ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

OeNB

# WEBINAR ZU DORA
# 5.11.2024

# Begrüßung

# DORA: ANWENDBARKEIT AB 17.1.2025

**… eine neue Ära beginnt…**

## Unterstützung durch FMA / OeNB

- FMA-DORA-Website, inkl. Q&A
- Sektorale Veranstaltungen, Webinare
- DORA-Gap-Analyse

## Ziele

- Stärkung der IKT- und der Cybersicherheit
- Konsolidierung & Verbesserung der Anforderungen zu digitalen Risiken

## Geltungsbereich

- Breites Anwendungsspektrum
- Annähernd alle von der FMA beaufsichtigten Unternehmen

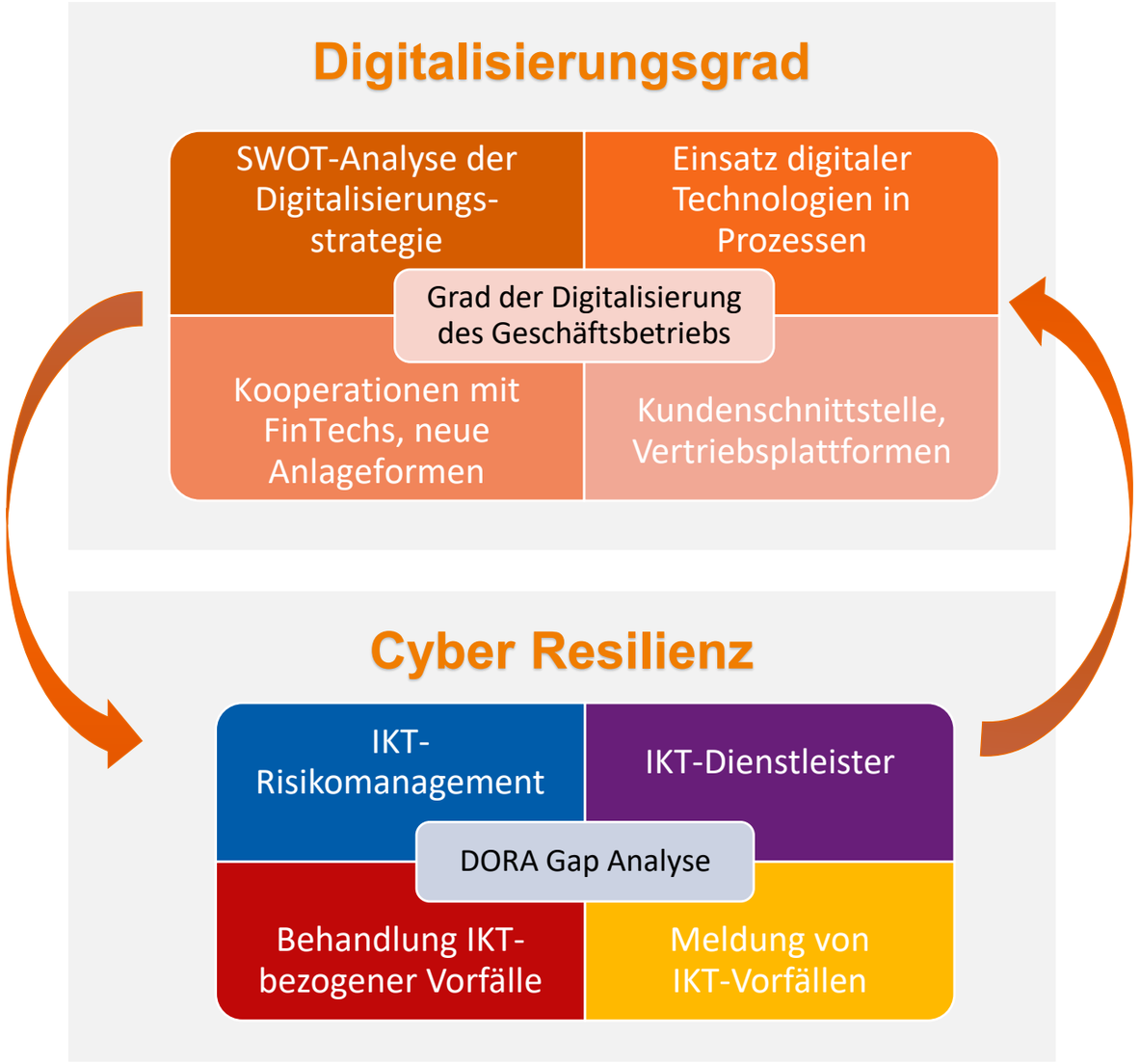
# AGENDA

- Begrüßung
  Michael Hysek
- Austrian Digital Finance Landscape: DORA Gap Analyse
  Stanislava Saria
- Regulatorischer Rahmen
  Sabine Balogh-Preininger
- DORA-Themen
  - IKT-Risikomanagement
    Andreas Griessner, Norbert Fröhlich
  - IKT-bezogene Vorfälle
    Raphaela Pöttinger, Alexander Natter, Ulrike Rhomberg
  - Testen der digitalen operationalen Resilienz
    Alexander Natter
  - Management des IKT-Drittparteienrisikos
    Alexander Kiennast, Karl Machan
  - Überwachungsrahmen für kritische IKT-Drittdienstleister
    Michael Mandelburger
- Meldungen in der Praxis
  Erich Obwexer
- Beantwortung der über Chat eingebrachten Fragen
- Ausblick

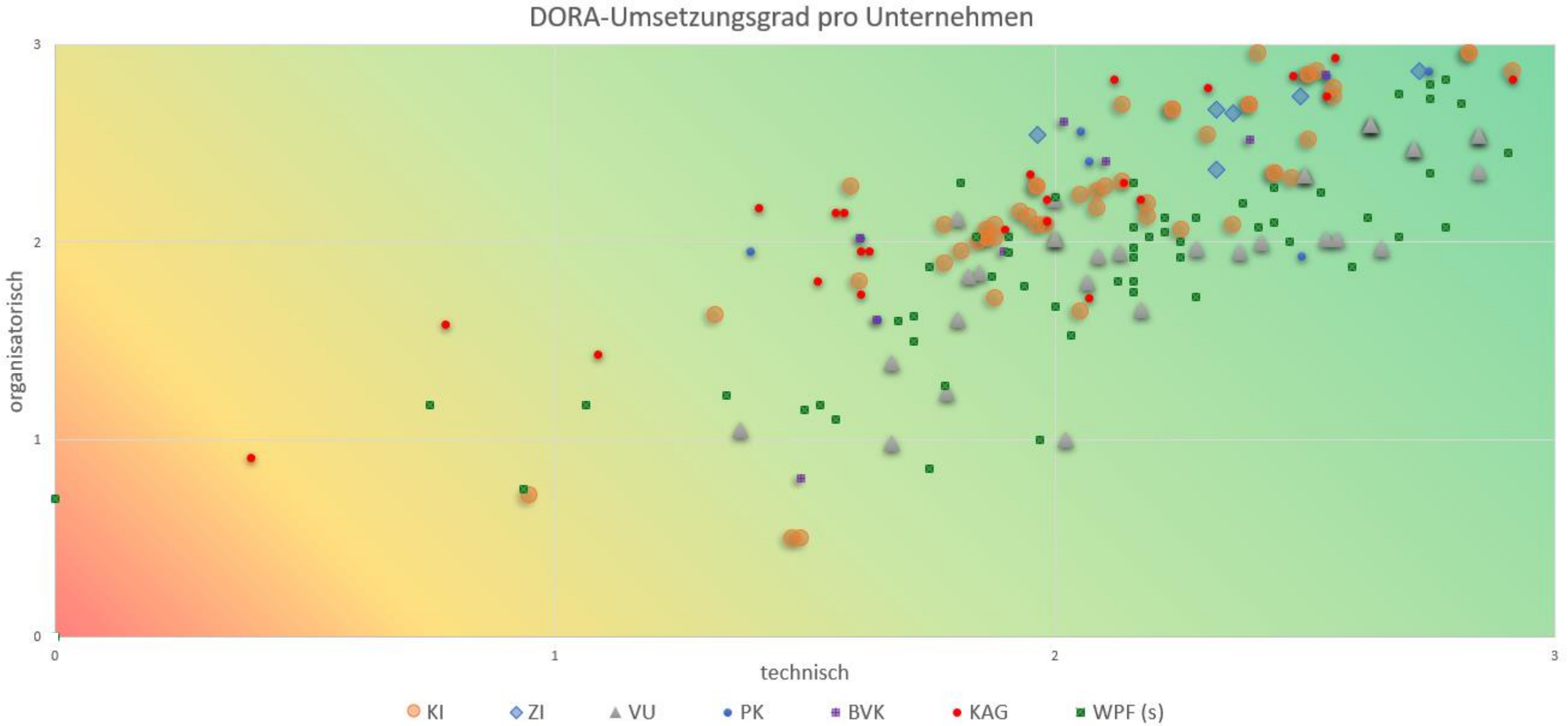
# DORA Gap Analyse 2024

# AUSTRIAN DIGITAL FINANCE LANDSCAPE 2024

- Inhalt:
  - den Grad der Digitalisierung des Geschäftsbetriebs sowie
  - die operationale Resilienz der Unternehmen am ö FM zu evaluieren.
- **Ziele (beaufsichtigte Unternehmen):**
  - Möglichkeit, die unternehmensinterne Implementierung der neuen regulatorischen Vorgaben kritisch zu hinterfragen und bei Bedarf gezielt weitere Verbesserungen vorzunehmen.
- **Ziele (FMA):**
  - die digitalisierungsgetriebenen Entwicklungen und Abhängigkeiten am Finanzmarkt in die (individuelle) **Risikobeurteilung** und die **Priorisierung** der Aufsichtsagenden einfließen zu lassen,
  - die Aufsichtsintensität der einzelnen beaufsichtigten Unternehmen risikoadäquat zu bestimmen und ggf.
  - zielgerichtete präventive Maßnahmen zu ergreifen und
  - die für den ö FM relevanten IKT-Dienstleister zu identifizieren.
- Durchführungszeitraum: Mai – November 2024

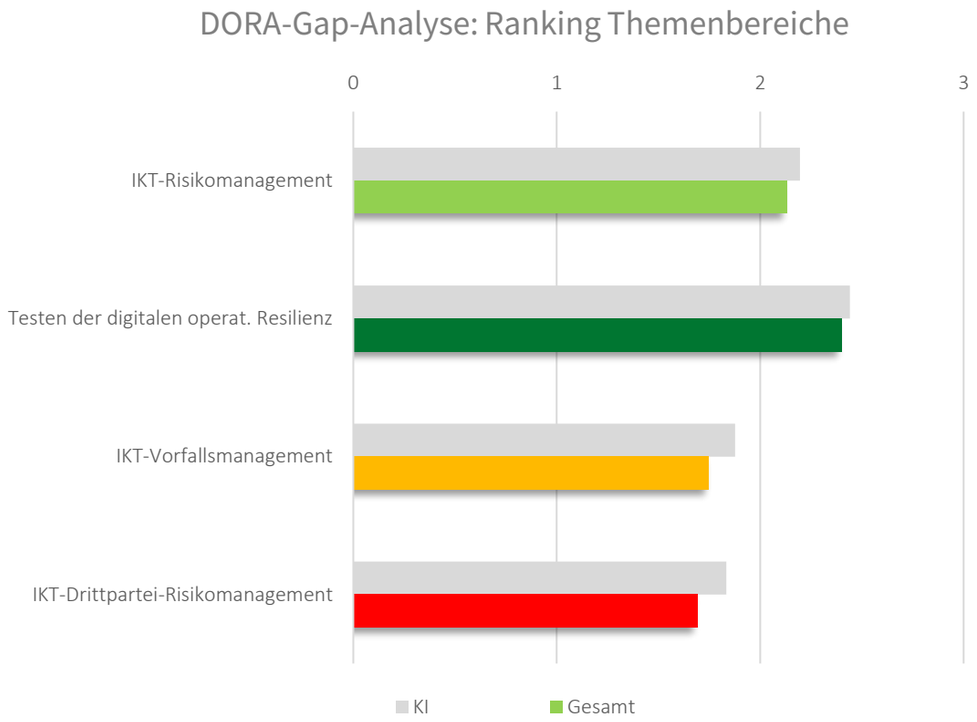


# 1) RANKING UNTERNEHMEN (FMA-DORA-GAP ANALYSE)

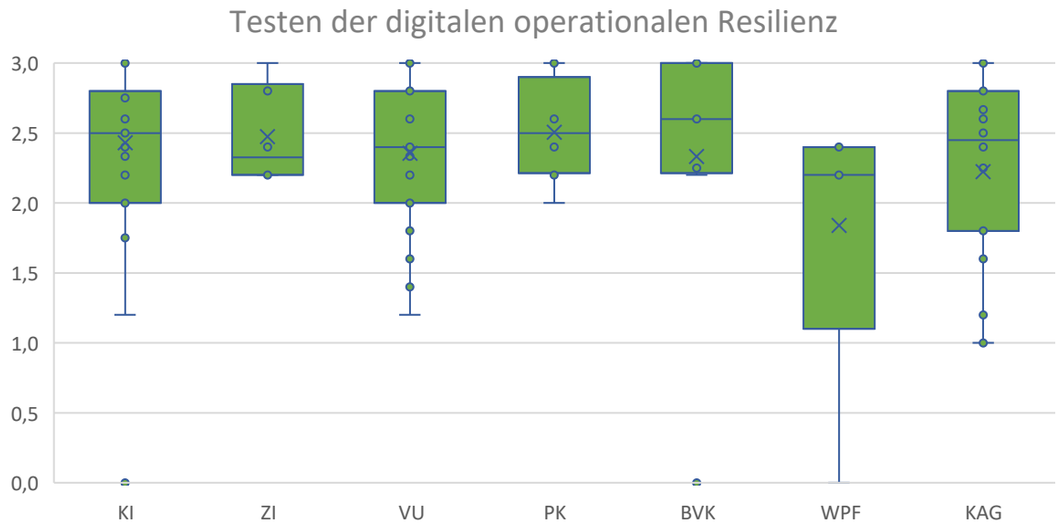


# 2) RANKING THEMENBEREICHE (FMA-DORA-GAP ANALYSE)

- Der größte Handlungsbedarf besteht beim
  - IKT-Drittpartei-Risikomanagement und
  - IKT-Vorfallsmanagement.

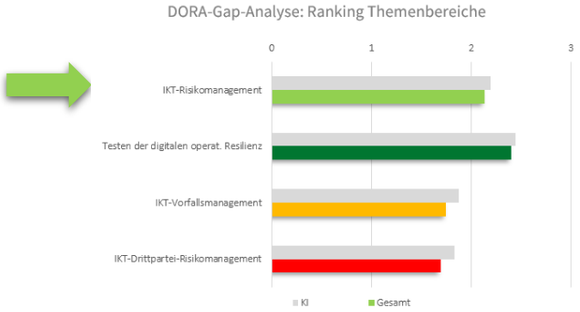



ABER auch beim Testen der digitalen operationalen Resilienz eine große Bandbreite bei der Vorbereitung der Umsetzung:

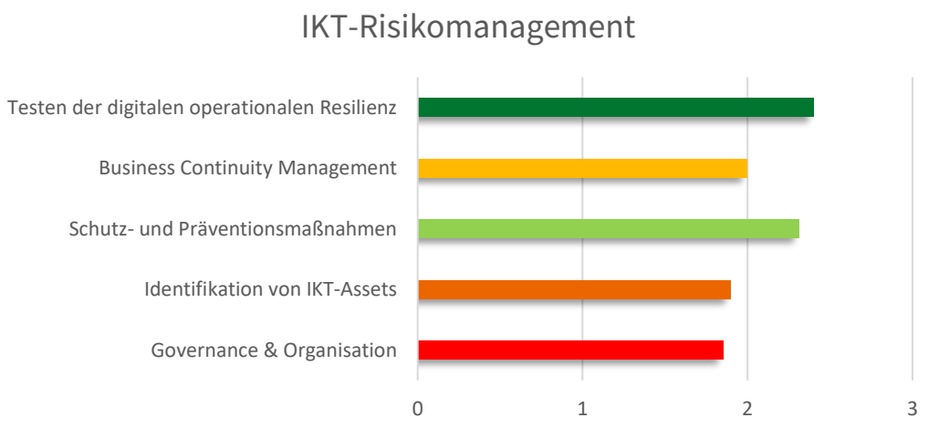


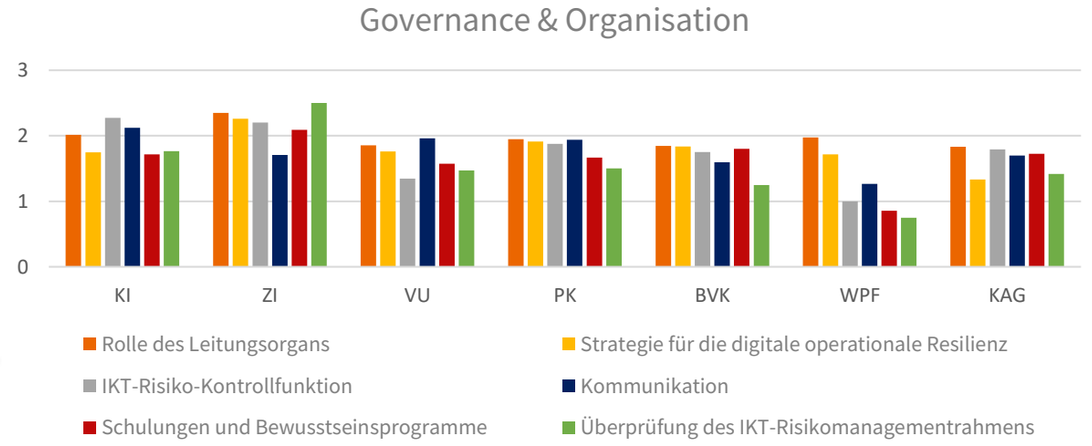

Quelle: FMA, Austrian Digital Finance Landscape 2024

# WO BESTEHEN DIE GRÖßTEN „GAPS“ ?
## A) „IKT-RISIKOMANAGEMENT“

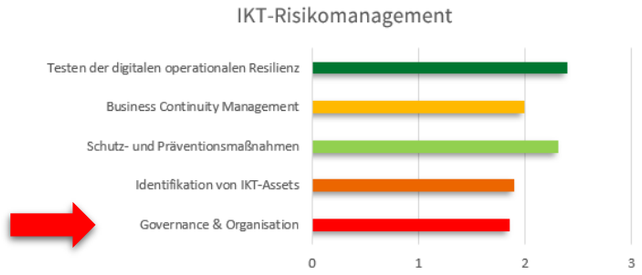



- Die DORA-Umsetzung war Mitte 2024 insb. in den folgenden Bereichen noch im Gange:
  - **Governance & Organisation**: In vielen Fällen waren u.a. noch dokumentarische Aufgaben und Freigaben der Geschäftsleitung offen.
  - Für die **Inventarisierung von IKT-Assets** waren zT noch umfangreichere technische Umsetzungen erforderlich.



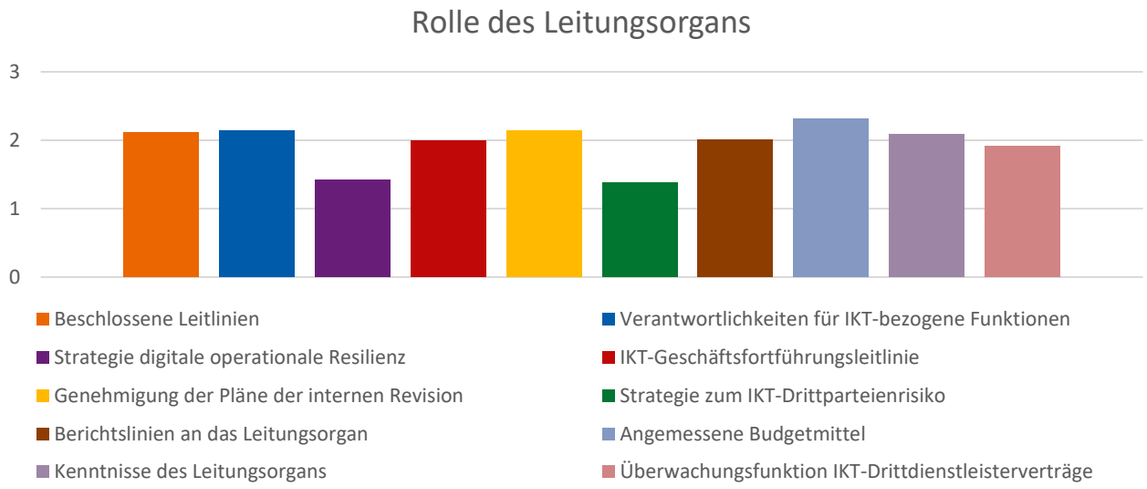




Quelle: FMA, Austrian Digital Finance Landscape 2024



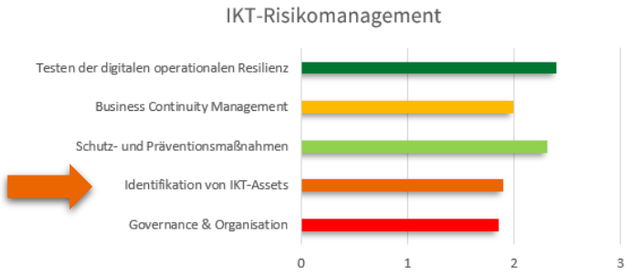

# A) IKT-RISIKOMANAGEMENT: GOVERNANCE & ORGANISATION

- Leitungsorgane haben bereits verbreitet **Leitlinien** beschlossen, die nunmehr auch Authentizität, welche auf die Vertrauenswürdigkeit der Datenquelle abstellt, explizit thematisieren. ✓
- Genehmigung der **Pläne der internen Revision** in Bezug auf die Prüfungen im IKT-Bereich für 2025 bzw. die darauffolgenden Jahre. ✓

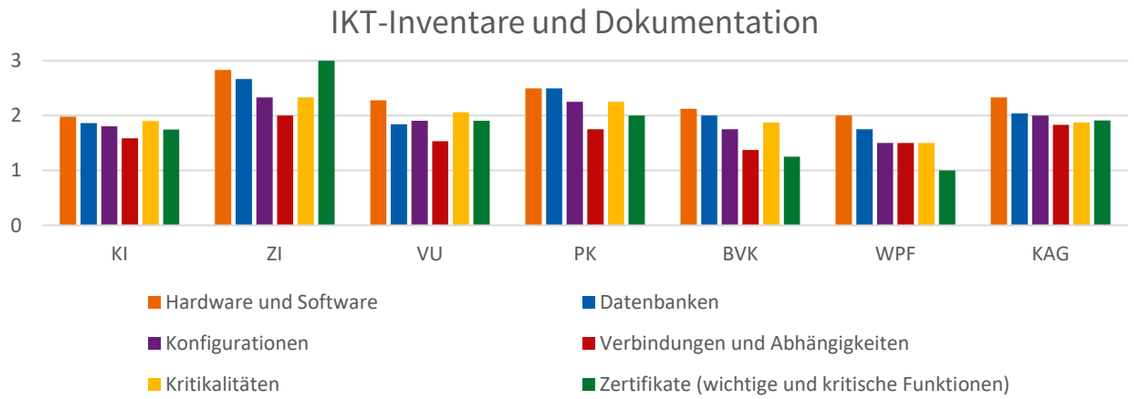



Quelle: FMA, Austrian Digital Finance Landscape 2024

- **Berichtslinien**, die es dem Leitungsorgan ermöglichen, ordnungsgemäß über IKT-Drittdienstleister, Erkenntnisse zu Tests der digitalen op. Resilienz, IKT-bezogene Vorfälle und die Aktivierung von IKT-Geschäftsfortführungs- und IKT-Reaktions- und Wiederherstellungsplänen informiert zu werden.
- Eine **Funktion zur Überwachung der Verträge mit IKT-Drittdienstleistern** ist teils noch einzurichten oder ein Mitglied der Geschäftsleitung ist mit dieser Funktion noch zu betrauen.
- **Schulungsprogramme:** Einbindung des Personals von IKT-Drittdienstleistern (Art 30 Abs 2 lit i iVm Art 13 Abs 6 DORA-Level 1: „Where appropriate“)
- **Regelmäßige Überprüfung des IKT-Risikomanagementrahmens** inkl. Bericht zum Review des IKT-RM inkl. Sicherheitsmaßnahmen / Bedrohungslage
- Ein **Kommunikationsplan** hat (je nach Sachlage) die Offenlegung zumindest schwerwiegender IKT-bezogener Vorfälle oder Schwachstellen gegenüber den folgenden Adressaten vorzusehen (Art 14 Abs 1 DORA-Level 1):
  a) den Kunden,
  b) den anderen Finanzunternehmen,
  c) der Öffentlichkeit.




# A) IKT-RISIKOMANAGEMENT: INVENTARISIERUNG VON IKT-ASSETS



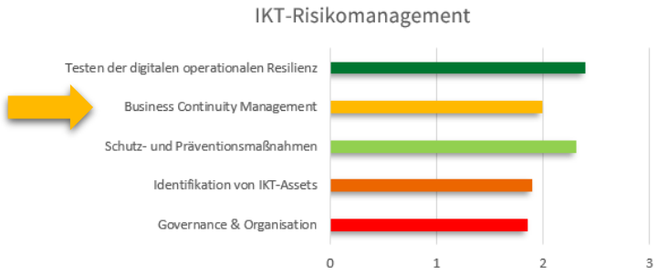

Quelle: FMA, Austrian Digital Finance Landscape 2024

- Die meisten Unternehmen verfügen bereits über umfassende **Hardware- und Softwareinventare** (dies ist schließlich die notwendige Basis für die meisten IKT-Sicherheitsmaßnahmen).

- Ab 17.1.2025 müssen die Inventare jedoch zusätzlich auch umfassen
  1) **Informations-Assets** (= vom Unternehmen genutzte Daten und Datenbanken)
  2) **Konfigurationen** von Informations- und IKT-Assets
  3) **Abhängigkeiten** zw. den verschied. Informations- und IKT-Assets
  4) **Kritikalitäten** der IKT-Assets und Informations-Assets und
  5) **Zertifikate** von IKT-Assets, die kritische oder wichtige Geschäftsfunktionen unterstützen (inkl. Info zu deren Ablauf, um ggf. eine Erneuerung zeitnah anstoßen zu können).

- Diese zusätzlich zu erfassenden Informationen sind oft noch nicht oder in unterschiedlichsten Systemen (z.B. Lizenzmanagement) vorhanden und noch zu ergänzen oder zu zentralisieren.
  - Nicht alle Unternehmen verfügen über ein **Inventarisierungstool**, in welchem all diese Informationen abbildbar und über automatisierte Schnittstellen aktualisierbar sind.

# A) IKT-RISIKOMANAGEMENT: BUSINESS CONTINUITY MANAGEMENT




- Als Teil des IKT-Risikomanagementrahmens sind auch angemessene IKT-Reaktions- und Wiederherstellungspläne festzulegen, die auch bestimmte vorgegebene Szenarien zu berücksichtigen haben, wie zB (Art 26 Abs 2 VO (EU) 2024/1774)

a) Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und redundanten Systeme;

b) Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt und in denen die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle eines relevanten IKT-Drittdienstleisters gebührend berücksichtigt werden;

c) teilweiser oder vollständiger Ausfall von Räumlichkeiten, insbesondere auch von Büro- und Geschäftsräumen, sowie von Rechenzentren;

d) erheblicher Ausfall von IKT-Assets oder der Kommunikationsinfrastruktur;

e) Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern oder von Mitarbeitern, die für die Gewährleistung der Betriebskontinuität zuständig sind;

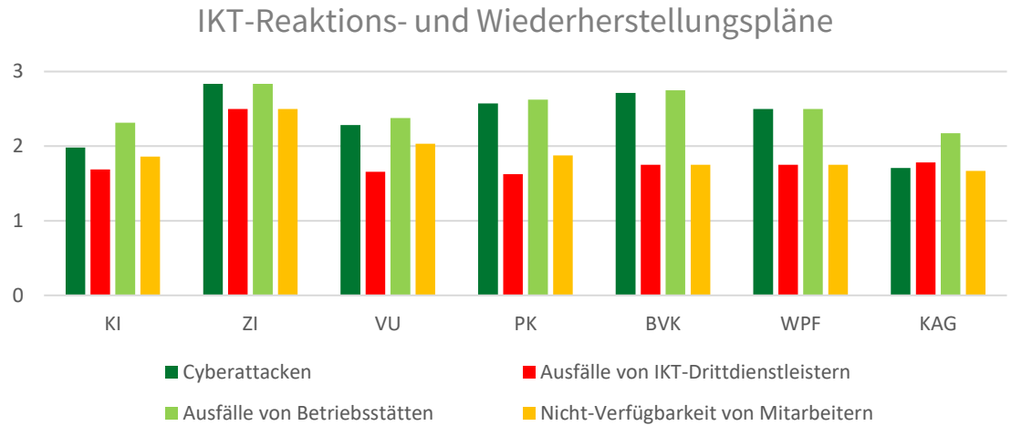
f) Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

g) Angriffe durch Insider;

h) politische und soziale Instabilität, sofern relevant auch im Sitzland des IKT-Drittdienstleisters und am Standort der Datenspeicherung und -verarbeitung;

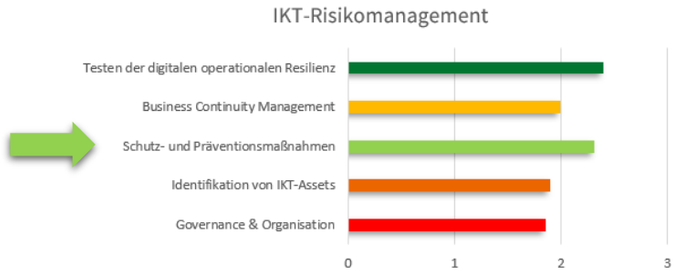
i) weitverbreitete Stromausfälle.

- Dabei zeigt sich, dass insb. Auswirkungen von Insolvenzen oder sonstigen Ausfällen eines relevanten IKT-Drittdienstleister noch nicht in diese Pläne einbezogen sind.




Quelle: FMA, Austrian Digital Finance Landscape 2024

# A) IKT-RISIKOMANAGEMENT:
# SCHUTZ- UND PRÄVENTIONSMAßNAHMEN





Quelle: FMA, Austrian Digital Finance Landscape 2024

**Entwicklungsfelder:**

Insbesondere Kryptographie und Schlüsselmanagement sowie Projekt- und Change-Management verlangen unter DORA eine umfassendere Auseinandersetzung als nach den gängigen IKT-Standards, die in der Praxis noch nicht voll abgebildet ist.

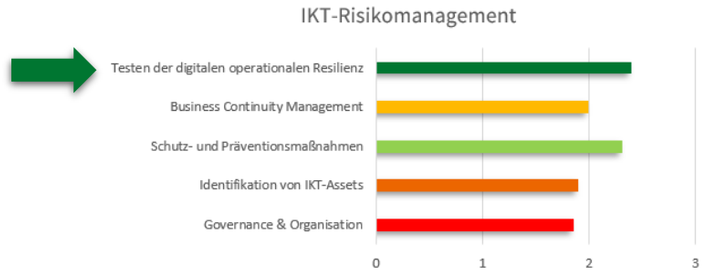
- **Verschlüsselung während der Verarbeitung (in use):** Ist diese nicht möglich, sind die Daten in einer getrennten und besonders geschützten Umgebung zu verarbeiten bzw. es sind andere geeignete Maßnahmen zu treffen (Art 6 Abs 2 VO (EU) 2024/1774).

- **Landkarte aller Netzwerkverbindungen und Datenflüsse:** Die Dokumentation und Aktualisierung der Landkarte inkl. Analyse der Datenströme befindet sich tw. noch in Umsetzung.

- **Systeme** zur aktiven Überwachung von Logs und **zur aktiven Alarmgenerierung** inkl. automatischer Warnmechanismen für MA, die für Reaktionsmaßnahmen zuständig sind. **Log-Halteperioden** sind teilweise noch zu definieren.

- Bei Zugriffskontrolle und Rechtemanagement besteht Anpassungsbedarf hinsichtlich der **Trennung kritischer Rollen**, um zu verhindern, dass sich Einzelpersonen durch Kombination mehrerer Zugriffsrechte unautorisierten Zugang zu kritischen IKT-Systemen oder Daten verschaffen können (teils noch zu viele Domain Admins eingesetzt).

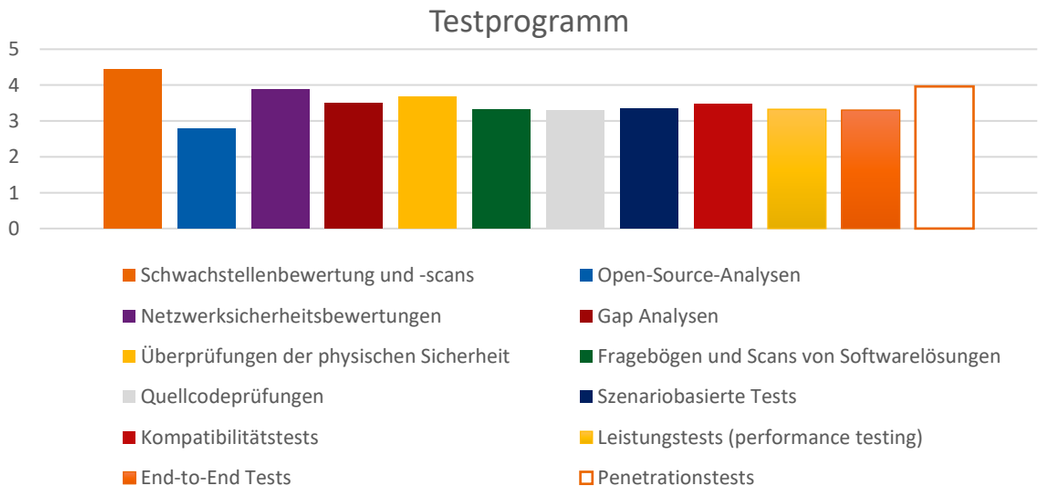
# A) IKT-RISIKOMANAGEMENT:
# TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ




- **Schwachstellenbewertungen und -scans** laufend auch bzgl. eines breiteren Scopes sind bereits Standard. Für IKT-Assets, die kritische oder wichtige Funktionen unterstützen, sind diese gemäß DORA mindestens einmal wöchentlich durchzuführen.
- **Penetrationstests** werden verbreitet laufend zumindest für Teilbereiche eingesetzt.
- **Quellcodeprüfungen** werden bei Anwendungen oft nicht offengelegt, weshalb bei der Einführung eine genaue Prüfung des Verkäufers erfolgt.
- **Szenariobasierte Tests** werden oft in Form von Table Top Exercises, im Rahmen von Penetrationstests oder für relevante Applikationen durchgeführt.
- **Kompatibilitätstests** werden etwa während der Entwicklung oder bei Neuanschaffungen im Rahmen von Projekten durchgeführt.
- **Leistungstests** werden zB in Folge von Performanceproblemen initiiert oder für relevante Applikationen durchgeführt.
- **Statische /dynamische Sicherheitstests** bei Scans von Softwarelösungen eingesetzt.
- **End-to-End Tests** nehmen meist IKT-Drittdienstleister für Applikationen vor.
- **Gap Analysen** etwa iZm ISO/IEC 27000 und Gruppenkontrollkatalogen.

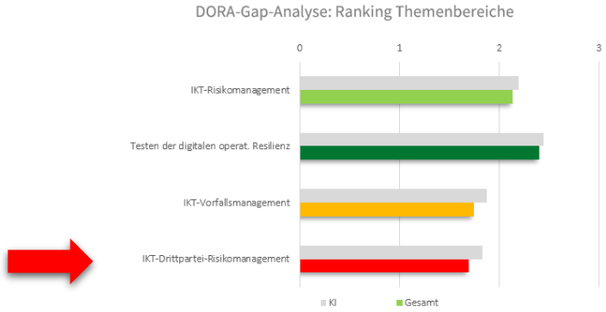
**Entwicklungsfelder:**

- **Risikobasierter Ansatz:** Verfahren zur Priorisierung, Klassifizierung und Behebung von identifizierten Problemen sind tw. noch anzupassen.
- **Testfrequenz:** mindestens jährliche Tests von IKT-Systemen und -Anwendungen, die kritische / wichtige Funktionen unterstützen

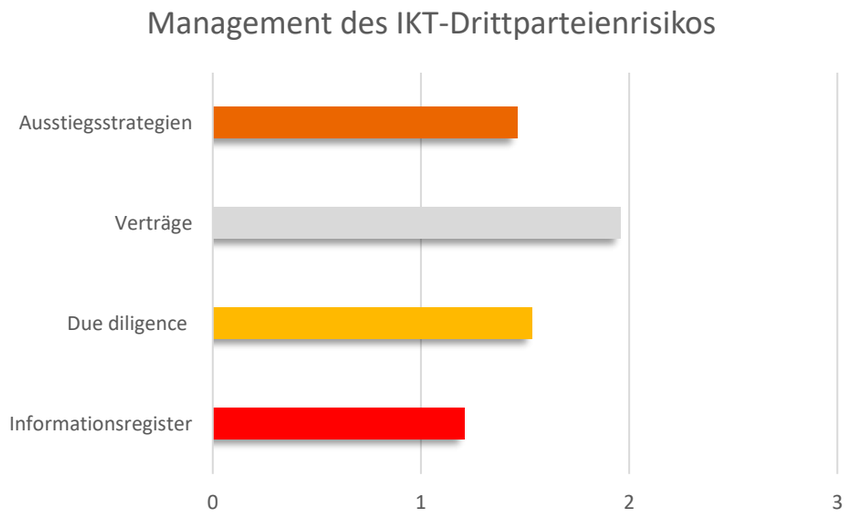



Quelle: FMA, Austrian Digital Finance Landscape 2024

# B) IKT-DRITTPARTEI-RISIKOMANAGEMENT




- In allen Phasen der Einbindung einer Drittpartei (vor, während und nach Bezug einer IKT-Dienstleistung) sind Maßnahmen zu setzen und ist die Dienstleistung im Rahmen des Risikomanagements aktiv zu erfassen.
- Das Informationsregister wird als größte Herausforderung gesehen.

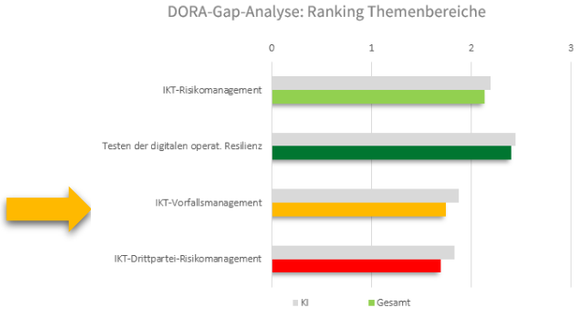



Quelle: FMA, Austrian Digital Finance Landscape 2024

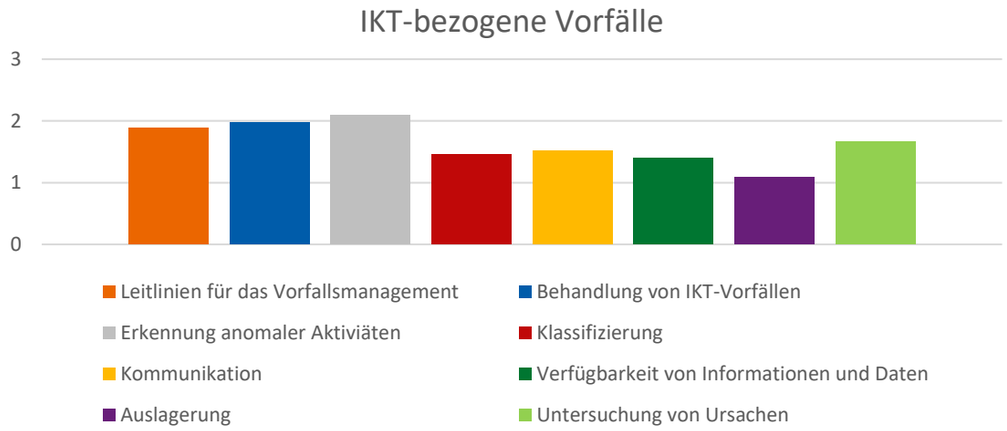
**Entwicklungsfelder:**

- **Due Diligence:** Kriterien, die vor Vertragsabschluss mit einem IKT-Dstl zu prüfen sind (zB ausreichende Informationssicherheit bei Dstl), die Ausübung der Auditrechte, die Überwachung der ganzen Subdienstleisterkette.
- **Verträge mit IKT-Dstl:** DORA definiert Mindestbestandteile, welche in IKT-Dienstleisterverträgen enthalten sein müssen. Für Dienstleistungen, welche kritische und wichtige Funktionen betreffen, kommt ein erweiterter Katalog zur Anwendung.
  - noch nicht vollumfänglich in bestehenden Verträgen berücksichtigt
- **Ausstiegsstrategien:** teilweise Tests und Übungen (zB Tabletop-Exercises) vorgesehen: Good Practice, um Nutzen aus den Ausstiegsplänen zu ziehen.
- **Informationsregister:** Bislang meist risikobasiert vorgegangen, um zuerst kritische Dienstleistungen in vollem Umfang abbilden zu können.
  - Etliche Auslegungsfragen offen (zB wann liegt eine „IKT-Dienstleistung“ gemäß Art 3 Z 21 iVm Art 28 DORA vor?).

# C) IKT-BEZOGENE VORFÄLLE




- Bezüglich des Incident Managements verfügen Finanzunternehmen über ausgeprägte Erfahrung hinsichtlich der Erkennung anomaler Aktivitäten, zB aus Logs oder aus potentiellen internen und externen Cyberbedrohungen.




Quelle: FMA, Austrian Digital Finance Landscape 2024

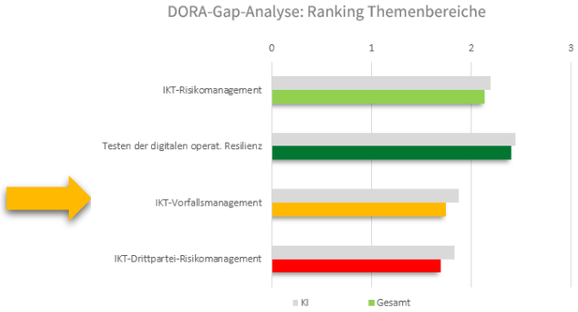
**Entwicklungsfelder:**

- Bei Kommunikation ist der **Prozess zur zeitgerechten Meldung** von schwerwiegenden IKT-bezogenen Vorfällen (inkl. freiwilliger erheblicher Cyberbedrohungen) an die zuständige Behörde meist noch zu definieren.

- Die **Verfügbarkeit der Meldeinhalte** zu Erst-, Zwischen- und Abschluss-meldungen schwerwiegender IKT-bezogener Vorfälle (inkl. wiederholt auftretender Vorfälle) ist teilweise noch zu evaluieren bzw. sicherzustellen.

- **Nachträgliche Prüfungen der Vorfälle**, um die Ursachen zu untersuchen und erforderliche Maßnahmen zu definieren (forensische Analysen etc.).

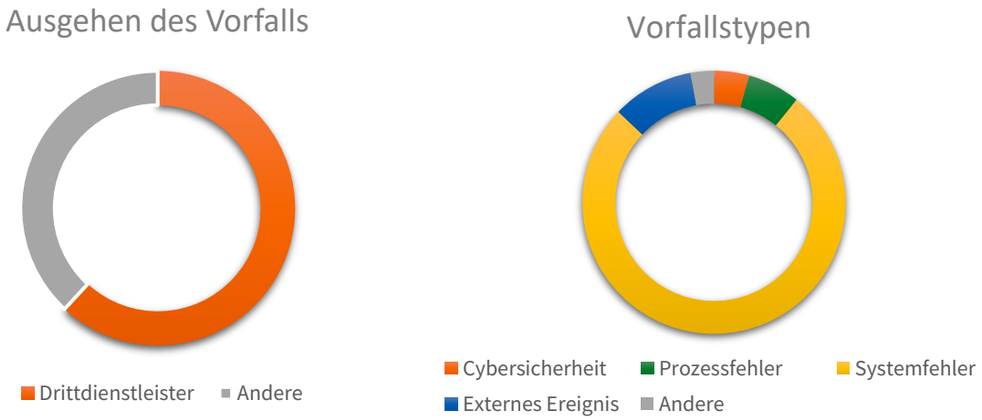
# REALITY CHECK




## Cyber-Vorfälle:

- Nach wie vor gehen im Aggregat **2/3 der Vorfälle** bei beaufsichtigten Unternehmen von **IKT-Drittdienstleistern** aus.
  - Das veranschaulicht die Sinnhaftigkeit der neuen DORA-Vorgaben zu IKT-Drittdienstleistern und zur Implementierung eines Überwachungsrahmens für kritische IKT-Drittdienstleister.

- Die meisten Vorfälle sind auf **Systemfehler** zurückzuführen: 2023 waren das rd 75% und 2024 rd 80%.




Quelle: FMA, Austrian Digital Finance Landscape 2024

## Cyberversicherung:

- Die **von der FMA beaufsichtigten Unternehmen** haben 2023 insgesamt rd. **41 Mio. Euro** an Prämien für abgeschlossene Cyberversicherungen gezahlt. Diese können zum Großteil dem KI-Sektor zugeordnet werden.
  - Abgesehen von den Sach- und Assistance-Leistungen betrugen Versicherungsleistungen 2023 rd. 71 Tsd. Euro.

- Die von den öVU für den **expliziten Cyberrisikoschutz** verrechneten Prämien beliefen sich 2023 auf **12 Mio. Euro** (Anstieg seit 2022 um 12%).
  - Trotz des erneuten Anstiegs ist der Anteil des Cyberversicherungsmarkts am Gesamtprämienvolumen 2023 iHv 22 Mrd. Euro gering.
  - Abgesehen von den Sach- und Assistance-Leistungen lagen die Versicherungsleistungen der ö VU 2023 bei rd. 1,3 Mio. Euro und haben sich im Vergleich zu 2022 um 3% erhöht.

# Regulatorischer Rahmen

# DORA-ENTWICKLUNG (EXEMPLARISCH)

# RECHTLICHE RAHMENBEDINGUNGEN

## DORA-VO & DORA-RL

| DORA-VO & DORA-RL | Anwendbarkeit |
|---|---|
| **DORA-Verordnung** | |
| DORA-VO | 17.01.2025 vom |
| **DORA-Richtlinie** | |
| DORA-RL | 14.12.2022 |

## DORA-Vollzugsgesetz

| AT: | Inkrafttreten |
|---|---|
| **DORA-Vollzugsgesetz** | |
| DORA-VG | 17.01.2025 |
| | **Ende Begutachtung** |
| **FMA-Verordnungen** | |
| FMA-IPV | 15.11.2024 |
| FMA-GebV | 15.11.2024 |

## EU-SCICF

| EU-SCICF (Behandlung in DORA-Gremien): | Frist |
|---|---|
| **EU-Systemic Cyber Incident Coordination Framwework** | |
| Basis: ESRB-EU-SCICF-Empfehlung (ESRB/2021/17) | |
| A1 ESA-Final Report on EU-SCICF-development | 16.07.2024 |
| A2 ESA-Final Report on impediments, barriers | 16.07.2025 |
| C EC-Final Report on changes to Union legal framework | 16.01.2026 |

## DORA-Spezifizierungen: Delegierte VO, RTS, ITS, Guidelines

### DORA-Spezifizierungen: RTS, ITS, Guidelines

| DORA-Art. | Thema | Frist (für die Vorlage an die EK) | | | |
|---|---|---|---|---|---|
| | | Sep 23 | Jan 24 | Jul 24 | Jan 25 |
| | **IKT-Risikomanagement** | | | | |
| Art. 15 | Delegierte VO_weitere Harmonisierung des IKT-Risikomanagements | | ✓ | | |
| Art. 16 | Delegierte VO_vereinfachter IKT-Risikomanagementrahmen | | ✓ | | |
| | **Testen der digitalen operationalen Resilienz** | | | | |
| Art 26 (11) | Final Draft RTS zu bedrohungsorientierten Penetrationstests | | | ✓ | |
| | **IKT-bezogene Vorfälle** | | | | |
| Art 11 (11) | Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste | | | ✓ | |
| Art 18 (3) | Delegierte VO_Klassifizierung von IKT-bezogenen Vorfällen | | ✓ | | |
| Art 20a | Final Draft RTS zur Meldung schwerwiegender IKT-bezogener Vorfälle | | | ✓ | |
| Art 20b | Final Draft ITS zu Berichtsdetails zu IKT-bezogenen Vorfällen | | | ✓ | |
| Art 21 | - Bericht zur Zentralisierung der Meldungen | | | | in Arbeit |
| | **Management des IKT-Drittparteienrisikos** | | | | |
| Art 28 (9) | Final Draft ITS zum Informationsregister zu vertraglichen Vereinbarungen zu IKT-Dienstleistungen | | EK-Ablehnung 3.9.2024 | | |
| Art 28 (10) | Delegierte VO_Leitlinie für die Nutzung von IKT-Dienstleistungen | | ✓ | | |
| Art 30 (5) | Final Draft RTS on subcontracting ICT services (2. Policy Batch an EK) | | | ~ | |
| | **Überwachungsrahmen für kritische IKT-Drittdienstleister** | | | | |
| Art 31 | Delegierte VO_Kriterien für die Einstufung von CTPPs | ✓ | | | |
| Art 32 (7) | Leitlinien für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden zur Struktur des Überwachungsrahmens | | | ✓ | |
| Art 41 | Final draft RTS zur Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten (zB zu von IKT-Dienstleistern bereitzustellenden Informationen) und Final draft RTS zu JETs (Mandat der HLGO) | | | ✓ | |
| Art 43 (2) | Delegierte VO CTPP-Gebühren | ✓ | | | |

# ALLGEMEINE FRAGEN ZU DORA: Q&A

## Anwendungsbereich

**1) Gilt DORA auch für Leasingunternehmen?**

1) Diese unterliegen nicht dem Anwendungsbereich gem. §§ 2 und 3 DORA-Vollzugsgesetz.

Abhängig von Art und Umfang der Einbindung der hier angesprochenen Gesellschaften in die IT-Infrastruktur des Konzerns kann die Umsetzung einzelner Erfordernisse auch für ursprünglich nicht von Scope der DORA erfasste Unternehmen erforderlich sein. Es sollte vermieden werden, dass niedrige Standards bei tief in die IT-Prozesse und -Systeme eines Konzerns integrierten Einheiten die Erfüllung der Erfordernisse für die der DORA unterliegenden Einheiten gefährden.

Ausgestaltungen der Schnittstellen wäre zu klären! So sieht zB Art 8 DORA-VO vor, dass Finanzunternehmen kontinuierlich alle Quellen für IKT-Risiken ermitteln und Cyberbedrohungen und IKT-Schwachstellen bewerten.

Je nach Ausgestaltung der Schnittstellen, könnten sich auch weitere Anforderungen, zB bezüglich Alarmschwellen und -kriterien zur Erkennung von anomalen Aktivitäten oder zu IKT-bezogenen Vorfällen ergeben (Art 17 DORA-VO).

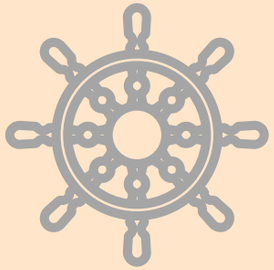
# DORA-THEMEN

**IKT-Risikomanagement**

**IKT-bezogene Vorfälle**

**Testen der digitalen operationalen Resilienz**

**Management des IKT-Drittparteienrisikos**



**Überwachungsrahmen für kritische IKT-Drittdienstleister**

**Informationsaustausch & Notfallübungen**

**Proportionalität:**

- Allgemeines Proportionalitäts-prinzip (generell & speziell)
- Vereinfachte IKT-RM-Vorgaben

# DORA-Themen: IKT-Risikomanagement

# IKT-RISIKOMANAGEMENT

- Governance und Organisation (Art. 5)
- IKT-Risikomanagementrahmen (Art. 6)
- IKT-Systeme, -Protokolle und –Tools (Art. 7)
- Identifizierung (Art. 8)
- Schutz und Prävention (Art. 9)
- Erkennung (Art . 10)
- Reaktion und Wiederherstellung (Art. 11)
- Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung (Art. 12)
- Lernprozesse und Weiterentwicklung (Art. 13)
- Kommunikation (Art. 14)
- Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risiko-management (Art. 15)
- Vereinfachter IKT-Risikomanagementrahmen (Art. 16)

# IKT-RISIKOMANAGEMENT: DELVO (EU) 2024/1774

## TITEL II - HARMONISIERUNG V. PROZESSEN U. RICHTLINIEN F. IKT-RISIKOMANAGEMENT

- Richtlinien, Verfahren, Protokolle u. Tools
  - Richtlinien, Verfahren u. Tools
  - IKT-Risikomanagement
  - Management von IKT Assets
  - Verschlüsselung u. Kryptografie
  - IKT-Betriebssicherheit
  - Netzwerksicherheit
  - IKT-Projekt und Änderungsmanagement
  - Physische Sicherheit / Umweltereignisse
- RL f. Personalpolitik u. Zugangskontrolle
- IKT-Vorfallserkennung und Reaktion
- IKT-Geschäftsfortführung
- Bericht Überprüfung IKT-Risikomanagement-rahmen

## TITEL III: VEREINFACHTER IKT-RM-RAHMEN

- Vereinfachter IKT-Risikomanagementrahmen
- Minimierung der Auswirkung von IKT-Risiken
- IKT-Geschäftsfortführung
- Überprüfung vereinfachter IKT-Risiko-managementrahmen

# IKT-RISIKOMANAGEMENT: Q&A

1/2

1) **Wie findet Proportionalität in DORA bzgl. des IKT-Risikomanagements Anwendung?**

2) **Braucht jedes Unternehmen eine IKT-Risiko-Kontrollfunktion?**

3) **Kann die IKT-Risiko-Kontrollfunktion durch den CISO wahrgenommen werden?**

4) **Wie ist die Funktion eines externen CISO zu bewerten - in Hinblick auf die IKT-Risiko-Kontrollfunktion?**

1) Auf mehreren Ebenen:
   - Ausnahmen für Kleinstunternehmen
   - Vereinfachter Risikomanagementrahmen gem. Art. 16 DORA
   - Risikobasierter Ansatz: vgl. Art. 1 RTS Risikomanagement (DelVO 2024/1774)
   - Allgemeiner Grundsatz der Verhältnismäßigkeit Art. 4 Abs. 1 DORA

2) Ja, außer es handelt sich um ein Kleinstunternehmen, oder es ist der vereinfachte Risikomanagementrahmen anwendbar (vgl Art. 6 und 16 DORA; ErwG 43 DORA).

3) Ja, die Erfordernisse aus Art. 6 Abs. 4 DORA sind zu berücksichtigen (insb. drei Verteidigungslinien).

4) Es ist zu prüfen ob die Aufgaben des externen CISO, die Aufgaben aus der Kontrollfunktion gem. Art. 6 Abs. 4 DORA abdecken.
   - Bei Auslagerungen sind die jeweiligen sektorspezifischen Bestimmungen einzuhalten und zu berücksichtigen.
   - Konkrete institutsspezifische Ausgestaltungen wären im Einzelfall zu beurteilen.

# IKT-RISIKOMANAGEMENT: Q&A

**2/2**

5) **Was könnte als DORA-Notfall oder Krise verstanden werden?**

6) **Darf das Unternehmen selbst klassifizieren, ob Änderungen an IKT-Funktionen/Assets wesentlich sind (Art. 8 Abs. 3 DORA)?**

7) **Wie wird die Auswirkungstoleranz definiert?**

8) **Müssen bei extern, exklusiv für die Bank entwickelten, IKT-Systemen statische und dynamische Tests durchführbar sein?**

5) In Art. 26 Abs. 2 RTS Risikomanagement (DelVO 2024/1774) sind Szenarien beschrieben: bspw. Cyberangriffe, teilweiser Ausfall in IKT-Assets/Kommunikation, Stromausfälle.

6) Ja, die Entscheidung ist vom Unternehmen selbst zu treffen. Ein gewisser Bezug zu den Kritikalitätsklassifizierungen der betroffenen IKT-Funktionen/Assets wäre bei dieser Einschätzung zu erwarten.

7) Der Ausdruck „Auswirkungstoleranz mit Blick auf IKT-Störungen (Art. 6 Abs. 8 lit. b DORA) bezieht sich aus Sicht der FMA auf alle IKT-Störungen und inkludiert auch IKT-Vorfälle. Es sind monetäre (zB Kosten für Vorfälle), als auch nicht monetäre Auswirkungen (zB Verfügbarkeit der Daten) zu untersuchen und zu berücksichtigen.

8) Finanzunternehmen implementieren Richtlinien für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen. Hierbei sind sämtliche in Art. 16 RTS Risikomanagement (DelVO 2024/1774) geforderten Elemente zu berücksichtigen – ein vergleichbarer Standard ist sicherzustellen.

Weitere Details finden Sie auf der Homepage der FMA unter Aufsicht/Querschnittsthemen/DORA/Risikomanagement

# DORA-Themen:
# IKT-bezogene Vorfälle

# IKT-BEZOGENE VORFÄLLE

- Prozess für die Behandlung IKT-bezogener Vorfälle (Art. 17)
  - Dokumentation von IKT-bezogenen Vorfällen
  - Zuständigkeiten
  - Kommunikationspläne
  - Eskalation
  - Verfahren für Gegenmaßnahmen

- Klassifizierung von IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen (Art. 18)
  - Kriterien zur Klassifizierung von Vorfällen in DelVO (EU) 2024/1772 geregelt
  - Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554

# IKT-BEZOGENE VORFÄLLE

## KLASSIFIZIERUNGSANSATZ

| Verpflichtendes Kriterium |
| --- |
| Kritikalität der betroffenen Dienste |

& zusätzlich entweder

| I. Erfolgreicher, böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme, sofern dieser zu Verlusten von Daten führen kann. |
| --- |

| II. Überschreitung der Schwellenwerte von mindestens zwei weiteren Kriterien: |
| --- |
| Betroffene Kund:innen, finanzielle Gegenparteien oder Transaktionen |
| Reputationsschaden |
| Dauer und Ausfallzeiten des Vorfalls |
| Geografische Ausbreitung |
| Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten |
| Wirtschaftliche Auswirkungen |

# IKT-BEZOGENE VORFÄLLE

| Kriterium DelVO (EU) 2024/1772 | Schwellenwerte |
|---|---|
| **Kritikalität der betroffenen Dienste** | **Jede Auswirkung** auf kritische Dienste<br>a) zur Unterstützung kritischer oder wichtiger Funktionen<br>b) die eine Konzession oder Registrierung erfordern bzw. beaufsichtigt werden<br>c) sofern ein erfolgreicher, böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme vorliegt |
| **Verluste von Daten** | **a) Jede Auswirkung** auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten, sofern dies negative Auswirkungen auf die Umsetzung der Geschäftsziele oder Erfüllung der regulatorischen Anforderungen hat<br>**b) Jeder erfolgreiche, böswillige und unbefugte Zugriff auf Netz- und Informationssysteme**, welcher **nicht unter Punkt a)** fällt und zu einem **Datenverlust führen kann** |

# IKT-BEZOGENE VORFÄLLE

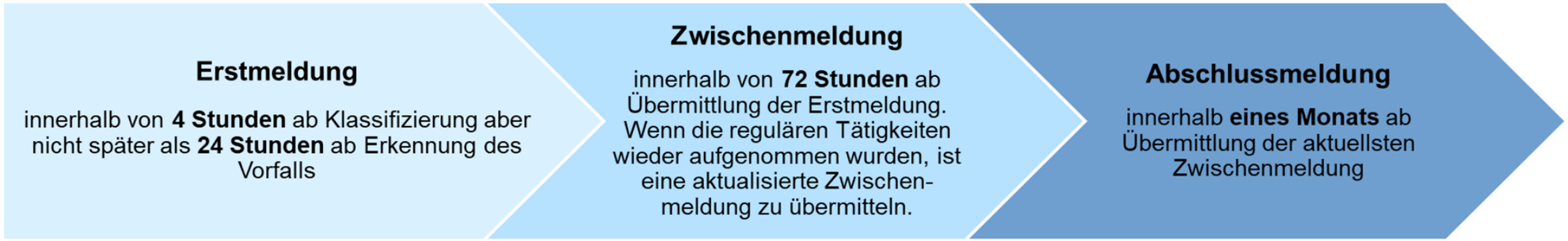
| Kriterium DelVO (EU) 2024/1772 | Schwellenwerte |
|---|---|
| **Kunden, finanzielle Gegenparteien und Transaktionen** | a) > 10 % aller Kunden, welche diesen Service nutzen<br>b) > 100.000 Kunden<br>c) > 30 % aller zentralen Gegenparteien<br>d) > 10% der üblichen durchschnittlichen Anzahl an Transaktionen<br>e) > 10% des üblichen durchschnittlichen Transaktionsvolumens<br>f) alle festgestellten Auswirkungen auf Kunden oder finanzielle Gegenparteien, die vom Finanzinstitut als relevant eingestuft werden |
| **Dauer und Ausfallzeiten** | ➢ > 24 Stunden<br>➢ > 2 Stunden bei kritischen Funktionen, sofern keine kürzere Dauer aufgrund anderer EU-Regularien vorgeschrieben ist |
| **Wirtschaftliche Auswirkungen** | ➢ die direkten und indirekten Bruttokosten und -verluste überschreiten **EUR 100 000** oder werden voraussichtlich **EUR 100 000** überschreiten |

# IKT-BEZOGENE VORFÄLLE

| Kriterium DelVO (EU) 2024/1772 | Schwellenwerte |
|---|---|
| **Geografische Ausbreitung** | ➢ Liegt vor (Betroffenheit von mindestens zwei MS) |
| **Reputationsschäden** | Grad der Bekanntheit des Vorfalls beispielsweise:<br>➢ Medienaufmerksamkeit<br>➢ Nichterfüllung der aufsichtlichen Anforderungen<br>➢ Kundenverlust, mit Auswirkungen auf das Geschäft |
| **NEU:**<br>**Recurring Incidents**<br><br>*Kein Kriterium ieS.* | ➢ Sofern einzelne Vorfälle nicht als kritisch eingestuft werden, jedoch im Zeitraum der letzten **sechs Monate mindestens zwei Mal** aufgetreten sind und die **gleiche Grundursache** aufweisen<br>➢ Gilt nicht für Institute, welche dem simplifizierten IKT-RMF unterliegen, sowie Kleinstunternehmen |

# IKT-BEZOGENE VORFÄLLE

- Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen (Art. 19) & RTS und ITS zur Präzisierung der Meldung
  - Zuständige Behörde: FMA
    - Meldeweg: FMA Incoming-Plattform
    - Formular für die Einmeldung
    - Weiterleitung an ESAs (EBA, EIOPA, ESMA), EZB, NIS-Behörde, …
  - Fristen




Wochenend- und Feiertagsbestimmungen: verlängerte Meldefristen bis 12 Uhr des nächsten Arbeitstages

  - Freiwillige Meldung erheblicher Cyberbedrohungen

# IKT-BEZOGENE VORFÄLLE: Q&A

## IKT-bezogene Vorfälle

1) **Ersetzt DORA die PSD2-Meldung und die Meldung nach SSM Cyber Incident Reporting für SI?**

2) **Ist die FMA die einzige zuständige Behörde für die Meldungen, die sich aus der DORA-VO ergeben?**

3) **Leitet die FMA die Meldungen gem Art 19 DORA weiterhin an die NIS-Behörde weiter?**

4) **Wird es  weiterhin ein konsolidiertes Reporting geben?**

1) Die Reduktion von Doppelmeldungen war eines der erklärten Ziele von DORA (geäußert insb in ErwG 23); ab Anwendbarkeit von DORA ersetzt daher aller Voraussicht nach die Meldung gem Art 19 DORA die Meldung gem PSD2 sowie gem SSM Cyber incident reporting.

2) Gemäß Art. 19 Abs. 1 iVm. Art. 46 DORA ist die FMA die zuständige Behörde im Hinblick auf die Meldung von IKT-bezogenen Vorfällen und Cyber-Bedrohungen. Dies gilt auch gemäß Art. 19 Abs. 1 2. Absatz für signifikante Kreditinstitute.

3) Die FMA ist verpflichtet, die Meldung an die ESAs, ggf EZB sowie die NIS-Behörde weiterzuleiten. DORA ist als lex specialis zur NIS2-RL zu sehen.

4) Gem Art 7 des draft-ITS gibt es die Möglichkeit, unter gewissen Voraussetzungen aggregierte Meldungen abzugeben.

# EU-SYSTEMIC CYBER INCIDENT COORDINATION FRAMEWORK

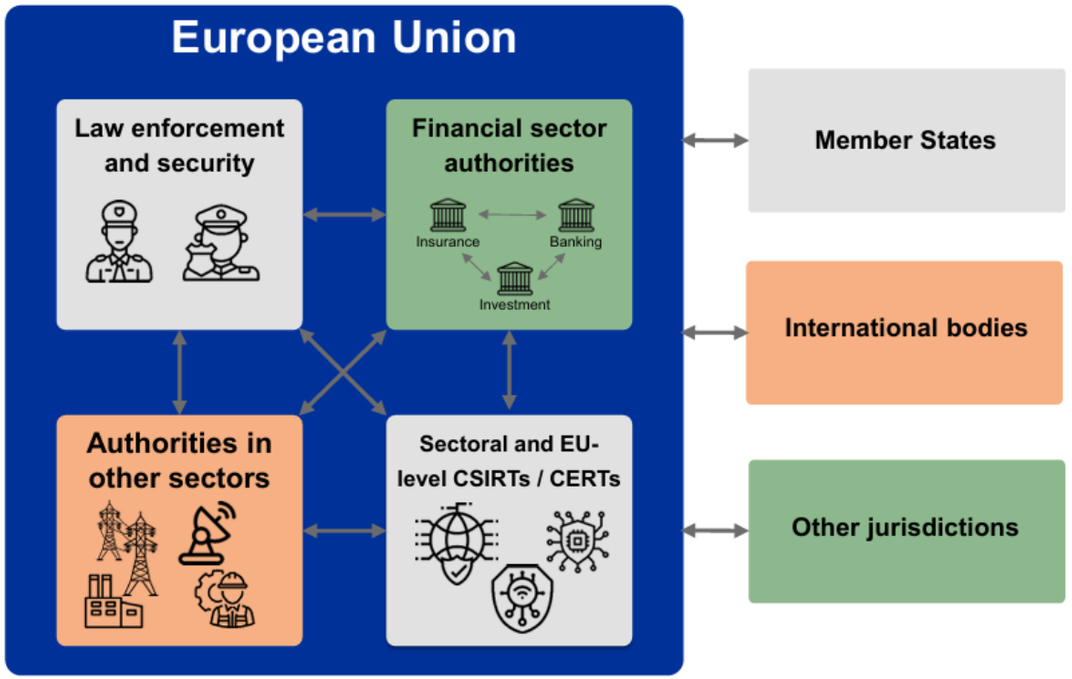
## EU-WEITER KOORDINIERUNGSRAHMEN IN BEZUG AUF SYSTEMISCHE CYBERVORFÄLLE

**ZIEL: WAHRUNG DER FINANZSTABILITÄT BEI SYSTEMISCHEN CYBERKRISEN**

- **Grundlage:**
  ESRB-Empfehlung zu einem europaweiten Koordinierungsrahmen für betreffende Behörden in Bezug auf systemische Cybervorfälle (ESRB/2021/17),
  ⇨ **freiwillige Teilnahme der Mitgliedstaaten**

- Einbettung in die europäische (Cyber-)Sicherheitsarchitektur

- **Maßnahmen im Rahmen des EU-SCICF:**
  - Rascher Informationsaustausch zwischen Behörden
  - EU-weit sektorübergreifende Koordination
  - Abgestimmte externe Kommunikation




Quelle: ESRB, Mitigating systemic cyber risk (europa.eu)

# DORA-Themen:
# Testen der digitalen operationalen Resilienz

# TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ

## ART 24 - ALLGEMEINE ANFORDERUNGEN FÜR PRÜFUNGEN DER BETRIEBSSTABILITÄT DIGITALER SYSTEME

- Finanzunternehmen haben ein umfassendes Programm zur Prüfung der digitalen Betriebsstabilität im Rahmen des IKT-Risikomanagementrahmens zu erstellen und zu implementieren
- Prüfungen sind von unabhängigen internen oder externen Prüfer:innen durchzuführen. Bei internen Prüfer:innen: Sicherstellung ausreichender Ressourcen und Berücksichtigung allfälliger Interessenskonflikte
- Follow-Up-Prozess
- Prüfung bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen: mindestens einmal jährlich

## ART 25 - TESTEN VON IKT-TOOLS UND -SYSTEMEN

- Das Programm umfasst je nach Kriterien des Unternehmens angemessene Tests wie etwa:
  - Schwachstellenbewertung und -scans
  - Open-Source-Analysen
  - Netzwerksicherheitsbewertungen
  - Lückenanalysen
  - Überprüfungen der physischen Sicherheit
  - Fragebögen und Scans von Softwarelösungen
  - Quellcodeprüfungen soweit durchführbar
  - Szenariobasierte Tests
  - Kompatibilitätstests
  - Leistungstests
  - End-to-End-Tests
  - Penetrationstests

# TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ: Q&A

1) **Sind Penetrationstests gemäß Art. 25 (1) DORA-VO optional, da die Formulierung „wie etwa“ auf eine beispielhafte Aufzählung hinweist und somit dem Verhältnismäßigkeitsgrundsatz folgt?**

1) Die in Art 25 Abs 1 DORA -VO angeführten Tests sind beispielhaft zu verstehen. Es wird nicht erwartet, dass alle Finanzunternehmen alle dort angeführten Tests durchführen. Das Testprogramm eines jeden Instituts soll jedoch entsprechend dem Grundsatz der Verhältnismäßigkeit ausgestaltet sein.

   Während die Vorgaben der Art 24 und 25 DORA-VO grundsätzlich für alle Finanzunternehmen gelten, sind erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT nur von ausgewählten Finanzunternehmen, die von der FMA rechtzeitig verständigt werden, durchzuführen.

   TLPT sind in Art 3 Z 17 DORA-VO definiert als: „bedrohungsorientierte Penetrationstests (TLPT — Threat-Led Penetration Testing)“. TLPT gibt einen Rahmen vor, der Taktiken, Techniken und Verfahren realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet. TLPT ermöglichen einen kontrollierten, maßgeschneiderten und erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des jeweiligen Finanzunternehmens.

# DORA-Themen:
# Management IKT-Drittparteienrisiko

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## THEMENÜBERBLICK

- **RECAP: IKT-DRITTPARTEIENRISIKO UNTER DORA**
- **BEGRIFFSDEFINITION IKT-DIENSTLEISTER**
- **STATUS INFORMATIONSREGISTER, HINWEIS ZU KONSOLIDIERUNG**
- **ERGEBNISSE & LESSONS LEARNED DRY RUN**

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

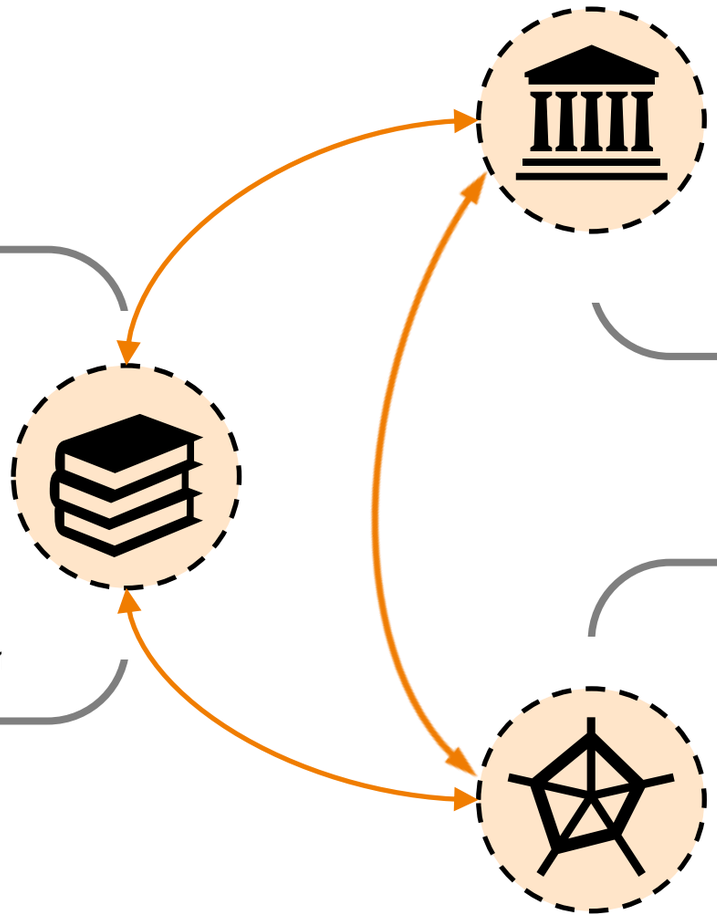
## ÜBERBLICK: DRITTPARTEIENRISIKO UNTER DORA

### Governance der IKT-Dienstleister

- Berücksichtigung im Risikomanagement
- Vorgaben zur Steuerung und Kontrolle
- Mindestvertragsinhalte

### Register der IKT-Dienstleister

- Laufend aktualisiertes Register der IKT-DL pro FI
- Umfasst zusätzliche Informationen über DL
- Mindestens jährlich an FMA übermittelt
- Grundlage für Identifikation kritischer Dienstleister



### Zentrale Beaufsichtigung kritischer IKT-DL

- Betrifft größte IKT-Dienstleister in EU
- Multinationale ESA-Aufsichtsteams
- Berücksichtigung von Prüfergebnissen durch FMA und FI

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## HINWEISE ZUR DEFINITION VON ‚IKT-DIENSTLEISTUNGEN' UNTER DORA

- **IKT-Dienstleistungen (DORA-VO Artikel 3, Ziffer 21)**

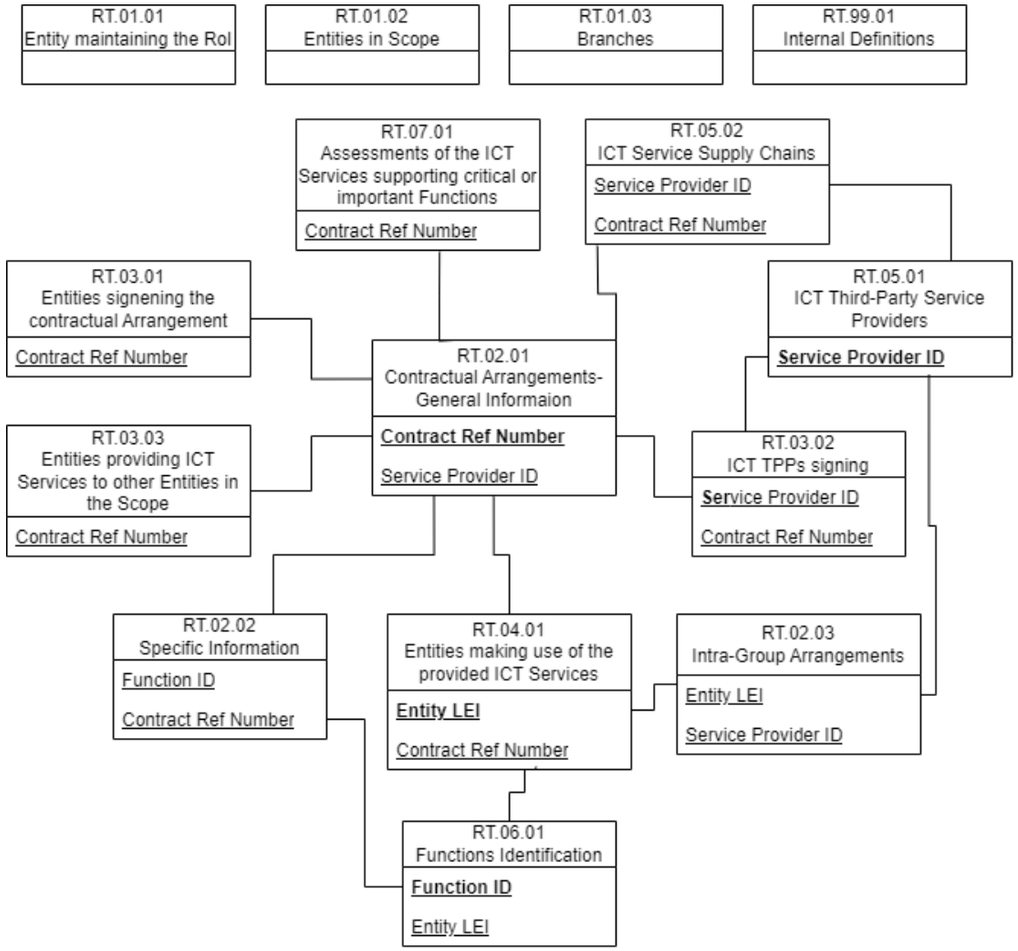
  *digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden […]*

  - Kriterium ‚**Bereitstellung von Diensten**' – hier sollte ein Bezug zur Geschäftstätigkeit vorhanden sein, z.B. wird die reine Erfüllung aufsichtlicher Meldepflichten von der FMA nicht als ‚IKT-Dienstleistung' gesehen.
  - Kriterium ‚**dauerhafte Bereitstellung**' – einmalige und kurzfristige Leistungen (z.B. der reine Kauf von Hardware oder Software) würden dieses Kriterium nicht erfüllen; sobald eine Verknüpfung mit laufender Leistung (z.B. Wartung/Support) gegeben ist, ist es allerdings im Regelfall erfüllt; ebenso können Ketten von Werkverträgen zum selben Thema als laufend bereitgestellte Leistung gesehen werden.
  - Kriterium ‚**digitale Dienste und Datendienste über IKT-Systeme**' – hier sei auf Annex III des ITS zum Informationsregister verwiesen (JC 2023 85_Final report on draft ITS on Register of Information); eine geschlossene Liste von 19 Arten der IKT-Dienstleistung ist enthalten; passt ein Service in keine der Kategorien, ist dies ein Hinweis darauf, dass möglicherweise keine IKT-Dienstleistung nach DORA vorliegt.

  - KEINE Berücksichtigung von Kritikalität; gruppeninterne Dienstleister sind explizit inkludiert; Annex III Kategorien von IKT-Dienstleistungen recht weit gefasst.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## STATUS UND TIMELINE INFORMATIONSREGISTER




- Die Informationsregister werden voraussichtlich mit dem **Cutoff-Date 31.03.2025** einzumelden sein.
- Die FMA wird nach aktuellem Plan die Register bis 30.04.2025 an die ESAs weiterleiten müssen.
- Um Zeit für Nachmeldungen, Validierung, Korrekturen und Formatkonvertierung zu lassen, wird eine **Abgabe an die FMA Anfang April** nötig sein.
- Für die Veröffentlichung der finalen Templatespezifikation ist noch kein Termin bekannt.
- Die Änderungen im Vergleich zum Dry Run sollten sich nach aktuellem Informationsstand auf Feldbezeichnungen und drei neue Spalten im Sheet 05.01 beschränken.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## UPDATE: KONSOLIDIERUNG DES INFORMATIONSREGISTERS

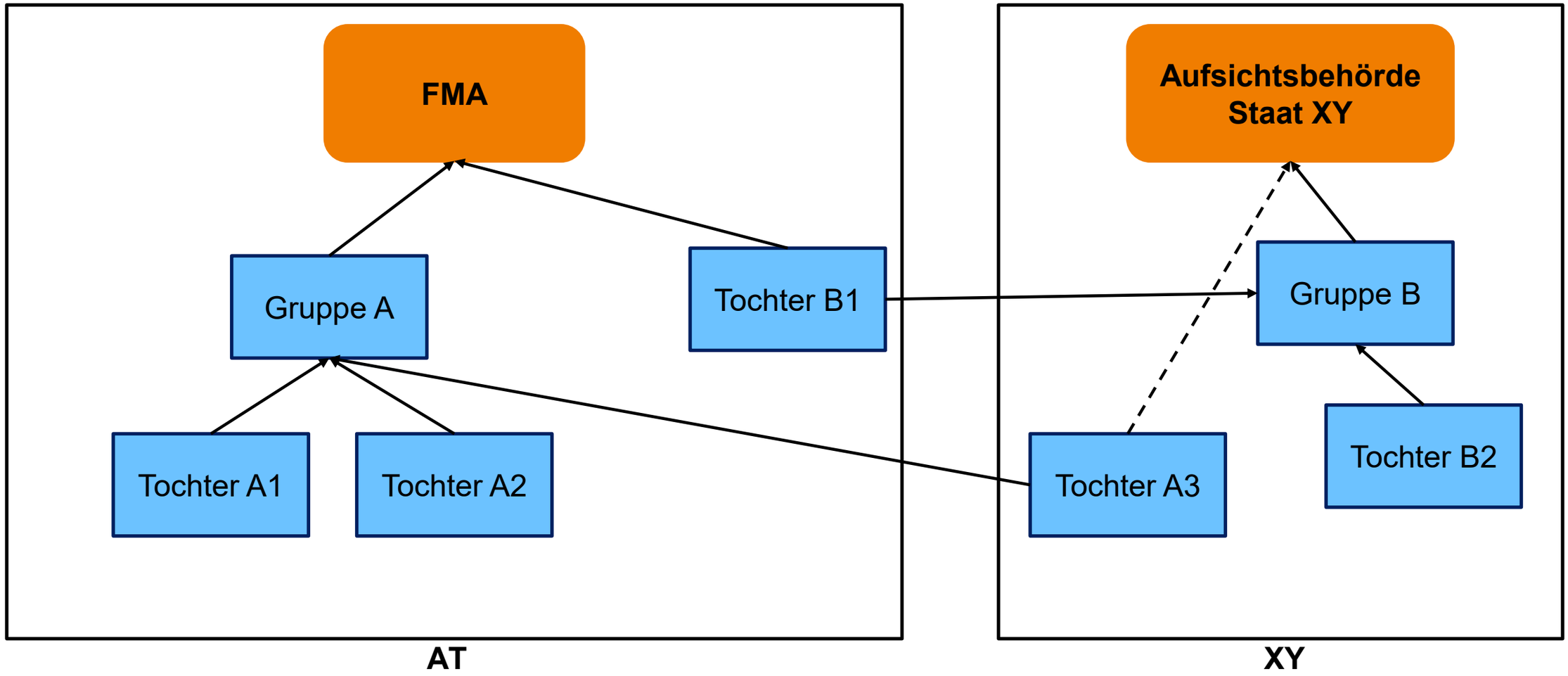
- Informationen aus FAQ #42: DORA Dry Run FAQ (Updated).pdf
- Vollständige **Konsolidierung der Register auf Gruppenebene** vorgesehen (über Ländergrenzen hinweg)
- Tochtergesellschaften können von lokalen Aufsichtsbehörden dennoch zur Vorlage der Einzelregister aufgefordert werden

→ **Gruppen mit Sitz in AT**: Konsolidieren die Informationsregister aller unter DORA fallenden Tochterunternehmen und leiten das volle Register an die FMA weiter

→ **AT Tochterunternehmen ausländischer Gruppen**: Leiten ihr individuelles Register an die Gruppe weiter UND leiten ihr individuelles Register an die FMA weiter (auf Basis der entsprechenden Anforderung nach DORA-VO, Artikel 28, Ziffer 3)

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

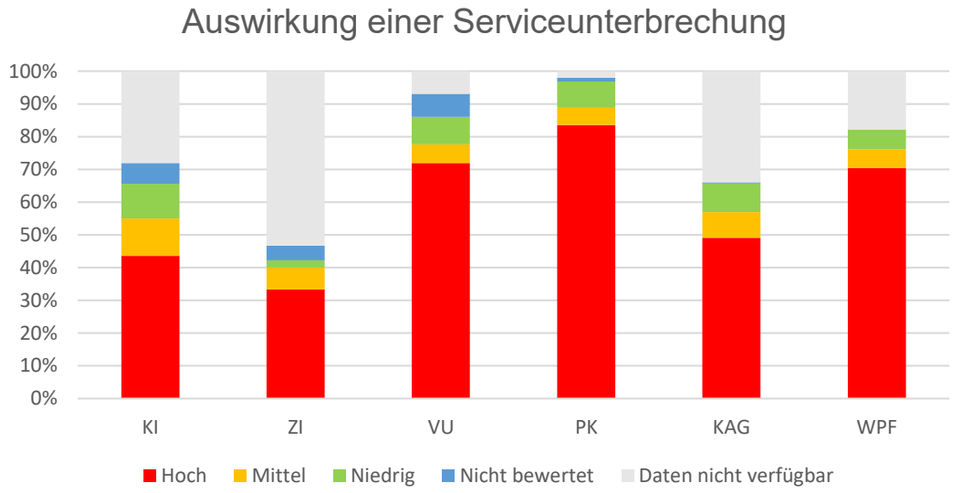
## UPDATE: KONSOLIDIERUNG DES INFORMATIONSREGISTERS

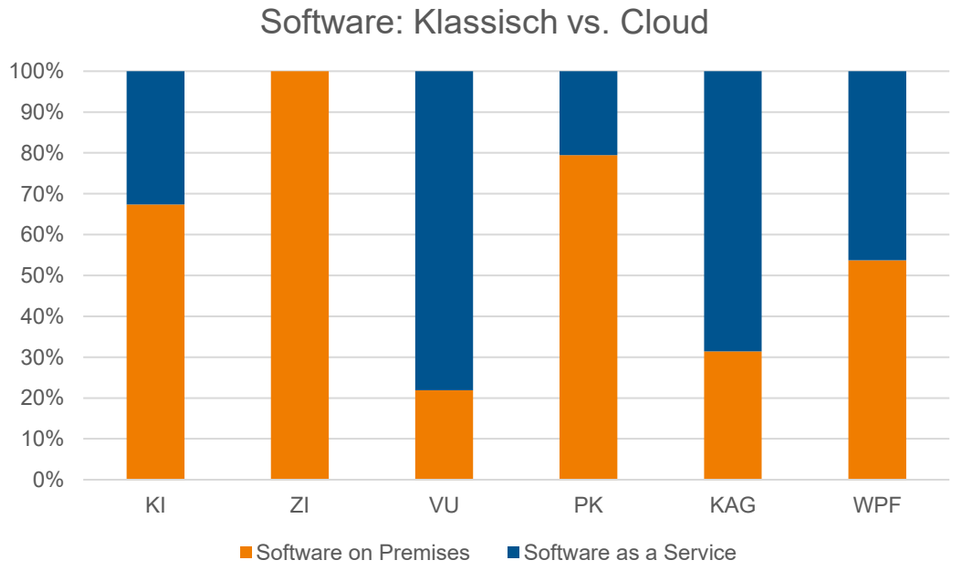


# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## DRY RUN: ERGEBNISSE IM ÜBERBLICK

- 250 österreichische FI waren in den Abgaben zum Dry Run vertreten.
- Die Veröffentlichung der Ergebnisse ist im Rahmen der Digitalisierungsstudie geplant.
- Nicht-finalisierte Natur der Informationsregister verhindert absolute Aussagen aus den Daten.
- Meldungen zeigen jedoch hohe Anzahl an für das Unternehmen wichtigen und schwer substituierbaren Dienstleistern.
- Steigender Stellenwert von Cloud SaaS im Vergleich zu ‚klassischem' Bezug von Software unter Lizenz.



# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

## DRY RUN: LESSONS LEARNED

- **ESA Feedback** ist eingelangt, Aufbereitung und Verteilung durch FMA noch ausständig und im November geplant.

- **Datenqualität** wurde von Finanzunternehmen auf, den Umständen entsprechend, hohem Niveau sichergestellt (fast alle Abgaben verarbeitbar, ein Großteil der Bezüge auflösbar).

- Dennoch können einige **häufiger auftretende Probleme** identifiziert werden:
  - Nicht zusammenpassende Schlüsselfelder
  - Verwaiste Einträge (z.B. Dienstleister ohne passende Verträge)
  - Abgaben insgesamt (wie erwartet) noch nicht vollständig
  - Relativ breite Definition von Dienstleistern unter DORA zu beachten (z.B. Microsoft, auch ohne Nutzung von Azure)

  → FMA plant Unterstützung durch Vorab-Validierung der Abgaben, um Rückfragen/Nachforderungen nach Möglichkeit zu vermeiden.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A

1/9

1) **Kann die FMA die Ansicht teilen, dass jedes vom Geltungsbereich der DORA-VO umfasste Institut zwar ein Sub-konsolidiertes Melderegister vorweisen können muss, allerdings nicht in der für die elektronische Verarbeitung notwendigem Format?**

2) **Wird die Befüllung des Registers mit strukturierten Textinhalten erfolgen und nicht analog zum Dry Run mittels Coding?**

3) **Wird die deutsche Sprache zur Befüllung des Informationsregister akzeptiert?**

1) Jedes Finanzunternehmen muss ihr Register jederzeit übermitteln können (Art. 28 Abs. 3 vierter Unterabsatz DORA-VO). Das Template-Format für die Übermittlung wird per ITS festgelegt. Es ist hier, zumindest sobald es um die Übermittlung an die Aufsichtsbehörden geht, kein Spielraum für ein eigenes ‚nicht elektronisch verarbeitbares' Format gegeben.

2) Es ist zu erwarten, dass analog zum Dry Run die eingabeeingeschränkten Felder (Drop-Down-Auswahl) wieder mit Codewerten zu befüllen sein werden.

3) Ja, die Finanzunternehmen dürfen die Informationsregister in der Amtssprache ihres Mitgliedstaates befüllen.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**4) Wie sind Dienstleistungen einzumelden, die nach der EBA keine Auslagerung (weil sie unter eine taxativ genannte Ausnahme fallen) darstellen, aber nach der DORA-VO als IKT-Dienstleistung einzustufen sind, die kritische und wichtige Funktionen unterstützen (zB PSA)?**

**5) Finanzunternehmen verwenden Social Media-Plattformen (Instagramm, Facebook, TikTok, Wikipedia, etc.) zu Marketing-zwecken. Nach der DORA-VO stellt dies eine IKT-Drittdienstleistung dar. Schriftliche Aufforderungen zur Bereitstellung von Informationen (zB für das Inforegister) oder Unterfertigung von (DORA-konformen) Zusatzvereinbarungen bleiben unbeantwortet. Welche Vorgehensweise in der Praxis erwartet die Aufsicht diesbezüglich?**

4) Die Einstufung als IKT-Dienstleistung unter DORA sowie ggf. die Behandlung im Informationsregister sind unabhängig von sektoralen Auslagerungsvorgaben zu sehen.

5) Diesbezüglich erfolgt eine ESA-Anfrage.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**6) Stellen reine Software-Lizenzen ohne weiterführende Services (zB Software-Updates) eine IKT-Dienstleistung nach der DORA-VO dar? Dies würde bedeuten, dass diese Dienstleister weder im Informations-register anzuführen sind noch die Anforderungen an die Mindestvertrags-inhalte iSd DORA-VO bei solchen Verträgen erforderlich bzw. anwendbar sind.**

6) Wird Software einmalig zugekauft und liegt keine weitere laufende Leistung vor, fällt dies prinzipiell nicht unter die Definition von IKT-Dienstleistung nach DORA. Allerdings ist eine Nutzung einer Software, die keinerlei Software-Updates bzw. Sicherheitspatches zur Verfügung stellt, aus IKT-Risikomanagementsicht kritisch zu hinterfragen.

Sobald allerdings Updates und Patches zur Verfügung gestellt werden, liegt eine IKT-Dienstleistung nach DORA vor. Es ist dabei unerheblich, ob die vom Dienstleister bereitgestellten Updates automatisch erfolgen oder selbst heruntergeladen werden müssen.

Diesbezüglich erfolgt allerdings auch noch eine Anfrage an die ESA. Sicherheitshalber sollte man vorerst die gesamte Software ins RoI eintragen.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



7) **Finanzunternehmen verwenden unterschiedlichste Plattformen bzw. auch OpenSource-Produkte (z.B. GitHub, etc.). Es gibt hier nur die AGBs auf der Webseite – keine individuellen Verträge. Wie soll man damit umgehen?**

8) **Sind z.B. der Marktinformationsdienst Bloomberg (historische und Echtzeitdaten über Bloomberg Terminal) oder die Rechtsdatenbank LexisNexis (browserbasiert) oder ein virtuelles Recruiting-Tool IKT-Dienstleistungen iSv DORA? Es sind wohl alles IKT-Dienste allerdings nicht zwingend erforderlich für die Ausübung der Geschäftstätigkeit**

7) Prinzipiell ist hier ebenfalls im Rahmen des Risikomanagements zu beurteilen, ob sensible bzw. kritische Daten verarbeitet werden und ob verwendeten Tools/Plattformen, etc. den IKT-Sicherheitsstandards des Finanzunternehmens entsprechen.

   In Bezug auf den Umgang mit AGB – keine individuellen Verträge erfolgt eine Anfrage an die ESA.

8) Zur Einordnung wären Detailangaben erforderlich. In diesem Zusammenhang verweist die FMA auf Annex III Draft ITS on RoI.

   Bloomberg: 5. Provision of data; LexisNexis: 5. Provision of data

   Das Informationsregister umfasst alle bezogenen IKT-Dienstleistungen, nicht nur jene deren Ausfall die Geschäftstätigkeit signifikant beeinträchtigen würde.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**9) Wie muss die vertragliche Ausgestaltung aussehen, wenn IKT-Dienstleistungen über einen zwischengeschalteten Händler (Reseller) bezogen werden, der ja selbst keine IKT-Dienstleistungen erbringt? In diesen Fällen besteht in der Praxis lediglich mit dem Reseller ein Vertragsverhältnis, jedoch nicht mit dem tatsächlichen IKT-Dienstleister. Müssen dem Reseller die verpflichtenden DORA-Kündigungsbestimmungen auferlegt werden und dem „eigentlichen“ IKT-Drittdienstleister die übrigen DORA-Vertragsbestimmungen?**

9) Hier kommt es auf die konkrete Ausgestaltung der Verträge an. Besteht tatsächlich nur ein Vertrag mit dem Reseller, würde dieser als IKT-Dienstleister auftreten, wodurch alle DORA-Mindestvertragsinhalte anwendbar wären. Die eigentlichen IKT-Unternehmen wären dann dessen Subdienstleister.

Werden allerdings über den Reseller rein nur Softwarelizenzen erworben und von diesem keine weiteren Leistungen bezogen, während der Softwarehersteller im Rahmen der Lizenz für Updates und Support zuständig ist, wäre der Softwarehersteller und nicht der Reseller als Dienstleister zu führen.

Sobald der Reseller aber eine weitere Dienstleistung (z.B. Support) erbringt, ist er jedenfalls als IKT-Dienstleister zu führen.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**10) Sind Werkverträge (Zielschuldverhältnisse) im Zusammenhang mit IKT-Diensten (z. B. Verträge über die Entwicklung und Lieferung von Individualsoftware) als Verträge über IKT-Dienstleistungen im Sinne des Art 3 Z 21 DORA zu qualifizieren?**

**11) Zu Art 30 Abs 2 lit h DORA: Welche Kündigungsrechte und welche damit zusammenhängenden Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechen den Erwartungen der FMA und der Abwicklungsbehörden?**

10) Grundsätzlich ist Softwareentwicklung eine IKT-Dienstleistung im Sinne von DORA. Bei Werkverträgen mit relativ kurzer Laufzeit, die mit keinen weiteren laufenden Leistungen verbunden sind, kann argumentiert werden, dass kein 'service on an ongoing basis' nach Art 3 vorliegt.

Sobald es sich z.B. um länger laufende Vereinbarungen mit stetiger Zulieferung von Subpaketen, oder eine Kette nacheinander abgeschlossener Werkverträge zum selben Thema handelt, wäre auch eine IKT-Dienstleistung im Sinne von DORA gegeben.

11) Die FMA orientiert sich hier direkt an den Vorgaben der DORA-Verordnung: die mindestens zu inkludierenden Kündigungsrechte sind in Artikel 28 der DORA-Verordnung, unter Ziffern 7 und 8 aufgelistet. Die Festlegung angemessener Kündigungsfristen obliegt der Maßgabe und Risikoeinschätzung des Unternehmens.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**12) Wurden bereits Standardvertragsklauseln im Sinne des Art 30 Abs 4 DORA entwickelt?**

**13) Kann davon ausgegangen werden, dass regulierte Finanzdienstleistungen nicht als IKT-Dienstleistungen iSd DORA zu qualifizieren sind?**

12) Der FMA sind dazu keine Aktivitäten bekannt.

13) Die Frage wird in Gremien noch abgestimmt. Die endgültige Beantwortung wird dann auf der FMA-DORA-Website veröffentlicht.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**14) Sind Plattformen, über welche Finanzunternehmen im Rahmen ihrer gesetzlichen Meldepflichten Daten an die zuständigen Behörden übermitteln, im Informationsregister zu führen?**

14) In diesen Fällen wird keine Dienstleistung bezogen, sondern eine Meldepflicht erfüllt. Insofern liegt keine IKT-Drittdienstleistung vor.

**15) Im Rahmen der DORA-Veranstaltung der BaFIN wurde ein IKT-Prüfschema mit 7 Kriterien vorgestellt, ob es sich bei dem Leistungsbezug um eine IKT-Dienstleistung handelt. Wird das Prüfungsschema von der FMA übernommen?**

15) FMA AT verweist auf die Definition zu IKT-Dienstleistungen (Art 3 (21) DORA-VO) sowie auf den Bezug zur Geschäftstätigkeit (zB ist dieser bei Erfüllung einer reinen Meldeverpflichtung gs nicht gegeben) sowie auf Annex III zum Draft ITS on RoI. In letzterem finden sich Typen von IKT-Dienstleistungen, auf die bei der Einordnung referenziert werden kann.

# MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS: Q&A



**16) Wie ist das Verhältnis der ex-ante Anzeige gem Art 28 Abs 3 DORA zu sektorspezifischen Vorgaben im Bereich Auslagerungen/Delegationen?**

16) Die sektorspezifischen Vorgaben bleiben neben den Vorgaben zur ex-ante Anzeige gem Art 28 Abs 3 DORA bestehen. Das bedeutet, dass künftig bei einer Vereinbarung über die Nutzung von IKT-Drittdienstleistungen zu prüfen ist, ob (zusätzlich zur Anzeige gem Art 28 Abs 3 DORA) weitere sektorspezifische Anzeigeverpflichtungen ausgelöst werden. Die Anzeigen können, wo möglich, in einem Anzeigevorgang an die FMA übermittelt werden.

# DORA-Themen: Überwachungsrahmen für kritische IKT-Drittdienstleister

# ÜBERWACHUNGSRAHMEN FÜR KRITISCHE IKT-DRITTDIENSTLEISTER

- **Ziel:**
  - Überwachung von für Finanzunternehmen kritischen IKT-Drittdienstleistern
  - Bewertung des adäquaten IKT-Risikomanagements

- **Kritische IKT-Drittdienstleister:**
  - Bestimmung auf Basis des Informationsregisters & vorgegebener Kriterien
  - Antrag von IKT-Drittdienstleistern zur Prüfung auf Kritikalität möglich

**Bestimmung im 2. Halbjahr 2025**

- **Federführende Überwachungsbehörde:**
  - EBA, ESMA oder EIOPA
  - Basis: Nutzung durch Finanzunternehmen

- **Folgemaßnahmen zuständiger Behörden:**
  - Kommunikation der in Empfehlungen festgestellten Risiken an beaufsichtigte Unternehmen
  - Letztes Mittel: Vollständige oder tw. Aussetzung der Dienstleistungen

# ÜBERWACHUNGSRAHMEN FÜR KRITISCHE IKT-DRITTDIENSTLEISTER

## Joint Committee (JC)

- Einstufung & Ernennung kritischer ICT-TPPs
- Jährliche Veröffentlichung der kritischen ICT-TPPs
- Annahme von gemeinsamen Positionen
- Jährlicher Bericht an EP, EK und Rat

## Oversight Forum

ESA-Vorsitzende, NCAs, ggf NIS-Behörden (Beobachter: ESA-Exekutivdirektoren, EK, ESRB, EZB, ENISA)

- Vorbereitung Einstufung & Ernennung kritischer ICT-TPP & gemeinsamer Positionen & jährlicher Bericht
- Jährliche Bewertung Überwachungs-tätigkeit
- Koordinierungs-förderung
- Konsultation zu Empfehlungen des LO an ICT-TPPs

## Joint Oversight Network (JON)

LOs (ECB, ENISA may be called for advice)

- LO-Abstimm-ungen

## Lead Overseers (LOs)

EBA EUROPEAN BANKING AUTHORITY · ESMA · eiopa

- Bewertung des adäquaten IKT-RM
- Jährlicher Überwachungsplan
- Befugnisse: zB Informationen, Untersuchungen, Prüfungen, Empfehlungen, Anforderung von Berichten zu Maßnahmen, Zwangsgelder
- Berichte an JON, NCAs
- Veröffentlichung der Nicht-Befolgung von Empfehlungen

## Joint Examination Teams (JETs)

ESAs, NCAs (ICT-TPP-Nutzung durch FEs)
(freiwillig: NIS2-Behörden, NCAs mit ICT-TPP-Sitz)

- LO-Unterstützung

## Critical ICT-Third Party Providers (kritische ICT-TPPs)

zB potenziell Microsoft · SAP · ORACLE

- Benennung oder begründete Beantragung
- Erklärungen zum Überwachungsplan und zu Empfehlungen
- Kooperation mit LOs
- Anhörungsrecht zu Zwangsgeldern
- Bezahlung Überwachungsgebühren
- Vorgaben zu Drittländern (zB Tochterunternehmen)

## Board of Supervisors (BoS)

- Genehmigungen bzgl. der dem JC zugeordneten Tätigkeiten

## National Competent Authorities (NCAs)

zB BaFin · IVASS · FMA · DeNederlandscheBank EUROSYSTEEM

- Jährliche Übermittlung des Informationsregisters
- Maßnahmen bzgl. kritischer ICT-TPPs im Einvernehmen mit LO
- Information der beaufsichtigten Unternehmen zu Risiken (Basis: LO-Empfehlungen)
- Information an LO zu Herangehensweisen und Maßnahmen bzgl. Aufsichtsaufgaben
- Letztes Mittel: (Teil-)Aussetzung der Leistungen des kritischen ICT-TPP

## Supervised Financial Entities (FEs)

zB UNIQA · Allianz

- Inanspruchnahme von kritischen IKT-TPPs mit Sitz in einem Drittland nur, soferne ein Tochterunternehmen in der Union gegründet worden ist.
- Berücksichtigung der in den LO-Empfehlungen festgestellten Risiken
- Management des IKT-TPP-Risikos

# ÜBERWACHUNGSRAHMEN FÜR KRITISCHE IKT-DRITTDIENSTLEISTER: Q&A

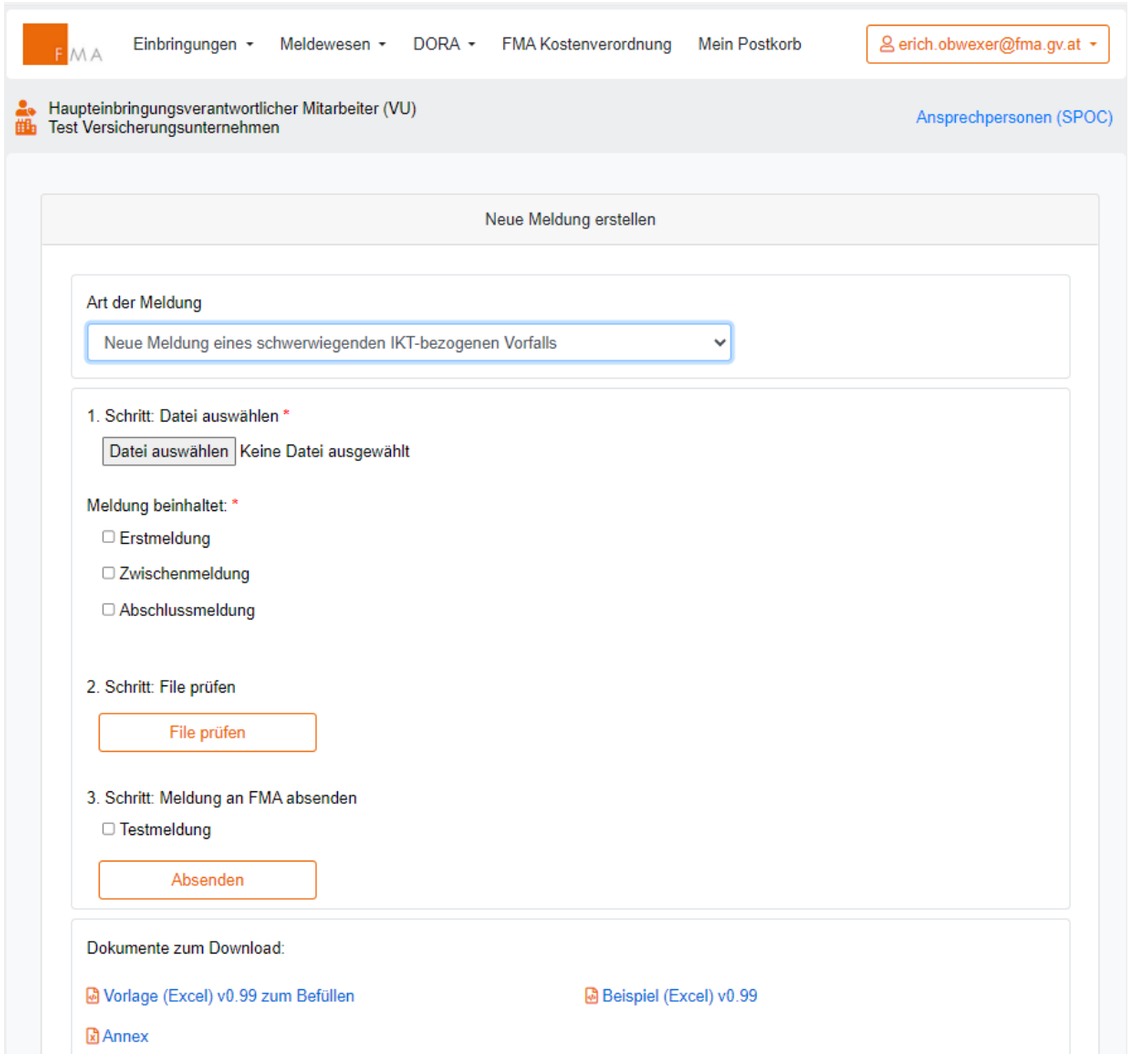
## Allgemeine Fragen zu DORA

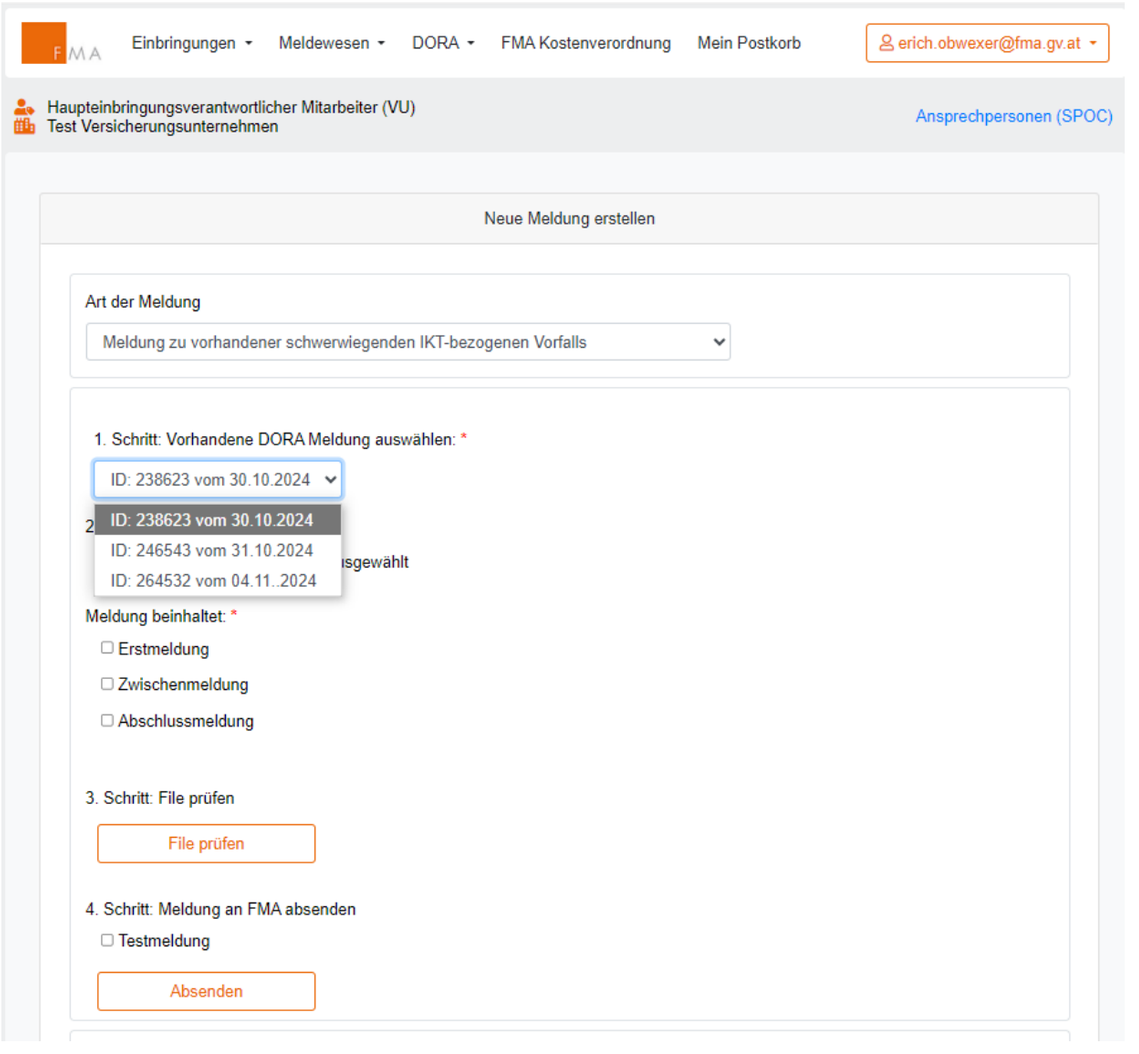
1) **Welche Unternehmen fallen unter die Definition kritischer ICT Provider nach der DORA-VO?**

1) Kritische IKT-Drittdienstleister werden auf Basis des Informationsregisters und vorgegebener Kriterien im zweiten Halbjahr 2025 durch die ESAs bestimmt werden. Auch auf Antrag von IKT-Drittdienstleistern ist eine Prüfung auf Kritikalität möglich.

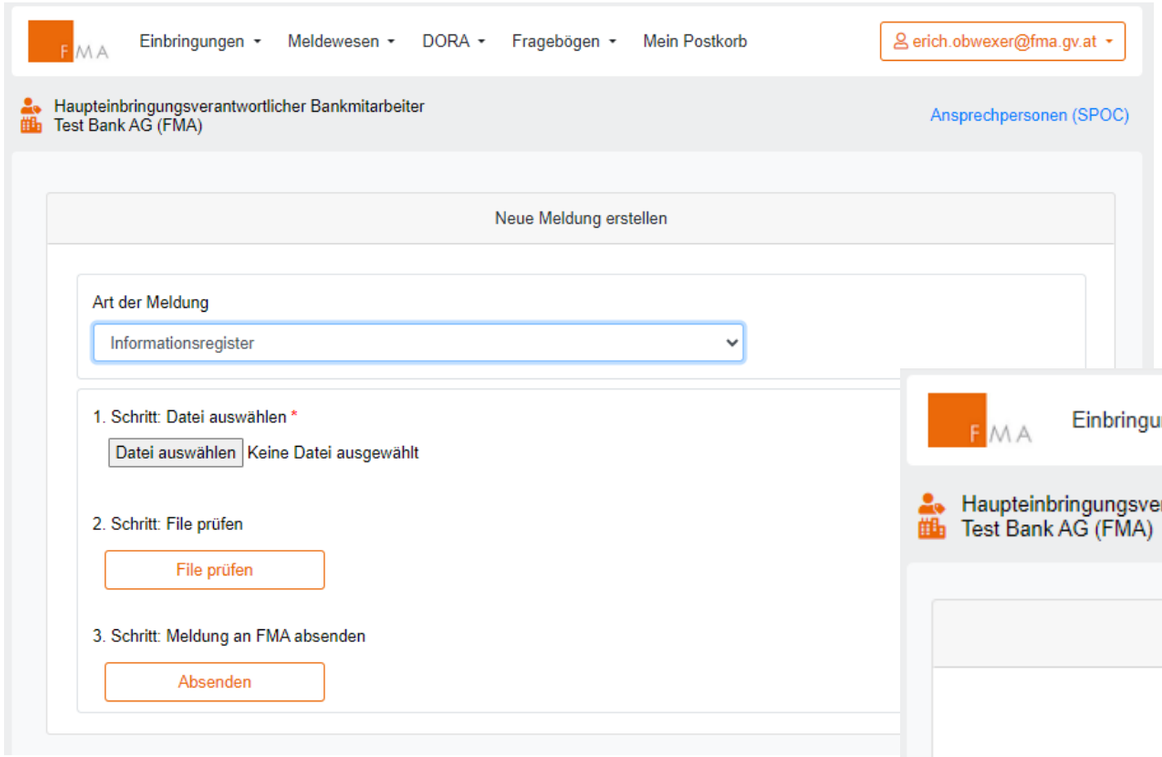
# Meldungen in der Praxis

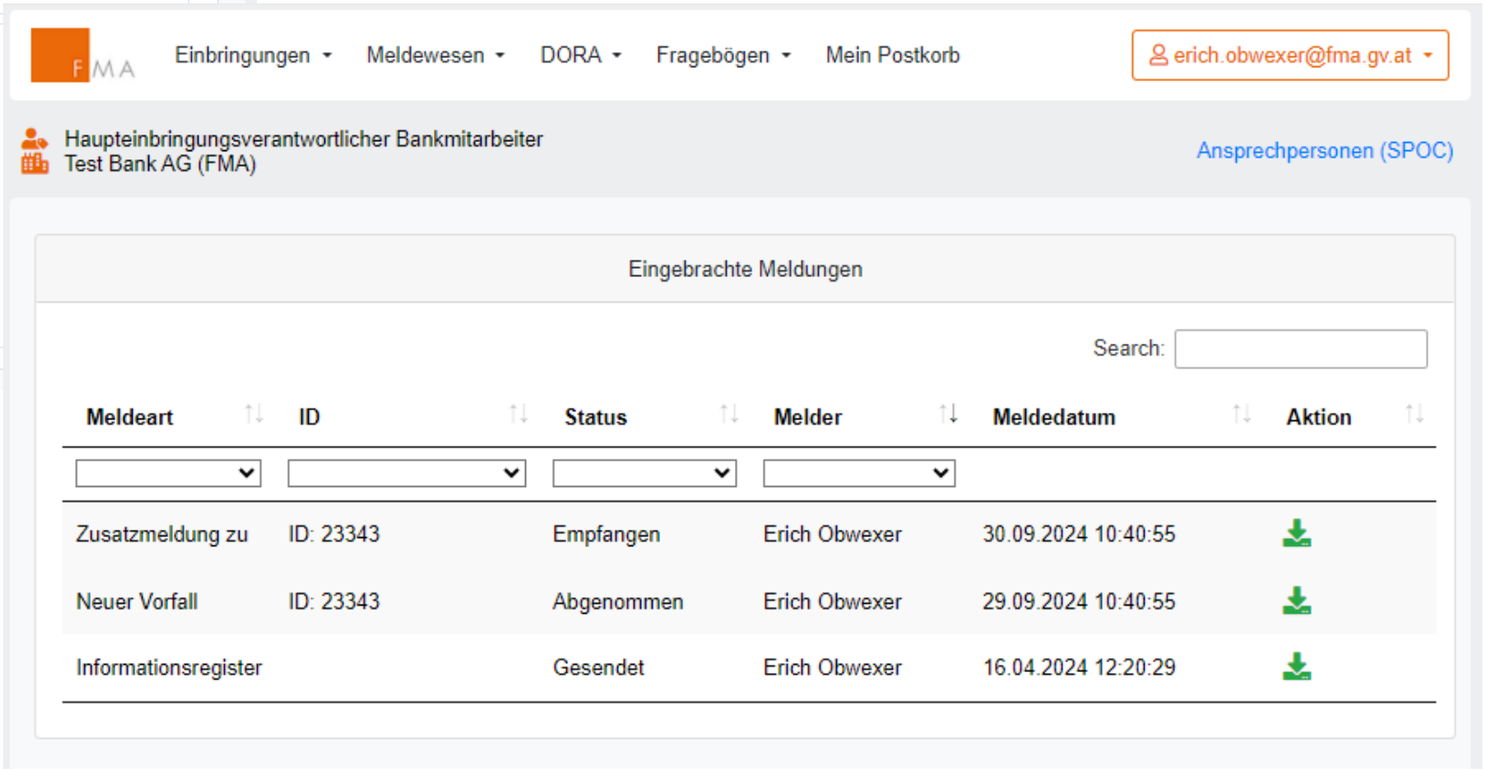
# MELDUNGEN: IKT-BEZOGENE VORFÄLLE



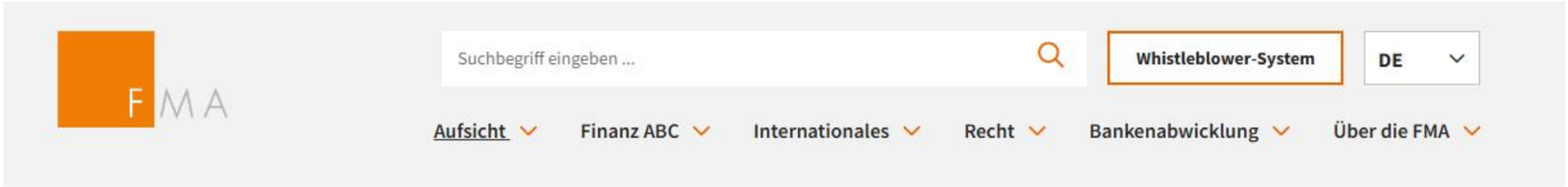
# MELDUNGEN: INORMATIONSREGISTER



# Ausblick

# FMA-DORA-WEBSITE




Startseite > Querschnittsthemen > DORA – Digitale operationale Resilienz im Finanzsektor

## DORA – Digitale operationale Resilienz im Finanzsektor


## News

ESA-Antwort zur Ablehnung des Draft ITS zum Informationsregister durch EU-Kommission

⇦ Updates folgen

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz