AUSTRIAN FMA · FINANCIAL MARKET AUTHORITY

DORA-DIALOG: TEIL 3

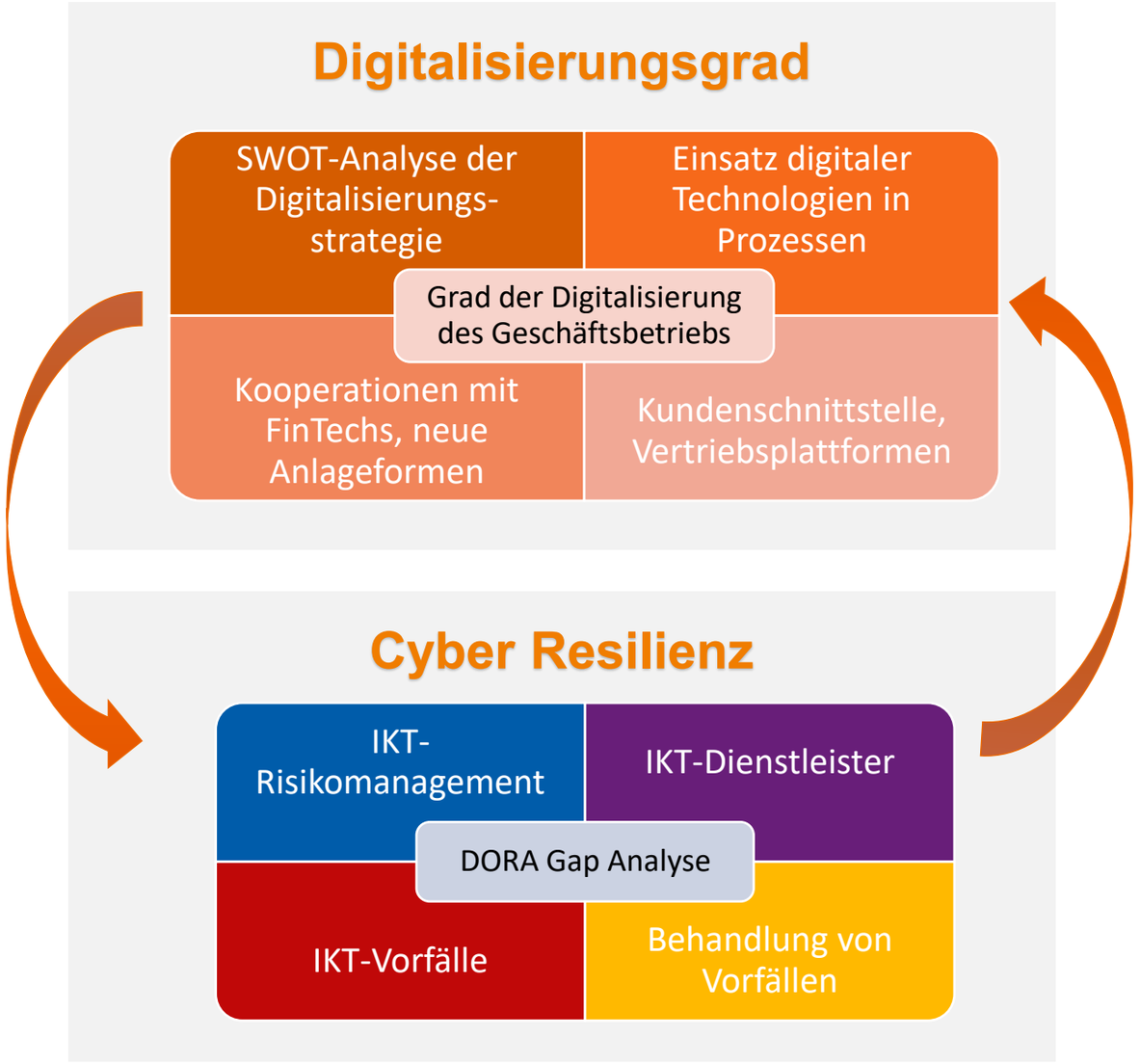
VERSICHERUNGSUNTERNEHMEN

JUDr. Stanislava Saria, PhD.
Mag. Sabine Balogh-Preininger, PRM
DI Alexander Kiennast

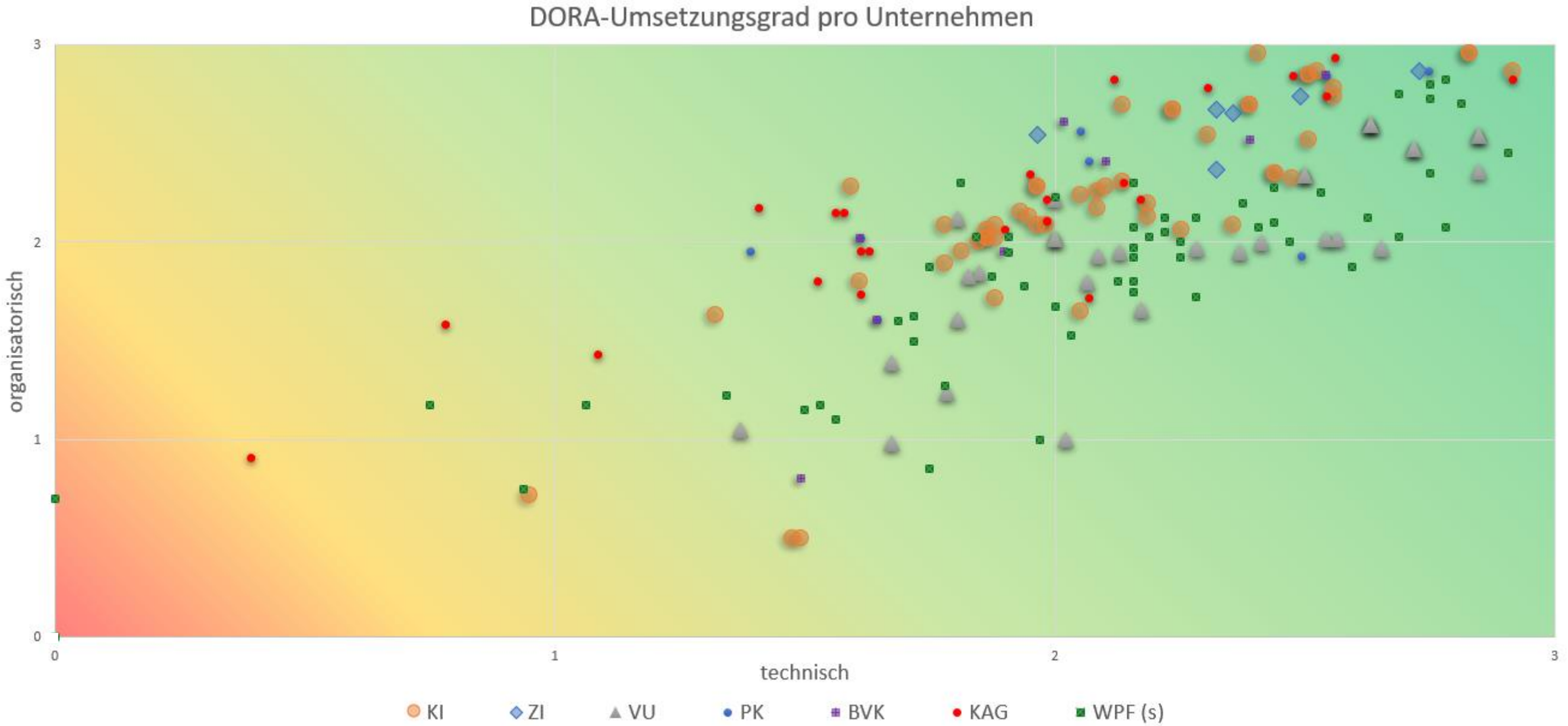
FMA, 12. November 2024

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 Finanzmarkt relevanten IKT-Dienstleister zu identifizieren.
- Durchführungszeitraum: Mai – November 2024

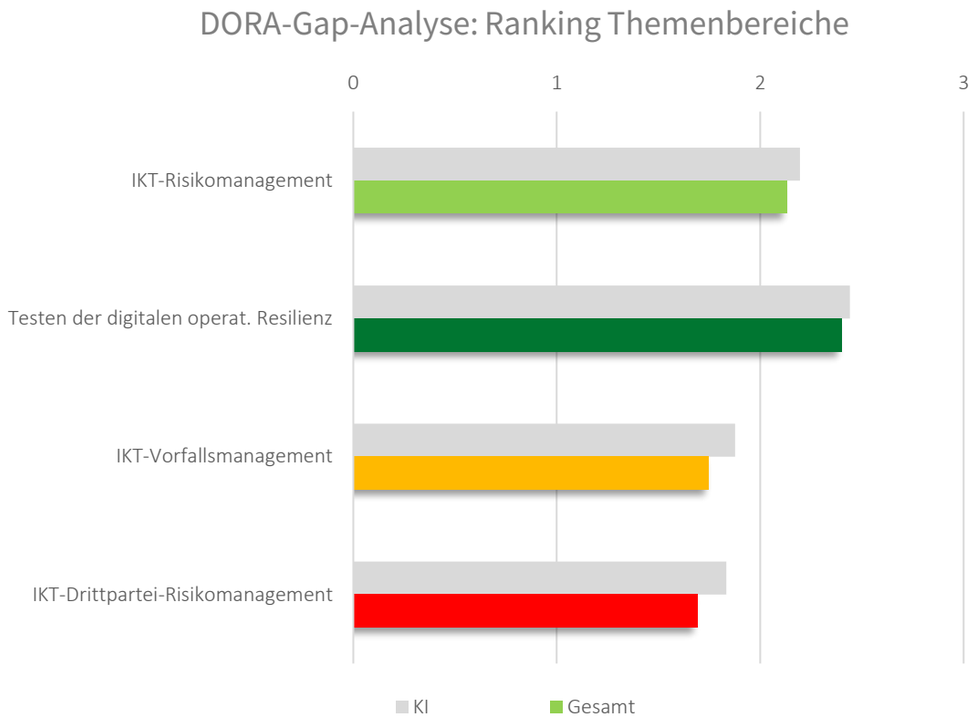


1) RANKING UNTERNEHMEN (FMA-DORA-GAP ANALYSE)

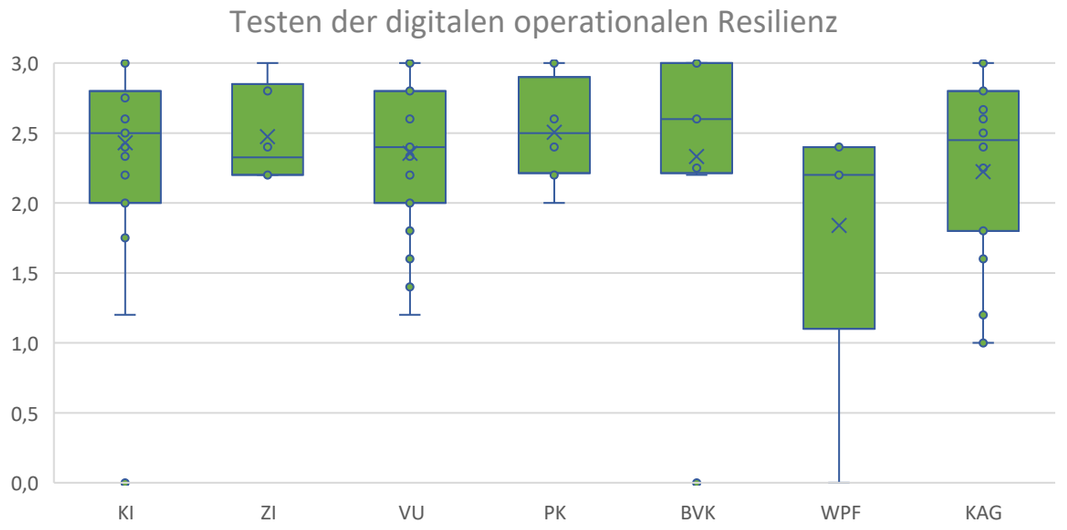


2) RANKING THEMENBEREICHE (FMA-DORA-GAP ANALYSE)

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

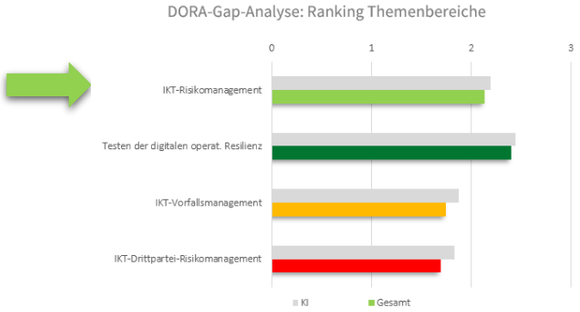


ABER auch beim Testen der digitalen operationalen Resilienz eine große Bandbreite bei der Vorbereitung der Umsetzung:

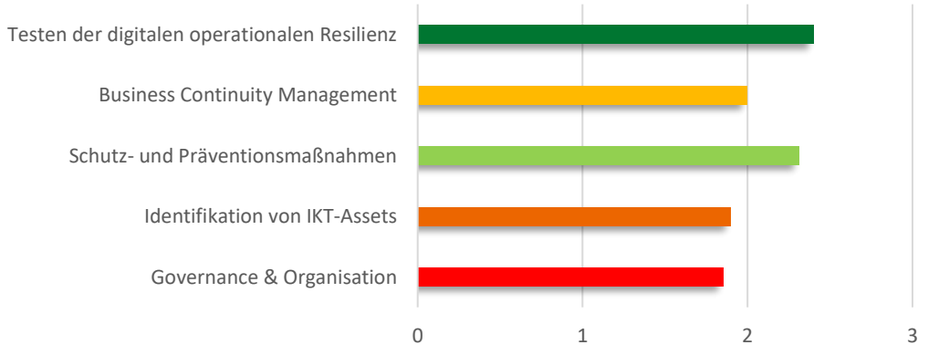


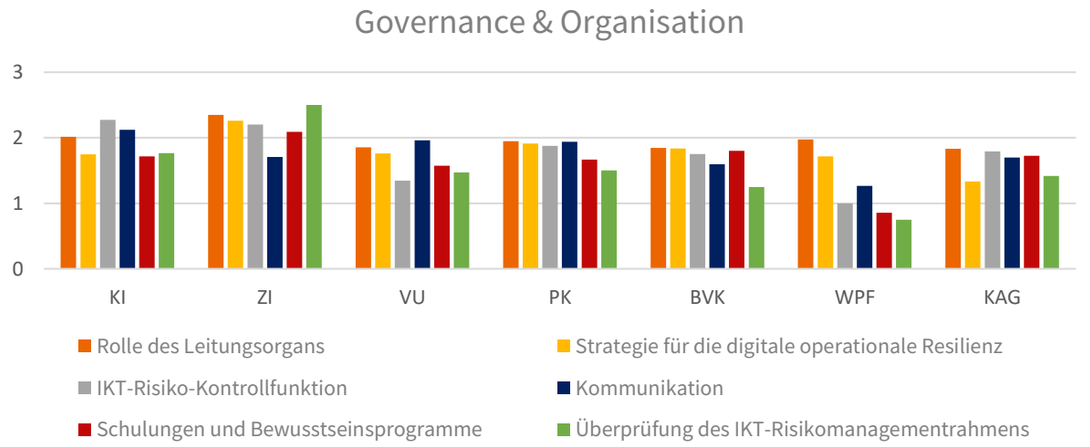
Quelle: FMA, Austrian Digital Finance Landscape 2024

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

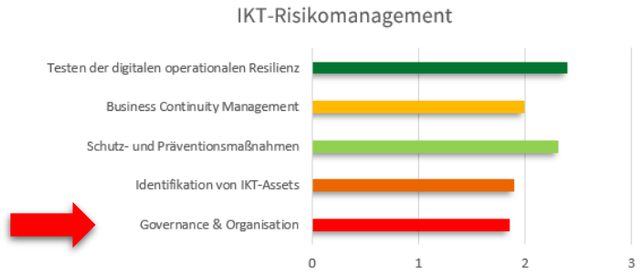


- Die DORA-Umsetzung war Mitte 2024 insb. in den folgenden Bereichen noch im Gange:
  - **Governance & Organisation**: In vielen Fällen waren u.a. noch dokumentarische Aufgaben und Freigaben der Geschäftsleitung offen.
  - Für die **Inventarisierung von IKT-Assets** waren zT noch umfangreichere technische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



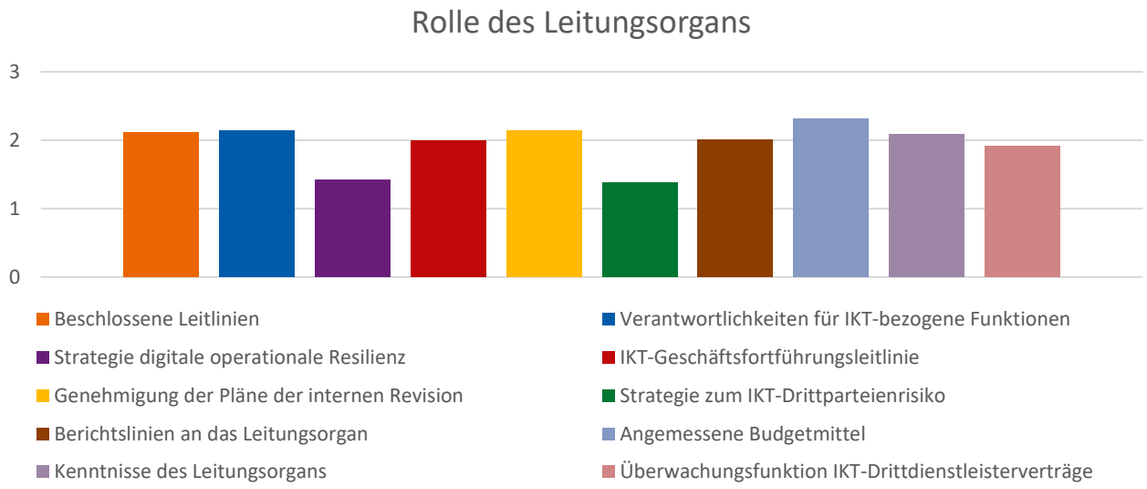


Quelle: FMA, Austrian Digital Finance Landscape 2024



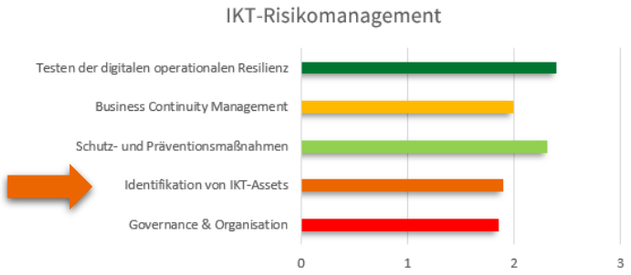
A) IKT-RISIKOMANAGEMENT: GOVERNANCE & ORGANISATION

- 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. ✓

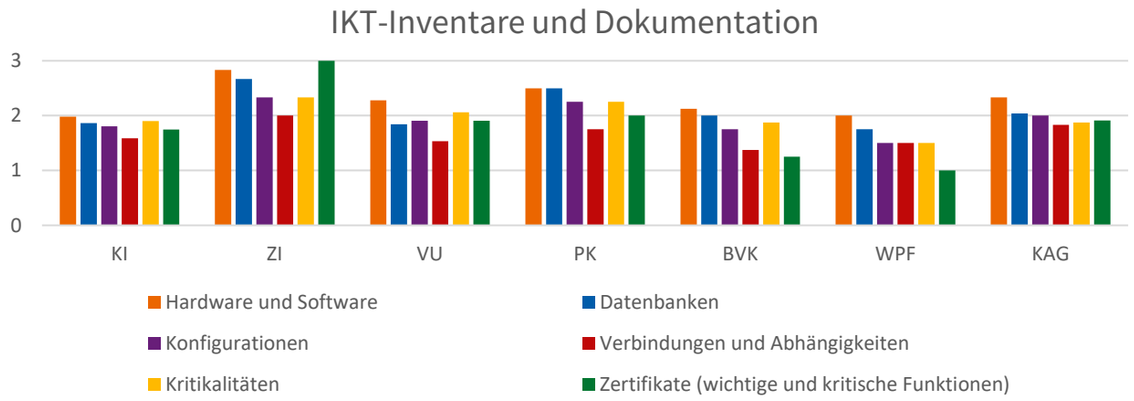


Quelle: FMA, Austrian Digital Finance Landscape 2024

- **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



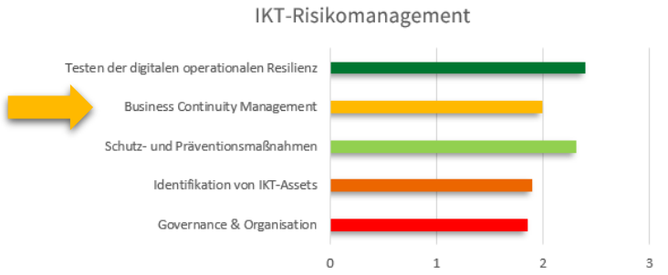
Quelle: FMA, Austrian Digital Finance Landscape 2024

- 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;

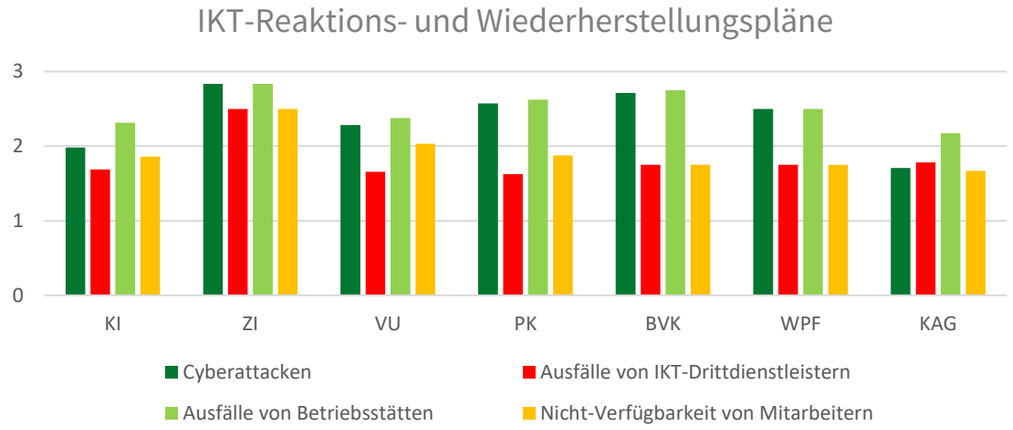
f) Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

g) Angriffe durch Insider;

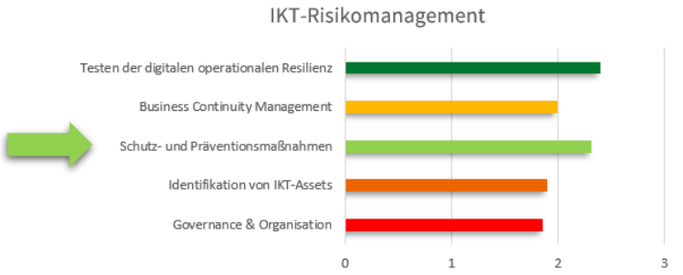
h) politische und soziale Instabilität, sofern relevant auch im Sitzland des IKT-Drittdienstleisters und am Standort der Datenspeicherung und -verarbeitung;

i) weitverbreitete Stromausfälle.

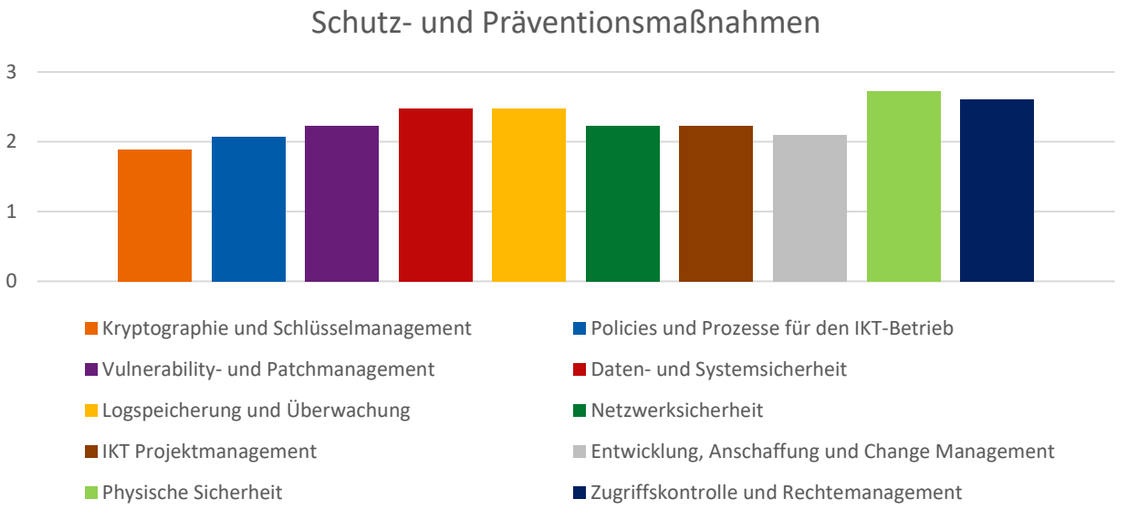
- Dabei zeigt sich, dass insb. Auswirkungen von Insolvenzen oder sonstigen Ausfällen eines relevanten IKT-Drittdienstleister noch nicht in diese Pläne einbezogen sind.



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.

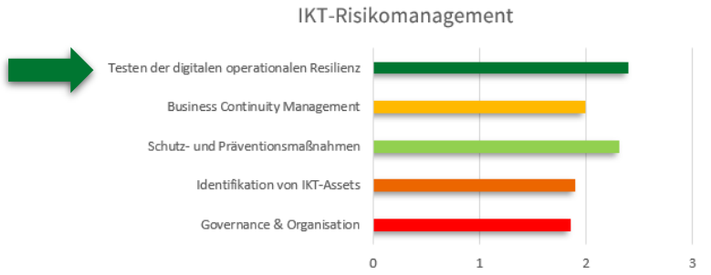
- **Verschlüsselung während der Verarbeitung (in use):** Ist diese nicht möglich, sind die Daten in einer getrennten und besonders geschützten Umgebung zu verarbeiten bzw. es sind andere geeignete Maßnahmen zu treffen (Art 6 Abs 2 VO (EU) 2024/1774).

- **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).

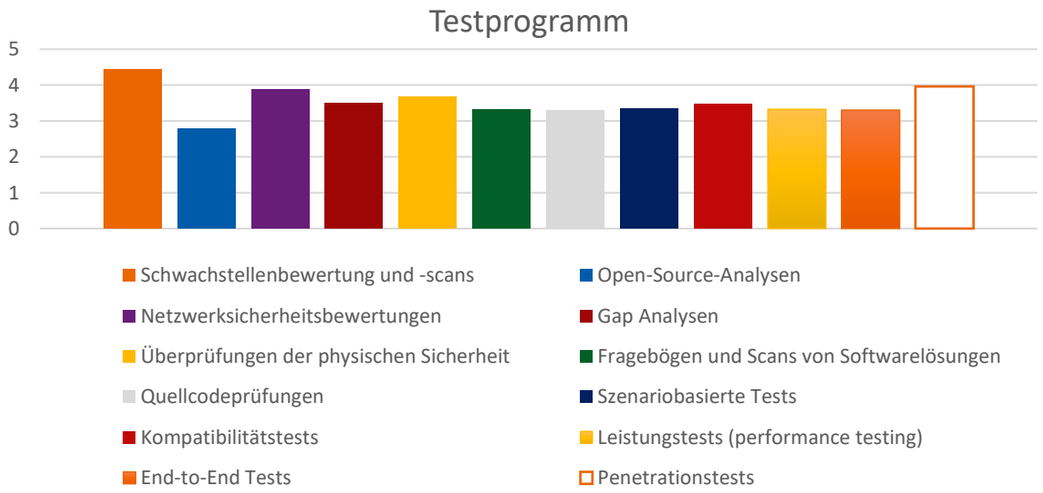
A) IKT-RISIKOMANAGEMENT:
TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ



- **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.

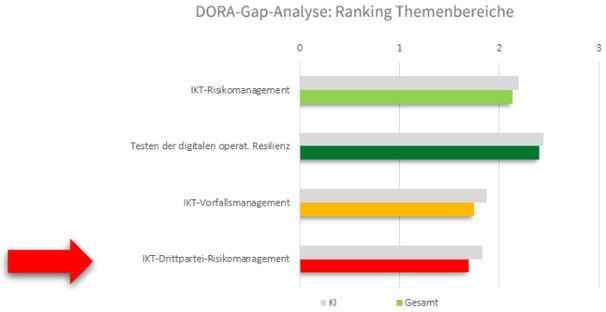
Entwicklungsfelder:

- **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

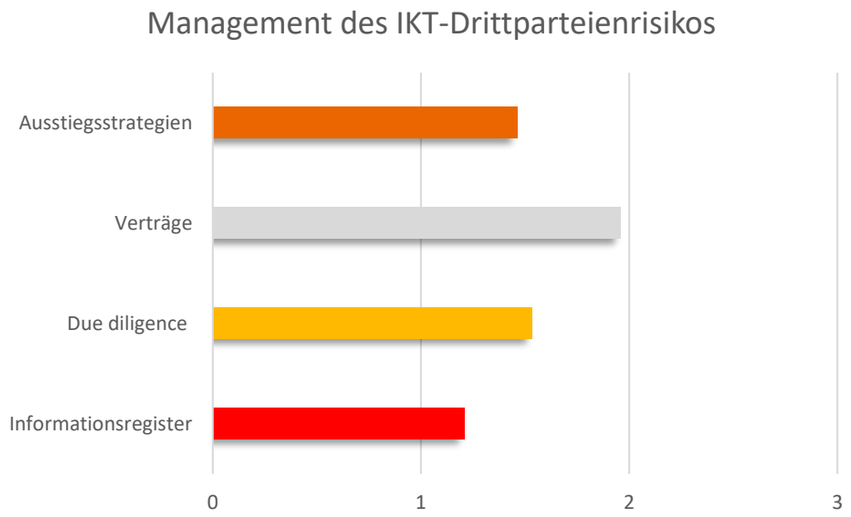


Quelle: FMA, Austrian Digital Finance Landscape 2024

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.

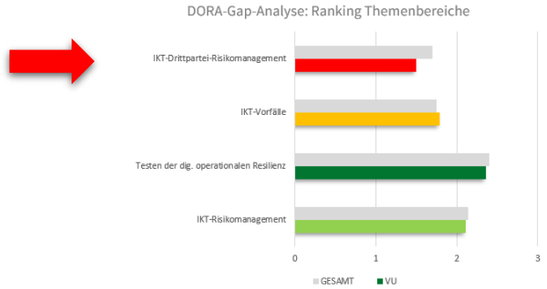


Quelle: FMA, Austrian Digital Finance Landscape 2024

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?).

WANN LIEGT EINE „IKT-DIENSTLEISTUNG“ VOR?



Art 3 Z 21 iVm Art 28 DORA:

Liegt ein **digitaler Dienst** u/o **Datendienst** vor?

Keine Definition in DORA; Annex 3 des ITS on RoI: „Data services“ = zB ‚Provision of data‘

Annex III

Type of ICT services

When referring to a type of ICT services in the templates of the register of information, only the identifier (from S01 to S19) of the relevant type of ICT services shall be reported.

Identifier	Type of ICT services	Description
S01	1. ICT project management	Provision of services related to Project Management Officer (PMO).
S02	2. ICT Development	Provision of services related to: business analysis, software design and development, testing.
S03	3. ICT help desk and first level support	Provision of services related to: helpdesk support and first level support on ICT incident
S04	4. ICT security management services	Provision of services related to: ICT security (protection, detection, response and recovering), including security incident handling and forensics.
S05	5. Provision of data	Subscription to the services of data providers. (digital data service)
S06	6. Data analysis	Provision of services related to the support for data analysis. (digital data service)
S07	7. ICT, facilities and	Provision of ICT infrastructure, facilities and

Wird diese Dienstleistung über ein **IKT-System** bereitgestellt?

Keine Definition in DORA; lediglich EIOPA Guidelines on information and communication technology security and governance („ICT systems: Set of applications, services, information technology assets, ICT assets or other information-handling components, which includes the operating environment.“)

Liegt eine **vertragliche Vereinbarung** mit dem IKT-Drittdienstleister vor?

Art 28 Abs 3 („vertragliche Vereinbarung“) iVm Art 3 Z 19 DORA („ein Unternehmen“)

- FMA (Incoming-Plattform): x
- Bloomberg: provision of data
- LexisNexis: provision of data
- Finanzunternehmen, die zB selbst „digitale Dienste“ für andere Finanzunternehmen erbringen (zB Zahlungs-Dstl) (bisher) nicht ausgenommen!

Erfolgt die Bereitstellung an einen / mehrere interne(n) u/o externe(n) **Nutzer(n)**?

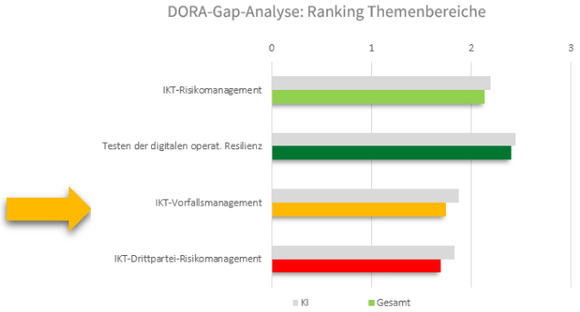
Wird die Dienstleistung **dauerhaft** bereitgestellt?

- Bloß gelegentlich? (zB Hobex)
- Bloßes Nutzungsrecht: x (aber wie im RM behandelt, wenn keine Up-dates & Patches??!)
- Nutzungsrecht + Wartung / Updates: IKT-Dstl!

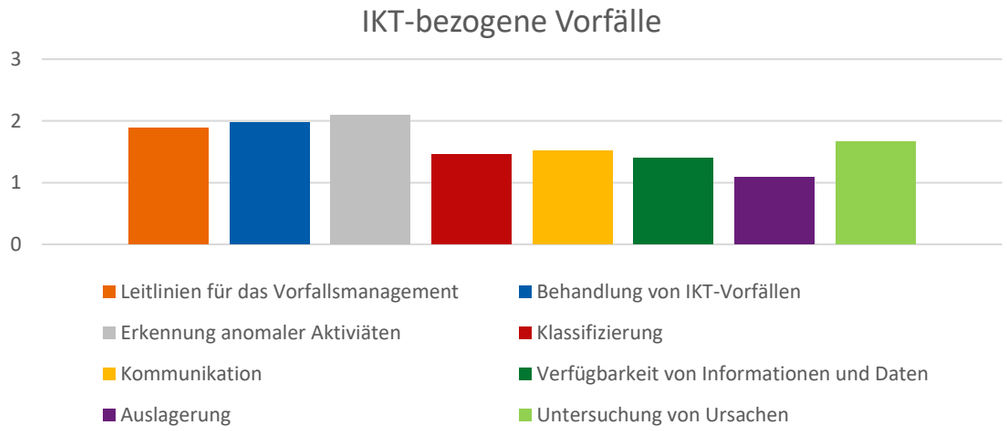
Wird die Dienstleistung für den eigenen operativen **Geschäftsbetrieb** bezogen?

IKT-Dienstleistung! ☺

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

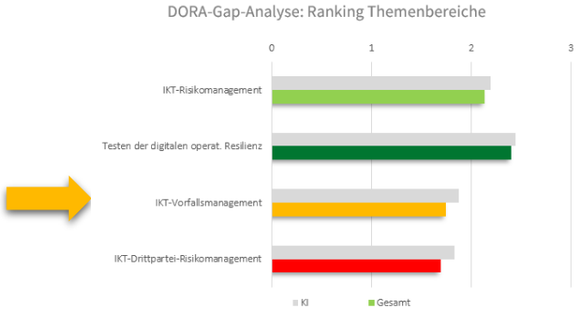
Entwicklungsfelder:

- 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.).

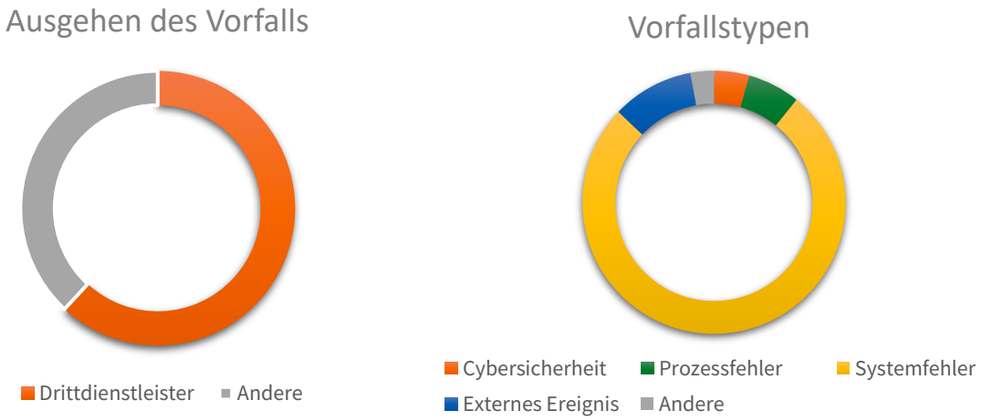
REALITY CHECK



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.

Regulatorisches Up-date

DORA-ENTWICKLUNG

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

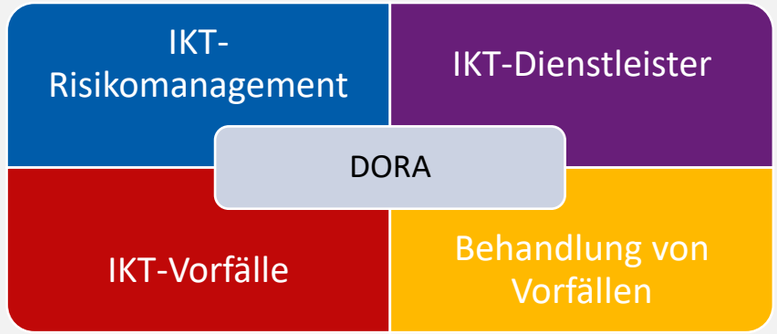
EU-SCICF (Behandlung in DORA-Gremien):	Frist
EU-Systemic Cyber Incident Coordination Framwework	
Basis: ESRB-EU-SCICF-Empfehlung (ESRB/2021/17)	
A1 ESA-Final Report on EU-SCICF-development	16.07.2024
A2 ESA-Final Report on impediments, barriers	16.07.2025
C EC-Final Report on changes to Union legal framework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

Q & A


IKT-Risikomanagement
IKT-Dienstleister
DORA
IKT-Vorfälle
Behandlung von Vorfällen

1) IKT-RISIKOMANAGEMENT:
A) ROLLE DER IKT-KONTROLLFUNKTION

Frage:

1. Wie kann die Sicherstellung der Aufgaben auf Level 2 unter Einbindung der IKT-Kontrollfunktion als gewährleistet gesehen werden?

Hinweise / Erwartungshaltung der FMA:

- Aufgabe: **„das Management und die Überwachung des IKT-Risikos“** (Art 6 Abs 4)
- Als Orientierungshilfe für die Festlegung des Aufgabenbereichs der IKT-Kontrollfunktion kann der Entwurf für Level 2-Rechtsakte* herangezogen werden:
  1. Beratung des Vorstands
  2. Berichterstattung an den Vorstand über die Ergebnisse der IKT-Risikoanalyse
  3. Monitoring / Überwachung des IKT-Risikos
  4. Definition der Ziele für die Informationssicherheit
  5. Festlegung der Leistungsindikatoren und der wesentlichen Risikokennzahlen
  6. Überwachung der Angemessenheit der Klassifizierung von Informations- und IKT-Assets
  7. Entwicklung und Überwachung der Durchführung von Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz.

(*Art. 2 Consultation paper on RTS on ICT risk management framework – wurde mangels Rechtsgrundlage nicht in den finalen Draft RTS übernommen)

IKT-RISIKOMANAGEMENT:
A) CISO ALS IKT-KONTROLLFUNKTION

Frage:

1. CISO als IKT-Risiko-Kontrollfunktion? Im 1. DORA-Dialog am 21. bzw. 23.2.2024 wurde berichtet, dass die IKT-Risiko-Kontrollfunktion operational, nicht aber zwingend organisatorisch getrennt sein muss von den Goverance-Funktionen und von der IT als Risk Owner (inkl. der Tasks der operationellen Info-Sicherheit). Bedeutet das, dass die Funktion vom CISO wahrgenommen werden darf? Falls ja, was ist dabei zu beachten?

Best practice:

1) **Direkte Unterstellung unter den Vorstand** (über eine Stabstelle oder über einen Bereich, der zB im Bereich CRO angesiedelt ist)
2) Kombination von verschiedenen Second line-Funktionen in einer Struktur (zB als Chief Resilience officer) grds. möglich.

Hinweise / Erwartungshaltung der FMA:

- Die IKT-Risiko-Kontrollfunktion kann auch durch den CISO wahrgenommen werden, sofern „ein angemessenes Maß an Unabhängigkeit“ gemäß Art 6 Abs 4 DORA-VO gewährleistet ist.

- **„Ein angemessenes Maß an Unabhängigkeit“** (Art 6 Abs 4 DORA-VO) setzt voraus:

  1. Klare Zuweisung von Zuständigkeiten
  2. Angemessene Ressourcenausstattung; ausreichende fachliche Qualifikation
  3. Direkte Berichtslinie an den Vorstand
  4. Weisungsfreiheit (Keine „Lenkung“: der Vorstand darf nicht Handlungen setzen oder seinen Einfluss ausüben, um zu verhindern, dass die Feststellungen / Warnungen der IKT-Risiko-Funktion von den Entscheidungen / Handlungen des Vorstands abweichen)
  5. Freier Zugang zu Mitarbeitenden & Informationen
  6. **„operationale“ (nicht aber zwingend eine organisatorische) Trennung** von
     - der IT als risk owner inkl. der tasks der operat. Info-Sicherheit
     - den Governance-Funktionen inkl. RM-Funktion, der internen Revision

IKT-RISIKOMANAGEMENT:
B) ROLLE DER COMPLIANCE-FUNKTION

Frage:

1. Welche Aufgaben sollte die Compliance Funktion in Bezug auf IT Compliance im speziellen mit Bezug auf DORA wahrnehmen?

Es ist aber **nicht** die Aufgabe der Compliance-Funktion,

a) die „übrigen" aufsichtsrechtlich normierten Compliance-Funktionen (zB die „Funktion zur Überwachung der Verträge mit IKT-Drittdienstleistern" gemäß Art 5 Abs 3 DORA-VO), zu kontrollieren (das ist die Aufgabe der internen Revision!) oder

b) ihre Agenden zu duplizieren (das würde ua dem Grundsatz einer angemessenen Trennung der Zuständigkeiten widersprechen).

Hinweise / Erwartungshaltung der FMA:

- Aufgaben der Compliance-Funktion gem § 118 VAG und Art 270 Abs 2 DelVO

  1. **Frühwarnfunktion:** Eine laufende Beobachtung des Rechtsumfelds!
  2. **Beratung des Vorstands:** Die Beratung soll rechtmäßige Entscheidungen durch den Vorstand ermöglichen. Daraus ergibt sich auch, dass vor Entscheidung durch den Vorstand auch die relevanten rechtlichen Analysen vorliegen müssen!
  3. **Compliance-Risiko-Analyse:** Die möglichen Risiken aus der Nicht-Einhaltung von DORA (inkl. RTS etc.) identifizieren & beurteilen!
  4. **Angemessenheitskontrolle:** Bewertung der Angemessenheit der vom VU getroffenen Maßnahmen zur Verhinderung einer Non-Compliance.

- Der **Grundsatz der wechselseitigen Zusammenarbeit** mit den anderen Govern.-Funktionen (inkl. IKT-Risikokontrollfunktion!) (Art 268 Abs 1 L2-VO [EU] 2015/35) impliziert, dass sich diese einzelnen Funktionen vor der Befassung des Vorstands bei Bedarf abstimmen.

Vgl. auch *Korinek/S. Saria* in *Korinek/G. Saria/S. Saria,* VAG § 118 Rz 31, 38 (Stand 1.11.2020, rdb.at)

IKT-RISIKOMANAGEMENT:
C) INFORMATIONSASSETS

Fragen:

1. Welcher Abstraktionslevel wäre angemessen?
   Und wie ist hinsichtlich der Bewertung deren Kritikalität vorzugehen?

Hinweise / Erwartungshaltung der FMA:

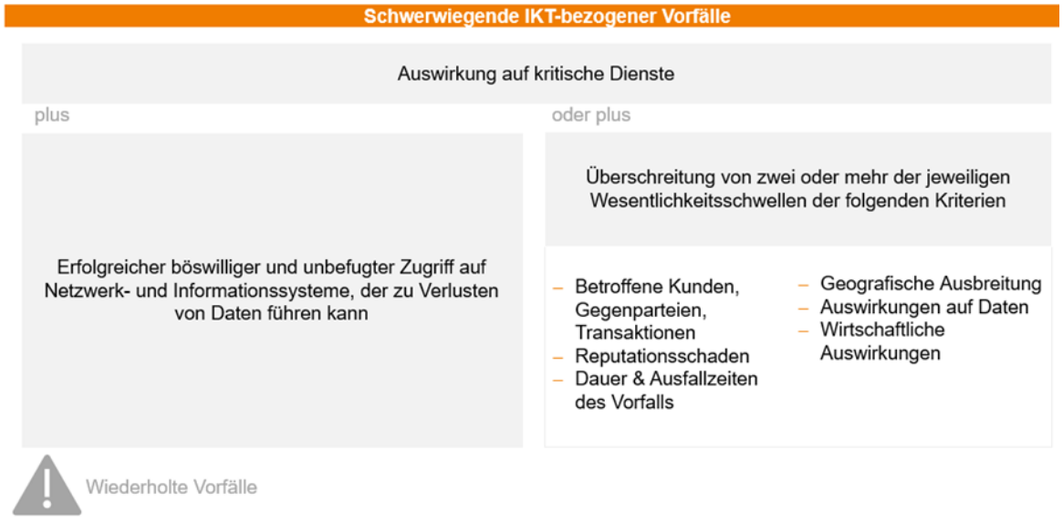
- Begriffsbestimmung in Art 3 Z 6 DORA-VO:
  „Informationsasset“ eine Sammlung materieller oder immaterieller Informationen, die geschützt werden sollten.

  Unternehmen haben selbst zu evaluieren, welche Informationen vor IKT-Risiken inkl. jener des unbefugten Zugriffs oder der unbefugten Nutzung zu schützen sind.

  Bei der Bewertung der Kritikalität können die in Art 3 (22) DORA-VO genannten Kriterien herangezogen werden.

2) IKT-VORFALLSMANAGEMENT

Klassifikation IKT-bezogener Vorfälle:



Fristgerechte Meldung schwerwiegender IKT-bezogener Vorfälle:

Hinweise aggregiertes Reporting:

- Finanzunternehmen sind zur Meldung verpflichtet (Art 19 Abs 1 DORA-VO).
  - Möglichkeit der Auslagerung der Meldeverpflichtung an einen Drittdienstleister (Art 19 Abs 5 DORA-VO)
    ⇨ Vorabinformation an FMA (Art 6 ITS on major ICT-related incidents)
  - Aggregiertes Reporting durch den Drittdienstleister für mehrere Finanzunternehmen möglich (Art 7 ITS on major ICT-related incidents)

Hinweise Wochenend- und Feiertagsbestimmung:

- Voraussichtliche keine Benennung weiterer signifikanter oder systemischer Finanzunternehmen, für welche die Wochenend- und Feiertagsbestimmung nicht gelten würde.

Hinweise zu FMA-Tätigkeiten:

- Weitermeldungen + Bewertung mit EIOPA (in Abstimmung mit ENISA) zur Relevanz in anderen Mitgliedstaaten + Treffen von Schutzvorkehrungen zur Finanzstabilität
- Empfangsbestätigung der Meldungen + Möglichkeit von Rückmeldungen + Berichte + Förderung Informationsaustausch zu Cyberbedrohungen

IKT-VORFALLSMANAGEMENT
A) WIRTSCHAFTLICHE AUSWIRKUNGEN

Fragen:

1. Wie werden Kosten und Verluste sowie finanzielle Wiedereinziehungen berücksichtigt bzw. berechnet?

Hinweise / Erwartungshaltung der FMA:

- Bei der Erstellung der rechtlichen Vorgaben wurde auf Kohärenz abgezielt:
  - Klassifizierung schwerwiegender IKT-bezogener Vorfälle:
    Kriterium wirtschaftliche Auswirkungen: Art 7 Delegierte VO (EU) 2024/1772 zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen (ohne Einrechnung von finanziellen Wiedereinziehungen)
  - Abschlussmeldung zu schwerwiegenden IKT-bezogenen Vorfällen:
    Relevant sind insb.:
    4.13 Amount of gross direct and indirect costs and losses und
    4.14. Amount of financial recoveries
    in Annex II ITS on major ICT-related incidents.
  - Aggregierte jährliche Kosten und Verluste:
    Bei Anforderung durch die zuständige Behörde, werden Kosten und Verluste für schwerwiegende IKT-bezogene Vorfälle sowie Wiedereinziehungen für das Referenzjahr – entsprechend der Leitlinien für die Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste – aggregiert. Intendiert ist dabei, dass Kosten auch auf Jahresbasis verfügbar sind.

IKT-VORFALLSMANAGEMENT
B) MELDEWEGE

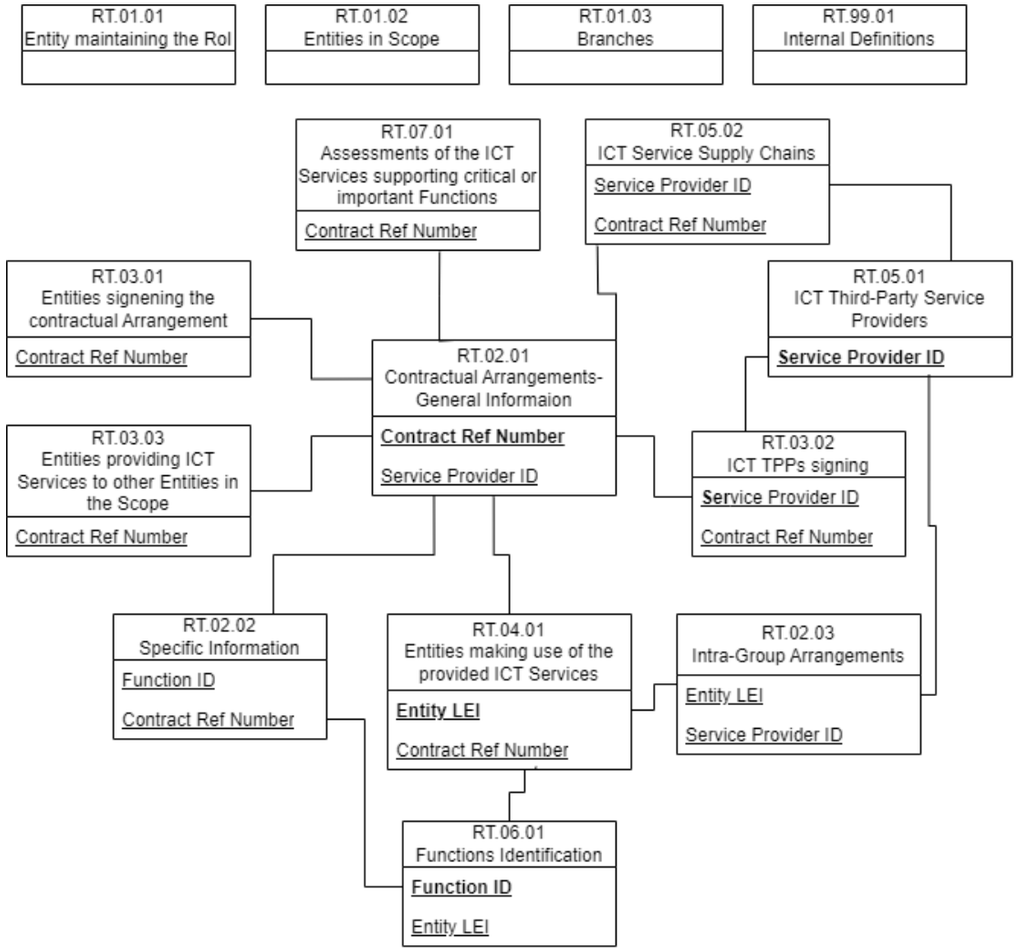
Fragen:

1. Wird es Schnittstellen zur Online-Plattform für Einmeldungen geben?
2. Und welche alternativen Wege werden für Meldungen vorgesehen?
3. Werden die auf Anfrage der Behörde zu erfolgenden Meldungen der geschätzten aggregierten jährlichen Kosten und Verluste auf demselben Wege zu erstatten sein wie die Meldungen von schwerwiegenden IKT-bezogenen Vorfällen?

Hinweise / Erwartungshaltung der FMA:

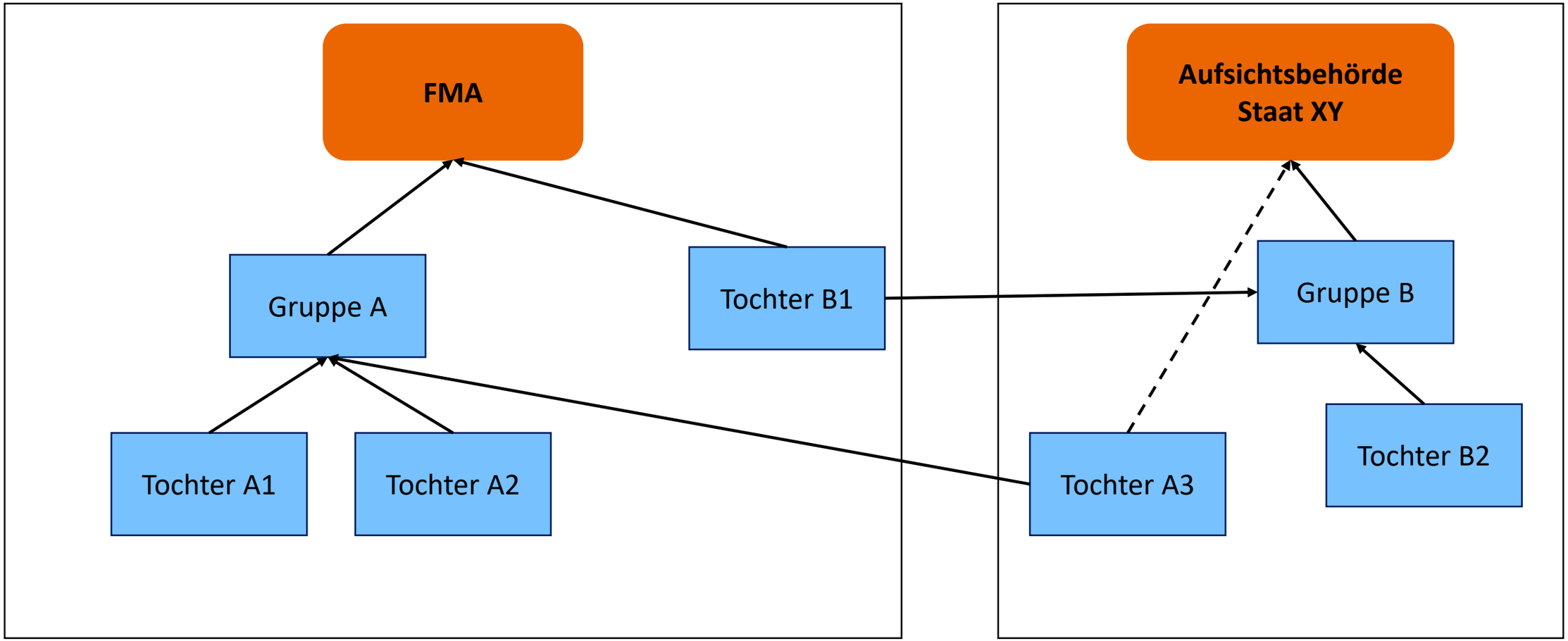
- Meldungen erfolgen gs. über die FMA Incoming-Plattform.
- Ein alternativer Meldeweg wird voraussichtlich über FTAPI ermöglicht.
- Meldungen zu jährlichen Kosten/Verlusten werden ggf über die FMA-Incoming Plattform erfolgen.

3) IKT-DRITTPARTEI-RISIKOMANAGEMENT:
A) ALLGEMEINE INFORMATION



- 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.

IKT-DRITTPARTEI-RISIKOMANAGEMENT:
B) KONSOLIDIERUNG INFORMATIONSREGISTER



IKT-DRITTPARTEI-RISIKOMANAGEMENT:
C) VERHÄLTNIS IT-GRUPPENPROVIDER ⇔ EXTERNE IKT-PROVIDER

Fragen:

Gemischte interne und externe Dienstleisterketten in Konzernstrukturen:

1. In RT.01.02 abzubildende Gesellschaften

2. Abbildung von Vertragsketten innerhalb des Konzerns in den einzelnen

3. Abbildung der Subdienstleister

Hinweise / Erwartungshaltung der FMA:

1. Grundsätzlich sind hier alle Gruppengesellschaften im Scope von DORA abzubilden, bei welchen es sich entweder um Finanzinstitute oder interne IKT-Dienstleister handelt.

2. Bei Vertragsketten ist in **RT.03.01** der tatsächliche Unterzeichner (nicht notwendigerweise Nutznießer) eines Dienstleistungsvertrages von Bezieherseite anzugeben. In **RT.03.03** wird der Unterzeichner von Dienstleisterseite angegeben. Mittels **RT.02.03** können Verträge einer Kette miteinander verknüpft werden. In **RT.04.01** sind die tatsächlichen Bezieher der Leistung (nicht administrativ zwischengeschaltete Einheiten) anzuführen.

3. In Sheet **RT.05.02** ist grundsätzlich die relevante Dienstleisterkette für kritische/wichtige Funktionen abzubilden, ungeachtet dessen, ob es sich um interne oder externe DL handelt. Bei internen DL gibt es zwei Besonderheiten:

    1. In Sheet **RT.05.02** ist bei vorgelagerten internen DL, jedenfalls der erste externe DL anzuführen – auch bei DL, die keine kritischen/wichtigen Funktionen unterstützen.

    2. In Sheet **RT.07.01** sind bei DL, welche kritische/wichtige Funktionen unterstützen, Details zum ersten externen DL anzuführen – auch wenn interne DL vorgelagert sind.

IKT-DRITTPARTEI-RISIKOMANAGEMENT:
D) AUSWAHL DER „LICENCED ACTIVITY“ (RT.06.01)

Fragen:

1. Lizenzierte Aktivitäten bei VU

2. Aktivitäten, die nicht direkt für Kernleistung, aber für die korrekte Erbringung der lizensierten Aktivität notwendig sind (z.B. Governance-Funktion)

3. Zuordnung von Aktivitäten, welche diese lizensierten Aktivitäten direkt unterstützen (bspw. Sanktionsprüfung vor Angebotslegung)

Hinweise / Erwartungshaltung der FMA:

1. Entsprechen Annex I und Annex II der SII-Richtlinie (2009/138/EC), dh z.B. Unfall, Krankheit, Landfahrzeug-Kasko,…

2. Auch Voraussetzungen aus der Konzessionierung wie z.B. Governance-Funktionen sind der lizenzierten Aktivität zuzuordnen

3. Auch Unterstützungsfunktionen wie z.B. Sanktionsprüfungen sind wenn möglich der lizenzierten Aktivität zuzuordnen (ansonsten im Informationsregister als ‚Support Function‘ anzuführen)

IKT-DRITTPARTEI-RISIKOMANAGEMENT:
E) ALLGEMEINE FRAGEN

Fragen:

1. Kritische Dienstleister (CTPPs) auf europäischer Ebene vs. kritische Dienstleister nach interner Definition des Unternehmens

2. Social Media Plattformen und Online Code-Repositories (z.B. Github)

3. Konzessionierte Unternehmen, welche IKT-Dienstleistungen erbringen

4. Softwarelizenzierung

Hinweise / Erwartungshaltung der FMA:

1. CTPPs werden von den ESAs voraussichtlich in der 2. Hälfte 2025 veröffentlicht. Sie sind grundsätzlich von Finanzunternehmen zu behandeln wie andere DL (mit dem Vorteil, dass zusätzliche zentrale Aufsichtsmaßnahmen gesetzt werden). Der Status des CTPP ist unabhängig davon, wie kritisch der DL für ein einzelnes Unternehmen ist- hier ist unter DORA die individuelle Einschätzung und die Verknüpfung mit kritischen/wichtigen Funktionen ausschlaggebend.

2. Frage, unter welchen Umständen hier keine IKT-Dienstleistung vorliegt, wird an ESAs gestellt.

3. Frage, ob es hier eine generelle Ausnahme vom Status des IKT-Dienstleisters geben wird, wird bei ESAs diskutiert.

4. Ist grundsätzlich im Annex III des ITS zum Informationsregister als Art der IKT-Dienstleistung verankert. Um die Definition voll zu erfüllen, sind allerdings auch Leistungen auf laufender Basis (Updates, Support) nötig.

IKT-DRITTPARTEI-RISIKOMANAGEMENT:
E) ALLGEMEINE FRAGEN

Fragen:

1. Klassifizierung als ‚Data Provider' nach Annex III des ITS

2. FAQs

Hinweise / Erwartungshaltung der FMA:

1. Wenn von einem Dienstleister periodisch auf elektronischem Wege Daten übertragen werden und diese im Rahmen von IKT-Systemen in Geschäftsprozessen genutzt werden, liegt sehr wahrscheinlich eine IKT-Dienstleistung iSv DORA vor. Die Technologie der Datenschnittstelle (csv, xml, etc.) ist dabei unerheblich

2. FAQs der ESAs, EBA und FMA zum Thema DORA-Drittparteienrisiko sind unter folgenden Links zu finden:
   - Joint Q&As – EIOPA
   - Preparation for DORA application | European Banking Authority
   - DORA – Überwachungsrahmen kritischer IKT-Drittdienstleistender - FMA Österreich

IKT-DRITTPARTEI-RISIKOMANAGEMENT:
F) FRAGEN ZU KONKRETEN DATENFELDERN

Fragen:

1. Ist in Feld RT.05.01.0080 (ID der DL-Konzernmutter) immer nach Möglichkeit ein LEI-Code anzugeben?

2. Wie ist Feld RT.02.02.0130 (Country of provision of the ICT services) zu interpretieren?

Hinweise / Erwartungshaltung der FMA:

1. Zu diesem (und einigen anderen) Feldern in welchen Identifikationscodes anzugeben sind, gibt es diese Vorgabe bislang nicht explizit. Intention des ITS scheint jedoch sein, primär LEI-Codes zu verwenden, sofern vorhanden. Eine entsprechende Einschränkung im finalen ITS ist also denkbar.

2. Hier ist der Staat zu hinterlegen, in welchem die Leistung tatsächlich vom Dienstleister erbracht wird (Ort der Datenspeicherung/Verarbeitung etc.).

Ausblick 2025

AUFSICHTS- UND PRÜFSCHWERPUNKTE 2025

- **Deep Dives zum digitalen Risikoprofil** auf Basis der „Austrian Digital Finance Landscape“ grds. mit allen Unternehmen
- **1. Meldung zu Register of Information**: Ermittlung der IKT-Verflechtungen am ö Finanzmarkt & Identifikation kritischer IKT-Dienstleister
- (Vorbereitung der) Durchführung von **Threat-Led Penetration Tests**
- **Vor-Ort-Prüfungen** zur IKT-Sicherheit im 2. HJ 2025