft werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren, gegen Cyberangriffe widerstandsfähig sind und jederzeit einsatzbereit sind. Falls erforderlich, sollen Schwachstellen, Mängel oder Lücken identifiziert und sofortige Abhilfemaßnahmen ergriffen werden. Das DORA ermöglicht eine angepasste Umsetzung der Anforderungen an die Stabilitätstests, abhängig von der Größe sowie dem Geschäfts- und Risikoprofil der Finanzunternehmen. Die Tests reichen von Standardtests der IKT-Werkzeuge und -Systeme für kleinere Unternehmen bis hin zu fortgeschrittenen Tests auf Basis von TLPT (Threat-Led Penetration Testing) für größere Finanzinstitute.

Handlungsbedarf

- Umfassende Auseinandersetzung mit allen Schwachstellen, die aus der Prüfung hervorgehen
- Umfassendes Programm zum Testen von IKT-Tools –und Systemen
- Umfang & Anforderungen an die bedrohungsorientierten Penetrationtests steigen
- Erhöhte Anforderungen und Nachweispflichten an (externe) Prüfer für Penetrationtest

Was ist der klassische Penetrationstest?

Hauptziel - Identifizierung möglichst aller Schwachstellen in einem System

Entstehende Nebeneffekte:

- Identifizierung von unsicheren Prozessen
- Steigerung der Effizienz eingesetzter Sicherheitsmaßnahmen
- Vermeidung von IKT-Vorfällen
- Bewertung vorliegender Risiken
- Je nach Szenario: Prüfung der Effektivität vorhandener Incident-Response-Verfahren

Kapitel IV, Testen der digitalen operationalen Resilienz

Art. 21 (1)

Vorhalten eines Testprogramms zur Prüfung der digitalen Belastbarkeit.

Art. 21 (2)

Das Testprogramm muss Testmaßnahmen im Einklang mit Art. 22 & 23 enthalten.

Art. 21 (3)

Das Testprogramm muss einen risikobasierten Ansatz verfolgen.

Art. 21 (4)

Tests müssen von unabhängigen Parteien durchgeführt werden.

Art. 21 (5)

Finanzunternehmen müssen ein adäquates Schwachstellenmanagement umsetzen.

Art. 21 (6)

Das Testprogramm muss kritische IKT-Systeme mindestens jährlich testen.

Art. 22 (1)

Das Testprogramm sieht für die Prüfung, Tests verschiedener Arten vor, jeweils dort wo angebracht:

- Schwachstellenbewertungen
- Open-Source-Analysen
- Netzsicherheitsbewertungen
- Gap Analysen
- Prüfungen der physischen Sicherheit
- Fragebögen und Scans von Softwarelösungen
- Quellcodeüberprüfungen
- Szenariobasierte Tests
- Kompatibilitäts- und Leistungstests,
- End-to-End-Tests
- Penetrationstests

Art. 22 (2)

Finanzunternehmen entsprechend Art. 2, (1), Punkt (f) & (g), müssen bei Einführungen oder Umstellungen kritischer Dienste Schwachstellenbewertungen durchführen.

Art. 23

Nähere Spezifizierung der Threat-Led-Penetration-Tests.

Art. 24

Eignung der Penetrationstester.

1. Regulatorische Grundlagen und Einstieg in DORA
2. Auslagerungsmanagement und Providersteuerung
3. PenTesting im Kontext von DORA
4. **Risikoorientierte Herangehensweise**
5. Q&A

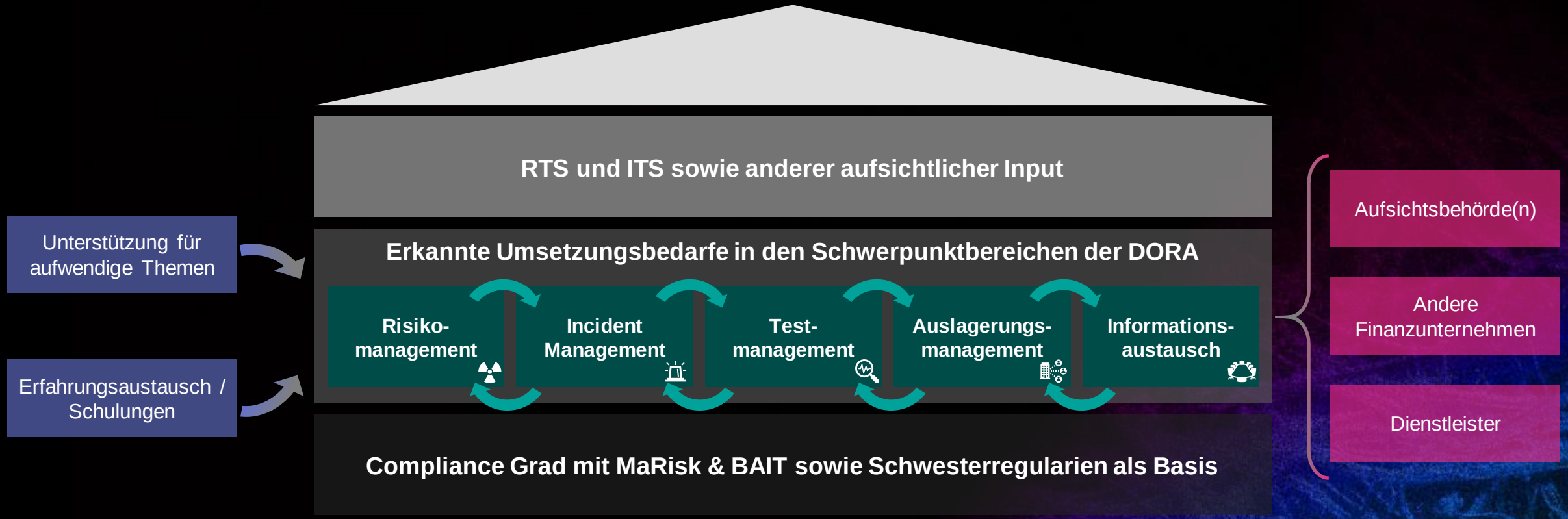
Praxiseinblick: Wie gehe ich bei der Einführung am Besten vor?

Entscheidend bei der Implementierung ist eine risikoorientierte Herangehensweise. Dabei sollte vom strategischen Gedanken geleitet ins Detail eingestiegen werden.

Während der Umsetzung sollten sich die Beteiligten über die aktuelle Regulatorik auf dem Laufenden halten, um etwaige Änderungen oder relevante Entwicklungen berücksichtigen zu können.

DORA: Evolution statt Revolution

Mit DORA werden wenig wirklich neue Themen eingeführt, vielmehr wird den Aspekten mehr Tiefe und vor allem mehr Breite eingeräumt.



Was sollten Sie heute mitnehmen?

Wir haben die drei unserer Meinung nach wichtigsten Punkte nochmal für Sie zusammengefasst.

Frühzeitige Auseinandersetzung mit den Inhalten & Start der **Umsetzung**, übrige regulatorische Entwicklungen peu à peu Einphasen

Vertragsgestaltung zeitnah angehen & **Dienstleister vorab in Kenntnis** setzen

Rechtzeitig **qualifizierte Tester** identifizieren & einbinden

Q&A

“Wichtig ist, dass man nie aufhört zu fragen.“

Albert Einstein

Kontaktmöglichkeiten

Pia Streicher
Senior Consultant IT-Security
bei ADWEKO Consulting GmbH

Carolin Neumeir
Teamlead Compliance & Security Consulting
bei matrix technology GmbH

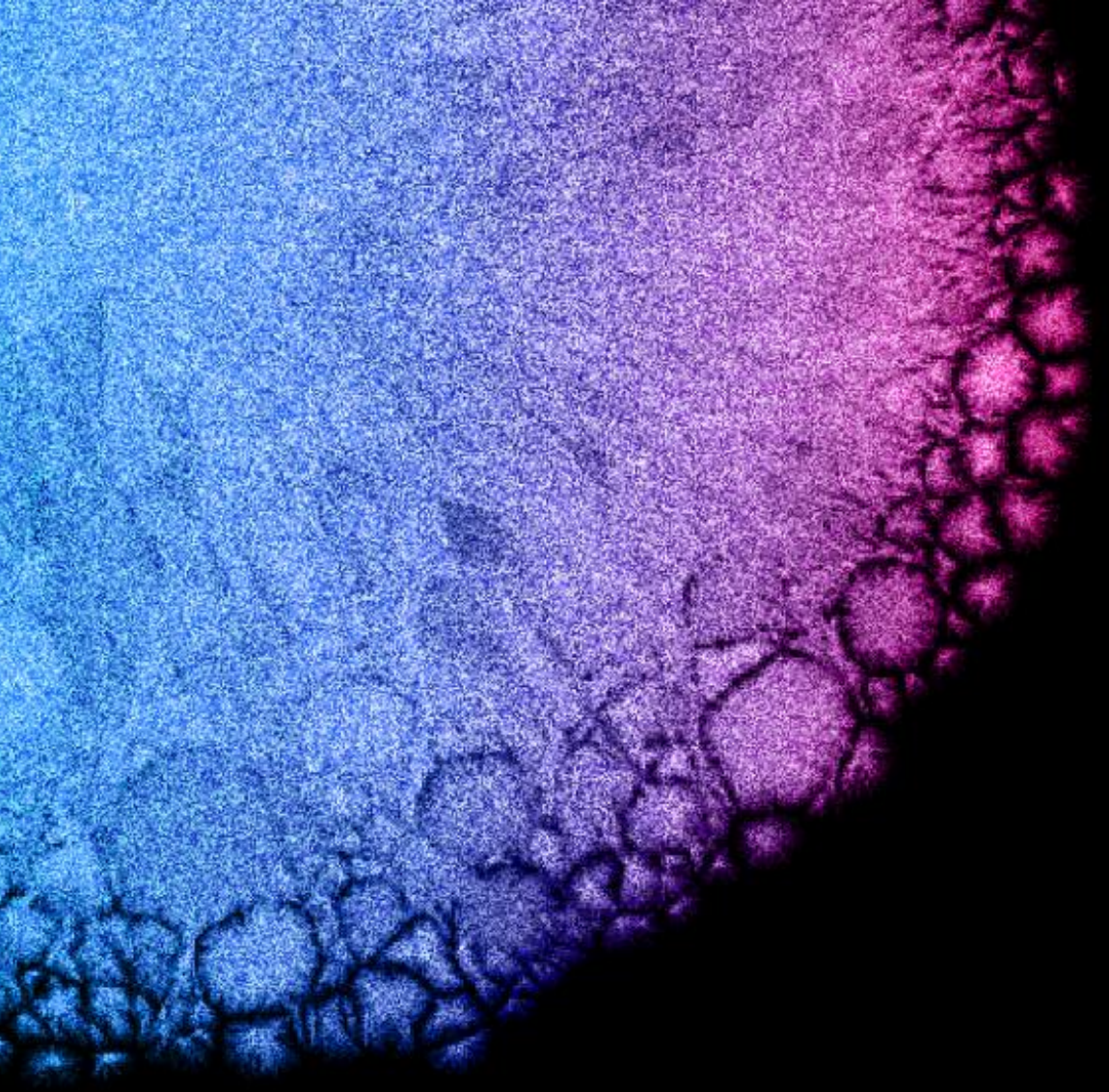
Johannes Rieder
Compliance Consultant
bei matrix technology GmbH

Jan Pawel Pasieka
Penetration Tester
bei e2 Security GmbH

Fränzis Horstmann
Account Operations Manager
bei X1F GmbH

Hannah Beck
Managing Marketing Expert
bei ADWEKO Consulting GmbH

Hendrik Dold
Director Corporate Communications
bei X1F GmbH



Vielen Dank für Ihre Aufmerksamkeit!


X1F