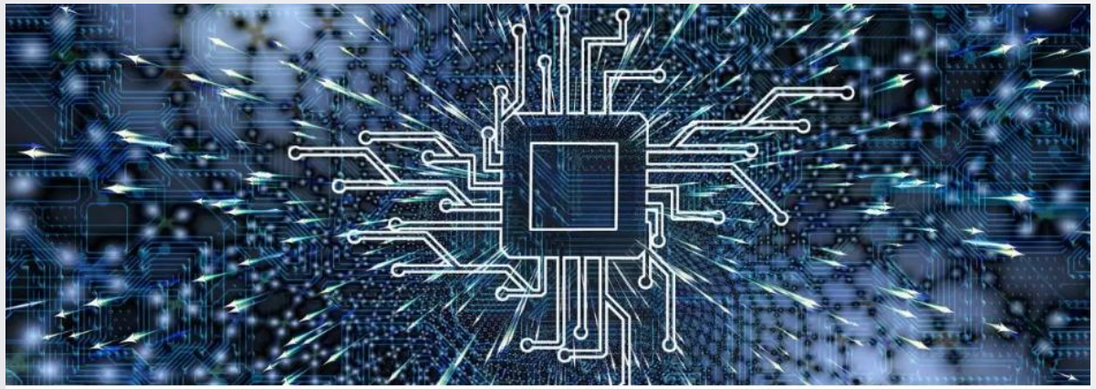
ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

EIN JAHR DORA – HIGHLIGHTS, HERAUSFORDERUNGEN & WAY FORWARD

18.2.2026

DORA feiert den ersten Geburtstag!



Cybersicherheit gestärkt: FMA und OeNB ziehen positive Bilanz nach einem Jahr DORA

16. Januar 2026 | Pressemitteilung

AGENDA

Begrüßung
Michael Hysek

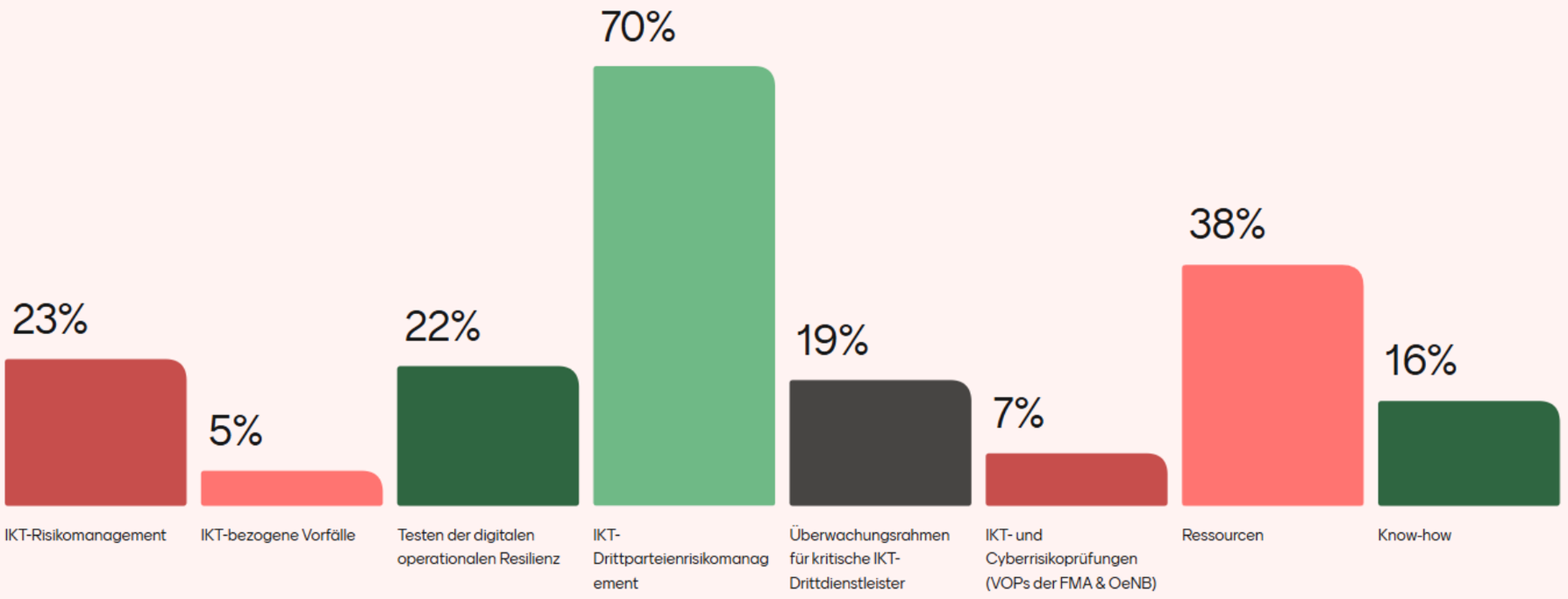
Erfahrungen und Erkenntnisse zu folgenden Bereichen

- IKT-Risikomanagement
  Anna Muri
- IKT-bezogene Vorfälle & Förderung Informationsaustausch
  Daniel Kirnbauer / Ulrike Rhomberg
- Testen der digitalen operationalen Resilienz
  Josef Mitterhöfer / Georg Eilnberger
- IKT-Drittparteienrisikomanagement
  Karl Machan
- Überwachungsrahmen für kritische IKT-Drittdienstleister
  Christian Haider
- IKT- und Cyberrisikoprüfungen
  Gernot Burgsteiner / Christian Steinmetz / Norbert Fröhlich

Ausblick
Sabine Balogh-Preininger

UMFRAGE

Was war im ersten Jahr DORA für Ihr Unternehmen die größte Herausforderung?



menti.com

3858 2042

176 of **202** responded

IKT-Risikomanagement

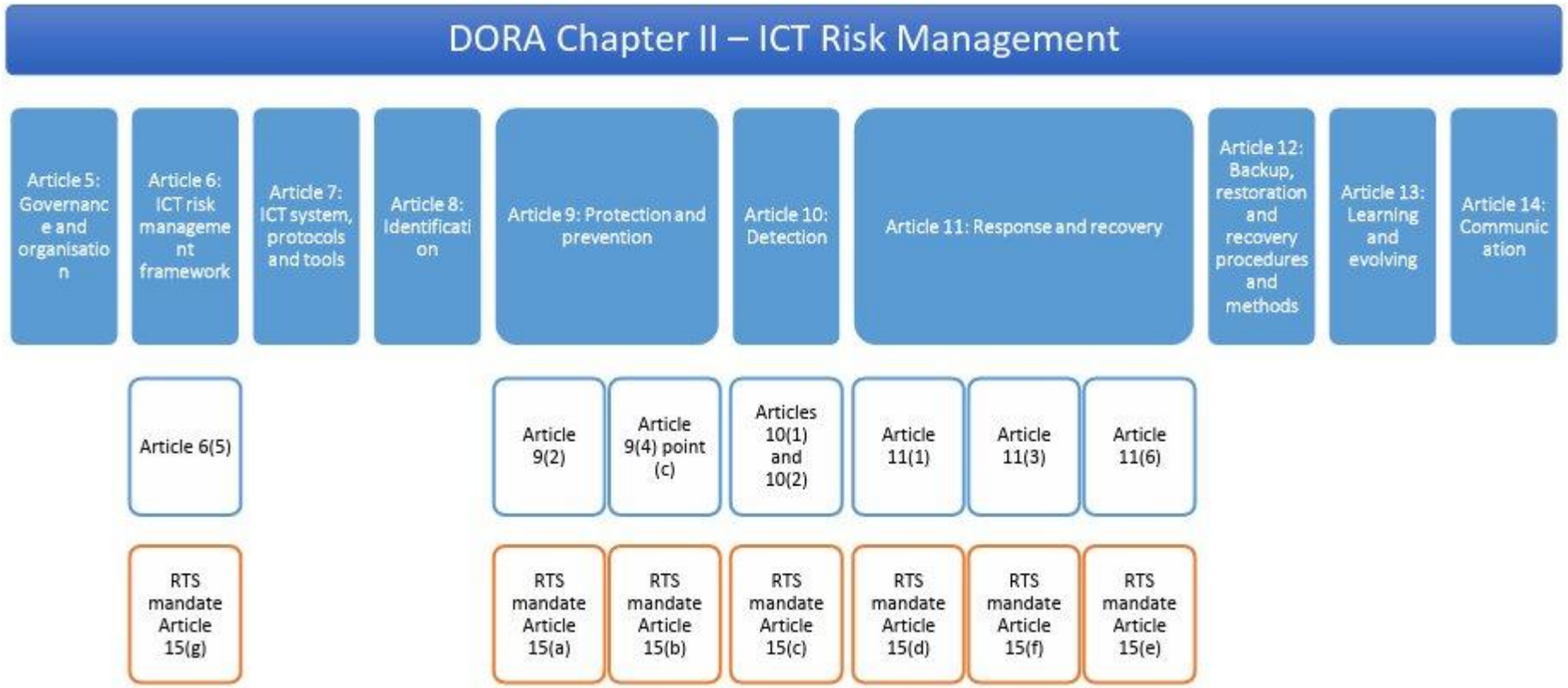
IKT-RISIKOMANAGEMENT

- Finanzunternehmen müssen über einen internen **Governance- und Kontrollrahmen** verfügen, der ein wirksames Management von IKT-Risiken gewährleistet
- In Art 5 – 16 DORA definiert

Governance & Organisation		
IKT-Risikomanagement Rahmen	IKT-Systeme, -Protokolle und -Tools	Identifizierung
Schutz & Prävention	Erkennung	Reaktion & Wiederherstellung
Backup, Wiedergewinnung und Wiederherstellung	Lernprozesse und Weiterentwicklung	Kommunikation

IKT-RISIKOMANAGEMENT

- Art 15 und 16 DORA beinhalten die von den ESAs zu erarbeitenden RTS:



IKT-GOVERNANCE: AKTUELLE WAHRNEHMUNGEN AUS DER BEHÖRDLICHEN AUFSICHT

Fit & Proper Test – DORA ist Bestandteil

- DORA ist seit 17.01.2025 fixer Bestandteil bei Fit & Proper Tests für Führungsfunktionen mit IT-Sicherheitsbezug.
- Grundlegende Anforderungen von DORA und IT-Sicherheit sowie deren Umsetzung im Unternehmen müssen verstanden werden. Proportionalität: Wissen je nach Ressort erforderlich.
- Grobe Defizite führen zur negativen Bewertung des Tests. Achtung: Zwei negative Bewertungen = fachliche Eignung nicht gegeben!

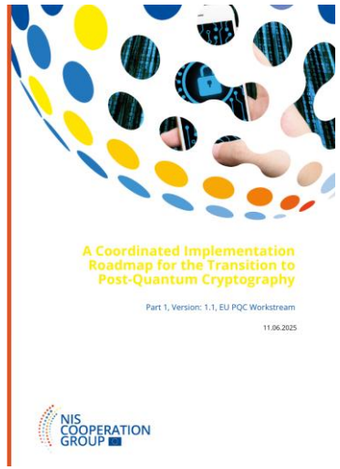
Unabhängigkeit der IKT-Kontrollfunktion

- Kritisch bis unzulässig: IKT-Kontrollfunktion in Personalunion mit IT-Leiter.
- Einsatz von externen CISO-Rollen bei kleinen Finanzunternehmen → bringen gezielt die benötigte Fachexpertise ein.

IKT-RISIKOMANAGEMENT: AKTUELLE WAHR-NEHMUNGEN AUS DER BEHÖRDLICHEN AUFSICHT

- **Aufsichtlicher Fokus beim IKT-Risikomanagement auf angemessene Vorkehrungen iHa**
  - Datenklassifizierung und IKT-Risikobewertung,
  - Vorschriften zur Verschlüsselung von Daten bei Speicherung/Verarbeitung/Übermittlung,
  - Krypto-Key-Management (Rotation, Rücknahme, etc.),
  - aktuellen Auswahlkriterien für kryptografische Techniken und Nutzungspraktiken,
  - Fähigkeit zur Aktualisierung kryptografischer Technologien
  - Register aller Zertifikate und Zertifikatsspeicher

- **Post Quantenverschlüsselung**
  - Die Roadmap for the Transition to Post-Quantum Cryptography (PQC) der NIS Cooperation Group fordert ähnliche Maßnahmen wie DORA (Art. 6 und 7 DelVO(EU) 2024/1774 zum Risikomanagement).
  - Unternehmen sollten frühzeitig auf PQC-Technologien achten und ihre Systeme entsprechend vorbereiten.
  - Der optimale Zeitpunkt für den Umstieg auf PQC liegt in der Verantwortung jedes Instituts – die FMA gibt diesen nicht vor.
  - Besonders bei Daten, die langfristig geschützt werden müssen (z.B. Vertragssignaturen), sollte PQC frühzeitig eingeplant werden.
  - Ein technologieorientiertes, vorausschauendes Handeln erleichtert die spätere Umstellung und erhöht die Sicherheit.

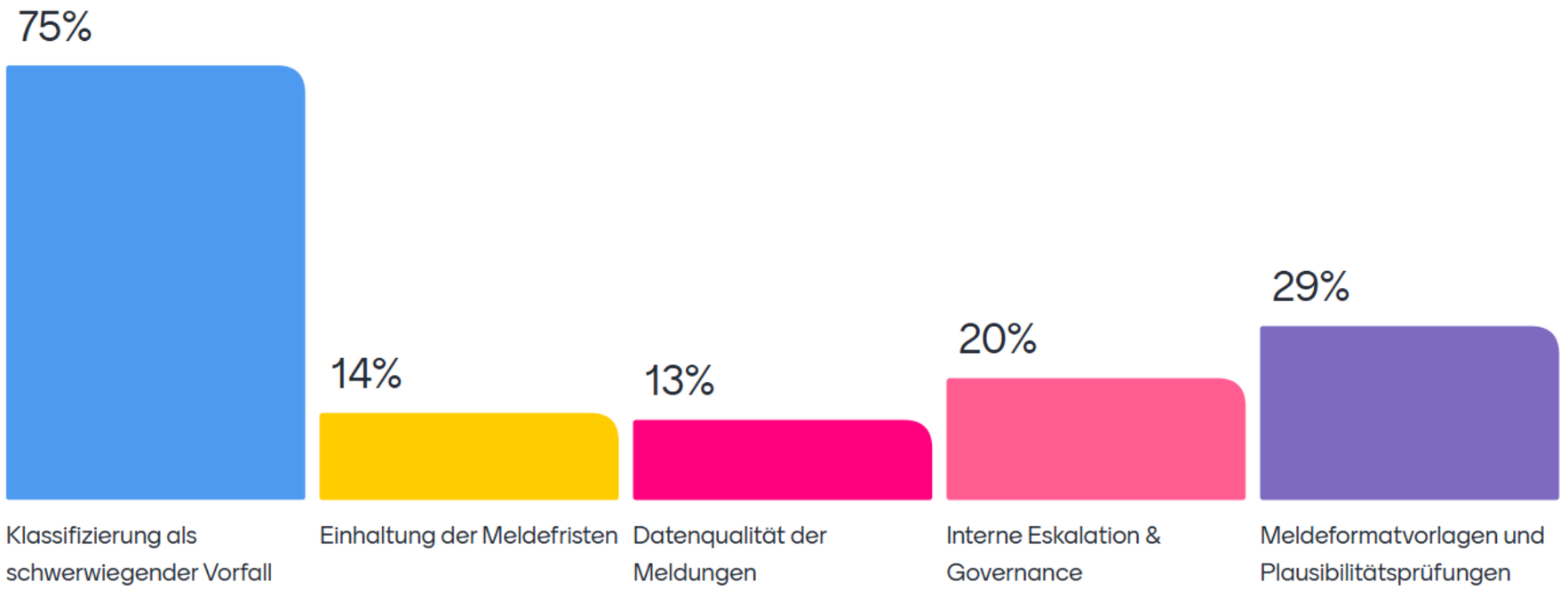


Online am 04.09.2025: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

IKT-bezogene Vorfälle & Förderung Informationsaustausch

UMFRAGE

Was stellt aktuell die größte Herausforderung im Umgang mit der Meldung von IKT-Vorfällen dar?



menti.com
1193 1792

163 of 200 responded

WAS IST DIE MELDEVERPFLICHTUNG SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE?

Seit 17. Jänner 2025 gilt die Meldeverpflichtung schwerwiegender IKT-bezogener Vorfälle nach DORA.

Meldung schwerwiegender IKT-bezogener Vorfälle

(Art. 19 Abs. 1 DORA)

- Werden Vorfälle als schwerwiegend iSd Art. 19 Abs. 1 DORA klassifiziert, so sind diese verpflichtend an die zuständige Behörde zu melden
- Klassifizierungskriterien definiert in Art. 18 DORA iVm DelVO (EU) 2024/1772

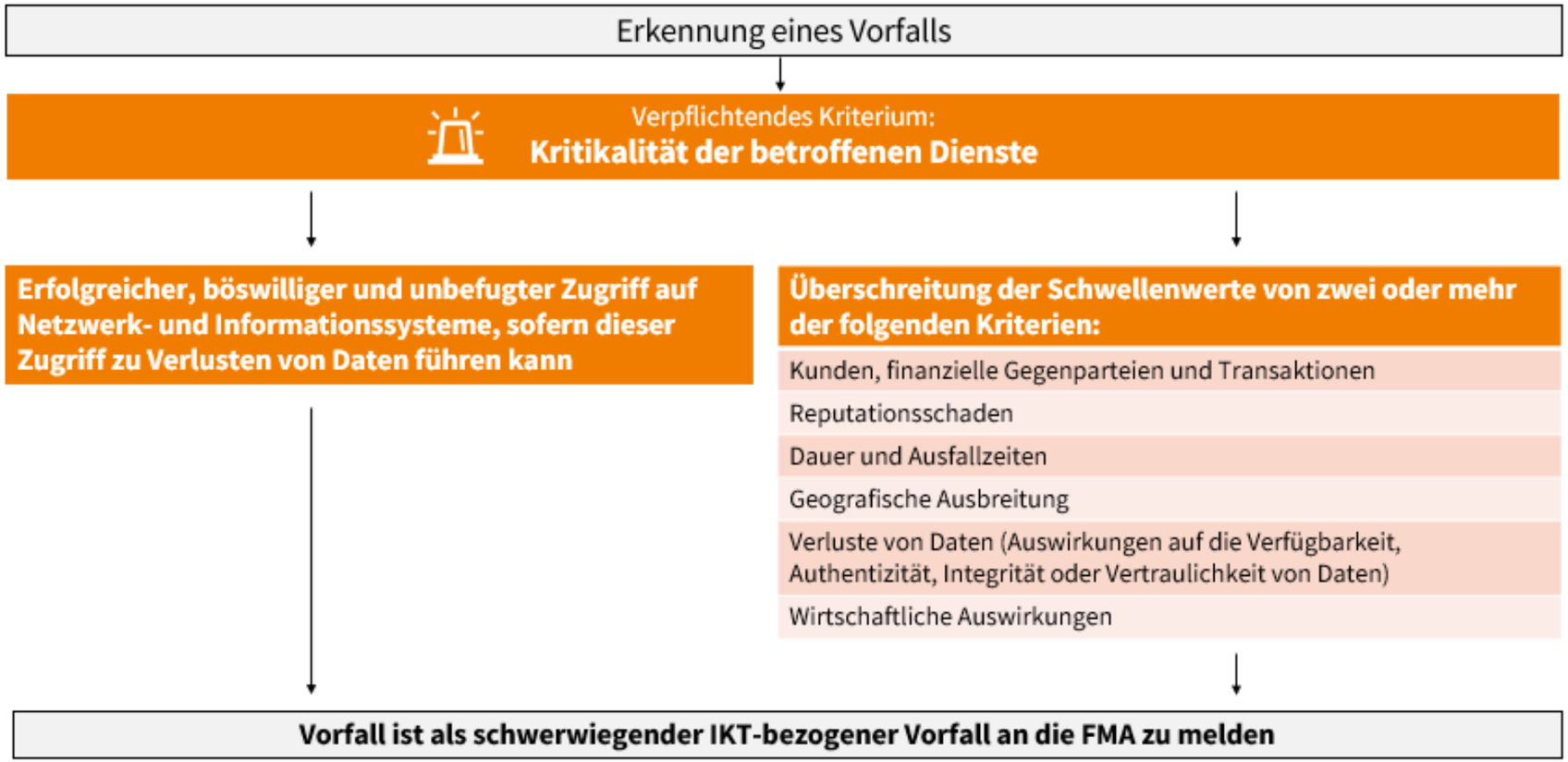
Freiwillige Meldung erheblicher Cyberbedrohungen

(Art. 19 Abs. 2 DORA)

- Unternehmen können erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist
- Wesentlichkeitsschwellen definiert in Art. 10 DelVO (EU) 2024/1772
- Ziel: Ermöglichung eines umfassenden Bilds über die Cybersicherheitslage

WAS GILT ALS KRITISCH/MELDEWÜRDIG?

Eine Meldeverpflichtung entsteht, wenn der Klassifizierungsansatz gem. Art. 8 DelVO (EU) 2024/1772 gegeben ist:



Hinweis auf EBA Q&A (2025_7613) zu Phishing-Angriffen: 2025_7613 Classification of phishing-attacks as a reportable major ICT-related incident | European Banking Authority

MELDUNGEN SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE

Fristen

Erstmeldung

Frist

- jedenfalls binnen **24 Stunden ab Erkennung** des Vorfalls & **binnen 4 Stunden ab Klassifizierung** als schwerwiegend

Zwischenmeldung

Frist

- binnen **72 Stunden** ab Übermittlung der Erstmeldung

Abschlussmeldung

Frist

- binnen **1 Monats** ab Übermittlung der (aktuellsten) Zwischenmeldung

Gegebenenfalls sind die Informationen zu aktualisieren!

Meldung an die FMA

Hinweise:

Sonderregelungen zu den Fristen in Art. 5 DelVO (EU) 2025/301 definiert

Reklassifizierungs-meldung jederzeit möglich

WAS MACHT DIE FMA MIT DEN EINGELANGTEN MELDUNGEN?

Prozess

- **Dokumentation und behördliche Bearbeitung** in FMA-Tool
  - Alle Meldungen werden **kurzfristig** geprüft
  - Jede Meldung wird iwF **umfassend analysiert**
  - Bei Beteiligung von IKT-Drittdienstleistern: Abgleich mit Informationen aus dem **Register of Information**
  - Automatische Weiterleitung an die jeweils zuständige Behörde (ESAs, EZB, NIS-Behörde, OeNB)

Praktische Hinweise

- **kleinere Mängel**:
  Kontaktaufnahme durch FMA mdB um Update gewisser Felder im Zuge der nächsten Einbringung

- ggf. kommt es zu einer **Aufforderung zur Stellungnahme** durch die FMA

MELDUNGEN SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE

Bisherige Beobachtungen und aufsichtliche Erwartungshaltung

Schwierigkeiten bei der Einmeldung

- Technische Herausforderungen aufgrund des neuen Meldetools

Fristen werden nicht eingehalten

- **Prozesse** und **Richtlinien** sind derart zu gestalten, dass die Fristen eingehalten werden
- **Sonderbestimmungen** in Art 5 Abs 2 bis Abs 5 DelVO (EU) 2025/301
- ggf. **Abstimmung mit IKT-Drittdienstleister** hinsichtlich Einhaltung der Fristen

Inhaltlich fehlerhafte Meldungen

- Erstmeldung falsch befüllt (z.B. "2.5 Betroffene kritische Dienstleistungen" nicht angegeben)
- Berechnungen in der Zwischenmeldung falsch (z.B. "Anzahl der betroffenen Kunden: 2798" ≠ "Prozentsatz der betroffenen Kunden: 0%")

- **Vorfalls-ID** wird im Zuge der erfolgreichen Einbringung der Erstmeldung übermittelt
  - → wurde teilweise bei Zwischen-, Abschluss- und Reklassifizierungsmeldungen nicht mehr angegeben

- **Fristverletzungen sind verwaltungs-strafbewährt**

DORA-VORGABEN ZU VORFALLSMELDUNGEN

Eskalation sicherstellen:
➡️ Kritische Vorfälle sind dem Leitungsorgan zu berichten

Rollen klar festlegen – Verantwortung übernehmen:
➡️ Funktionen & Zuständigkeiten definieren, dokumentieren und vom Leitungsorgan freigeben

Prozesse unternehmensspezifisch ausgestalten:
➡️ keine allgemeinen DORA bzw. FMA-Vorgaben

Alle Ebenen schulen:
➡️ von Mitarbeitenden bis Geschäftsleitung & Drittdienstleister!

Compliance sicherstellen – Prozesse & Richtlinien DORA-fit machen

IKT-Drittdienstleister steuern:
➡️ Zusammenarbeit & Fristen verbindlich regeln

Alle IKT-Vorfälle erfassen und dokumentieren:
➡️ auch unterhalb der Meldeschwelle!

Vorfälle professionell steuern:
➡️ Klare Kommunikationsstrategie entwickeln & Pläne festlegen!

Incident-Response-Verfahren einrichten:
➡️ schnelle Gegenmaßnahmen sicherstellen

MELDUNGEN SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE

Meldeverpflichtung gem. Art 19 Abs 1 DORA, wenn Vorfälle als schwerwiegend klassifiziert werden:

- **Klassifizierungskriterien** definiert in Art 18 DORA iVm DelVO (EU) 2024/1772
- Einhaltung der definierten die **Fristen** gem. Art 5 DelVO 2025/301
- Arten von Meldungen: **Erst-**, **Zwischen-**, **Abschluss-** und **Reklassifizierungsmeldung**

Anzahl der an die FMA gemeldeten Vorfälle im Jahr 2025:

Erstmeldungen	Q1 2025	Q2 2025	Q3 2025	Q4 2025	Summe
Anzahl gemeldete Vorfälle	**17**	**28**	**51**	**32**	**128**
davon als nicht schwerwiegend reklassifiziert	2	9	11	3	25
Gesamt	**15**	**19**	**40**	**29**	**103**

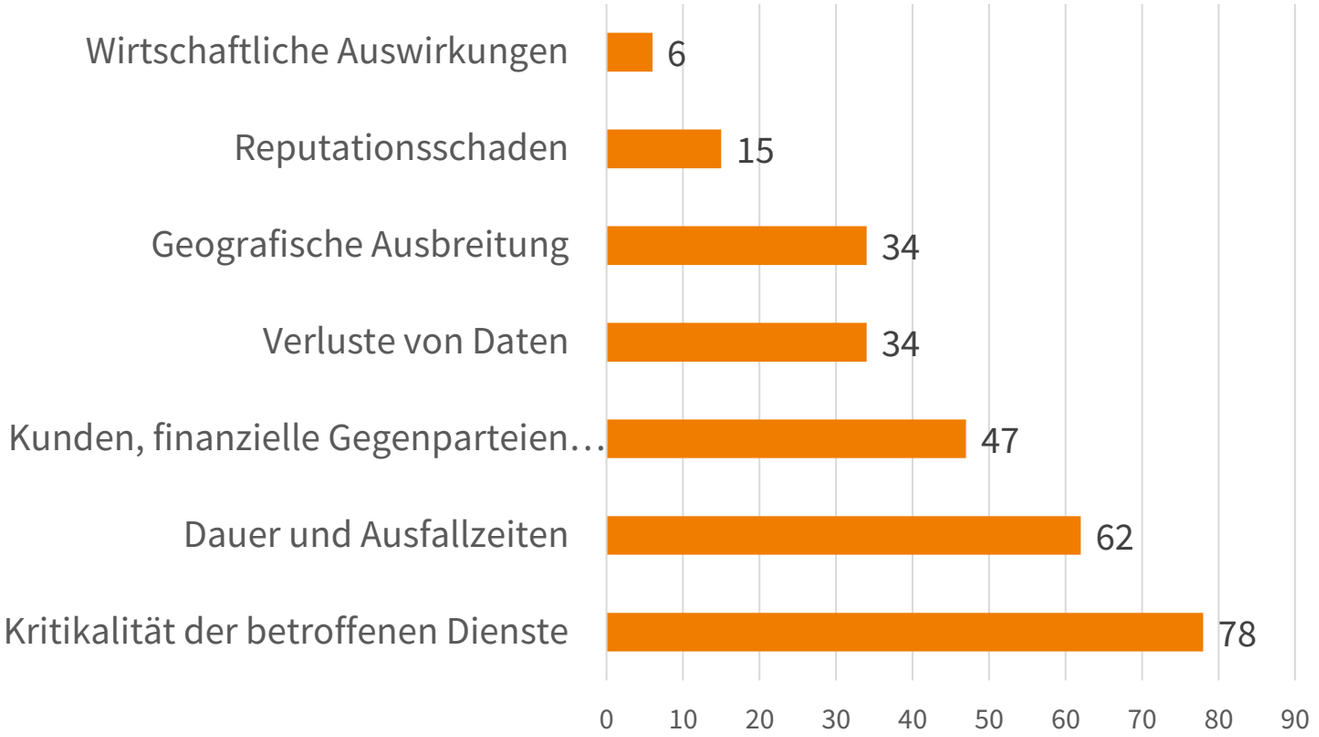
Hinweis: Die Aufstellung beinhaltet Einzelmeldungen und konsolidierte Meldungen gem. Art 7 Durchführungsverordnung (EU) 2025/302 sowie (von der FMA zugelassene) technisch-konsolidierte Meldungen.

MELDUNGEN SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE

Vorfälle je FMA-Bereich 2025

Sektoren	Anzahl
Bankensektor	75
Versicherungs-, Pensions-kassen- und Vorsorgekassensektor	7
Wertpapiersektor	21
	103

Erfüllte Klassifizierungskriterien 2025

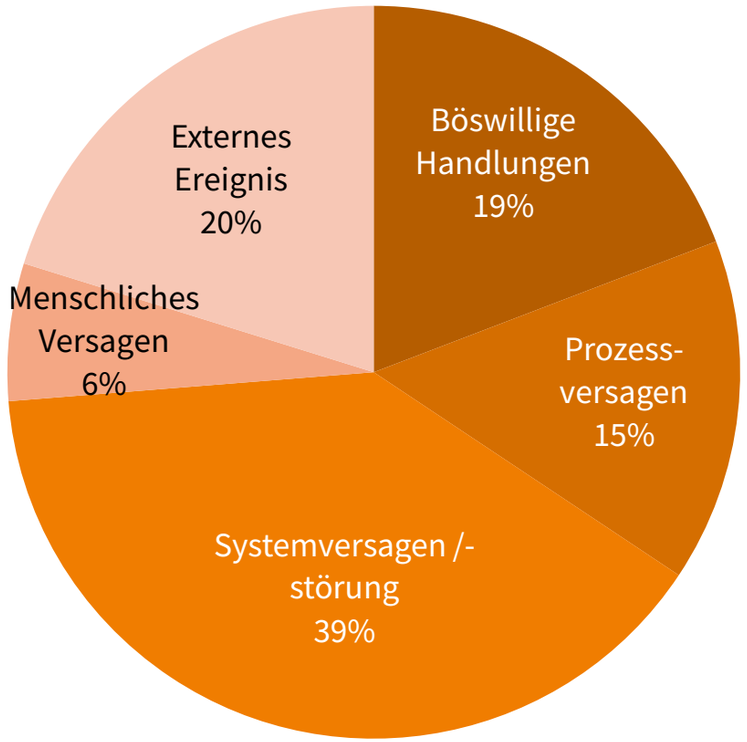


MELDUNGEN SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE

- Fast vier von zehn Vorfällen gehen auf technische Ausfälle oder Störungen zurück ➔ **Management struktureller oder infrastruktureller Schwachstellen** entsprechend wichtig.
- Externe Ereignisse und böswillige Handlungen zusammen machen fast 40% aus ➔ unterstreicht die **Relevanz von Risikomanagement, Prävention und Schutz vor externen Störungen**.
- **Management des Drittparteienrisikos** ist weiterhin ein zentrales Element für digitale operationale Resilienz.

Vorfallsmeldungen 2025:
Ursprung IKT-Drittdienstleister

Vorfallsmeldungen 2025:
Ursachen lt. Abschlussmeldungen



SICHERHEITSVORFÄLLE BEI IKT-DRITTDIENSTLEISTERN – BEISPIELE

Bei Bedarf kann die FMA **direkt Informationen von Drittanbietern einfordern** und die Kundeninformation kontrollieren.

Ransomware-Vorfälle

- Ransomware-Vorfälle bei IKT-Drittanbietern bergen erhöhtes Risiko für viele Finanzunternehmen.
- DORA-Meldepflicht gilt auch für Vorfälle durch IKT-Drittanbieter.
- Updates kompromittierter Anbieter sollten kritisch geprüft werden.

KI-Risiken

- KI-Systeme erfordern breiten Datenzugriff → größere Angriffsfläche und potenziell Vorfälle entlang der Lieferketten.
- Auch bei Innovationsprojekten wie KI müssen die in DORA geforderten Tests durchgeführt werden.
- KI sollte auch bei Angriffsszenarios und Red-Team-Tests miteinbezogen werden.

FÖRDERUNG INFORMATIONSAUSTAUSCH ZU CYBERBEDROHUNGEN

Rechtsgrundlage

Art 45 DORA-VO: Schaffung eines klaren Rahmens für den Informationsaustausch zu Cyberbedrohungen zwischen Finanzunternehmen

Möglichkeiten für Finanzunternehmen:

- Gezielte Teilnahme an bestehenden Informationsaustauschformaten.
- Mitwirkung an neuen Angeboten, z. B. CERT.at-Mailinglisten.
- Aktive Mitgestaltung zukünftiger Austausch- und Dashboard-Lösungen zur sektorweiten Lagebilderstellung.

Ressourcen & Weiterführendes:

- Informationen auf der FMA-DORA-Website
- Beiträge relevanter Interessensgruppen wie Watchlist Internet
- Anmeldung zu CERT.at-Newslettern für operative Threat-Informationen

Meldepflicht für Finanzunternehmen bei Teilnahme an Vereinbarungen über Informations-austausch!

Der strukturierte, vertrauenswürdige Informationsaustausch ist ein wesentlicher Hebel zur Erhöhung der operativen Resilienz und zur Stabilisierung des österreichischen Finanzmarktes.

Testen der digitalen operationalen Resilienz

TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ

- Die digitalen operationalen Resilienztests umfassen das **allgemeine Testprogramm**, welches von allen Finanzunternehmen zu erfüllen ist, und die auf Live-Produktionssystemen durchzuführenden **Threat Led Penetration Tests (TLPT)**, die nur bedeutende Finanzunternehmen* betreffen.

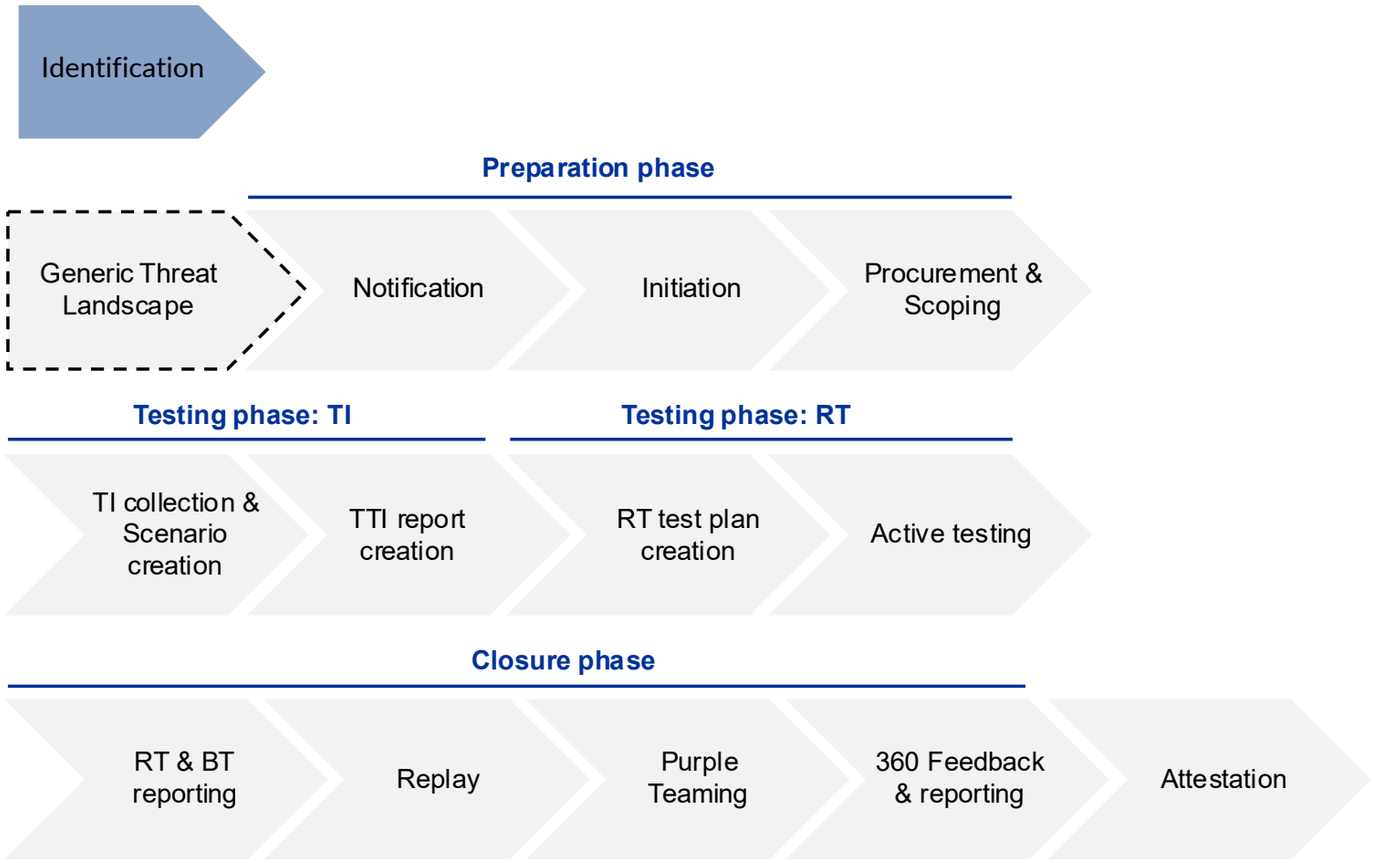
Allgemeines Testprogramm	Threat Led Penetration Tests (TLPT)
Umfassendes Programm für das Testen der digitalen operationalen Resilienz, welches von allen Finanzunternehmen zu erfüllen ist. z.B. Schwachstellenbewertungen und -scans, Gap Analysen, Quellcodeprüfungen, szenariobasierte Tests oder Penetrationstests	Bedeutende Finanzunternehmen haben verpflichtend so genannte Threat Led Penetration Tests (TLPTs) durchzuführen. TLPTs simulieren reale Cyberangriffe unter streng kontrollierten Bedingungen (und finden daher auch in der Produktionsumgebung statt) und sollen dazu beitragen Schwachstellen in kritischen IT-Systemen von Finanzunternehmen zu erkennen. TLPTs orientieren sich an der aktuellen globalen Bedrohungslage.
Die Tests werden von unabhängigen, internen oder externen Parteien durchgeführt.	Die TLPTs werden von unabhängigen externen Prüfern durchgeführt (sog. Red Teams).
Bei sämtlichen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, werden mindestens einmal jährlich angemessene Tests durchgeführt.	TLPTS müssen alle 3 Jahre für als kritisch eingestufte Unternehmen durchgeführt werden.
	Die konkrete Methodik beruht auf dem Rahmenwerk TIBER-EU. TIBER steht für „Threat Intelligence-Based Ethical Red Teaming“ und wird in Österreich durch TIBER-AT umgesetzt. Das TIBER Cyber Team der OeNB (TCT-AT) ist für TIBER-AT verantwortlich und begleitet alle Tests in Kooperation mit der Finanzmarktaufsicht (FMA) oder, im Fall bedeutender Kreditinstitute, mit der Europäischen Zentralbank (EZB). Nach Testabschluss erfolgt eine offizielle Attestierung durch die FMA bzw. die Europäischen Zentralbank (EZB), womit auch die Konformität der Tests mit den gesetzlichen Anforderungen bestätigt wird. 2025 wurden die ersten TLPTs gemäß TIBER-AT durchgeführt.

* Die Kriterien zur Identifikation bedeutender Finanzunternehmen sind in Art. 26 Abs. 8 DORA-VO geregelt und werden durch Art. 2 Delegierte Verordnung (EU) 2025/1190 präzisiert. Wesentliche Kriterien sind: wirkungsbezogene Faktoren, etwaige Bedenken hinsichtlich der Finanzstabilität sowie das spezifische IKT-Risikoprofil und der IKT-Reifegrad des Finanzunternehmens.

Threat-led Penetration Testing (TLPT) basierend auf dem TIBER-EU Rahmenwerk

Wesentliche Merkmale von TLPT

- Testen der kritischen **Live-Produktionssysteme**
- Von verpflichteten Finanzunternehmen **alle drei Jahre** durchzuführen
- Als **ergänzendes Mittel** zum klassischen Testprogramm (z.B. Pentests), nicht als Ersatz
- **Einbindung** der externen **IKT-Drittanbieter**, bei Auslagerung relevanter Funktionen
- Basiert auf dem **TIBER-EU** Rahmenwerk, das die Grundlage für **TIBER-AT** und **TIBER-SSM** ist.



TI = Threat Intelligence
TTI = Targeted Threat Intelligence

RT = Red Team
BT = Blue Team

Was ist die Generic Threat Landscape (GTL)?

Die GTL erfasst die **generelle Bedrohungslage im Cyberraum** des österreichischen Finanzsektors

Erfasst relevante **Bedrohungsakteure, Taktiken, Techniken** und globale sowie lokale **Trends** im österreichischen Finanzsektor

Die GTL dient primär als **Ausgangspunkt für TIBER-Tests** und wird darüber hinaus an **interessierte Finanzunternehmen** zur Information übermittelt.

Wird **halbjährig** von einem externen Dienstleister **erstellt**

Wechsel des GTL-Anbieters | Bisherige Hauptaussagen bleiben gültig

SecAlliance

↓

Deloitte.

Euer **Feedback** ist gefragt!

GTL Sommer 2025

Staatlich motivierter Akteure

- **Die wichtigsten Akteure:**

- **Network-Prepositioning-Aktivitäten** gewinnen an Bedeutung und sind eine **realistische Bedrohung**

Organisierte Cyberkriminalität (OCGs)

- **Ransomware, Datendiebstahl** und **Erpressung** bleiben dominierende Bedrohungen
- Finanzsektor weiterhin **attraktives Ziel** für OCGs
- **Datendiebstahl** finanzkritischer Informationen durch verschiedene Akteure
- „**Access-as-a-Service**“ boomt

Highlights der GTL Winter 2025/26: Österreich und die DACH-Region

DACH-Region

- Europa macht **22%** der weltweiten Opfer aus
- **>2.100 Ransomware-Opfer** auf Leak-Seiten seit Januar 2024
- **Deutschland** als **primäres Ziel** für Ransomware im Finanzsektor
- **Österreichische Institute erben signifikante Risiken** durch geteilte Service-Provider und die hohe Integration mit der DACH-Region

Österreich

- **32** gemeldete **Ransomware-Angriffe** im September 2025 markierte einen negativen Höhepunkt.
- Fast **80%** der Angriffe sind **Hands-on-Keyboard**
- **28%** der Angriffe stammen von **staatlichen Akteuren**
- **Tausende Vishing-Anrufe** und Impersonation-Versuche zielen direkt auf Mitarbeiter und Kunden ab.

Highlights der GTL Winter 2025/26: Angreifer werden schneller und raffinierter

- Der Bericht zeigt eine **signifikante Beschleunigung** der Angriffszyklen.
- Besonders die Zeitspanne zwischen Bekanntgabe einer Schwachstelle und deren aktiver Ausnutzung verkürzt sich drastisch.

Metrik	2024	2025	Veränderung
Ransomware deployment time	~48 Stunden	24 Stunden	-48% (schneller)
Time to identify breach	181 Tage	181 Tage	Stabil
Full breach lifecycle	258 Tage	241 Tage	-17 Tage (schneller)
KEVs* (am/vor CVE-Datum)	23,60%	32,10%	+8,5% (schneller)
Kompromittierte Zugangsdaten	Baseline	42%	Stark ansteigend

*KEVs = Known Exploited Vulnerabilities (Bekannte ausgenutzte Schwachstellen)

Angriffsfläche

- **VPN-Schwachstellen** bleiben ein kritischer Einstiegspunkt.
- **Firewall-Exploits** ermöglichten den Durchbruch des Perimeters.
- **Öffentlich zugängliche Anwendungen** (26% der Fälle).

Geschwindigkeit

- Durchschnittliche Zeit bis zum Exploit: **4** Tage in 2025 (von 5,4 Tagen in 2024).
- **32,1% der KEVs wurden am oder vor dem Datum der CVE-Veröffentlichung ausgenutzt.**
- Trend geht aufgrund von Automatisierung und KI in Richtung **Stunden oder Tage** nach der Bekanntgabe.

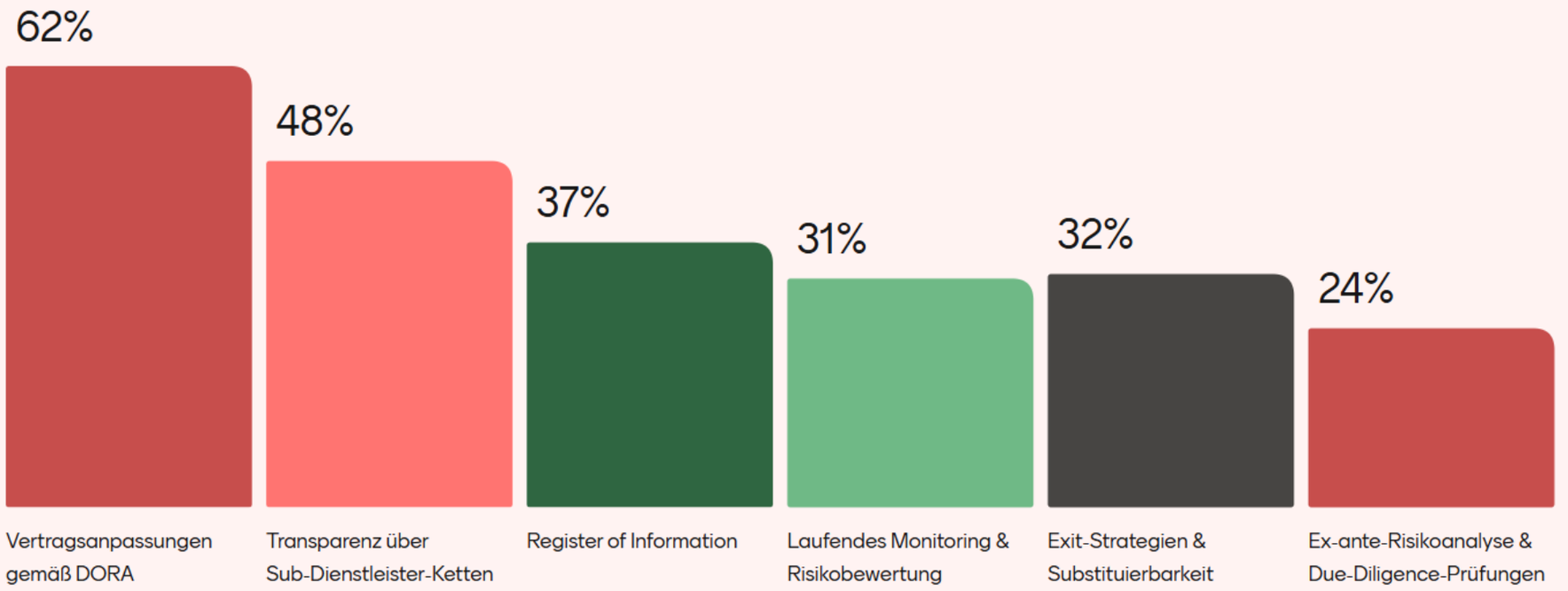
Volumen

- Gesamtjahr 2025: **48,185 CVEs**
- **432 CVEs** mit erstmaliger Ausnutzung in 2025.
- **331 Zero-Days** im Jahr 2024 identifiziert, davon wurden 30% aktiv ausgenutzt.

IKT-Drittparteienrisikomanagement

UMFRAGE

Wo liegt aktuell der größte Aufwand im IKT-Drittparteienrisikomanagement?

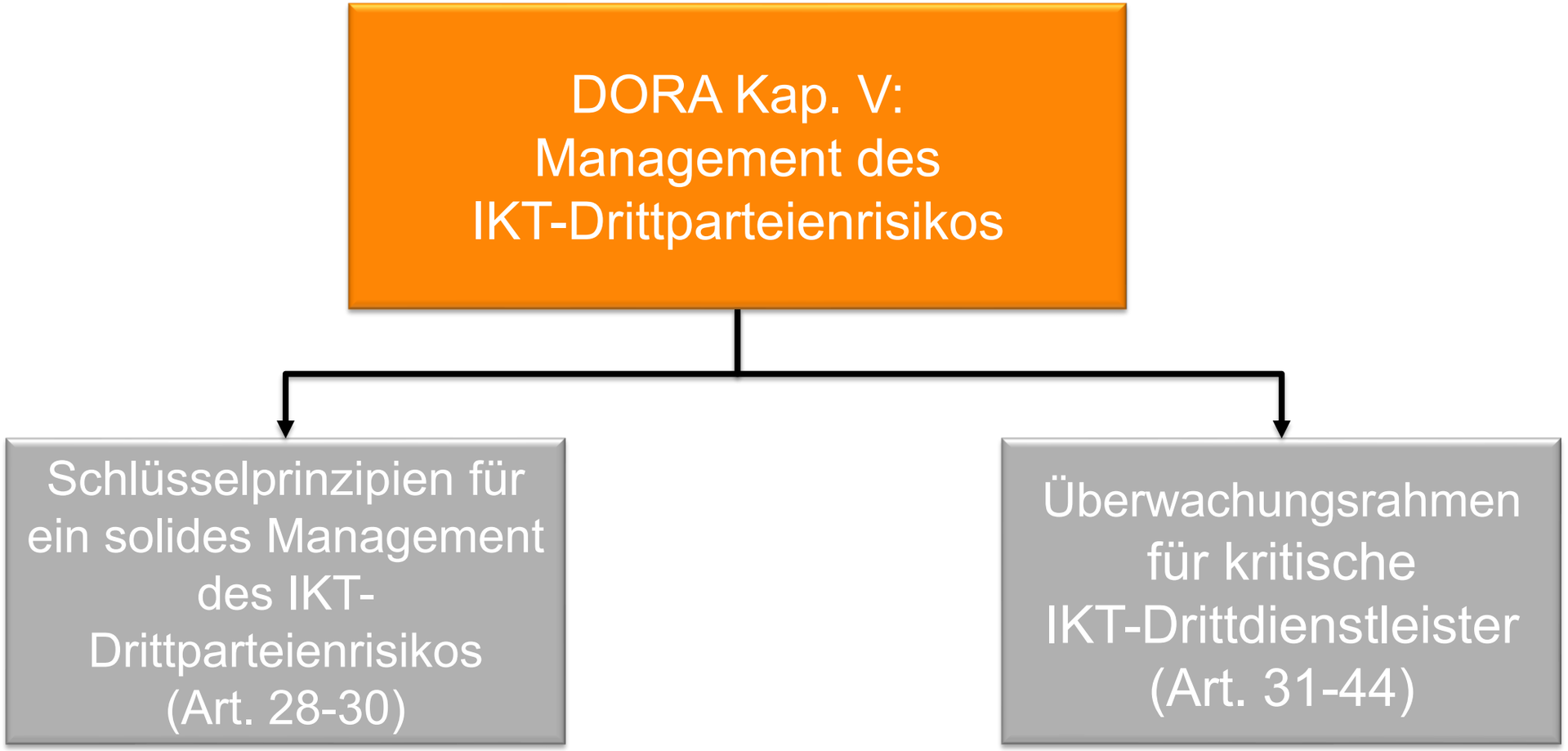


menti.com

8215 2818

156 of **169** responded

IKT-DRITTPARTEIENRISIKOMANAGEMENT

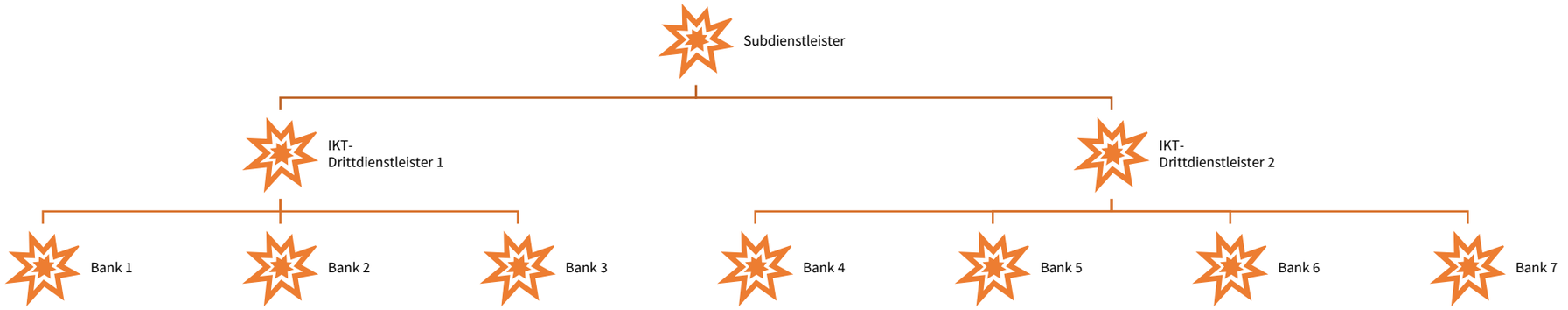


https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554#cpt_V

IKT-DRITTPARTEIENRISIKOMANAGEMENT

- **Verantwortung bleibt beim Institut:** Die Verantwortung für ausgelagerte IT-Services kann nicht übertragen werden – auch bei Nutzung von Drittanbietern bleibt das Institut haftbar.
- **Systemausfälle und Cyberangriffe:** Rund zwei Drittel der Vorfälle entstehen durch Drittanbieter und können zahlreiche Institute gleichzeitig betreffen.
- **Konzentrationsrisiken:** Gerade im österreichischen Finanzsystem mit vielen kleinen Instituten werden kritische Prozesse häufig ausgelagert, was das Risiko erhöht.
- **Effektive Aufsicht:** Nur durch gutes Management und Transparenz können Risiken frühzeitig erkannt und gezielt überwacht werden.

Ein Fehler bei einem (Sub-)Dienstleister kann die Sicherheit zahlreicher Institute gefährden – daher sind ein professionelles Management sowie eine gründliche Überwachung entscheidend, um Stabilität und Schutz zu gewährleisten.



Mehr Informationen:
https://www.fma.gv.at/querschnittsthemen/dora/dora-management-ikt-drittparteienrisiko/

IKT-DRITTPARTEIENRISIKOMANAGEMENT

- August 2025
- Ein Subdienstleister in 4. Ebene gehackt.
- Potentiell hunderte (IT-)Unternehmen verloren Salesforce Daten.
- Diese Daten beinhalten teilweise Zugangs- und Konfigurationdaten aus Supporttickets von z.B. österreichischen Finanzunternehmen.
- Wurde an FMA gemeldet.

Details z.B. unter
https://www.driftbreach.com/

KONKRETE HERAUSFORDERUNGEN IM 1. JAHR DORA

IKT-Drittparteienmanagement

Verträge

- Mindestvertrags-anforderungen der DORA waren in Altverträgen nicht abgebildet.
- Manche Dienstleister wollten/konnten die DORA Anforderungen nicht erfüllen.
- Für Subdienstleister(-ketten) noch komplexer

Überprüfungen

- Fragebögen mit teilweise mehr als 700 Fragen an Drittdienstleister kosten viel Zeit und Geld.
- Vor-OrtAudits erzeugen noch höhere Kosten.
- Die Bewertung von Zertifizierungen wie ISO27000, ISAE3402, SOC etc. ist oft komplex.

Bei Problemen?

- IKT-Drittdienstleister sind oft sehr schwer ersetzbar z.B. Bankenkernsysteme, Cloudanbieter
- Jahr(zehnt)elange Praktiken werden oft nur mit großem Widerstand geändert.
- FMA/OeNB Prüfungen und Interventionen wirken als massiver Beschleuniger.

DORA bewirkt eine notwendige Kulturänderung der gesamten IKT-Branche, die der mittlerweile sehr hohen Abhängigkeit gerecht wird.

Dieser Prozess wird sich noch fortsetzen, denn z.B. KI schafft neue Risiken.

EIN STRATEGISCHES INSTRUMENT: DAS REGISTER OF INFORMATION

Achtung: ROI-Abgabe bis 13.3.2026

Unsere Datenbasis für das IKT-Drittparteienmanagement

- **2025 erstmalig in allen DORA-Staaten erhoben**: Erstmalig wurde Transparenz bezüglich der globalen Abhängigkeiten zwischen Finanz- und IKT-Sektor geschaffen.
- Das „Register of Information“ zeigt,
  - welche IKT-Drittanbieter für
  - welche Funktionen in
  - welchem Umfang genutzt werden.
- **Es ist die einzige flächendeckend verfügbare Datenbasis für DORA.**
- Vor allem bei Cyberangriffen enorm wichtig, um Auswirkungen zu bemessen.

Überwachungsrahmen für kritische IKT-Drittdienstleister

ZWECK & ZIELSETZUNG

ZWECK

- Der Überwachungsrahmen dient der administrativen Steuerung und Durchführung von Überwachungsaktivitäten gegenüber kritischen Drittanbietern (CTPPs), die IKT-Dienstleistungen für Finanzunternehmen in der EU erbringen.

ZIELSETZUNG

- Die wirksame Aufsicht über kritische IKT-Drittanbieter, um Risiken frühzeitig zu erkennen und die Stabilität der von ihnen erbrachten Dienste für EU-Finanzunternehmen zu sichern.

WELCHE IKT-DIENSTLEISTER SIND ALS ‚KRITISCH' DESIGNIERT?

19 kritische IKT-Drittdienstleister

- Accenture plc
- Amazon web Services EMEA Sarl
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited

18.11.2025

Überwachungsaktivitäten

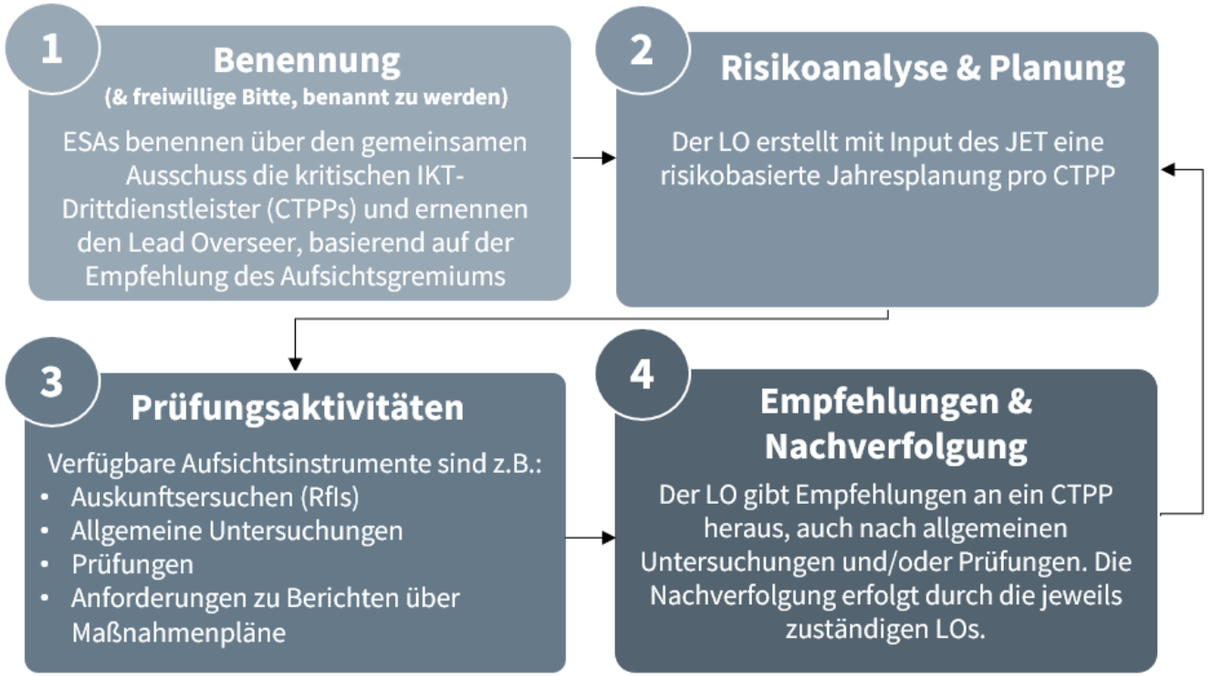


Figure 4: DORA oversight activities „Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

WIE ERFOLGT DIE BESTIMMUNG ALS ‚KRITISCH'?*

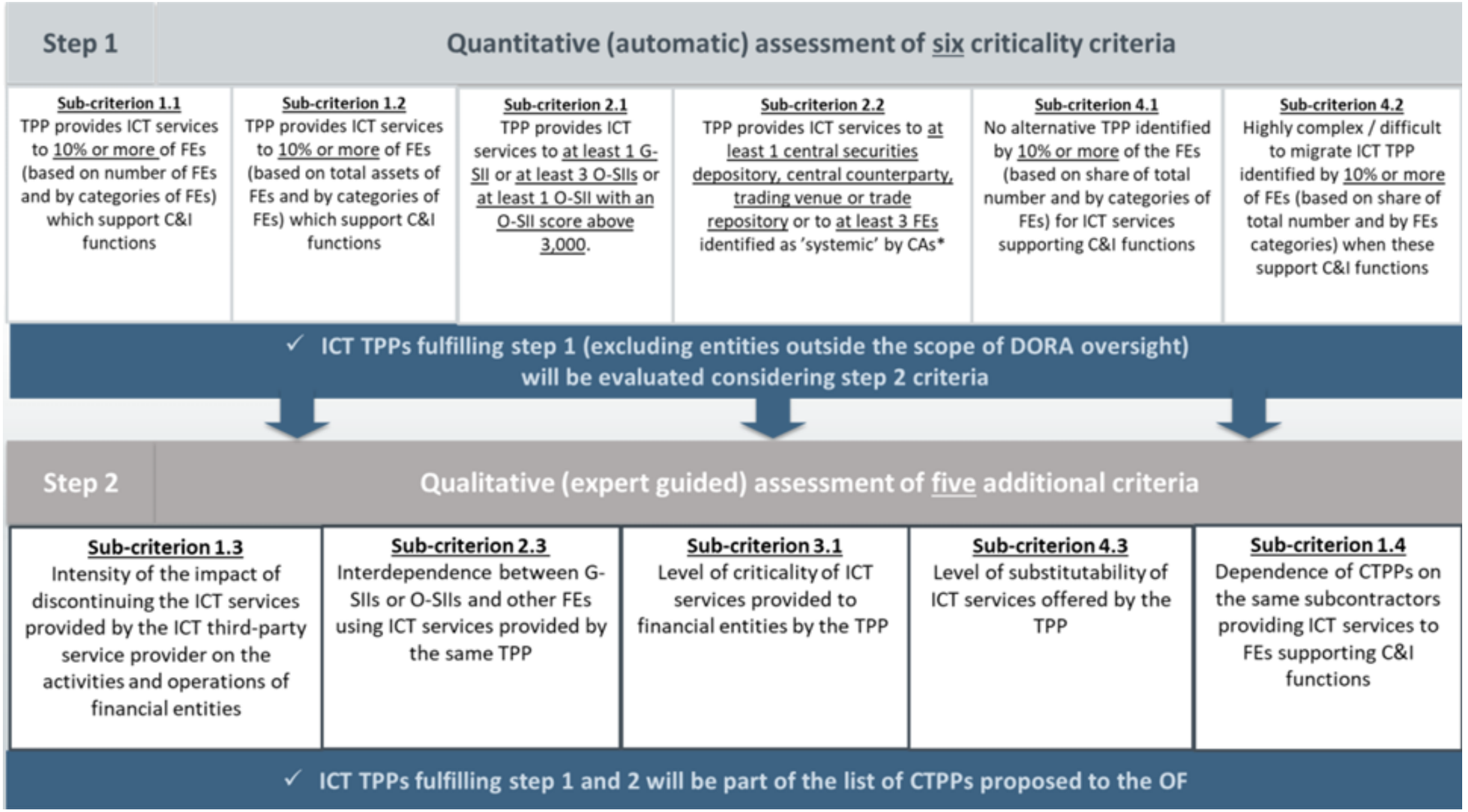
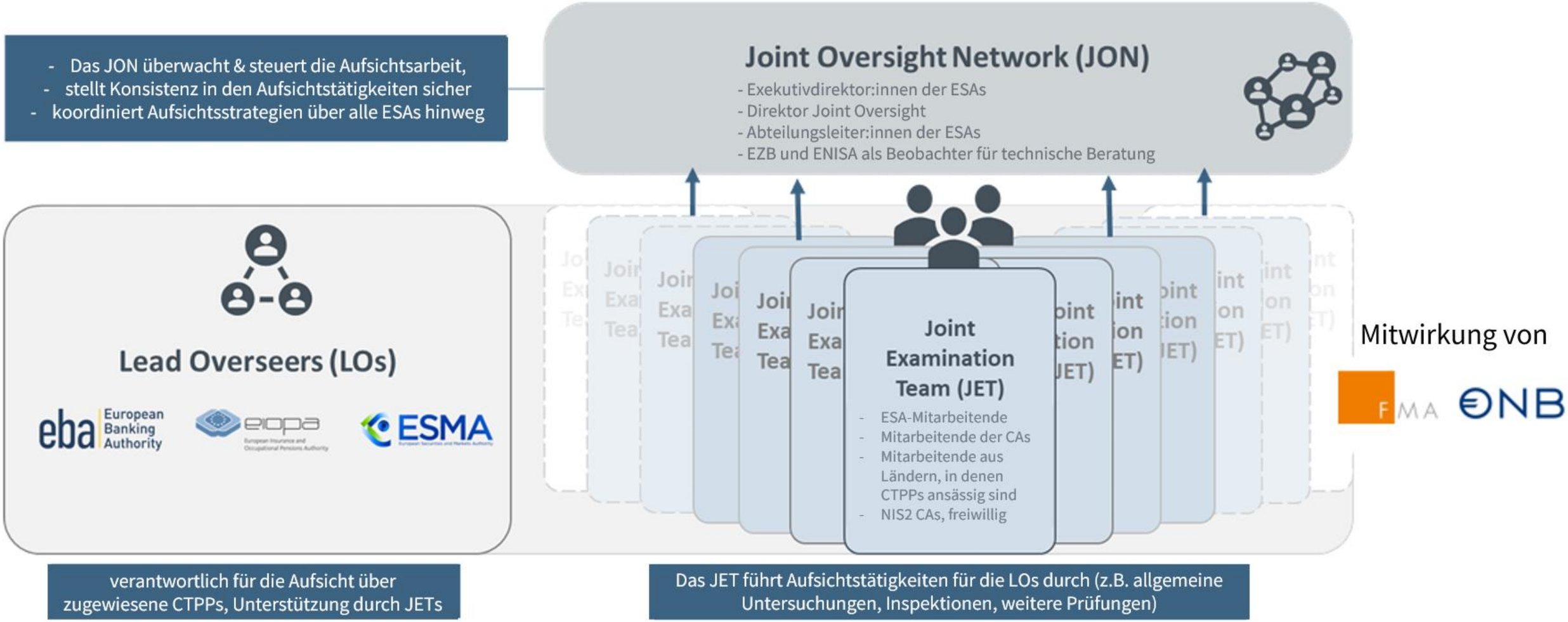


Figure 5: Criticality assessment criteria „Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

*** siehe DelVO (EU) 2024/1502**

WIE WIRKEN FMA & OENB IM ÜBERWACHUNGSRAHMEN MIT?



Mitwirkung von FMA OENB

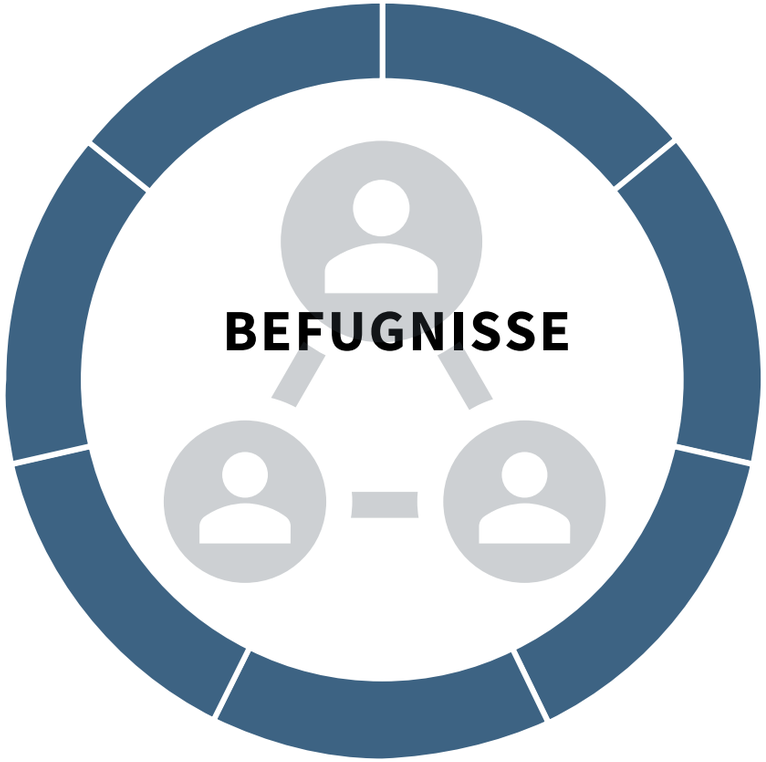
Ausschnitt aus: Figure 2: DORA oversight roles and functions , Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

BEFUGNISSE DER FEDERFÜHRENDEN ÜBERWACHUNGSBEHÖRDE

AUSKUNFTSERSUCHEN
(VERLANGEN DURCH BESCHLUSS)

AUSKUNFTSERSUCHEN
(EINFACHES ERSUCHEN)

OVERSIGHT-AKTIVITÄTEN
AUSSERHALB DER EU



ALLGEMEINE UNTERSUCHUNGEN

PRÜFUNGEN
ON-SITE / OFF-SITE

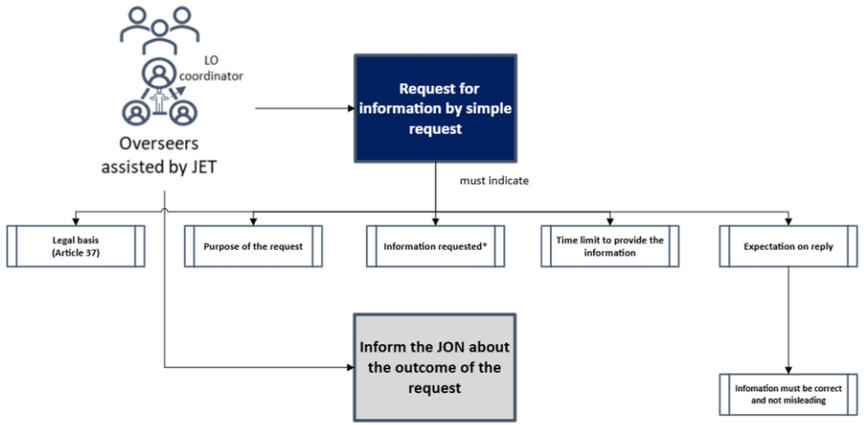
EMPFEHLUNGEN
ERTEILUNG & FOLLOW-UP

AUSKUNFTSERSUCHEN

Einfaches Ersuchen

Freiwillige Beantwortung, aber nicht falsch/irreführend

- Rechtsgrundlage, Zweck, Informationen, Frist
- JON & OF müssen konsultiert werden
- Ergebnis wird an JON berichtet

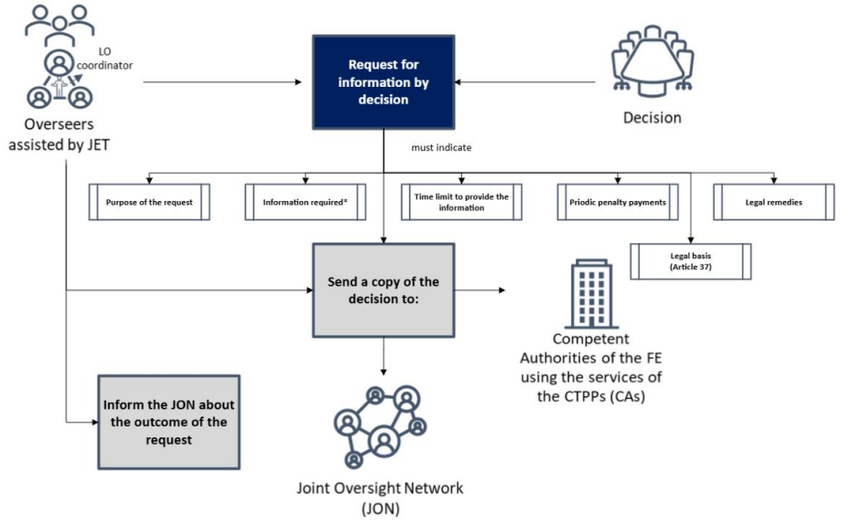


Ausschnitt aus: Figure 10: DORA oversight roles and functions , Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

Verlangen durch Beschluss

Verpflichtende Auskunft, mit Rechtsfolge & möglichen Sanktionen

- Beschluss durch Board of Supervisors
- Rechtsgrundlage, Zweck, Infos, Frist, Hinweis auf Rechtsmittel
- JON und CAs werden informiert
- CTPP haftet bei unvollständigen oder falschen Angaben



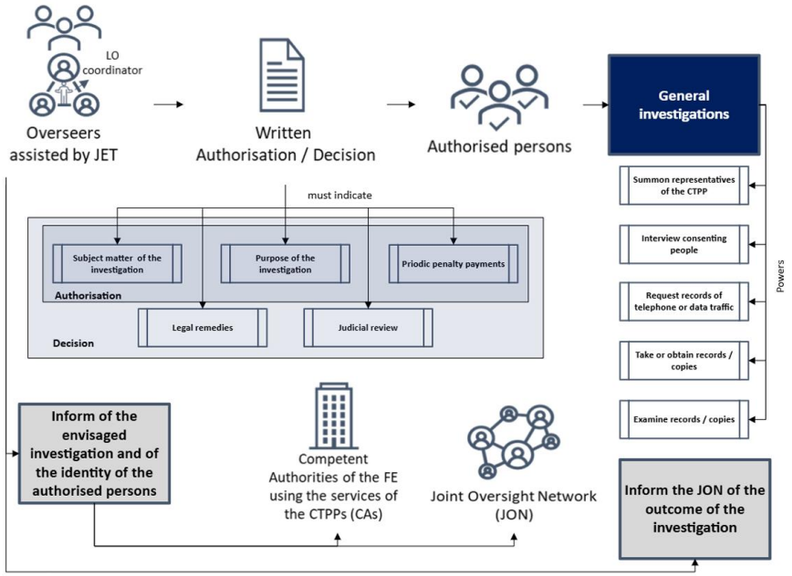
Ausschnitt aus: Figure 11: DORA oversight roles and functions , Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

ALLGEMEINE UNTERSUCHUNG & PRÜFUNGEN

Allgemeine Untersuchungen

Zugriff auf alle Aufzeichnungen, Daten, Verfahren

- Möglichkeit zu Interviews, Kopien, Traffic-Daten
- Enthält Zweck, Umfang, Befugnisse und potentielle Zwangsgelder
- Information jener zuständigen Behörden, deren Finanzunternehmen diese kritischen IKT-Drittdienstleister nutzen
- Abschluss: Empfehlungen innerhalb von 3 Monaten

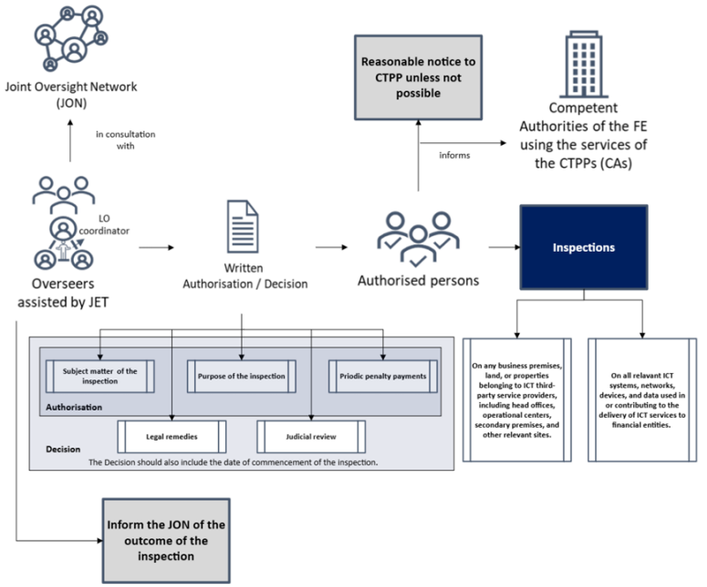


Ausschnitt aus: Figure 12: DORA oversight roles and functions , Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

Prüfungen

On-site oder off-site Untersuchungen

- Zugriff auf Räumlichkeiten, Systeme, Netzwerke, Daten
- Befugnis zu Betreten, Dokumentensichtung, …
- Vorab-Ankündigung, außer bei Vorliegen eines Krisenfalls
- Non-Compliance kann zu Meldung an zuständige Behörde führen
- Abschluss: Empfehlungen innerhalb von 3 Monaten



Ausschnitt aus: Figure 13: DORA oversight roles and functions , Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

EMPFEHLUNGEN – ERTEILUNG & FOLLOW-UP

Entstehen v.a. nach allgemeinen Untersuchungen oder Prüfungen

- Kritischer IKT-Drittdienstleister hat **30 Tage Zeit** für die Stellungnahme
- Nach Erhalt: **60 Tage für Mitteilung**, ob und wie die Empfehlung befolgt wird
- Möglichkeit von:
  - Follow-up-Berichten / Fortschrittsreports
  - Bewertung der Umsetzung durch Overseers

- Bei Nicht-Umsetzung: öffentliche Bekanntmachung oder Hinweise an zuständige Behörde

WORAUF WERDEN FINANZUNTERNEHMEN HINGEWIESEN? WELCHE INFORMATIONEN ERHALTEN SIE?

Verantwortung Unternehmen

- **Erwägungsgrund 92 DORA-VO:**
  - Finanzunternehmen müssen Risiken iZm der Nutzung von IKT-Drittdienstleistern selbst managen.
  - Die volle Verantwortung der Finanzunternehmen für die Einhaltung und Erfüllung aller DORA-Verpflichtungen bleibt unberührt.

- **Art 42 (3) DORA-VO:**
  - Die zuständigen Behörden unterrichten die betreffenden Finanzunternehmen über die Risiken, die in den Empfehlungen an kritische IKT-Drittdienstleister festgestellt worden sind.

  Beispiele
  - Aufforderungen, ihr eigenes IKT-Risikomanagement anzupassen
  - Hinweise darauf, welche Maßnahmen der CTPP setzt und welche Risiken bestehen bleiben

- **Gesamthafte Effekte:**
  - Förderung der Effizienz & Konvergenz des IKT-Risikomanagements, wodurch die digitale operationale Resilienz von Finanzunternehmen gestärkt wird.

Konsequenzen

- Vgl. Art 42 (6) DORA-VO
  - Als **letztes Mittel** dürfen Behörden verlangen, dass Finanzunternehmen die Nutzung kritischer IKT-Dienste vorübergehend (teilweise oder vollständig) aussetzen oder Verträge kündigen, bis die in den Empfehlungen festgestellten Risiken beim kritischen IKT-Drittdienstleister beseitigt sind.

OVERSIGHT-AKTIVITÄTEN AUSSERHALB DER EU

Hintergrund

Wenn die **Überwachungsziele nicht über das EU-Tochterunternehmen oder EU-Standorte erreicht werden können**, **darf die federführende Aufsichtsbehörde auch Drittland-Standorte des kritischen IKT-Drittdienstleisters prüfen** und dort die Befugnisse nach Art. 35(1)(a) und (b) (i.V.m. Art. 38(2)(a),(b),(d) und Art. 39(1),(2)(a)) ausüben.

Art. 31 (12) DORA-VO: Finanzunternehmen dürfen nur dann die Dienstleistungen eines IKT-Drittdienstleisters mit Sitz in einem Drittland in Anspruch nehmen, wenn er innerhalb von **zwölf Monaten** nach der Einstufung ein Tochterunternehmen in der Union gegründet hat.

Voraussetzungen

- Tätigkeit muss notwendig sein, um die Aufsicht sicherzustellen
- Direkter EU-Bezug: Die Räumlichkeiten werden zur Erbringung von Diensten an EU-FU genutzt
- CTPP muss zustimmen
- Drittstaat-Behörde darf nicht widersprechen
- ESAs müssen Kooperationsvereinbarungen mit Drittstaat-Behörden schließen

IKT- und Cyberrisikoprüfungen

BESONDERE HERAUSFORDERUNGEN BEI DER IMPLEMENTIERUNG IM LSI-BEREICH

- Anpassung von SLAs und Definition von KPIs
- Abbildung der Funktionstrennung und Einhaltung des „Least-Privilege-Prinzips“
- Trennung und Segmentierung von IKT-Systemen und –Netzwerken
- Dokumentationen bei historisch gewachsenen Systemen
- Umgang mit geteilten Assets bei Service Providern

- Beseitigung von Sicherheitslücken im Code von Altsystemen
- IKT-Revisionen bei Service Providern
- SIEM/SOC Implementierung ermitteln
- Sicherheitsvorgaben vs. gelebte Praxis
- Fehlende Toolunterstützung im IKT-Betrieb und der Softwareentwicklung

BEOBACHTUNGEN AUS SI-PRÜFUNGEN

EUROPEAN CENTRAL BANK
BANKING SUPERVISION

FMA OeNB

- Rollen- und Ressourcenkonflikte in den Three Lines of Defence
- Mängel der Datenqualität / Vollständigkeit im Asset Management
- Steuerung von Drittdienstleistern
- Mangelhaftes Management von IDV-(EUC-) Lösungen

- Berechtigungsmanagement: Least-privilege / Need-to-know-Prinzip
- Privileged Account Management Toxic rights combinations
- SIEM/SOC Implementierung ermitteln
- Sicherheitsvorgaben vs. gelebte Praxis

REGELMÄßIGE ÜBERPRÜFUNG DES IT-INTERNEN KONTROLLSYSTEMS (IT IKS)

- Vollständigkeit des IT IKS
  - Sind alle Kontrollen, die sich aus internen Leitlinien ergeben, implementiert?
  - Sind alle Kontrollen, die implementiert sind, dokumentiert und im IT IKS erfasst?
- Regelmäßige Überprüfungen des IT IKS
  - Design Effectiveness
  - Control Effectiveness
- Berücksichtigung der Ergebnisse aus den Überprüfungen im IKT-Risikomanagement.
- Berücksichtigung von Ergebnissen anderer Überprüfungen (z.B. Pen Tests, Security Audits) bei der Bewertung von Kontrollen und im IKT-Risikomanagement.

RISIKOORIENTIERTE TESTPLÄNE

- Testpläne wie zum Beispiel für Penetration Tests, BCM und Notfallübungen und Wiederherstellungstest sollen risikoorientiert erstellt werden.
- Die Ableitung von Testthemen, Scope und Häufigkeit muss basierend auf den Ergebnissen des IKT-Risikomanagementprozesses erfolgen und nachvollziehbar dokumentiert werden.
  - Einsatz von Ressourcen soll zielgerichtet erfolgen.
- Testpläne müssen in ein übergeordnetes Programm eingebunden sein und aufeinander abgestimmt sein.

SCHWACHSTELLENSCANS

- *Artikel 10 Abs. 2 (EU) 2024/1774 - Die in Absatz 1 genannten Verfahren für das Schwachstellen-Management sorgen dafür, dass die Durchführung automatisierter Schwachstellenbewertungen und -scans bei IKT-Assets gewährleistet und dabei sichergestellt wird, dass deren Häufigkeit und Umfang der im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung und dem Gesamtrisikoprofil des IKT-Assets entsprechen,*
- *Für die Zwecke von Buchstabe b führen die Finanzunternehmen die automatisierten Schwachstellenbewertungen und -scans für IKT-Assets bei IKT-Assets, die kritische oder wichtige Funktionen unterstützen, mindestens einmal wöchentlich durch.*

- Schwachstellenscans die nicht authentifiziert durchgeführt werden, haben eine stark eingeschränkte Aussagekraft. Insbesondere Assets die kritische und wichtige Funktionen unterstützen müssen authentifiziert gescannt werden.

IKT-Risikomanagement & Governance

- Fehlende oder unvollständige DORA Verweise in Richtlinien und Handbüchern
- Fehlende Angaben bzgl. der Bewertung einzelner Risiken und der Erfassung der IKT-DL
- Unvollständige Richtlinie für das Management von IKT-Assets
- IT Schulungskonzepte nicht differenziert genug, insbesondere für IT Mitarbeiter:innen

Management von IKT-Assets

- Unklare Definitionen bzgl. der Nutzung von IKT-Assets (zB private oder externe Geräte)
- Unvollständige Erfassung im IKT Asset Register
  - Peripheriegeräte werden nicht systematisch erfasst
  - Inventar enthält veraltete Datenbestände
  - Wesentliche Unternehmens Assets fehlen im Register

Management des IKT-Drittparteienrisikos

Vertragsgestaltung

- DORA relevante Verträge nicht oder verspätet aktualisiert
- Drittanbieter Verträge nur teilweise geprüft
- Unklare Formulierungen in DORA spezifischen Fragestellungen

Due Diligence & lfd. Monitoring von Risiken

- Aktualisierung der Dashboards zur IKT-Risikobewertung in Bezug auf KPI nicht genau definiert
- Risikoreports enthalten keine Angaben zu niedrigen Risiken oder deren Entwicklung
- Exit Strategien zu IKT-Dienstleistern unvollständig oder ohne Zeitplanung
- Physische Zutrittsregelungen unklar geregelt, bzw. fehlende Aufzeichnungen

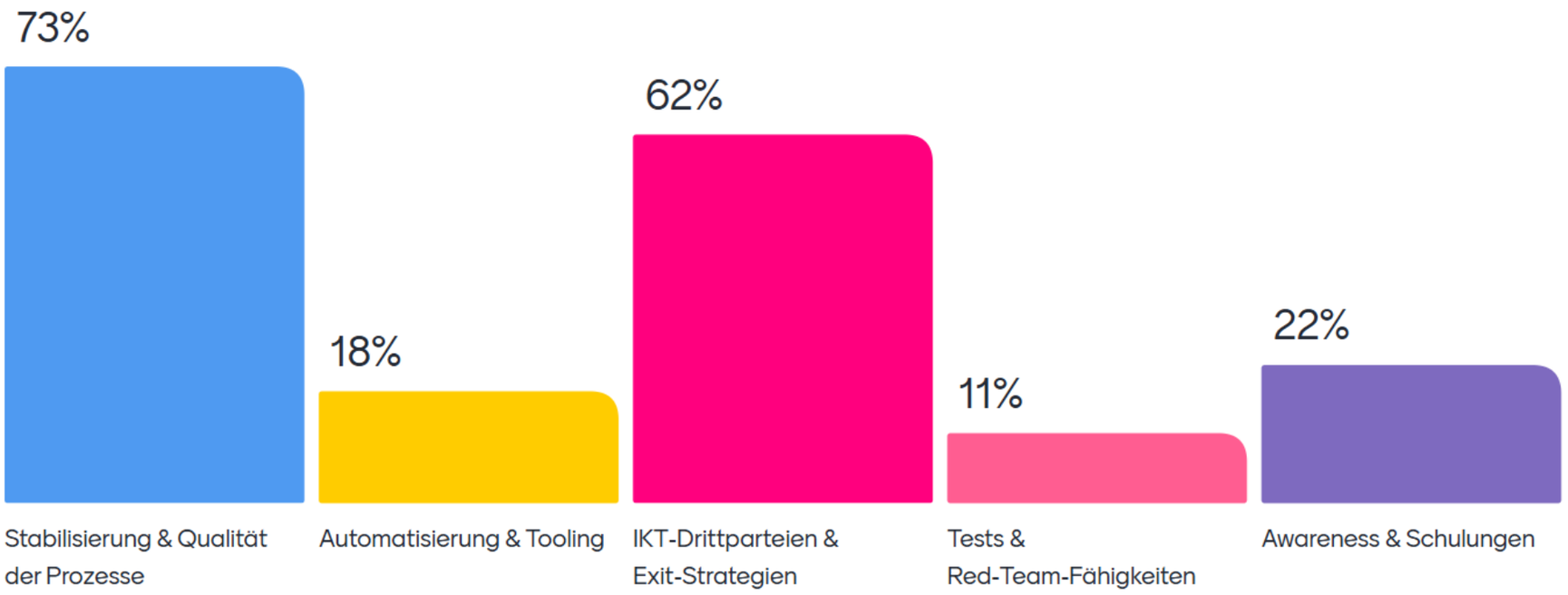
FALSCHE BEURTEILUNG, OB EINE FUNKTION KRITISCH ODER WICHTIG IST

- **Unternehmen sind angehalten ihre kritischen oder wichtigen Funktionen zu erfassen.**
- **Art. 3 Z 22 DORA:**
  „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die **finanzielle Leistungsfähigkeit** eines Finanzunternehmens oder die **Solidität** oder **Fortführung** seiner **Geschäftstätigkeiten** und **Dienstleistungen** erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung **die fortdauernde Einhaltung der Zulassungsbedingungen** und -**verpflichtungen** eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde;

- Die Einstufung der Kritikalität erfolgt nicht nach den gesetzten Maßnahmen, die die Ausfallswahrscheinlichkeit der Funktionen reduziert.
- D.h.: Auch wenn Vorkehrungen getroffen wurden, die einen Ausfall einer kritischen oder wichtigen Funktion nahezu verhindern, bleibt es trotzdem eine wichtige oder kritische Funktion!

UMFRAGE

Was ist Ihre wichtigste DORA-Priorität für 2026?



menti.com
5840 7062

112 of 120 responded

Ausblick

DIALOGUNTERLAGEN

Startseite > Querschnittsthemen > DORA – Digitale operationale Resilienz im Finanzsektor

DORA – Digitale operationale Resilienz im Finanzsektor

FMA-Aktivitäten

Die FMA wirkt in verschiedenen Gremien an der Rechtsweiterentwicklung und an Abstimmungen zur aufsichtlichen Konvergenz mit und unterstützt auch beaufsichtigte Unternehmen bei der DORA-Implementierung.

Einforderung Informationsregister 2026

FMA-OeNB-DORA-Dialog: Informationsregister und aktuelle Hinweise 23.10.2025

Veröffentlichung der Dialogunterlagen auf der FMA-DORA-Website

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz

OESTERREICHISCHE NATIONALBANK

EUROSYSTEM