AUSTRIAN FMA · FINANCIAL MARKET AUTHORITY

AUSTRIAN DIGITAL FINANCE LANDSCAPE 2024

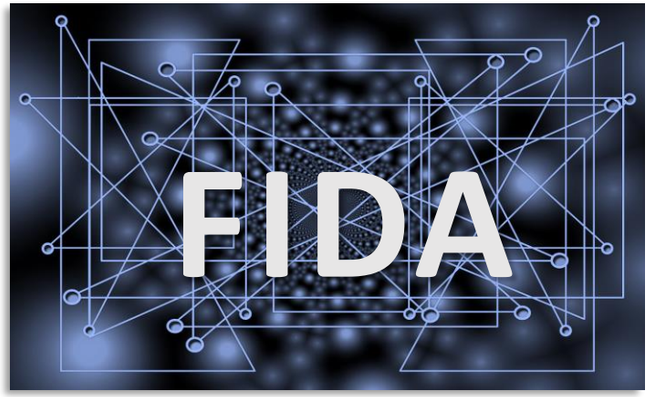
INKL. DRY RUN ZUM INFORMATIONSREGISTER

FMA, 4. Dezember 2024

AGENDA

1. **Begrüßung**
   - Peter Braumüller
2. **„Austrian Digital Finance Landscape“** inkl. DORA-Gap-Analyse
   - Stanislava Saria
3. **Regulatorisches Up-date & Take aways zu Incident Reporting**
   - Sabine Balogh-Preininger
4. **Ergebnisse des Dry runs zum Informationsregister**
   - Alexander Kiennast
5. **Follow-up und FMA-Aufsichtsschwerpunkte 2025**
   - KI / ZI / E-Geld-Institute: Anna Muri, Michael Mandelburger
   - VU / PK / BVK: Stanislava Saria
   - Marktinfrastrukturen: Eva Janos
   - WPF & Crowd-Dstl: Brigitte Botlik
   - KAG, ImmoKAG, AIFM: Norbert Fröhlich
   - Bankenabwicklung: Helene Salcher

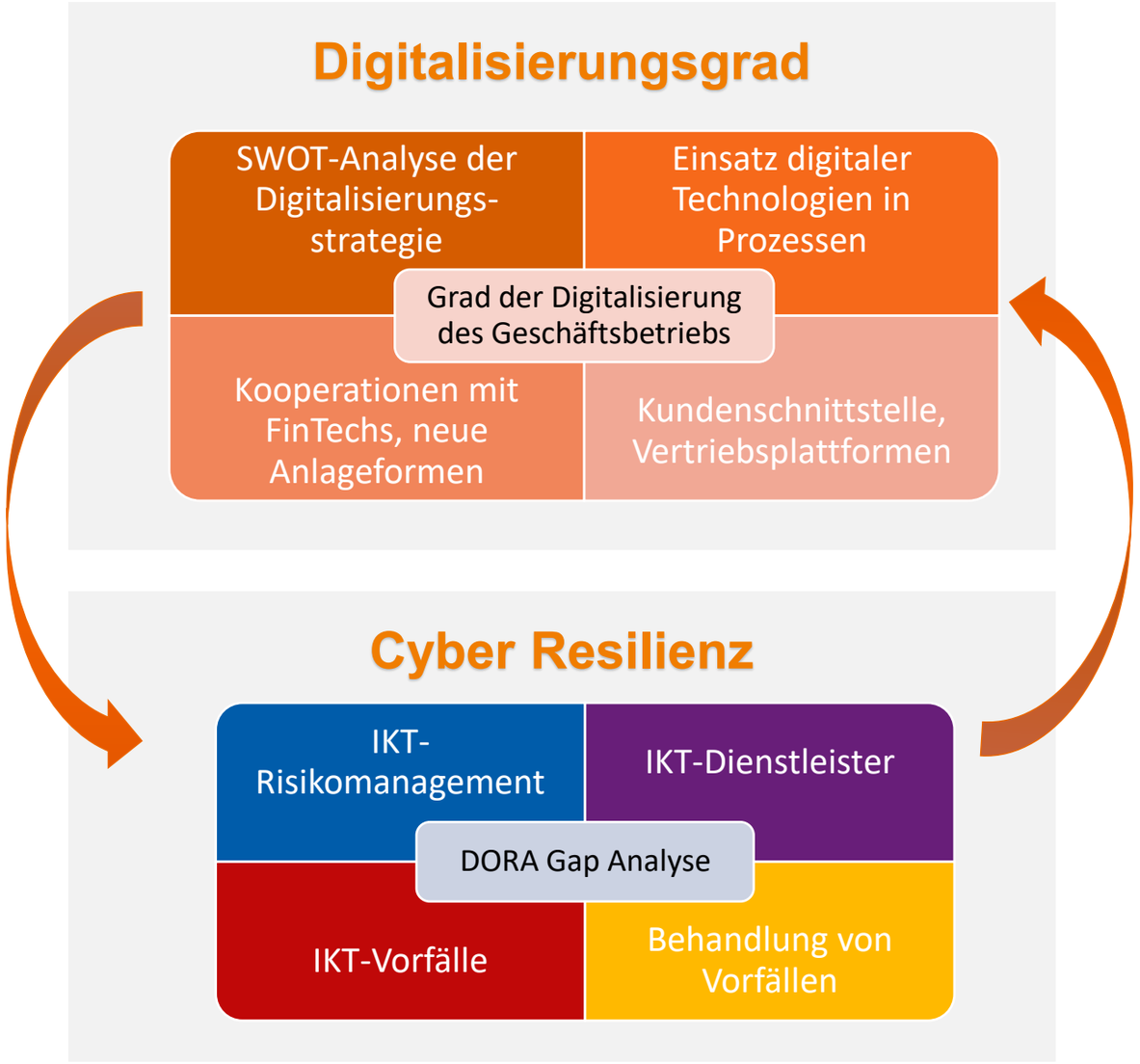
DORA / AIA / FIDA ANTE PORTAS…



	Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor	Verordnung (EU) 2024/1689 zur Festlegung harm. Vorschriften für künstliche Intelligenz	Vorschlag für eine Verordnung über einen Rahmen für den Zugang zu Finanzdaten
Anwendbar ab	▪ **17. Jänner 2025** (kein Grandfathering!)	▪ **2. Februar 2025** (**KI-Kompetenz** von mit KI-Systemen befassten Personen + **verbotene KI-Praktiken**) ▪ **2. August 2025** (Anforderungen an **General-purpose AI models** + **Governance** auf EU-Ebene + NCAs) ▪ **2. August 2026** (Hochrisikosysteme – Annex III [= zB Bonitätsbewertung]) ▪ **2. August 2027** (Hochrisikosysteme – Annex I [= products listed in EU legisl.])	▪ **24 Monate** nach dem Inkrafttreten der Verordnung ▪ **18 Monate** nach dem Inkrafttreten der Verordnung (Artikel 9 bis 13 = Dateninhaber und Datennutzer werden Mitglied eines „Systems für den Austausch von Finanzdaten“ + Zulassung von Finanzinformations-dienstleister [FISPs])

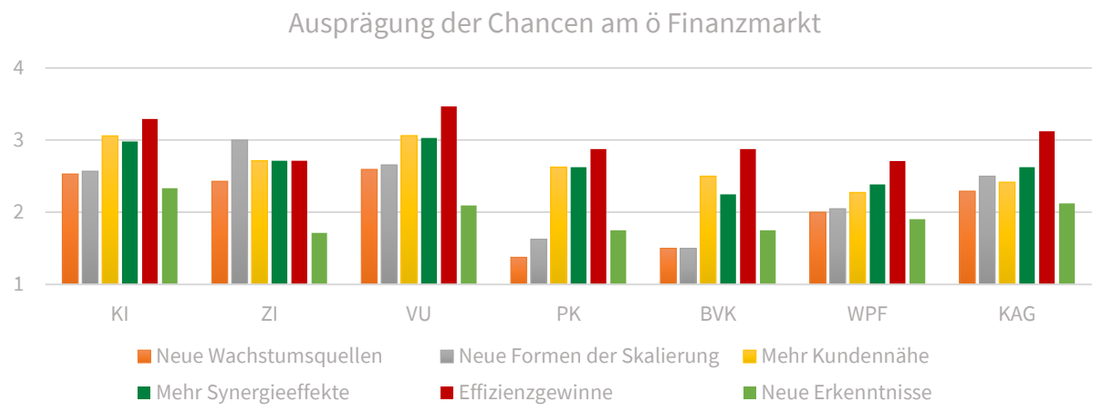
AUSTRIAN DIGITAL FINANCE LANDSCAPE 2024

- 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



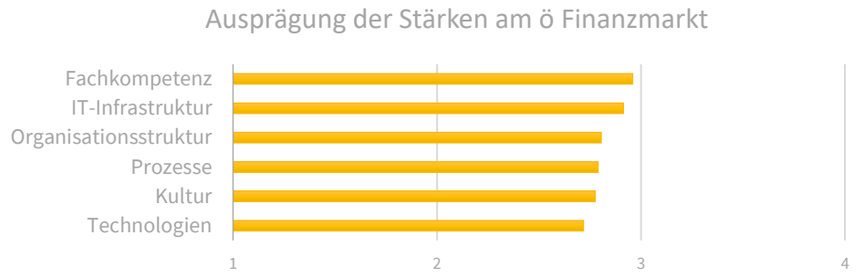
1) IST DAS UNTERNEHMEN STRATEGISCH RICHTIG AUFGESTELLT?

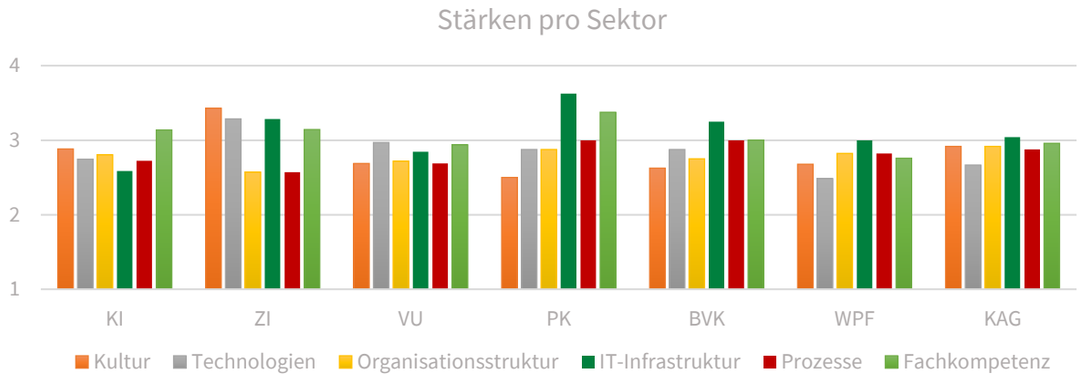
- Die Unternehmen am ö Finanzmarkt stufen die Digitalisierung als sehr relevantes Thema ein und sind bereit, Maßnahmen zu setzen, um diese Entwicklung für sich zu nutzen. Die Möglichkeit, dass es infolge der zunehmenden Digitalisierung zu Disruption kommt, wird nach wie vor als kaum denkbar eingestuft.
  - Auch der zunehmende Einsatz von künstlicher Intelligenz wird als Innovationstreiber, nicht jedoch als disruptiver Faktor betrachtet.
  - Die beaufsichtigten Unternehmen sehen bei der Digitalisierung primär die **Chance**, **Effizienzgewinne** und **Geschäftsoptimierung** zu erzielen.



Quelle: FMA, Austrian Digital Finance Landscape 2024;
Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Chance

Bei der Analyse ihrer Digitalisierungsstrategie sehen die Beaufsichtigten ihre **Stärken** vor allem in der **Fachkompetenz** und der **IT-Infrastruktur.**



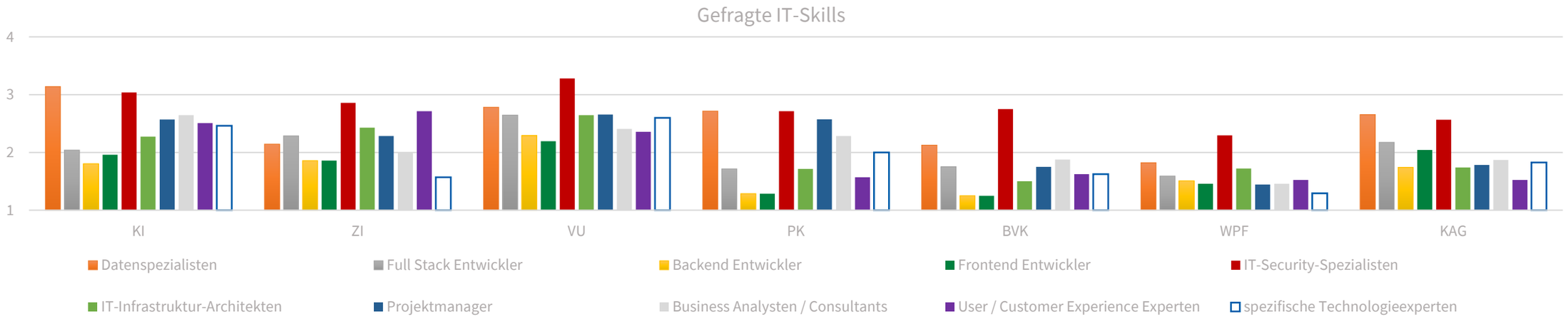


Quelle: FMA, Austrian Digital Finance Landscape 2024;
Durchschnittswerte pro Sektor mit 1: schwach, 2: eher schwach, 3: stark, 4: besonders stark

2) WELCHE **EXPERTISE** MUSS AUSGEBAUT WERDEN?

- Durch die voranschreitende Digitalisierung können neue Chancen und Möglichkeiten entstehen, welche gerade vor dem Hintergrund des steigenden Konkurrenzdrucks spezialisierte IT-Kompetenzen erfordern.

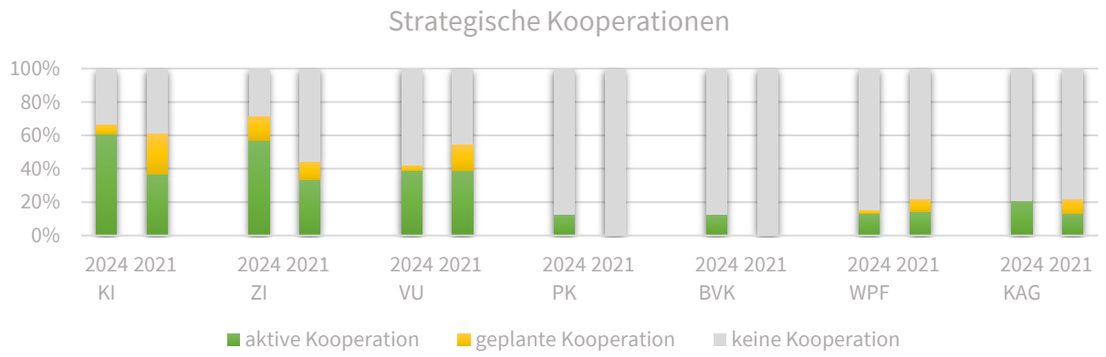
- Während 2021 neben **IT-Security- Spezialist:innen** (welche 2018 nur begrenzt im Fokus standen) Projektmanager:innen und Analyst:innen gesucht wurden, welche ein entsprechendes technisches Verständnis haben, um digitale Unterfangen zu leiten und zu unterstützen, herrscht nun Bedarf an Fachkräften verschiedener Disziplinen:
  - Tendenziell wird **Datenspezialisten**, **IT-Infrastruktur-Architekten** und **Management- bzw. Analystenstellen** mit Technikaffinität aktuell eine höhere Relevanz als
  - dem Tätigkeitsbereich der reinen Softwareentwicklung zugeschrieben.



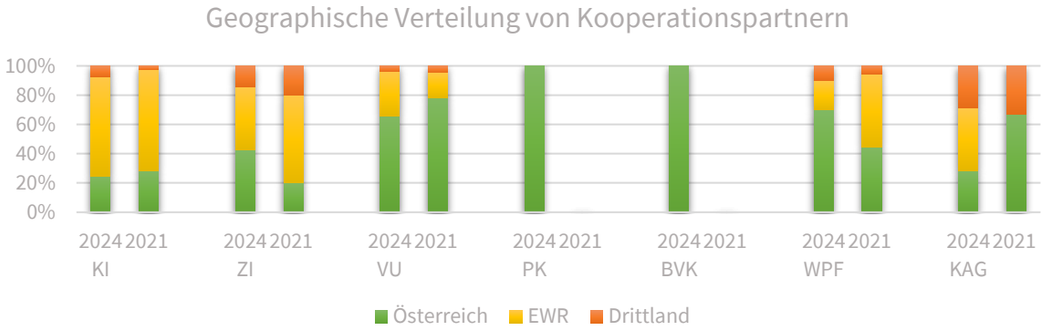
Quelle: FMA, Austrian Digital Finance Landscape 2024;
Durchschnittswerte pro Sektor mit 1: schwach, 2: eher schwach, 3: stark, 4: besonders stark

3) WELCHE KOOPERATIONEN SIND NOTWENDIG?

- Trotz der Marktbereinigung und Konsolidierung am FinTech-Markt in den letzten drei Jahren hält der **Trend zur Zusammenarbeit mit FinTech-Start-ups** an.
- Nicht nur die Zahl der Kooperationen mit FinTechs nimmt zu.
- Auch der Anteil der mit FinTechs kooperierenden Beaufsichtigten ist seit 2021 von 23 % auf 32 % gestiegen.
  - Insbesondere Kredit- und Zahlungsinstitute (je 60 %) sowie VU (40 %) gehen Partnerschaften mit FinTechs/InsurTechs ein.

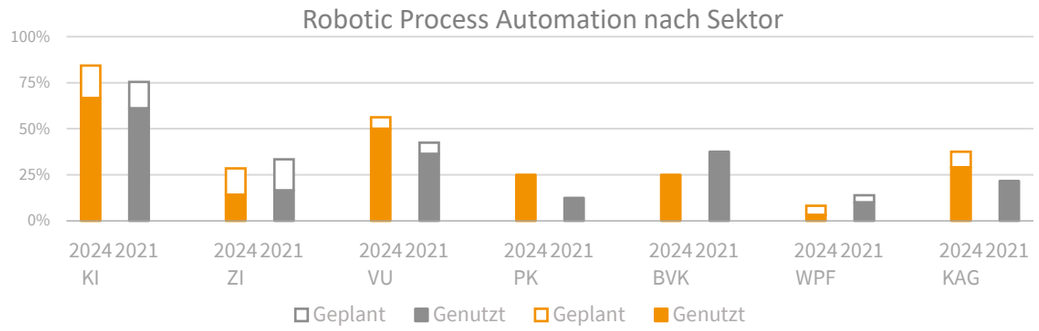


Quelle: FMA, Austrian Digital Finance Landscape 2024

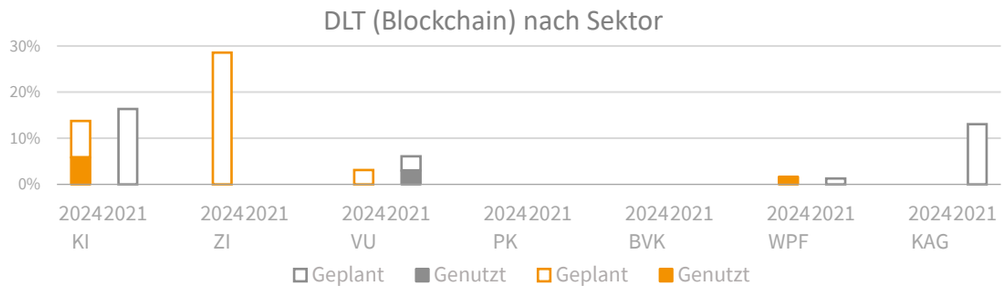


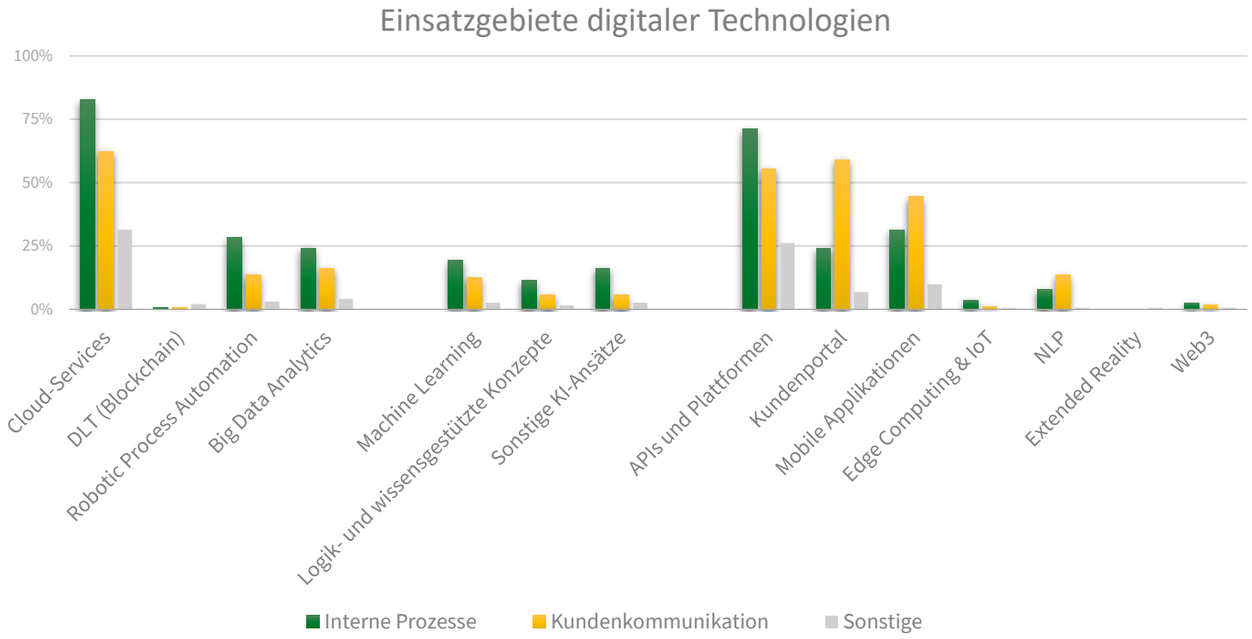
4) SIND DIE EINGESETZTEN DIGITALEN TECHNOLOGIEN NOCH ZEITGEMÄß?

- **Robotics:** Der Einsatz von RPA hat seit 2018 deutlich zugenommen; besonders stark bei den KI und VU.



- **Distributed-Ledger-Technologie (DLT):** Über den gesamten ö Finanzmarkt hinweg nutzen nur vier Unternehmen die DLT.

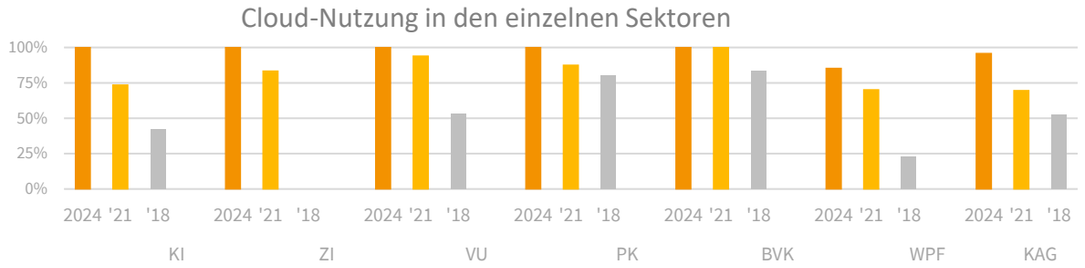




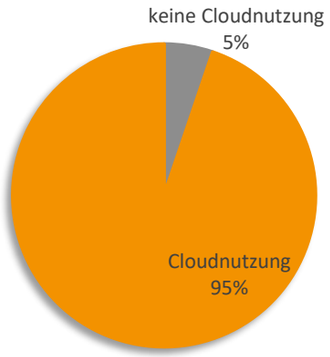
Quelle: FMA, Austrian Digital Finance Landscape 2024

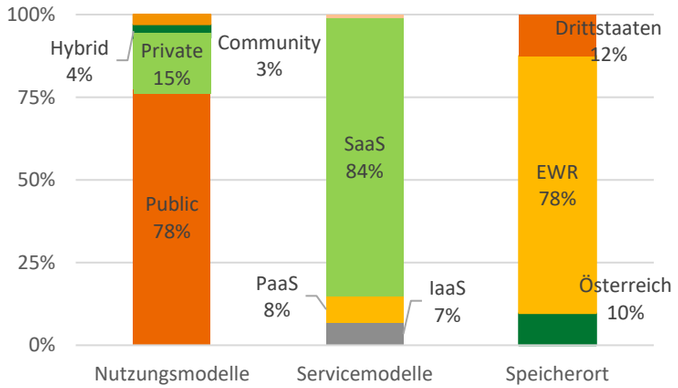
5) WELCHE DATEN LIEGEN IN EINER CLOUD?

- **Cloud services** haben seit 2018 stark an Bedeutung gewonnen und werden nun praktisch universell in allen Finanzmarktsektoren eingesetzt.

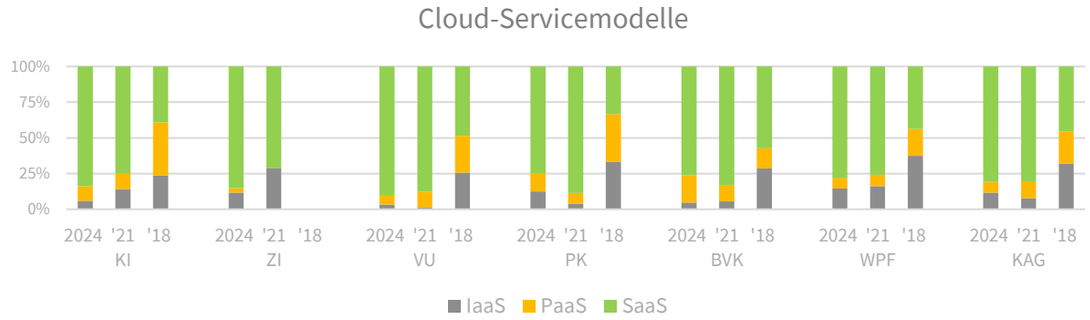


- Cloud services werden von 95 % der Beaufsichtigten in ihrem Geschäftsbetrieb genutzt.

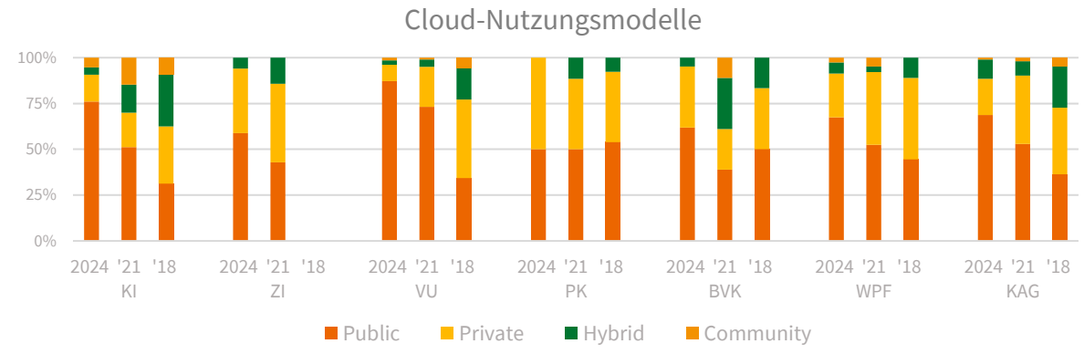




- 84% aller von den beaufsichtigten Unternehmen genutzten Cloud-Dienste sind dem **Servicemodell „Software as a Service“ (SaaS)** zuzurechnen.



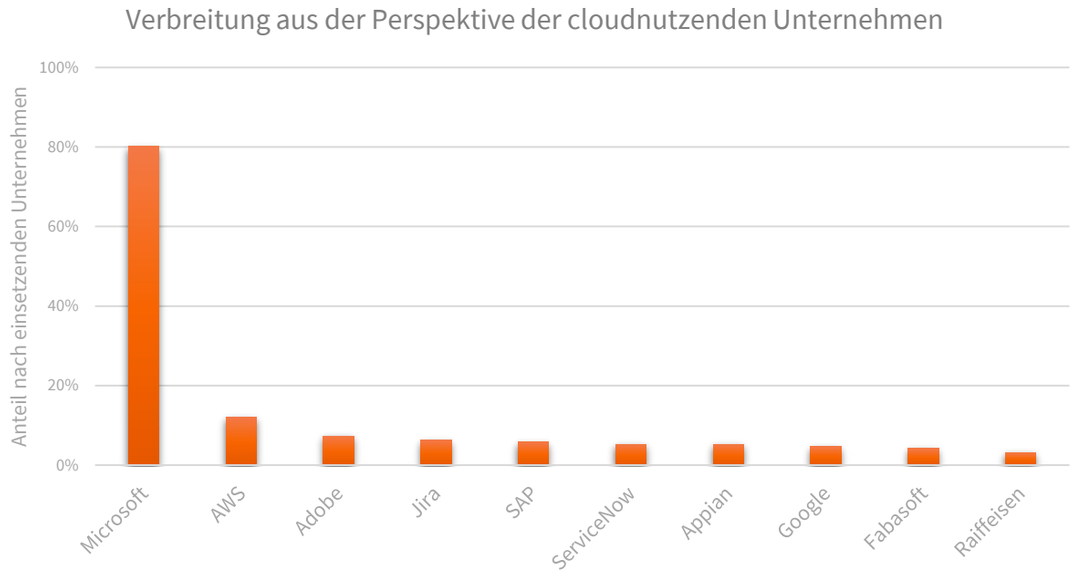
- Die Inanspruchnahme von **Public Clouds** hat sich seit 2021 erhöht. Aktuell entfallen rund 80% der Cloud-Services auf dieses Nutzungsmodell.

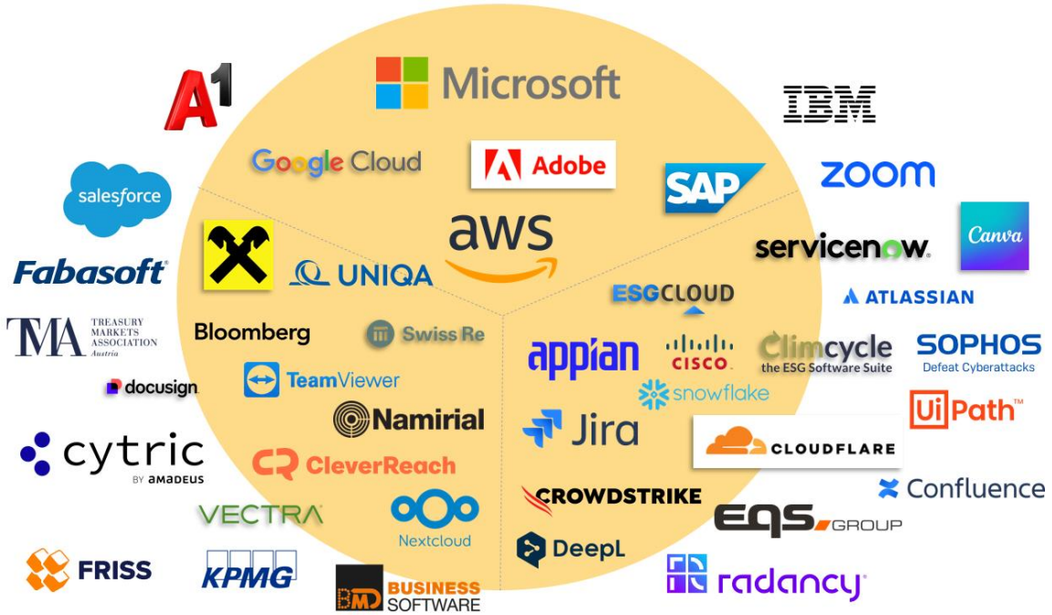


Quelle: FMA, Austrian Digital Finance Landscape 2024

LANDSCAPE DER CLOUD-DIENSTLEISTER AM Ö FINANZMARKT

- 80% der beaufsichtigten Unternehmen am ö Finanzmarkt verwenden mindestens ein **Microsoft-Produkt**; bei AWS sind es 12% der Unternehmen.
- Alle weiteren Anbieter haben nur einen einstelligen prozentuellen Anteil. Der österreichische Cloud-Anbieter Fabasoft kommt auf etwa 4%.

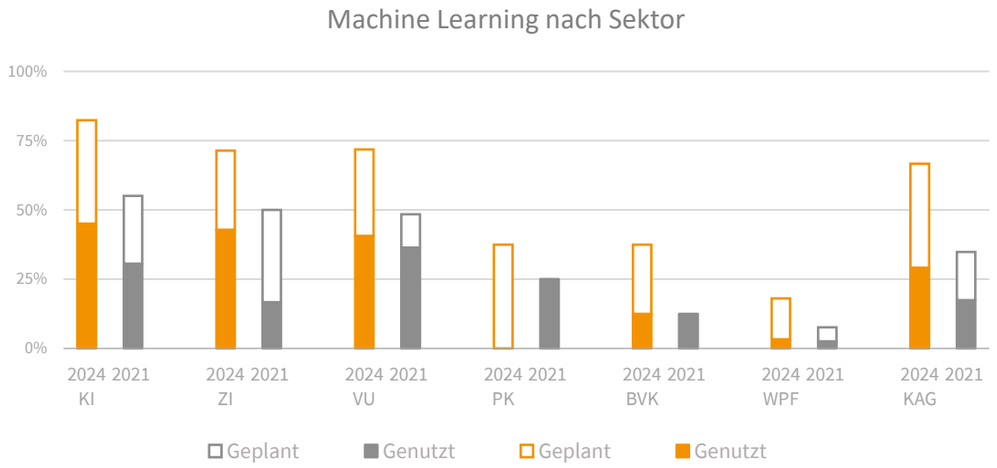




Quelle: FMA, Austrian Digital Finance Landscape 2024

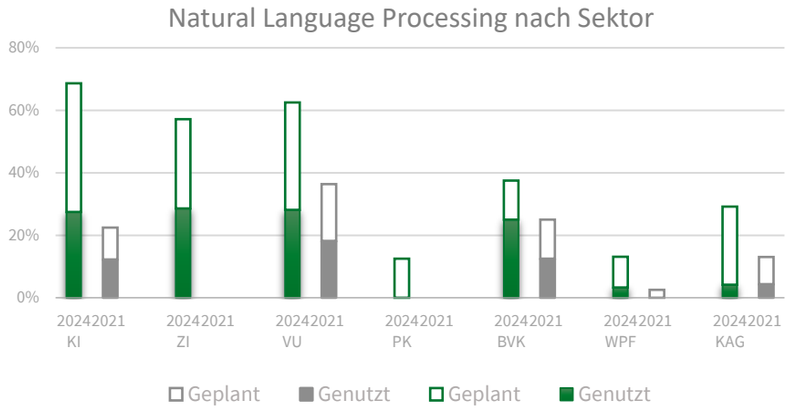
6) IN WELCHEN PROZESSEN WIRD KÜNSTLICHE INTELLIGENZ VERWENDET?

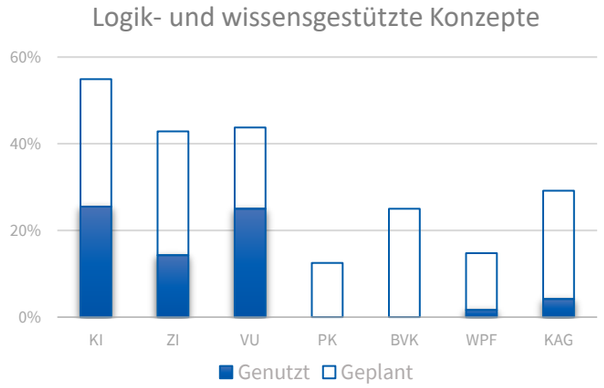
- **Machine Learning:** Mehr als ein Viertel der Beaufsichtigten (26 %) nutzt bereits ML in ihrer Geschäftstätigkeit.
  - Vorreiter beim Einsatz von maschinellem Lernen sind KI (45 %), Zahlungsinstitute (43 %) und VU (41 %).
  - Die Haupteinsatzgebiete sind **Ratingsysteme, Fraud Analytics**, Unterstützung in den Bereichen **IT, Verwaltung** und **Marketing**.

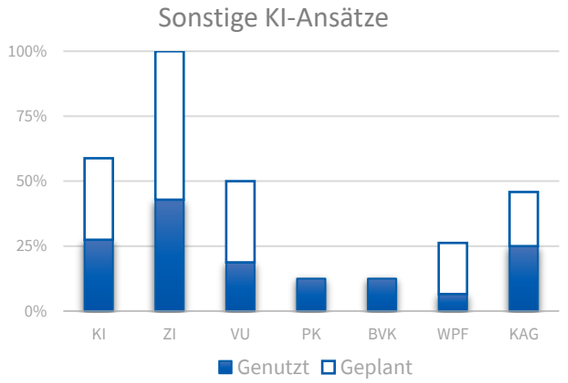


Quelle: FMA, Austrian Digital Finance Landscape 2024

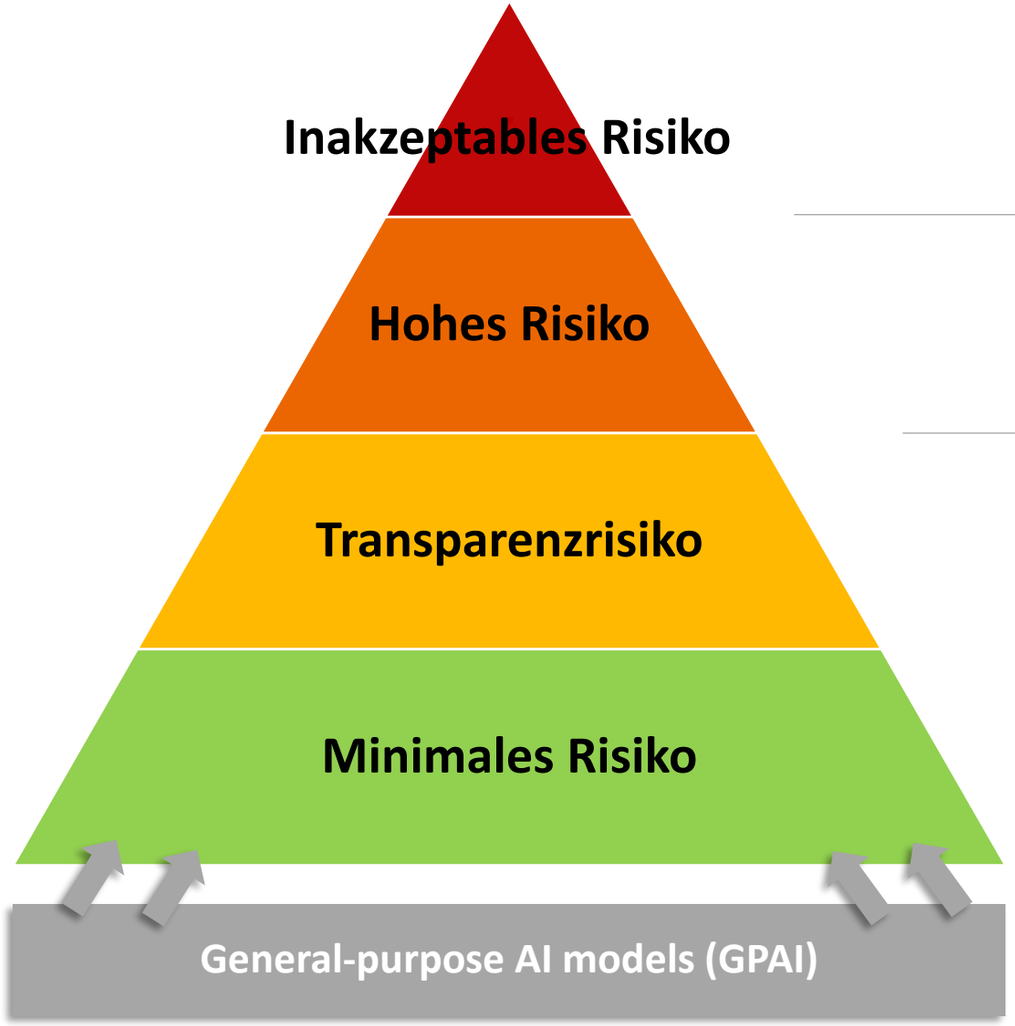
- **Natural Language Processing** hat seit 2021 an Bedeutung gewonnen.
  - In den Sektoren KI, ZI, VU und BVK beträgt der Nutzungsgrad bereits über 20%
  - Insb. **Chatbots** werden bei der Kundenkommunikation eingesetzt.







WELCHE ART VON RISIKO STELLT SIE DAR?



- **Ausnutzung von Verwundbarkeiten** in Bezug auf Alter, Behinderung, ...
- **Soziales Scoring**
- **Biometrische Kategorisierung** zur Ableitung der Rasse, politischer Meinungen, religiöser Überzeugungen, …

→ **Verbotene KI-Praktiken**

- KI-Systeme, die für die Kreditwürdigkeitsprüfung oder Risikobewertung und Preisbildung in Bezug auf natürliche Personen in der Lebens- / Krankenversicherung verwendet werden sollen (Annex III, 5 b und c).

→ **Konformitätsbewertung**
Gebrauchsanweisung/
Menschliche Aufsicht /
Folgenabschätzung in Bezug auf die Grundrechte

- **Risiken von Identitätsdiebstahl, Manipulation ,** Fehlinformationen oder Täuschung (z. B. Chatbots, Deep Fakes, KI-generierte Inhalte...)

→ **Information von natürlichen Personen, dass sie mit einem KI-System interagieren**

- Die Mehrzahl der KI-Systeme (z.B. Spamfilter) kann im Rahmen der bestehenden Regulierung ohne spezifische rechtliche Verpflichtungen entwickelt und eingesetzt werden. Freiwillig können sich die Anbieter dieser Systeme freiwilligen Verhaltenskodizes anschließen.

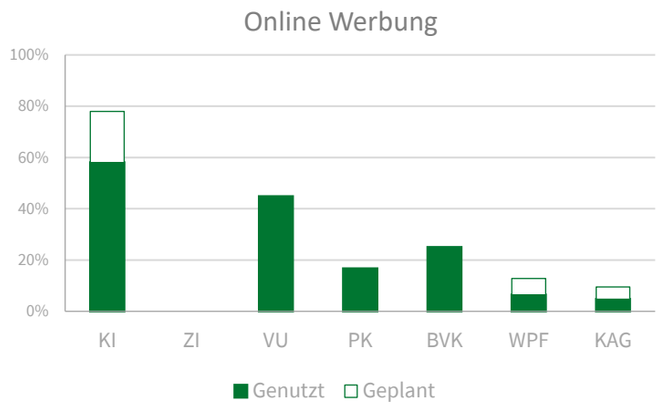
→ **KI-Kompetenz der Personen, die mit KI-Systemen befasst sind**

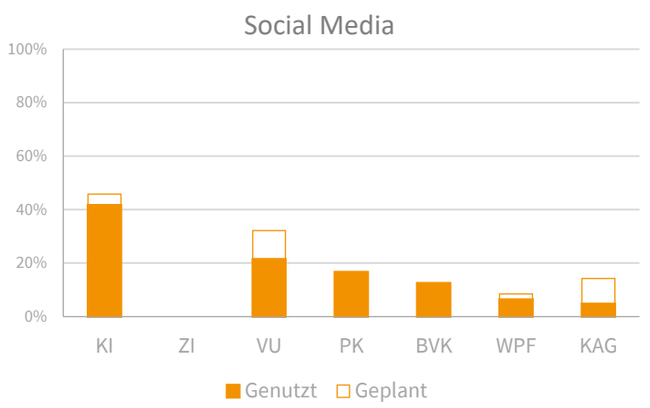
- GPAI models → **Transparenz**
- GPAI models with systemic risks (= GPAI mit “hohen Wirkungsfähigkeiten”) → **Transparenz, Risiko-bewertung und -mitigation**

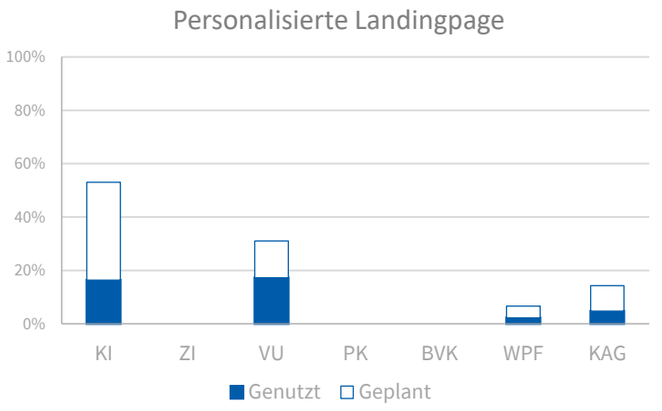
7) WIE STARK WIRD AUF DIGITALES MARKETING GESETZT?

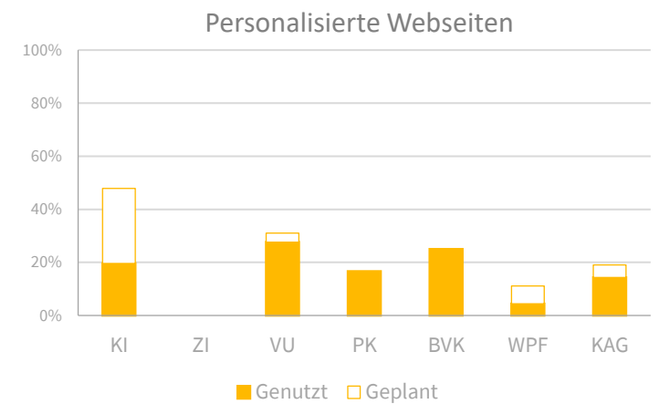
- Bei der **Marketing-Automatisierung** werden Nutzerprofile mit verhaltensbasierten Daten angereichert, um automatisierte Kampagnen für individuelle Kommunikation einzurichten.
- Marketing-Automation-Software wird vor allem durch KI (73%) und VU (34%) eingesetzt.
- Die häufigsten automationsunterstützten Marketingmethoden stellen hierbei
  - **Online Werbung** (zB Google-Ads im Rahmen von Werbekampagnen),
  - **personalisierte Landingpages** (Webpages mit Kampagnenbezug),
  - **Social Media** (gezielte Werbung auf den von Kund:innen genutzten Kanälen) und
  - **E-Mail** (zB Newsletter, Erstinformationen zu Produktneuheiten, Geburtstagswünsche).

  Auf **personalisierte Webseiten** (zB zur direkten Kundenansprache mit Bonusaktionen) bzw. Veranstaltungsmanagement (zB Kundenevents) wird etwas weniger abgestellt.





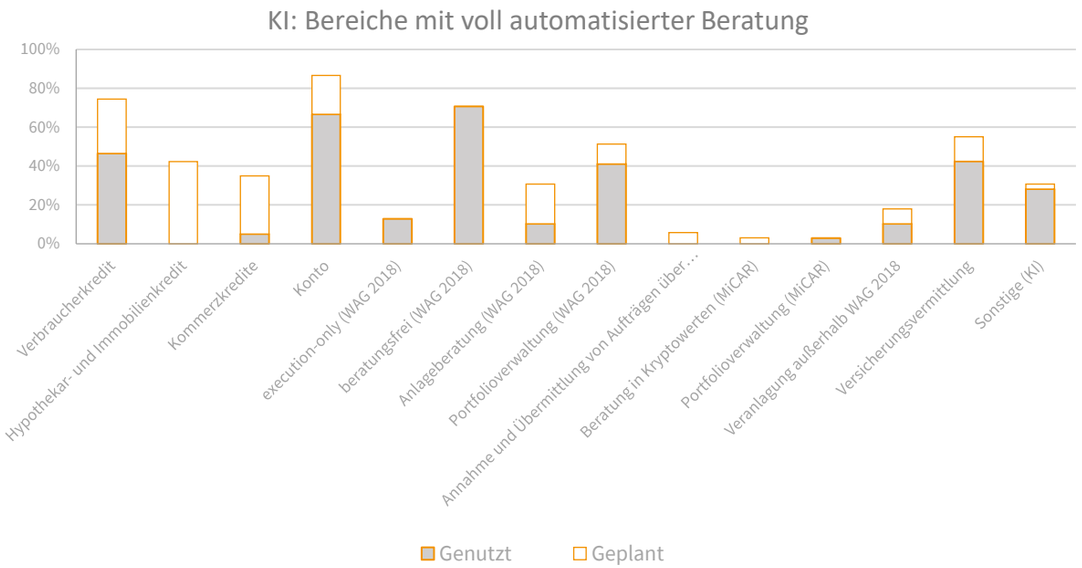




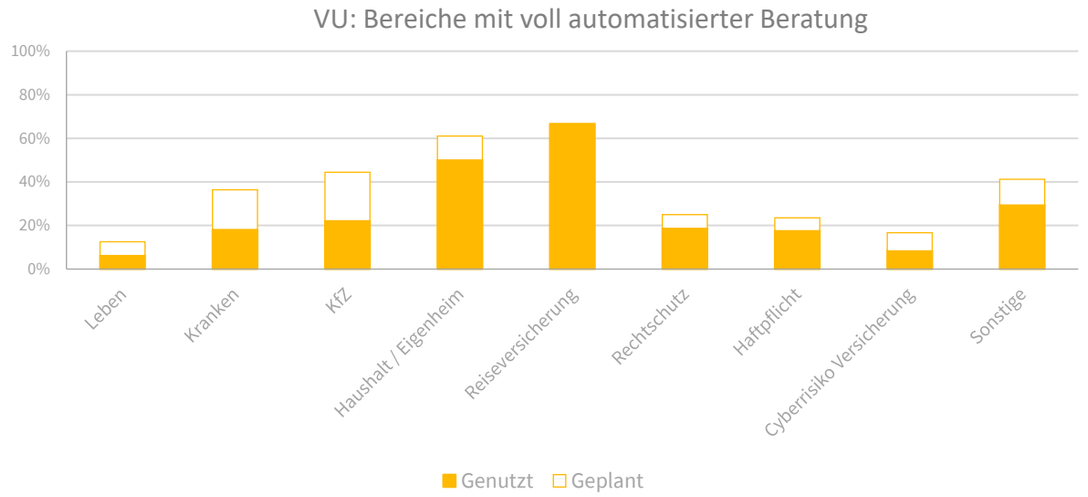
8) BEI WELCHEN PRODUKTEN KOMMT DIGITALE BERATUNG ZUM EINSATZ?

- Bei einer **automatisierten Beratung** wird die Beratung vollständig von einem automatisierten System erstellt (die persönlichen Anforderungen und Kundeninformationen werden digital analysiert, wonach das automatisierte System die Beratung erstellt und sie dem Kunden übermittelt).

- **KI** bieten eine automatisierte Beratung vor allem in den Bereichen Konto und Verbraucherkredite an. Bis 2027 werden insb. im Bereich Hypothekar-, Immobilien- und Kommerzkredite Erweiterungspotentiale gesehen.



- **VU:** In der Reiseversicherung bieten bereits 2/3 der VU, die dieses Produkt vertreiben, Abschlüsse mit einer voll automatisierten Beratung an (in der Haushaltsversicherung: 50%). In der Kranken- und KFZ-Versicherung wird bis 2027 mit weiterem Anstieg der automatisierten Beratung gerechnet.

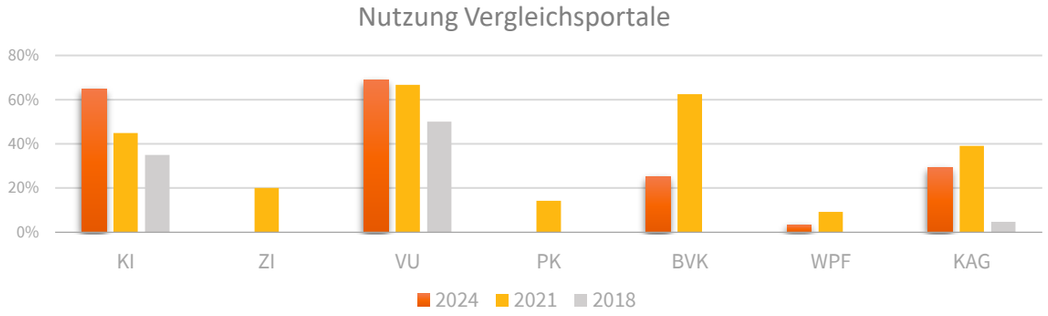


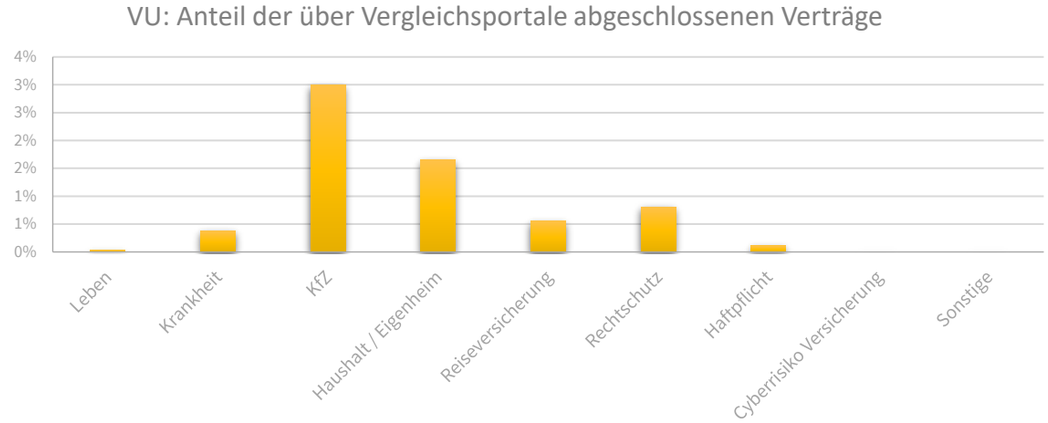
Quelle: FMA, Austrian Digital Finance Landscape 2024

9) ABSCHLÜSSE ÜBER VERGLEICHSPORTALE?

- Der prozentuelle Anteil des Absatzes über Vergleichsportale liegt bei den meisten Unternehmen nach wie vor im einstelligen Prozentbereich oder darunter. In den nächsten Jahren kann hier jedoch ein weiteres Wachstum erwartet werden.
- Mit steigender Nutzung von Vergleichsportalen steigt implizit auch der Bedarf an Fairness und Transparenz dieser Anbieter.

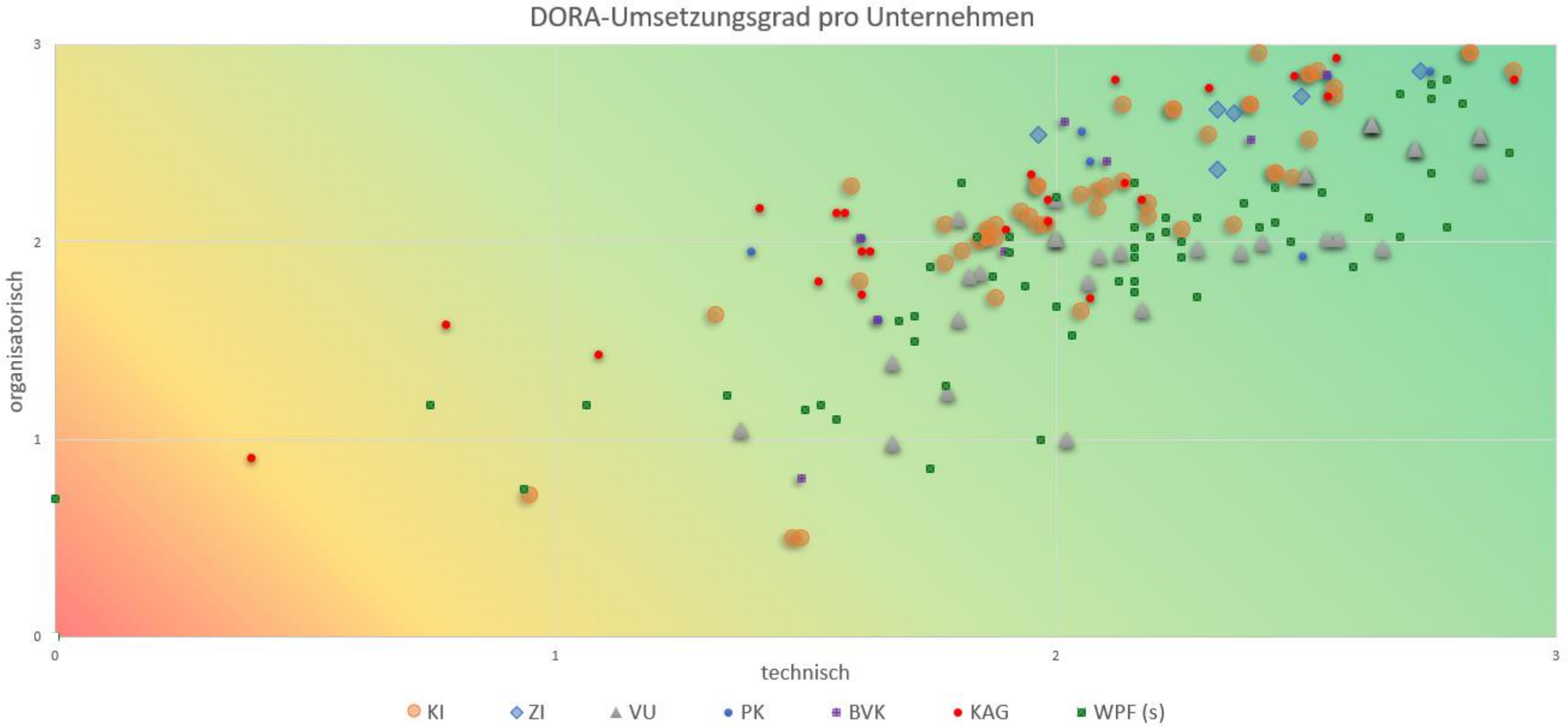
- Der Anteil der über Vergleichsportale abgeschlossen Verträge bei VU ist, obwohl fast **70%** der VU Vergleichsportale verwenden, weiterhin niedrig.





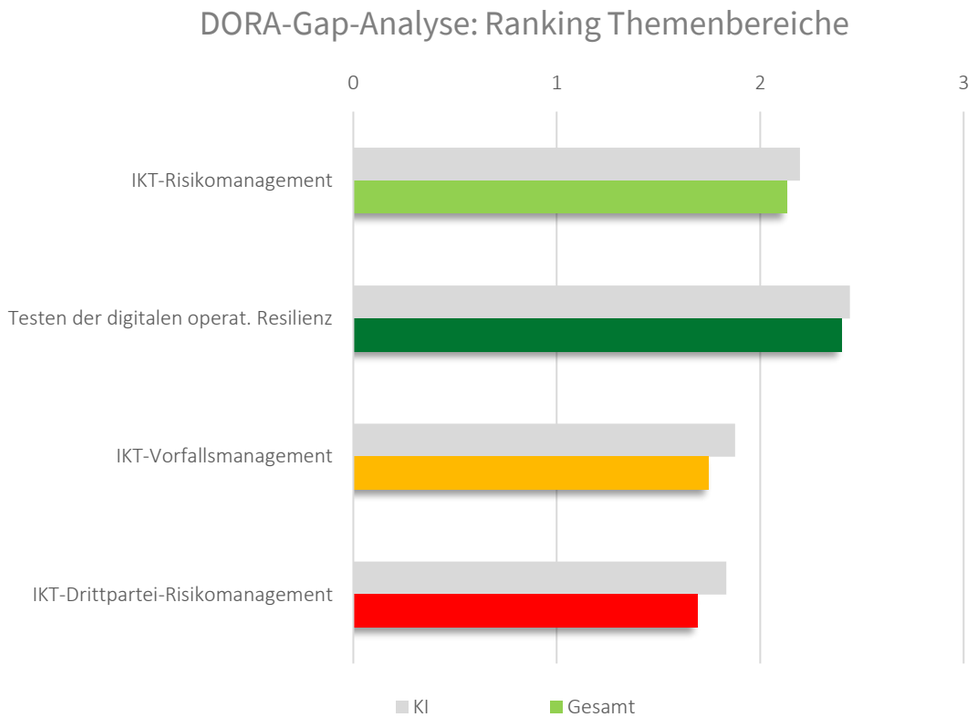
Quelle: FMA, Austrian Digital Finance Landscape 2024

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

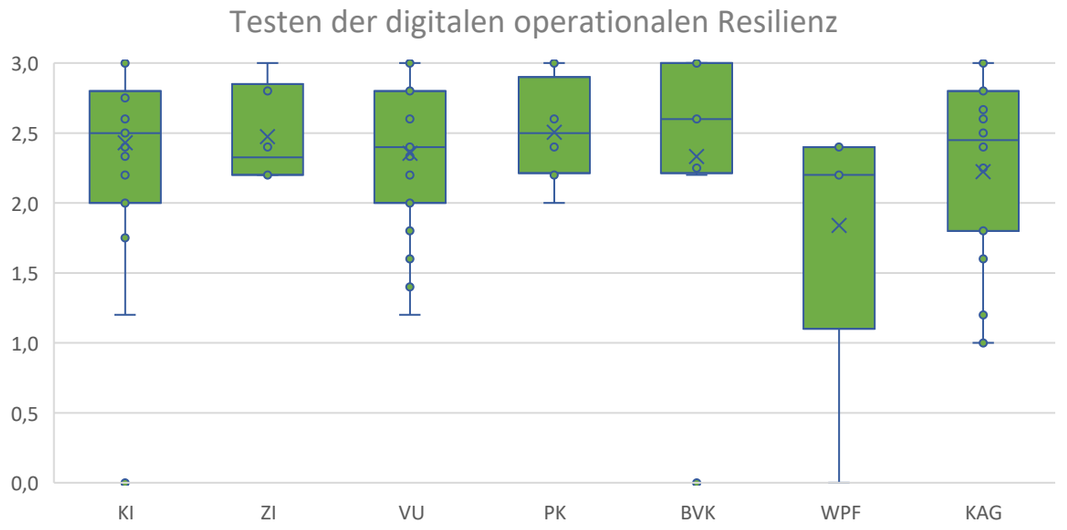


RANKING THEMENBEREICHE

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

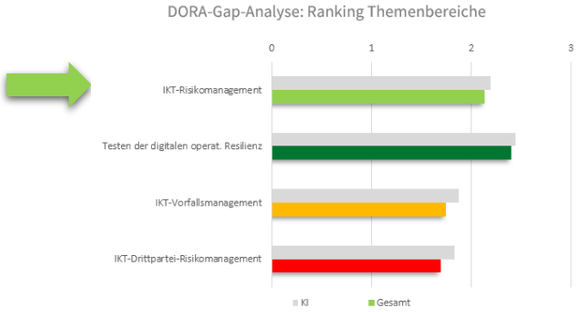


ABER auch beim Testen der digitalen operationalen Resilienz eine große Bandbreite bei der Vorbereitung der Umsetzung:

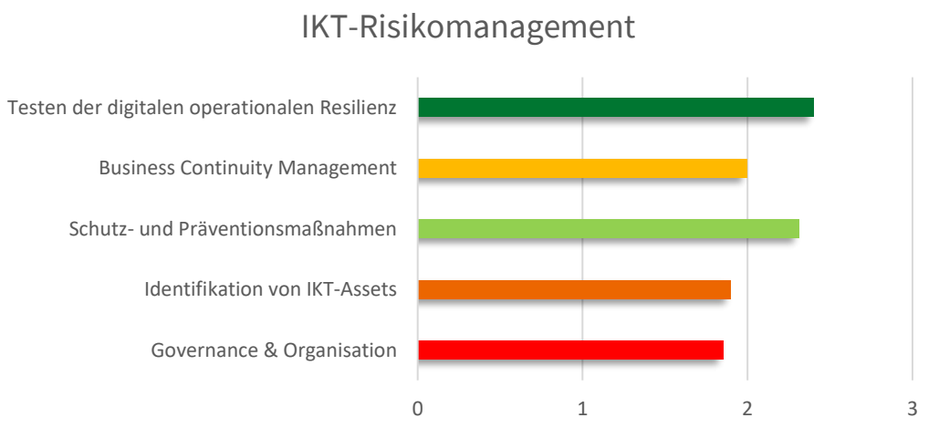


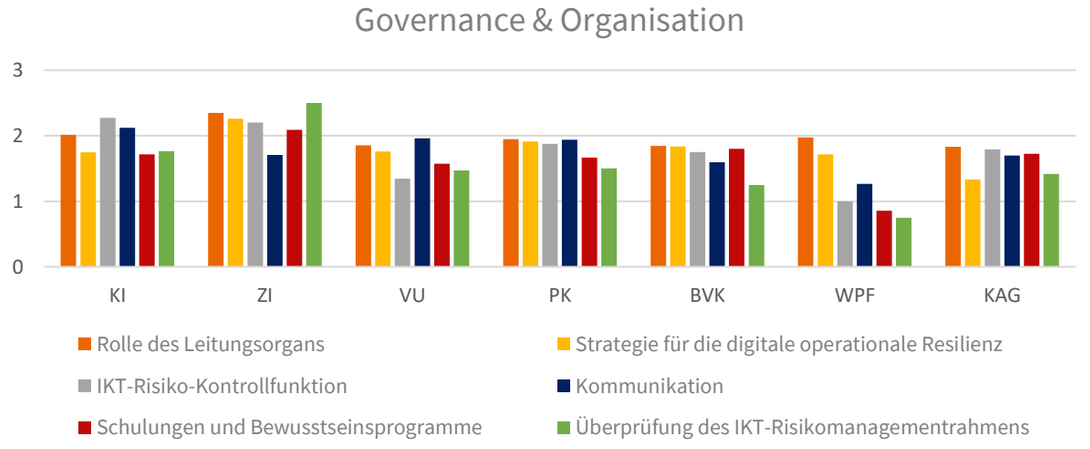
Quelle: FMA, Austrian Digital Finance Landscape 2024

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



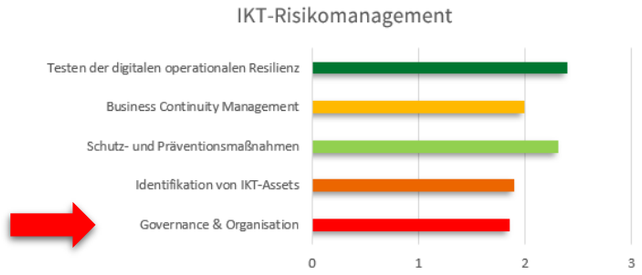
- Die DORA-Umsetzung war Mitte 2024 insb. in den folgenden Bereichen noch im Gange:
  - **Governance & Organisation**: In vielen Fällen waren u.a. noch dokumentarische Aufgaben und Freigaben der Geschäftsleitung offen.
  - Für die **Inventarisierung von IKT-Assets** waren zT noch umfangreichere technische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



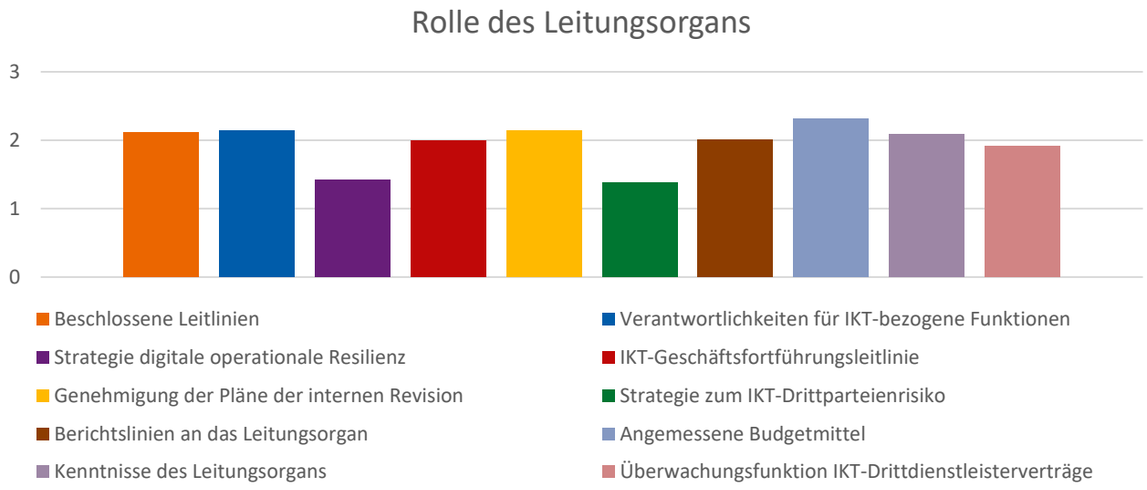


Quelle: FMA, Austrian Digital Finance Landscape 2024

A) IKT-RISIKOMANAGEMENT: GOVERNANCE & ORGANISATION



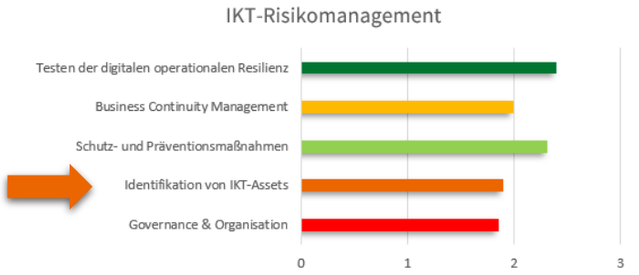
- Leitungsorgane haben bereits verbreitet **Leitlinien** beschlossen, die nunmehr auch Authentizität, welche auf die Vertrauenswürdigkeit der Datenquelle abstellt, explizit thematisieren. ✓
- Genehmigung der **Pläne der internen Revision** in Bezug auf die Prüfungen im IKT-Bereich für 2025 bzw. die darauffolgenden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

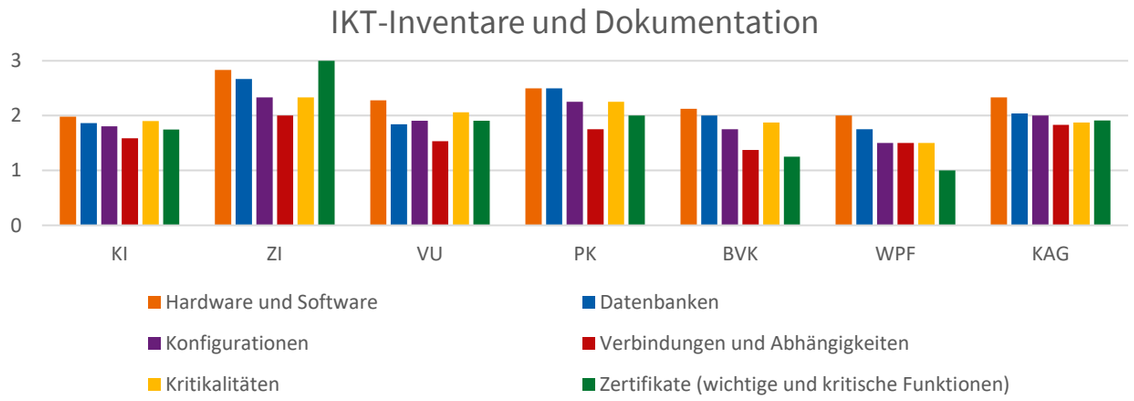


Quelle: FMA, Austrian Digital Finance Landscape 2024

- **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





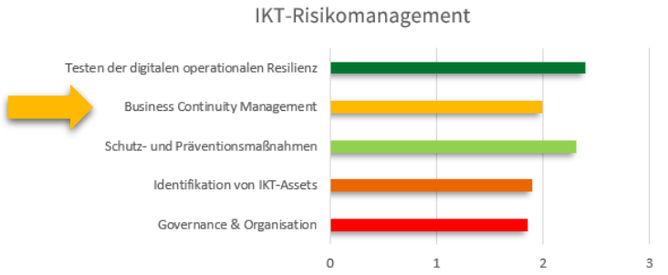
Quelle: FMA, Austrian Digital Finance Landscape 2024

- 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;

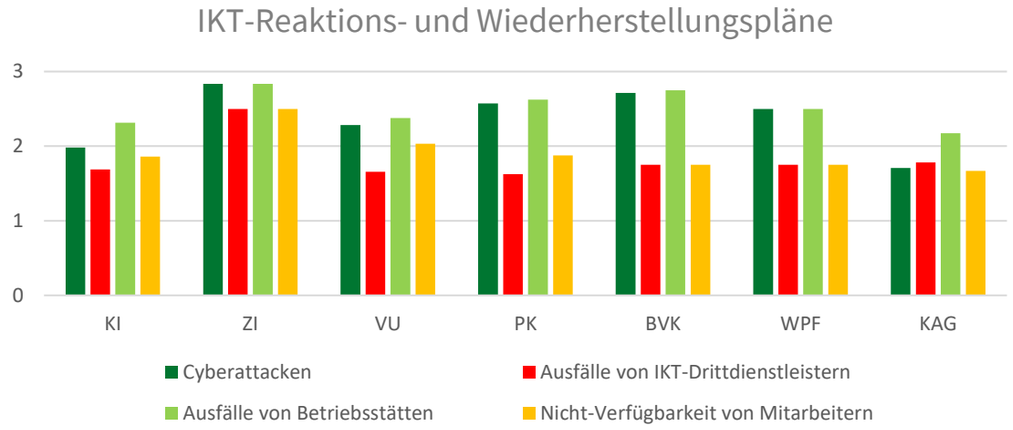
f) Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

g) Angriffe durch Insider;

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

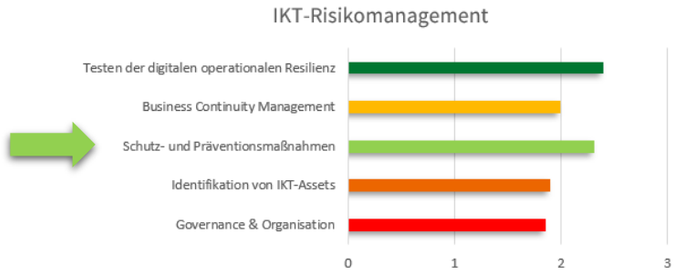
i) weitverbreitete Stromausfälle.

- 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.

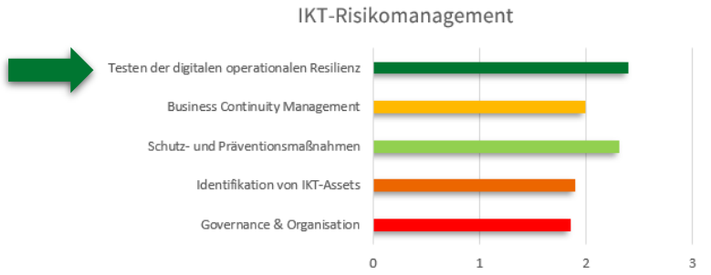
- **Verschlüsselung während der Verarbeitung (in use):** Ist diese nicht möglich, sind die Daten in einer getrennten und besonders geschützten Umgebung zu verarbeiten bzw. es sind andere geeignete Maßnahmen zu treffen (Art 6 Abs 2 VO (EU) 2024/1774).

- **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).

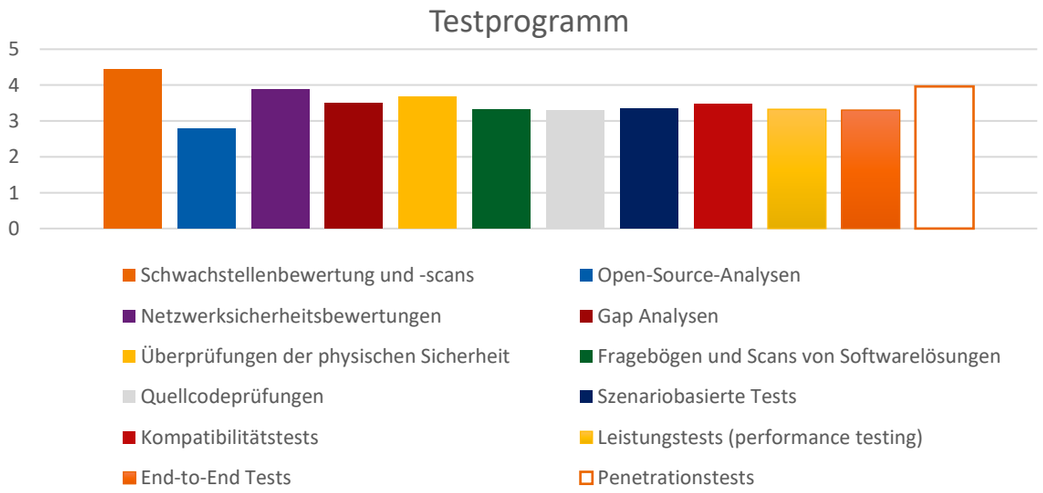
A) IKT-RISIKOMANAGEMENT:
TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ



- **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.

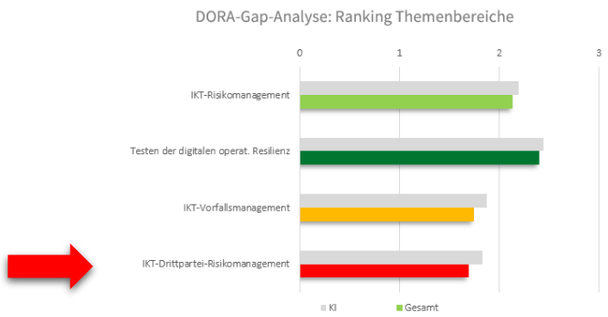
Entwicklungsfelder:

- **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

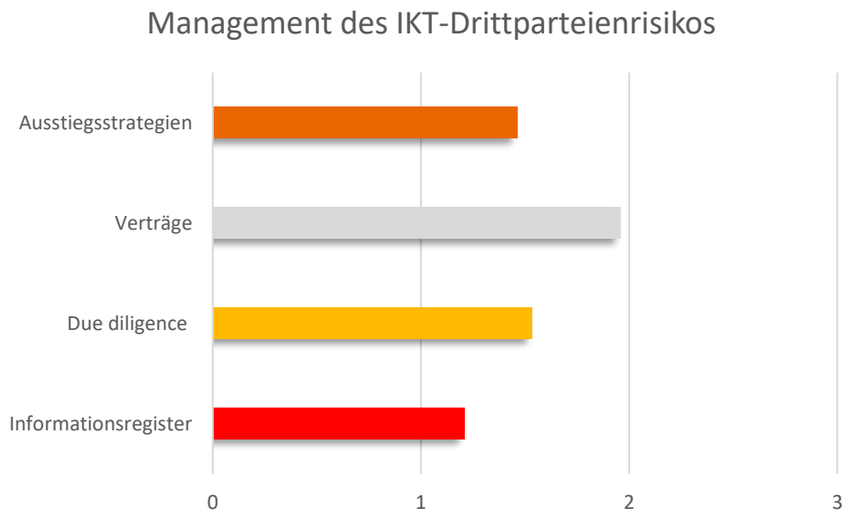


Quelle: FMA, Austrian Digital Finance Landscape 2024

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.

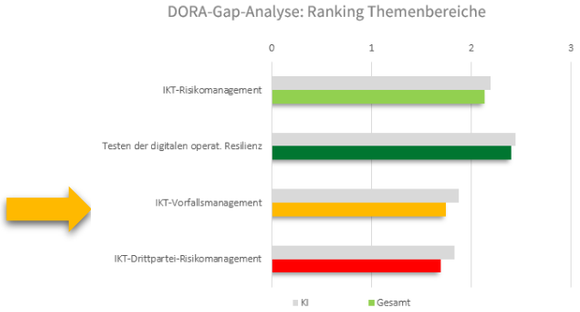


Quelle: FMA, Austrian Digital Finance Landscape 2024

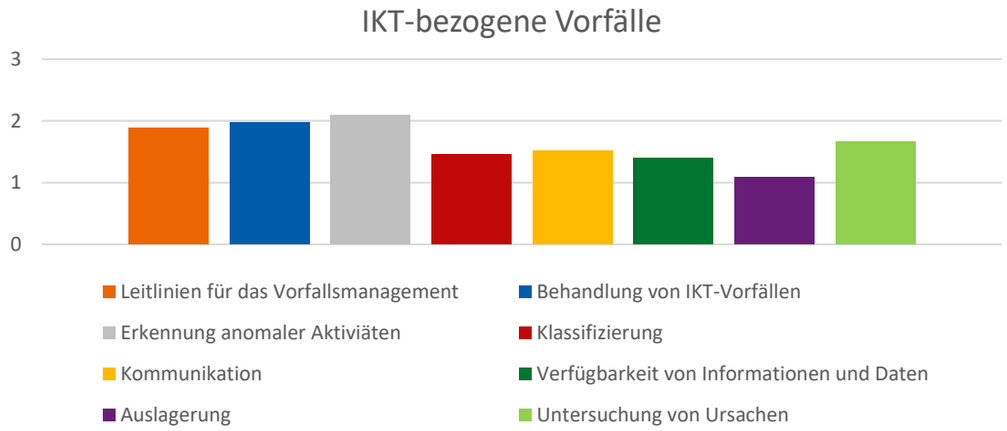
Entwicklungsfelder:

- **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

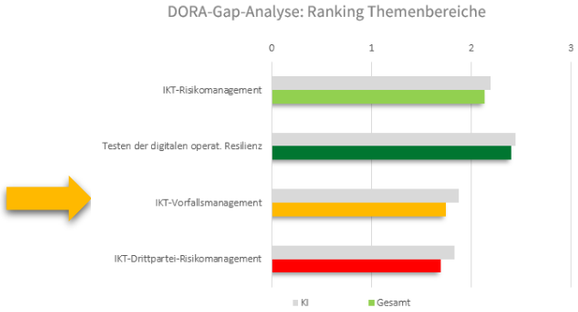
Entwicklungsfelder:

- 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



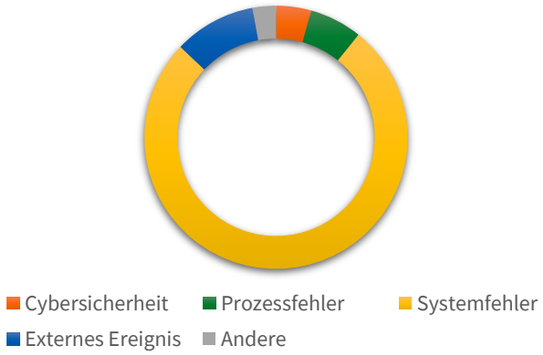
Cyber-Vorfälle:

- 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%.

Ausgehen des Vorfalls

Vorfallstypen



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%).
  - 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.

Cyber Incidents am ö Finanzmarkt / Lessons learnt & Way forward

EXKURS: DORA-ENTWICKLUNG

EXKURS: 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

	Inkrafttreten bzgl. DORA-Aspekte
FMA-Verordnungen	
FMA-IPV	17.01.2025
FMA-GebV	17.01.2025

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

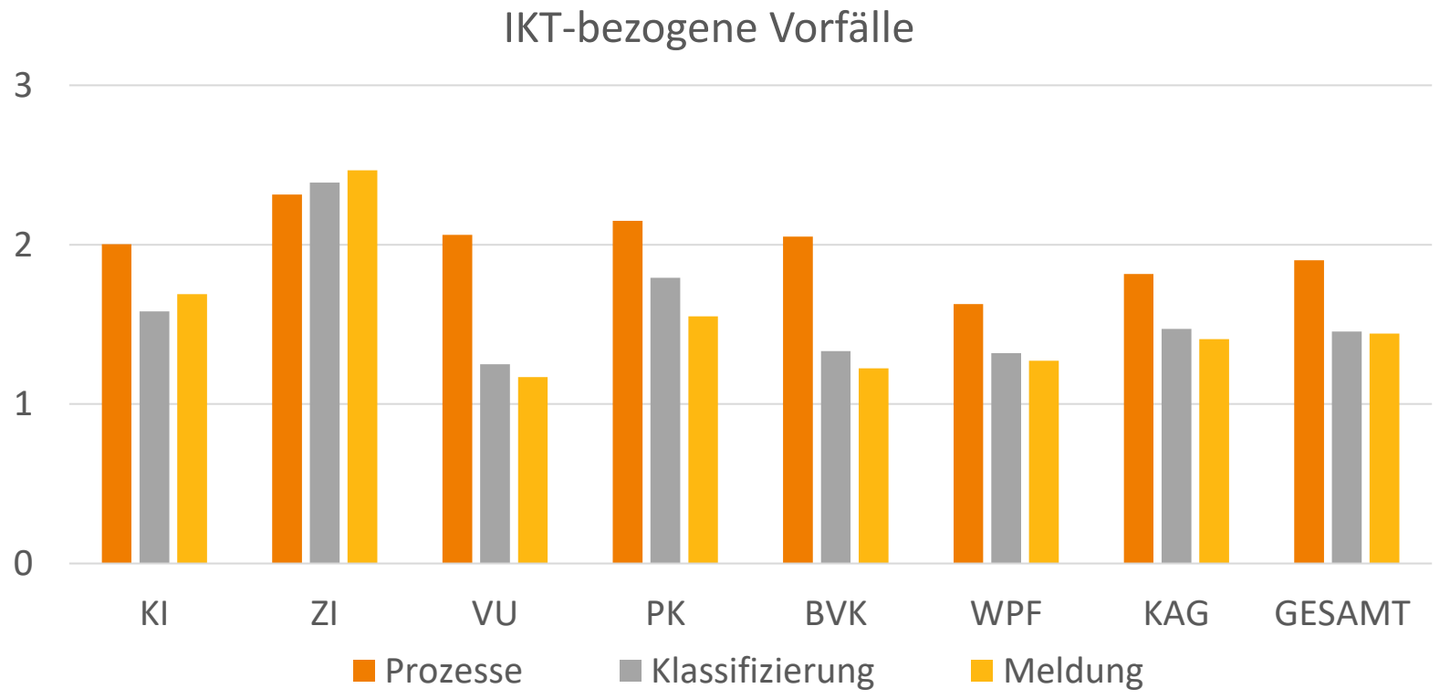
DORA-Art.	Thema	Frist (für die Vorlage an die EK)			
		Sep 23	Jan 24	Jul 24	Jan 25
	IKT-Risikomanagement				
Art. 15, 16	RTS 2024/1774_IKT-Risikomanagement		✓		
	Testen der digitalen operationalen Resilienz				
Art 26 (11)	Final Draft RTS zu bedrohungsorientierten Penetrationstests			✓	
	IKT-bezogene Vorfälle				
Art 11 (11)	Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste			✓	
Art 18 (3)	RTS 2024/1772_Klassifizierung von IKT-bezogenen Vorfällen		✓		
Art 20a	RTS zur Meldung schwerwiegender IKT-bezogener Vorfälle (adopted)			✓	
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)	ITS 2024/2956_Informationsregister		✓		
Art 28 (10)	RTS 2024/1773_Leitlinie_Nutzung von IKT-Dienstleistungen		✓		
Art 30 (5)	Final Draft RTS on subcontracting ICT services			~	
	Überwachungsrahmen für kritische IKT-Drittdienstleister				
Art 31	Delegierte VO 2024/1502_Kriterien für die Einstufung von CTPPs	✓			
Art 32 (7)	Leitlinien JC/GL/2024/36_für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden zur Struktur des Überwachungsrahmens			✓	
Art 41	RTS zur Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten (adopted) und Final draft RTS zu JETs (Mandat der HLGO)			✓	
Art 43 (2)	Delegierte VO 2024/1505_CTPP_Gebühren	✓			

Digital Operational Resilience Regulation - European Commission

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN

3) Anforderung voll erfüllt
2) Geringfügiger Anpassungsbedarf
1) Starker Anpassungsbedarf
0) Umsetzung erforderlich
x) n.a. (erläuterungsbedürftig)

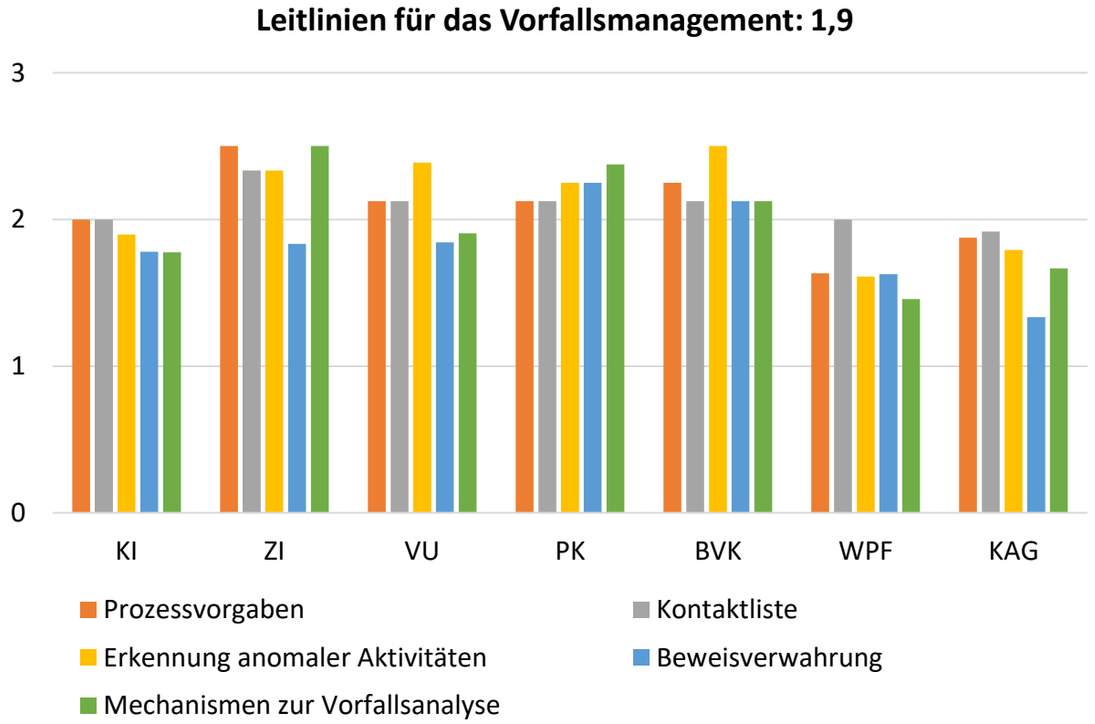


Quelle: FMA, Austrian Digital Finance Landscape 2024

Prozesse
1,9

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
LEITLINIEN FÜR DAS VORFALLSMANAGEMENT

Die IKT-Vorfallsmanagementpolicy umfasst:	Gesamt
- Prozessvorgaben	1,9
- Kontaktliste (interne Funktionen und externe Stakeholder)	2,0
- Umsetzung von Mechanismen zur schnellen Erkennung anomaler Aktivitäten	1,9
- Vorgaben für eine sichere Verwahrung von Beweisen zu IKT-Vorfällen, wobei diese auf die erforderliche Aufbewahrungszeit beschränkt ist	1,7
- Einrichtung von Mechanismen zur Analyse signifikanter oder sich wiederholender IKT-bezogener Vorfälle	1,8

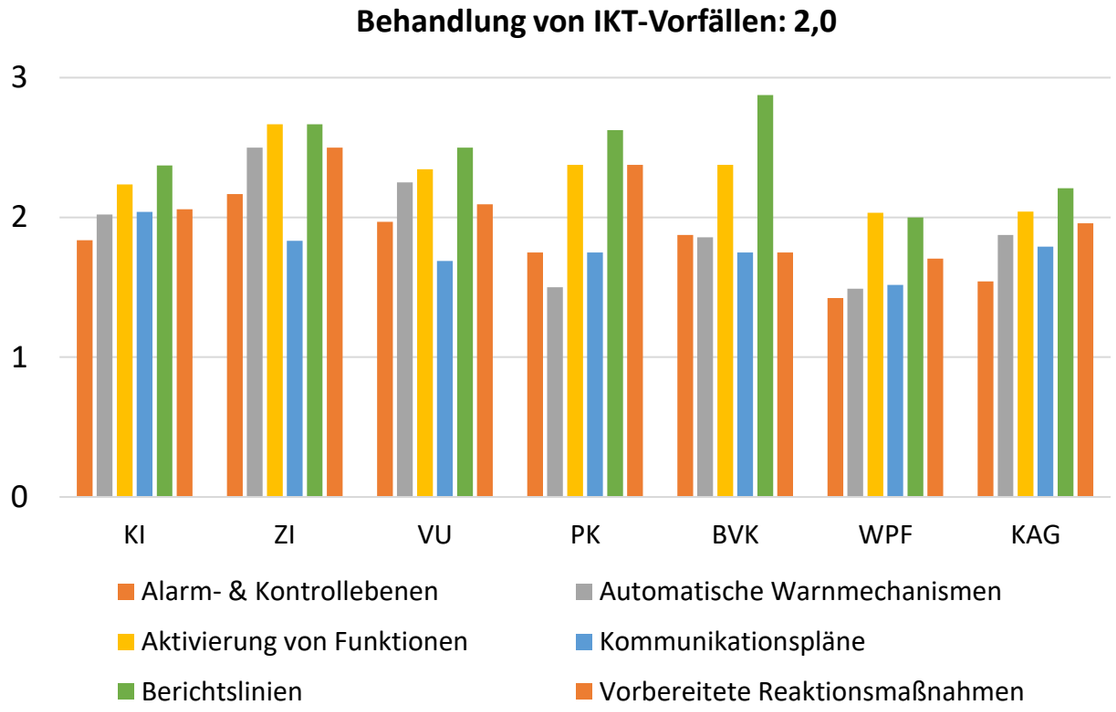


Quelle: FMA, Austrian Digital Finance Landscape 2024

Prozesse
1,9

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
BEHANDLUNG VON IKT-VORFÄLLEN

IZm der Behandlung von IKT-Vorfällen ist Folgendes implementiert:	Gesamt
- Einsatz mehrerer Kontrollebenen und Festlegung von Alarmschwellen und -kriterien (inkl. Frühwarnindikatoren)	1,7
- Verwendung automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind	1,9
- Zuweisung von Funktionen und Zuständigkeiten, die bei IKT-bezogenen Vorfällen aktiviert werden	2,2
- Ausarbeitung interner und externer Kommunikationspläne	1,8
- Berichtslinie an die jeweils zuständige Führungsebene und das Leitungsorgan bei schwerwiegenden IKT-bezogenen Vorfällen	2,3
- Vorbereitung von Reaktionsmaßnahmen zur Minderung von Auswirkungen	1,9

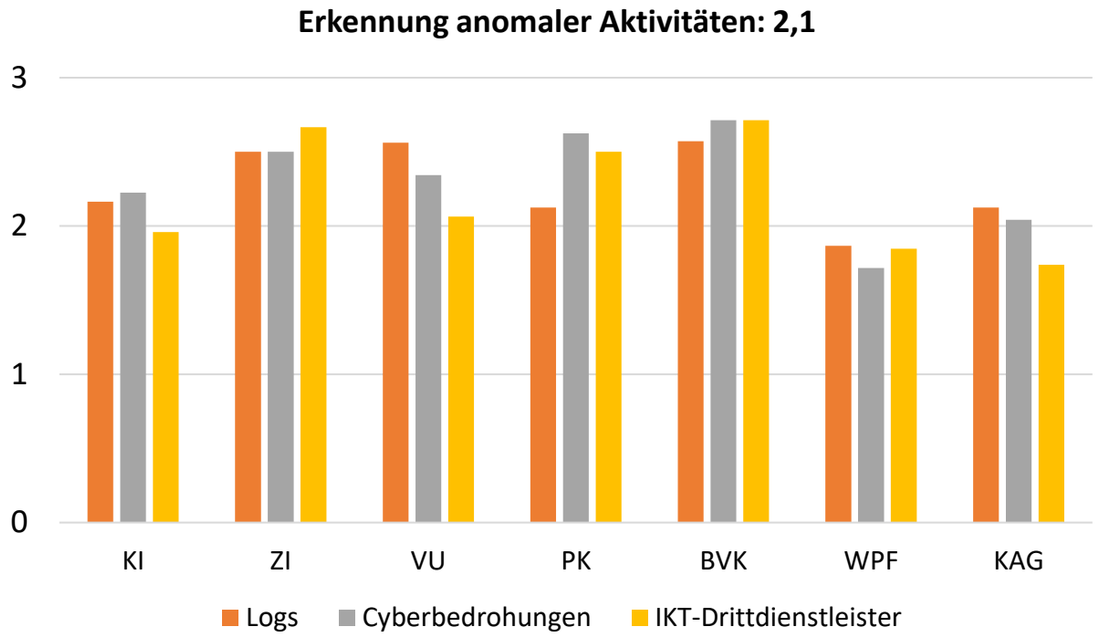


Quelle: FMA, Austrian Digital Finance Landscape 2024

Prozesse
1,9

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
ERKENNUNG ANOMALER AKTIVITÄTEN

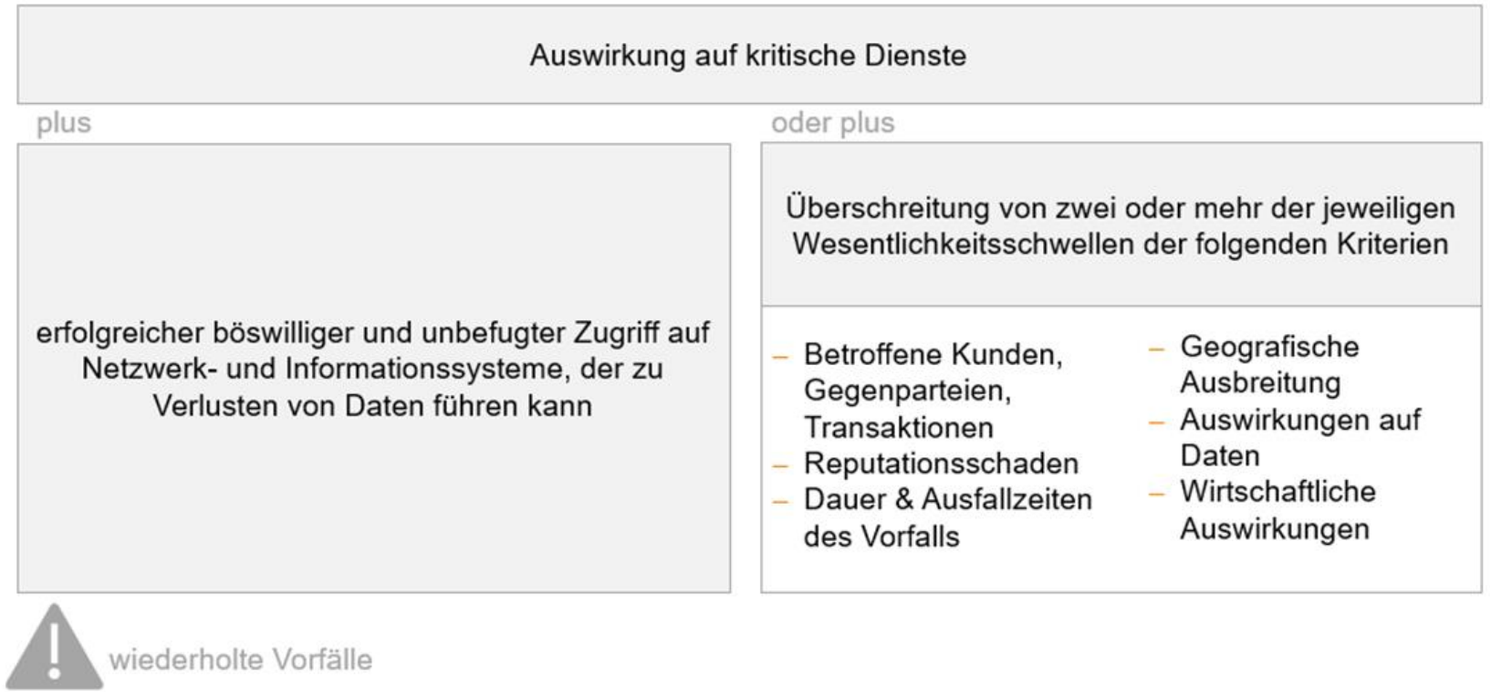
Folgende Informationen werden zur Erkennung bzgl. anomaler Aktivitäten genutzt:	Gesamt
- Logs, interne Informationen und von Anwendern gemeldete Probleme	2,2
- Potentielle interne und externe Cyberbedrohungen	2,1
- Meldungen von IKT-Drittdienstleistern	2,0



Quelle: FMA, Austrian Digital Finance Landscape 2024

Klassifizierung
1,5

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
KLASSIFIZIERUNG – SCHWERWIEGENDE VORFÄLLE



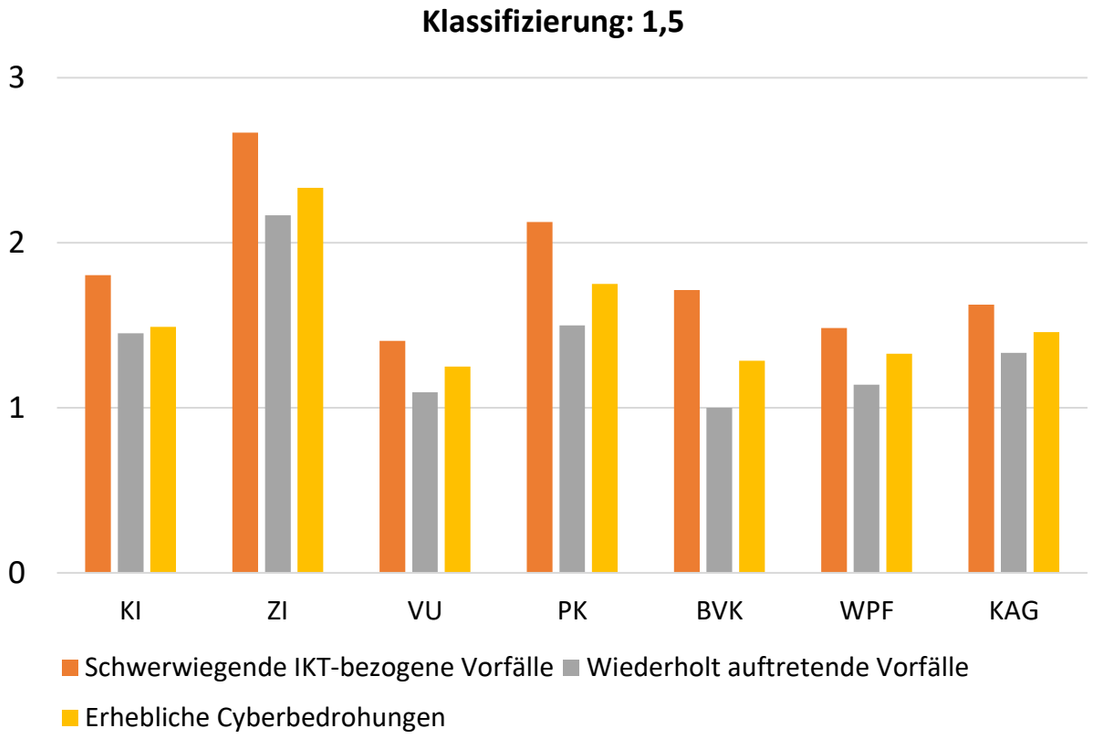
Kriterien der Schwellenwerte:

- DL-nutzende Kunden: 10% oder > 100.000
  Betroffene Gegenparteien: > 30%
  Transaktionen: > 10% tägl. Durchschn. Zahl oder täglicher Durchschnittswert
- Reputationsschaden: qualitativ
- Dauer: > 24 Stunden oder
  Ausfallzeit IKT-Dienste > 2 Stunden
- Geografische Ausbreitung: ≥ 2 Mitgliedstaaten
- Daten: Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten ⇨ negative Auswirkungen auf die Verwirklichung der Geschäftsziele oder auf dessen Fähigkeit, regulatorische Anforderungen zu erfüllen
- Wirtschaftliche Auswirkungen: > 100.000 Euro

Klassifizierung
1,5

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
KLASSIFIZIERUNG

Klassifizierung:	Gesamt
IKT-bezogene Vorfälle können zeitnah auf Basis der in Art 18 DORA-VO iVm RTS zur Klassifizierung von IKT-bezogenen Vorfällen vorgegebenen Kriterien als "schwerwiegend" klassifiziert werden	1,6
Wiederholt auftretende Vorfälle werden iHa mögliche gemeinsame Ursachen (innerhalb eines 6-Monats-Zeitraums) monatlich analysiert. Darauf aufbauend ist ein Prozess zur Überprüfung der kumulativen Überschreitung der Schwellenwerte eines schwerwiegenden IKT-bezogenen Vorfalls eingerichtet.	1,3
Eine Klassifizierung von **Cyberbedrohungen** als 'erheblich' kann zeitnah vorgenommen werden.	1,4



Quelle: FMA, Austrian Digital Finance Landscape 2024

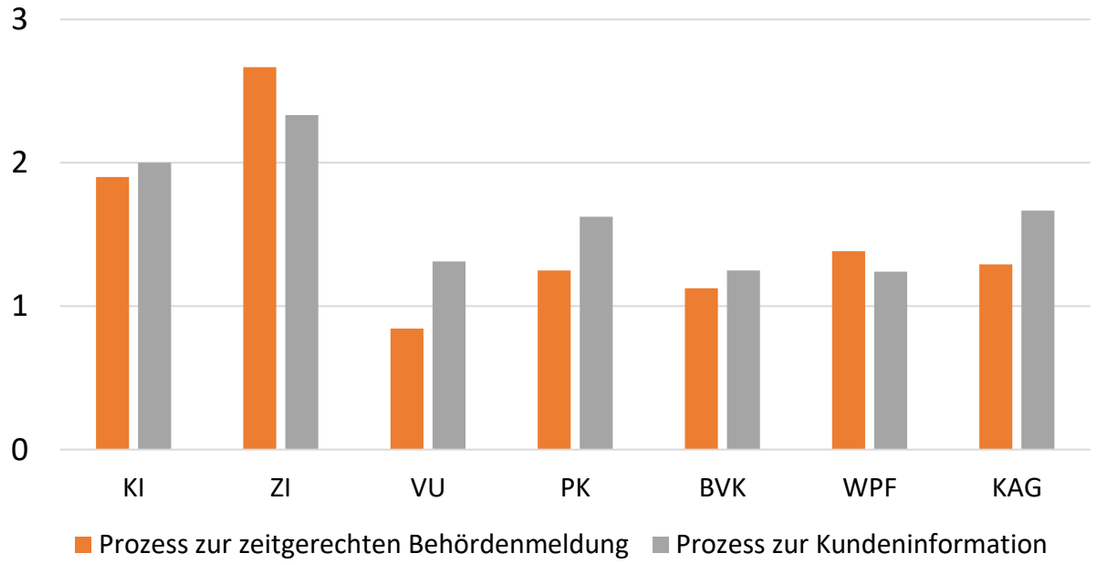
Meldung
1,4

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
KOMMUNIKATION

Kommunikation:	Gesamt
Der Prozess zur zeitgerechten Meldung von schwerwiegenden IKT-bezogenen Vorfällen (inkl. ggf freiweilliger erheblicher Cyberbedrohungen) an die zuständige Behörde wurde definiert.	1,5
Ein Prozess zur Kundeninformation über einen - die finanziellen Interessen von Kunden betreffenden - schwerwiegenden IKT-bezogenen Vorfall und die Maßnahmen, die ergriffen worden sind, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern, wurde definiert.	1,6

Möglichkeit der Auslagerung der Meldung: 55% der Unternehmen geben an, eine solche Auslagerung nicht vornehmen zu wollen	Gesamt
Bei Auslagerung der Meldepflichten zu schwerwiegenden IKT-bezogenen Vorfällen sowie zu freiwilligen Meldungen erheblicher Cyberbedrohungen an Drittdienstleister wurde die diesbezügliche Information der Aufsichtsbehörde gem. Art 6 ITS zu Meldeformularen vorbereitet. (Hinweis: Scores sind nicht bei Aggregationen berücksichtigt.)	1,1

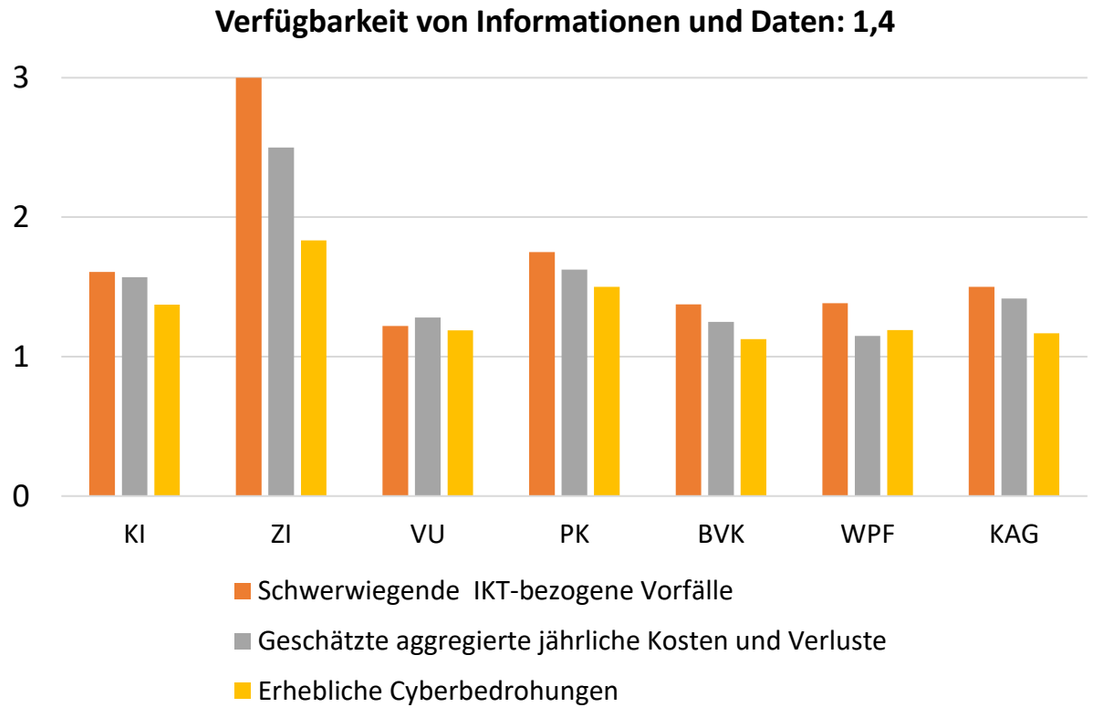
Kommunikation: 1,5



Meldung
1,4

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
VERFÜGBARKEIT VON INFORMATIONEN UND DATEN

Verfügbarkeit von Informationen und Daten zur Meldung	Gesamt
Die Verfügbarkeit der Meldeinhalte zu Erst-, Zwischen- und Abschlussmeldungen schwerwiegender IKT-bezogener Vorfälle (inkl. wiederholt auftretender Vorfälle) ist sichergestellt.	1,5
Die Verfügbarkeit der Meldeinhalte zu - auf Anfrage der Aufsichtsbehörde zu übermittelnden - geschätzten aggregierten jährlichen Kosten und Verlusten, die durch schwerwiegende IKT-bezogene Vorfälle verursacht worden sind, ist sichergestellt.	1,4
Die Verfügbarkeit der Meldeinhalte zu erheblichen Cyberbedrohungen wurde bereits evaluiert und ist sichergestellt.	1,3

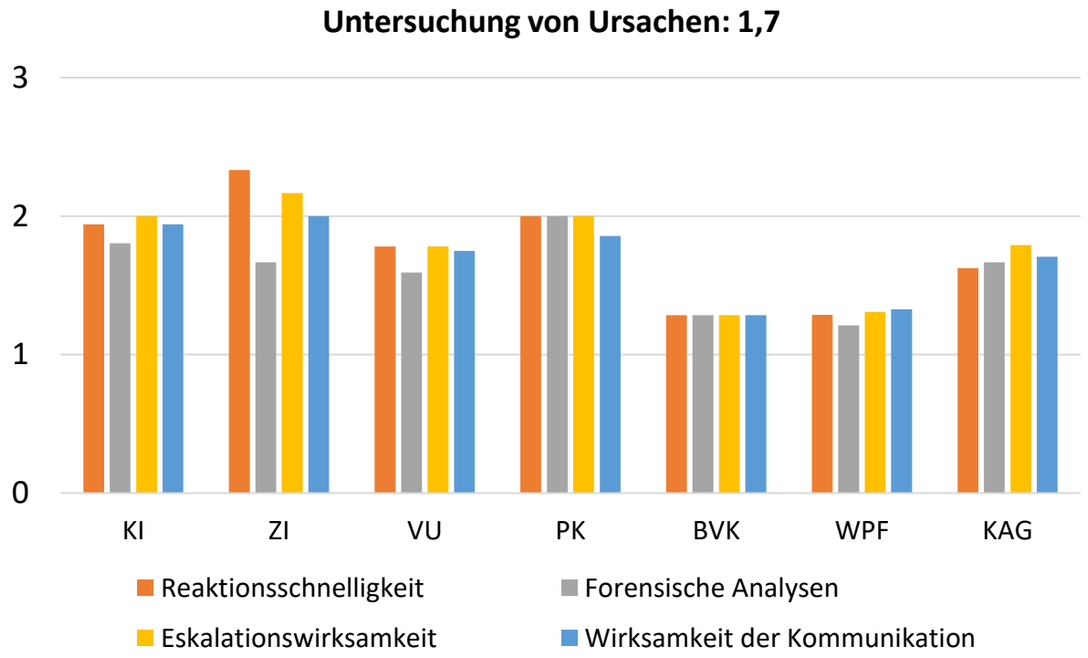


Quelle: FMA, Austrian Digital Finance Landscape 2024

Prozesse
1,9

IKT-BEZOGENE VORFÄLLE & CYBERBEDROHUNGEN
UNTERSUCHUNG VON URSACHEN

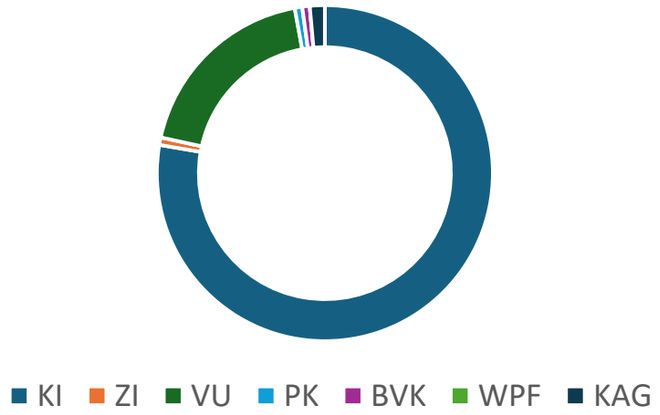
Nachträgliche Prüfungen IKT-bezogener Vorfälle beziehen sich auf die Wirksamkeit von Verfahren bzgl.:	Gesamt
- Schnelligkeit der Reaktion auf Sicherheitswarnungen und bei der Bestimmung der Auswirkungen von Vorfällen und ihrer Schwere	1,7
- Qualität und Schnelligkeit durchgeführter forensischer Analysen	1,6
- Wirksamkeit der Eskalation von Vorfällen	1,7
- Wirksamkeit interner und externe Kommunikation	1,7



Quelle: FMA, Austrian Digital Finance Landscape 2024

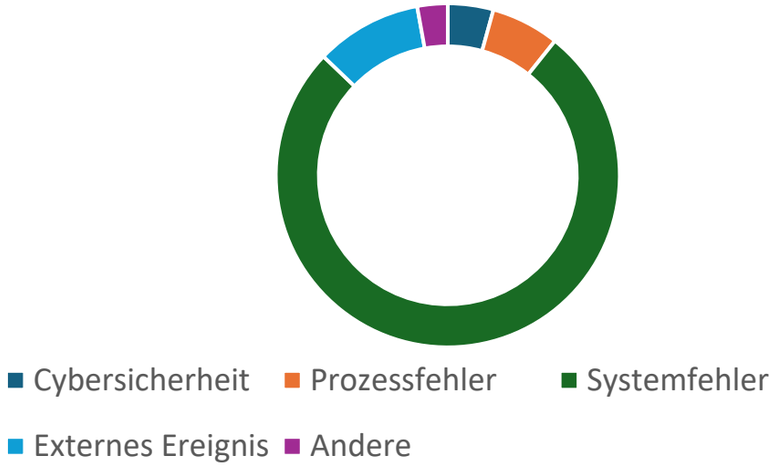
IKT-BEZOGENE VORFÄLLE: MELDUNGEN AUF BEST EFFORT BASIS

Anzahl Vorfälle nach Sektoren 2023

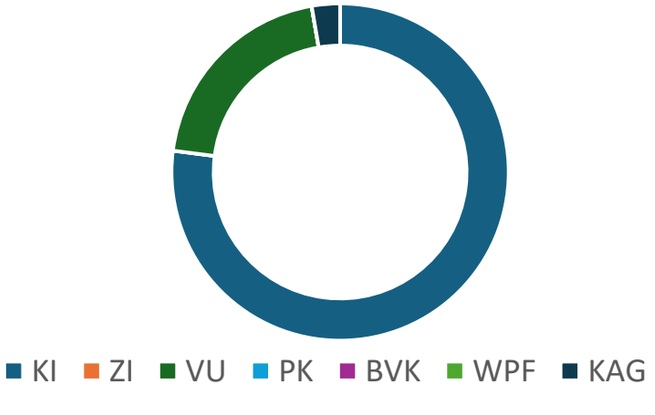


Indikation, zum Ausgehen des Vorfalls 2023

Klassifizierung des Vorfallstyps 2023

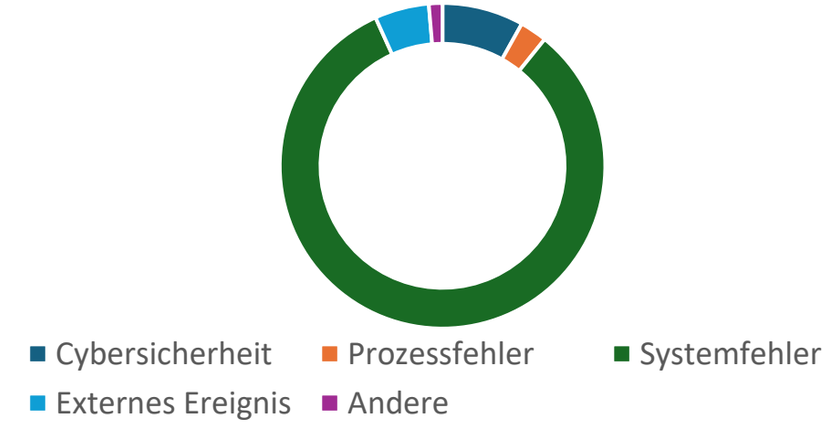


Anzahl Vorfälle nach Sektoren 2024 (bis 30.4.2024)



Indikation, zum Ausgehen des Vorfalls 2024 (bis 30.4.2024)

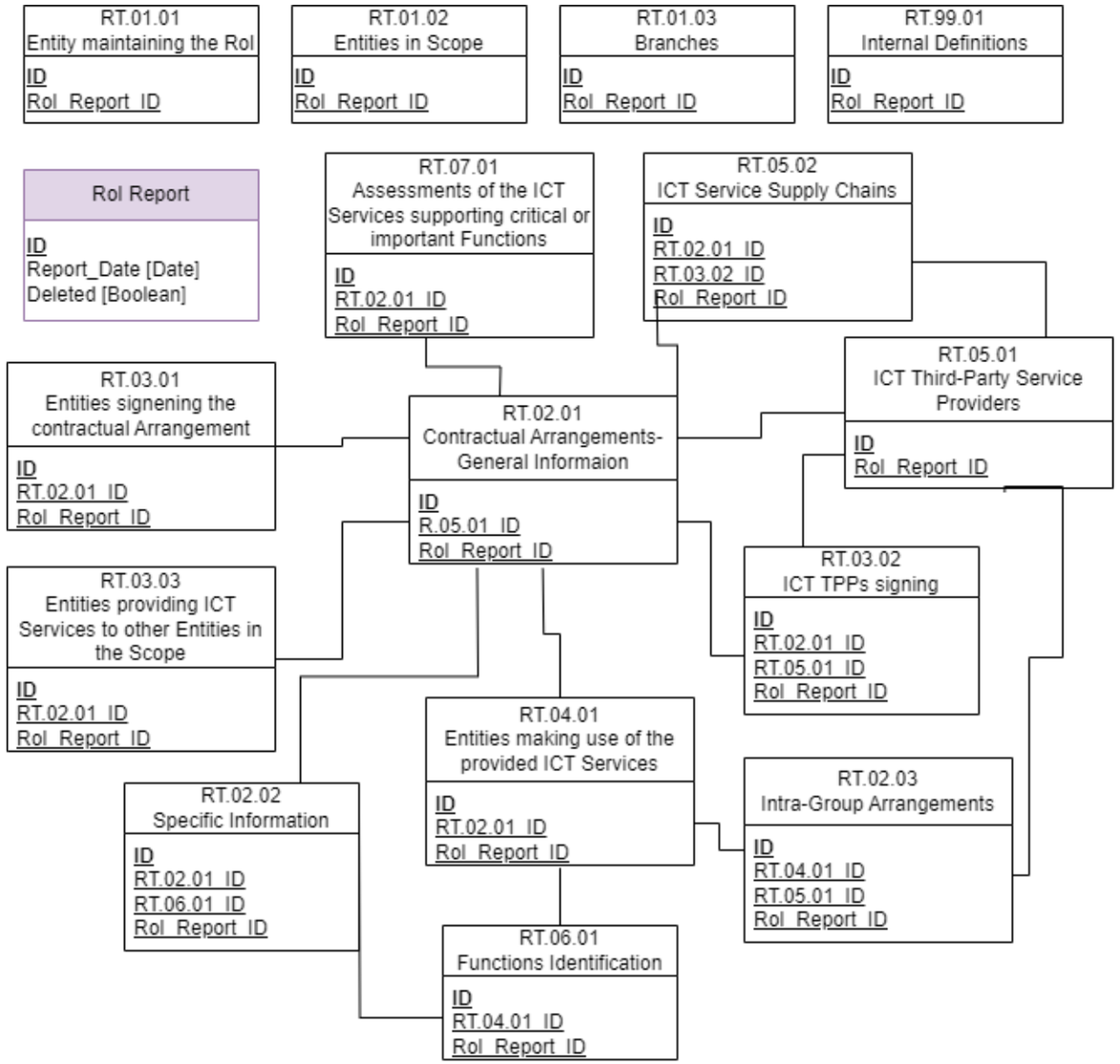
Klassifizierung des Vorfallstyps 2024 (bis 30.4.2024)



IKT-Vernetzungen am ö Finanzmarkt / Dry run: Lessons learnt & Way forward

IKT-VERNETZUNGEN

ÜBERSICHT: DORA INFORMATIONSREGISTER



- Recap: **Informationsregister aller IKT-Dienstleister** ist von den Beaufsichtigten ab 17.01.2025 laufend zu führen
- Siehe Grafik links: das **Register ist umfassend** und besteht aus einer **komplexen Struktur** aus zusammenhängenden Einzeltabellen
- Die enthaltenen Informationen werden zur Identifikation zentral für Europa wichtiger DL (CTPPs) herangezogen, erlauben aber auch der FMA:
  - Die Identifikation von Konzentrationsrisiken, sowohl bezogen auf einzelne DL als auch auf Konzerne oder geographische Gebiete
  - Die Erkennung digitaler Trends über die Art genutzter/eingestellter Dienstleistungen
  - Die zeitnahe Reaktion auf IKT-Vorfälle durch Identifikation von technisch verbundenen Unternehmen
- Allerdings: die Erstellung der Register ist eine **große Herausforderung** für die Beaufsichtigten, die Überwachung der Einbringung und Datenqualität sowie die interne Verarbeitung sind eine signifikante Aufgabe für die FMA

IKT-VERNETZUNGEN

ÜBERSICHT: INFORMATIONSREGISTER DRY RUN 2024

- Mitte 2024 wurde eine **Generalprobe der Informationsregister**-Übermittlung durchgeführt
- Diese im Rahmen der Digitalisierungsstudie 2024 durchgeführte Generalprobe wurde von Timeline und Fragebogen an eine parallel geplante ESA-Übung angepasst
- Im Gegensatz zu anderen teilnehmenden Staaten, hat die FMA in AT eine möglichst **hohe Marktabdeckung** angestrebt- von insgesamt 704 teilnehmenden Unternehmen stammten 250 aus Österreich und weitere 59 wurden über österreichische Gruppen eingebracht
- Bei der Analyse der Ergebnisse erwiesen sich die teilweise noch nicht vollständigen Register und Probleme mit der Datenqualität als Herausforderungen
- Feedback der ESAs eingetroffen und soll an Unternehmen weitergegeben werden

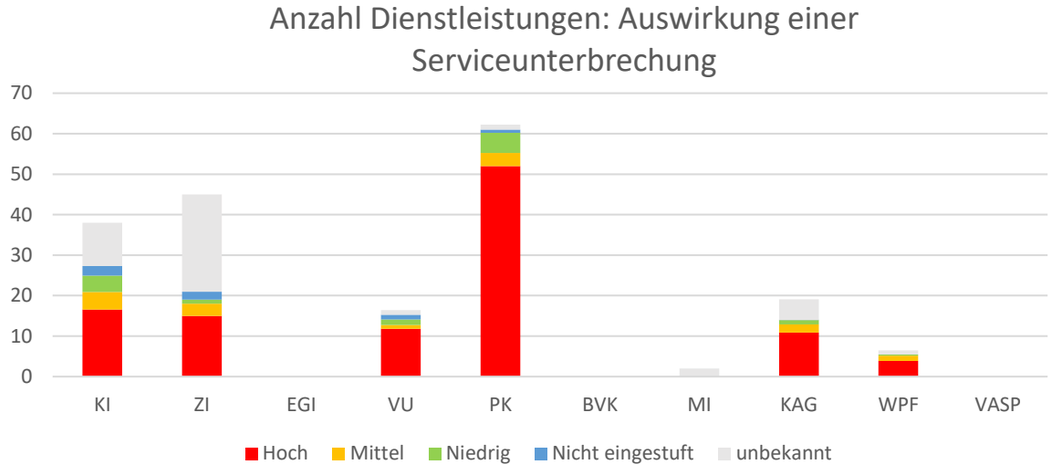
Lessons Learned Datenqualität:

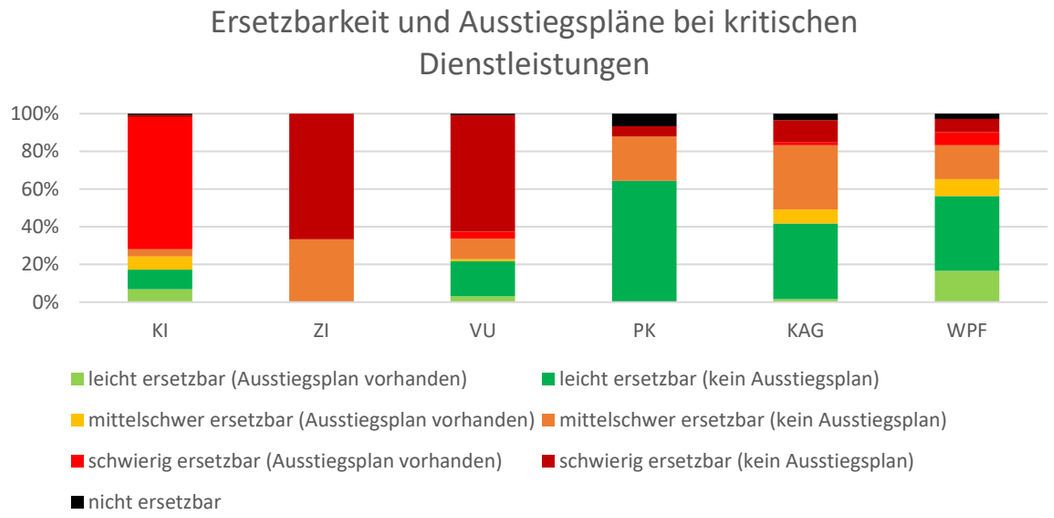
- Nicht zusammenpassende Schlüsselwerte bzw. fehlende Verknüpfungen
- Teilweise inhaltlich inkorrekte Angaben (z.B. falsche Konzession angegeben)
- Redundante Angaben
- Einige wenige Abgaben strukturell unbrauchbar
- Zahlreiche Anfragen durch Unternehmen

→ Automatisierungsunterstützer Validierungsprozess für 2025 angestrebt

IKT-VERNETZUNGEN
DRY RUN 2024: ERGEBNISSE

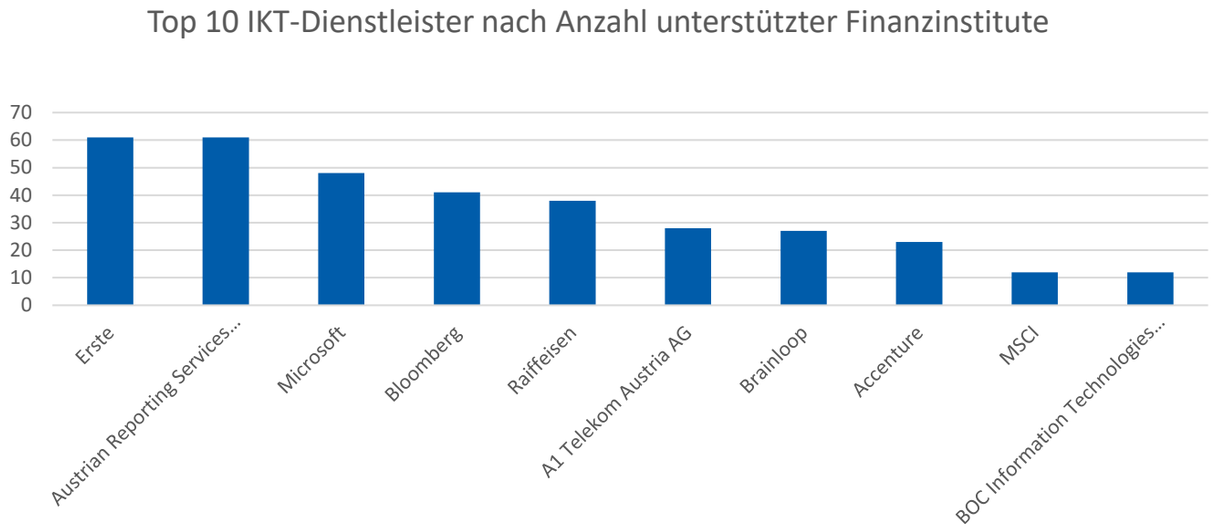
- Anmerkungen zur Marktabdeckung:
  - Kreditinstitute relativ stark vertreten, insgesamt jedoch alle Aufsichtsbereiche enthalten
  - Aufgrund teilweise noch unvollständiger Register sind kritische Dienstleister überdurchschnittlich vertreten
- Im Durchschnitt (abgesehen von Ausreißer bei PK und WPF) rund 13 kritische Dienstleistungen pro Unternehmen
- Diese Dienstleistungen sind zu einem guten Teil nur schwierig substituierbar
- Ausstiegspläne sind bislang beinahe ausschließlich bei KI vorhanden (bestehende sektorale Vorgaben)
- Insgesamt wird die starke Abhängigkeit der Finanzunternehmen von IKT-Dienstleistern (bereits bekannt durch nationale Schwerpunkte) durch die Ergebnisse der Generalprobe unterstrichen

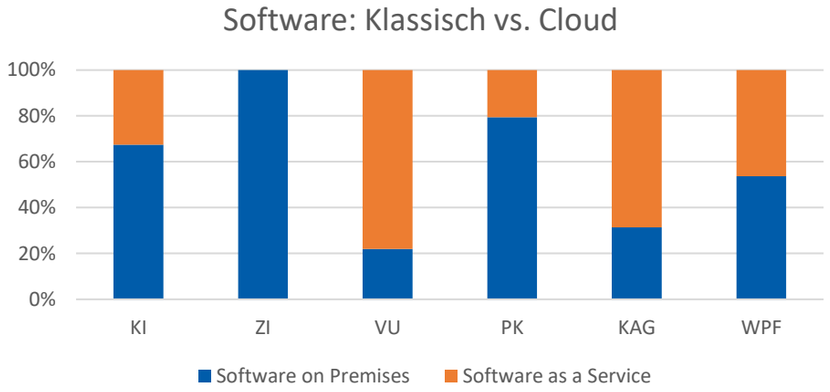




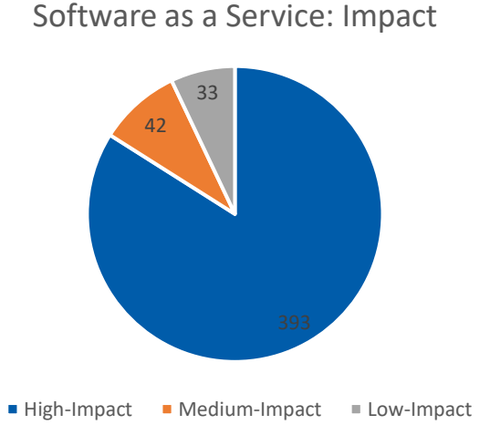
Quelle: FMA, Austrian Digital Finance Landscape 2024

IKT-VERNETZUNGEN
DRY RUN 2024: ERGEBNISSE





- Aufgrund teils noch unvollständiger Register ist eine abschließende Auflistung der Top-Dienstleister noch nicht möglich (z.B. DL wie Microsoft noch unterrepräsentiert)
- Hoher Einfluss von Software as a Service-Cloudlösungen ist erkennbar (andere Formen der Cloudnutzung weniger weit verbreitet)
- Diese von Cloudprovidern zur Verfügung gestellten Applikationen stellen wiederum oft wichtige und schwierig ersetzbare Services dar



Quelle: FMA, Austrian Digital Finance Landscape 2024

IKT-VERNETZUNGEN

EXKURS: BEDROHUNGSLAGE FÜR IKT-DIENSTLEISTER

IKT-Dienstleistungen können durch zahlreiche Bedrohungen unterbrochen werden:

- Cyberangriffe
- Systemausfälle
- Insolvenz von IKT-Dienstleistern
- Sanktionen oder politische Instabilität
- Rechtliche Bedenken und Datenschutz

Insbesondere Cyberangriffe erweisen sich als wachsendes Problem:

- Viele von der FMA erfasste Angriffe gehen auf IKT-Dienstleister zurück
- Angreifer umgehen Sicherheitsmaßnahmen bei FI und können mehrere Ziele gleichzeitig treffen
- Große IKT-Dienstleister (und somit auch abhängige Finanzunternehmen) können auch Ziel staatlicher Akteure werden

ENISA Threat Landscape 2024: Link

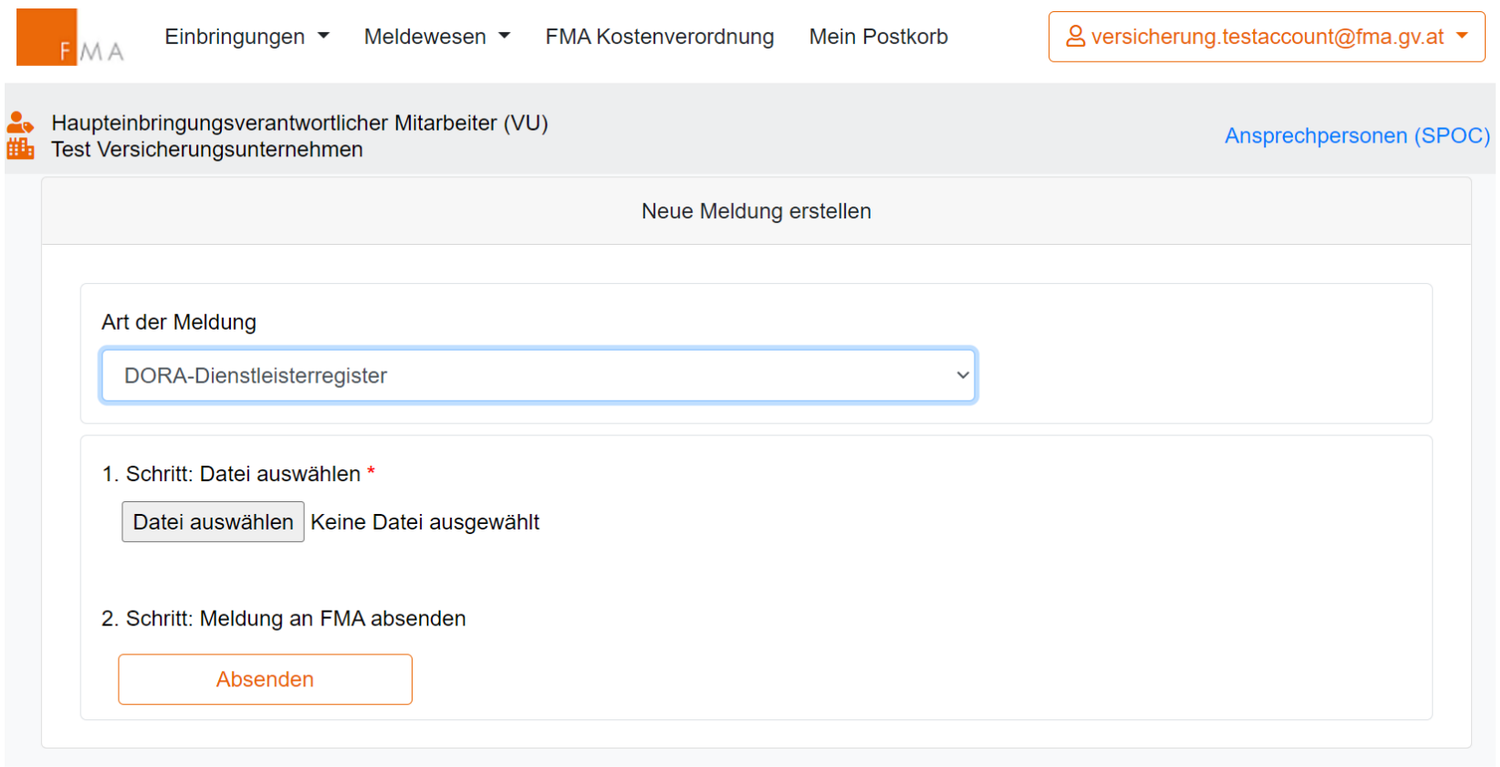
CSRB Bericht zu Microsoft Masterkey-Vorfall 2023: Link

Crowdstrike-Vorfall 2024: Link

XZ-Utils Angriffsversuch 2024: Link

IKT-VERNETZUNGEN

AUSBLICK: ÜBERMITTLUNG DER INFORMATIONSREGISTER



Screenshot: Meldeformular für Informationsregister-Einbringungen über IP

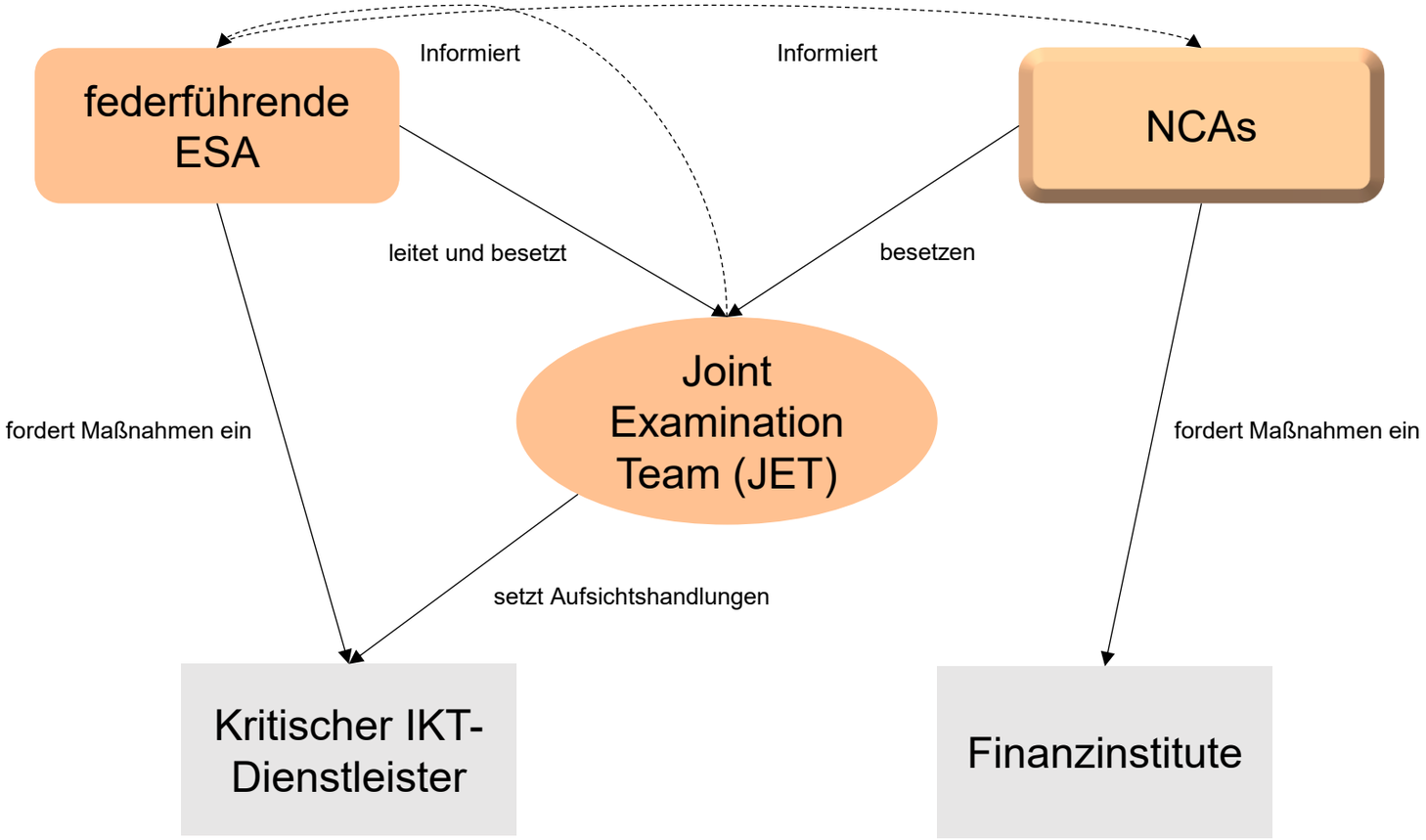
- Die Informationsregister werden voraussichtlich mit dem **Cutoff-Date 31.03.2025** einzumelden sein.
- Die FMA wird nach aktuellem Plan die Register bis 30.04.2025 an die ESAs weiterleiten müssen.
- Um Zeit für Nachmeldungen, Validierung, Korrekturen und Formatkonvertierung zu lassen, wird eine **Abgabe 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-VERNETZUNGEN

AUSBLICK: ÜBERWACHUNG ZENTRALER DIENSTLEISTER

Auf europäischer Ebene ist folgender Prozess geplant:

- Auf Basis der Informationsregister werden in Europa agierende ‚kritische' Dienstleister (CTPP) identifiziert
- Eine der drei ESAs übernimmt die Federführung bei der Aufsicht über einen CTPP
- Für jeden CTPP wird (unter Involvierung der NCAs) ein zentrales Aufsichtsteam (JET) gebildet
- JETs setzen Aufsichtshandlungen wie z.B. Vor-Ort-Prüfungen, Interviews und Erhebungen
- CTPPs müssen als Reaktion auf Findings Maßnahmensetzungen deklarieren
- NCAs werden über relevante Findings bei CTPP informiert



Quelle: FMA

Ausblick 2025

AUFSICHTS- UND PRÜFSCHWERPUNKTE 2025

- Grundsätzlich alle Sektoren:
  - **Deep Dives / Einsichtnahmen zum digitalen Risikoprofil** auf Basis der „Austrian Digital Finance Landscape“
  - **1. Meldung zu Register of Information**: Ermittlung der IKT-Verflechtungen am ö Finanzmarkt & Identifikation kritischer IKT-Dienstleister
  - **Vor-Ort-Prüfungen** zur IKT-Sicherheit ab 2. HJ 2025
- KI, VU und Marktinfrastrukturen:
  - (Vorbereitung der) Durchführung von **Threat-Led Penetration Tests**
- Marktinfrastrukturen:
  - Integration der DORA - Aufsicht, als Teil der operativen Aufsicht der MIF´s
  - Dora Managementgespräche
  - Vor-Ort-Prüfungen nach Prüfplan
- Bankenabwicklung:
  - Entwicklung eines Datenanalysetools zur Auswertung und Analyse der bereitgestellten Daten in einer Abwicklung
  - Ausarbeitung eines Testprogramms zur Stärkung der Abwicklungsbereitschaft