ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

FMA/OENB-DORA-DIALOG
IT-PROVIDER IM FOKUS

Online, 18. November 2026

UMFRAGE 1 - JETZT ABSTIMMEN UNTER…

menti.com

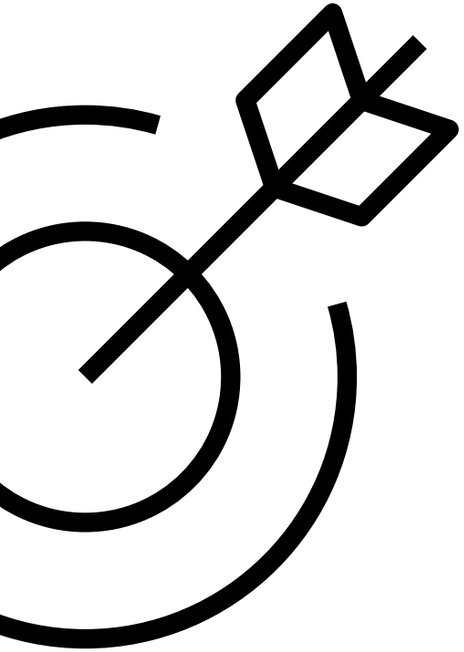
8145 6972



AGENDA



- Begrüßung & Umfrage
  FMA: Michael Hysek / OenB: Gabriela de Raaij
- Verhältnis IKT-Drittdienstleister und Aufsicht
  FMA: Anna Muri
- Zusammenspiel mit NIS2, Lead Overseer und Aufsicht
  FMA: Anna Muri
- DORA-Inhalte und Fokusthemen für IKT-Drittdienstleister
  FMA: Anna Muri, Laura Strobl, Norbert Fröhlich, Alexander Mitter, OeNB: Alexander Natter
- Erfahrungen aus der direkten Prüfung von IKT-Drittdienstleistern nach DORA
  OeNB: Gernot Burgsteiner
- Q&A und Abschluss
  FMA: Anna Muri



Verhältnis IKT-Drittdienstleister und Aufsicht

VERHÄLTNIS IKT-DRITTDIENSTLEISTER UND AUFSICHT

„einfache“ IKT-Drittdienstleister

(Art 3 Z 19 DORA)

- „*ein Unternehmen, das IKT-Dienstleistungen bereitstellt*“
- Keine **direkte** Aufsicht über IKT-Drittdienstleister
- Aber: Das Wort „IKT-Drittdienstleister“ kommt in DORA **328** Mal vor
- **Ohne Kooperation der IKT-Drittdienstleister ist keine DORA-Compliance durch Finanzunternehmen möglich**

kritische IKT-Drittdienstleister

(Art 3 Z 23 DORA)

- ein IKT-Drittdienstleister, der gemäß Artikel 31 DORA als kritisch eingestuft wurde;

„IKT-Dienstleistungen“: digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste;

VERHÄLTNIS IKT-DRITTDIENSTLEISTER UND AUFSICHT

Einfache IKT-Drittdienstleister

- DORA indirekt anwendbar
- FMA kann Vor-Ort Prüfungen durch OeNB beauftragen
- FMA kann jederzeit Auskunft verlangen

Kritische IKT-Drittdienstleister

- Werden direkt von der sog federführenden Überwachungsbehörde (EBA, EIOPA, ESMA) überwacht
- Direkter Kontakt mit FMA nur, wenn dies zuvor mit der federführenden Überwachungsbehörde abgesprochen ist

§ 70. BWG

1.(1)In ihrem Zuständigkeitsbereich als Bankenaufsichtsbehörde […] kann die FMA unbeschadet der ihr auf Grund anderer Bestimmungen dieses Bundesgesetzes zustehenden Befugnisse jederzeit zur Beaufsichtigung der Kreditinstitute, Kreditinstitute-Verbünde und der Kreditinstitutsgruppen

2. 1.

3. von Kreditinstituten […] **und Dritten, an welche diese Unternehmen betriebliche Funktionen oder Tätigkeiten ausgelagert haben, einschließlich IKT-Drittdienstleistern** […], die Vorlage von Zwischenabschlüssen, von Ausweisen in bestimmter Form und Gliederung und von Prüfungsberichten verlangen, ferner von den Kreditinstituten, […] **und Dritten, an welche diese Unternehmen betriebliche Funktionen oder Tätigkeiten ausgelagert haben, einschließlich IKT-Drittdienstleistern** […] Auskünfte über alle Geschäftsangelegenheiten fordern, in die Bücher, Schriftstücke und Datenträger Einsicht nehmen […].

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

Überwachungsaktivitäten

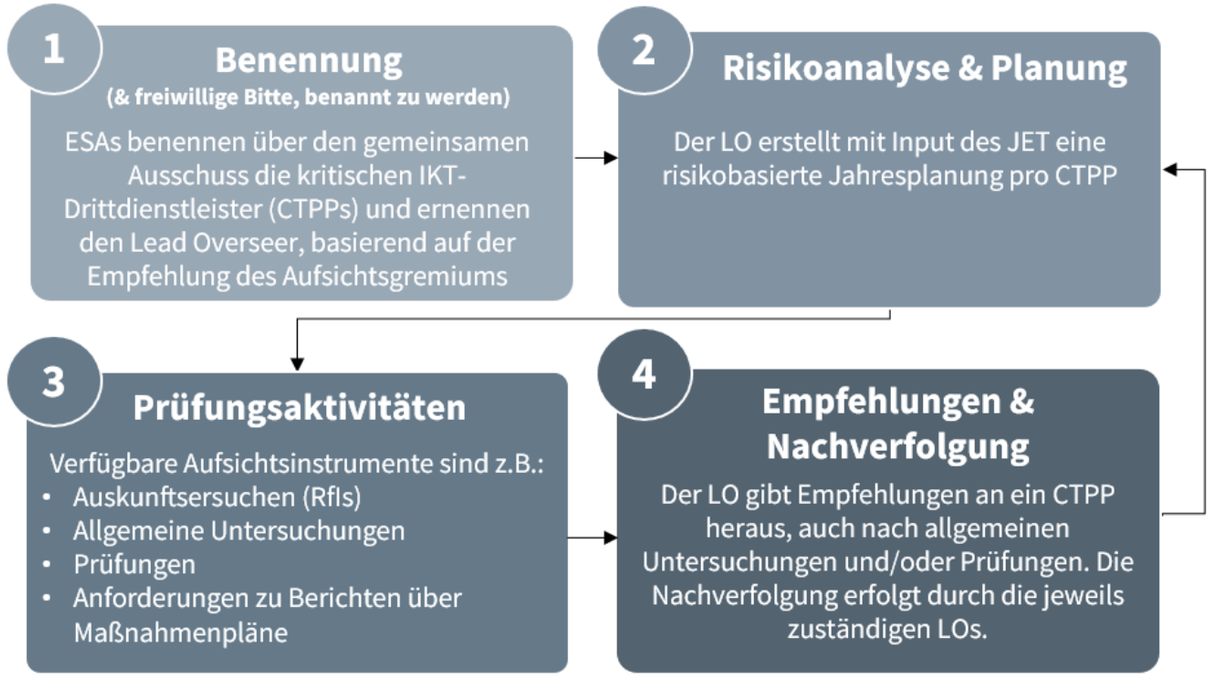


Figure 4: DORA oversight activities „Digital Operational Resilience Act (DORA): Oversight of critical third-party providers: Guide on oversight activities, JC 2025 29

WIE WIRKEN FMA & OENB IM ÜBERWACHUNGSRAHMEN MIT?

- Das JON überwacht & steuert die Aufsichtsarbeit,
- stellt Konsistenz in den Aufsichtstätigkeiten sicher
- koordiniert Aufsichtsstrategien über alle ESAs hinweg

Joint Oversight Network (JON)

- Exekutivdirektor:innen der ESAs
- Direktor Joint Oversight
- Abteilungsleiter:innen der ESAs
- EZB und ENISA als Beobachter für technische Beratung

Lead Overseers (LOs)

eba European Banking Authority

eiopa

ESMA

verantwortlich für die Aufsicht über zugewiesene CTPPs, Unterstützung durch JETs

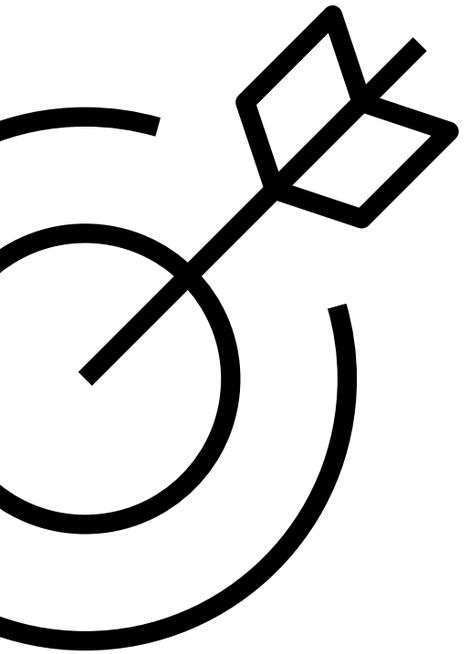
Joint Examination Team (JET)

- ESA-Mitarbeitende
- Mitarbeitende der CAs
- Mitarbeitende aus Ländern, in denen CTPPs ansässig sind
- NIS2 CAs, freiwillig

Das JET führt Aufsichtstätigkeiten für die LOs durch (z.B. allgemeine Untersuchungen, Inspektionen, weitere Prüfungen)

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

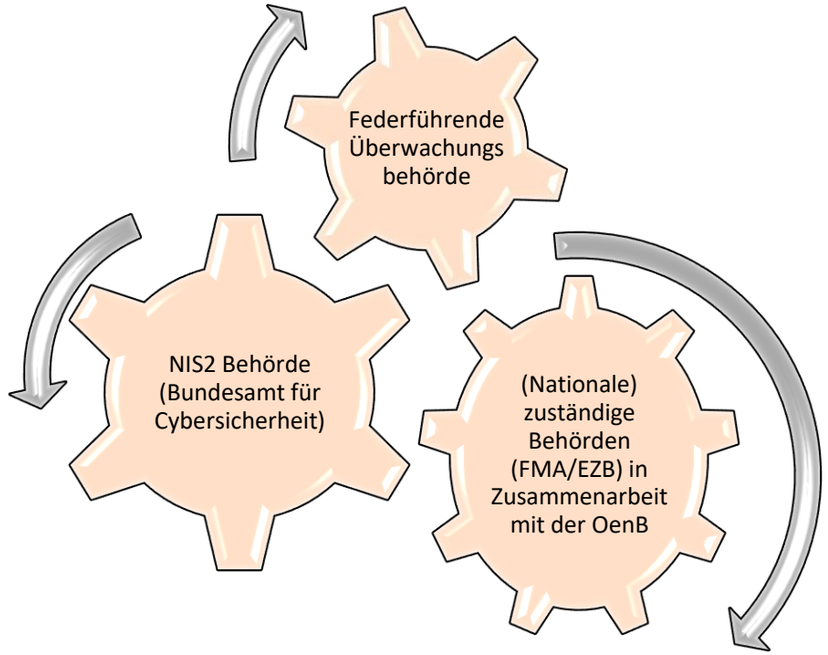


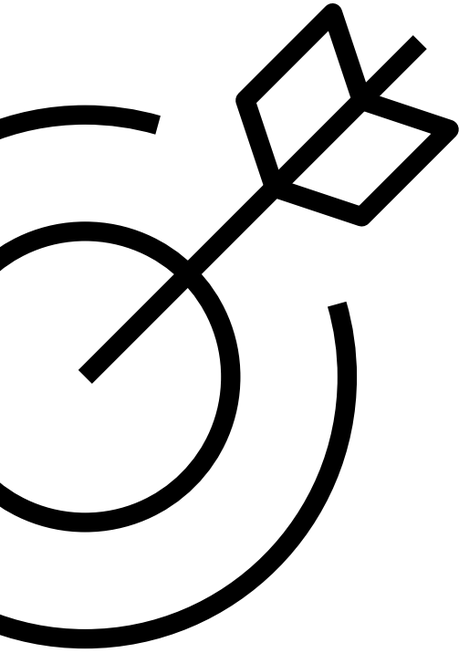
Zusammenarbeit NIS2-Behörde, federführende Überwachungsbehörde und Aufsicht

ZUSAMMENARBEIT NIS2-BEHÖRDE, FEDERFÜHRENDE ÜBERWACHUNGSBEHÖRDE UND AUFSICHT

GRUNDSÄTZE DER ZUSAMMENARBEIT

- Bundesamt für Cybersicherheit = zentrale Anlaufstelle für IKT-Drittdienstleister, die NIS2 unterliegen
- Federführende Überwachungsbehörde = zentrale Anlaufstelle für kritische IKT-Drittdienstleister
- Die zuständigen Behörden = zentrale Anlaufstelle für Finanzunternehmen, die ihrer Aufsicht unterliegen
- Intensiver Informationsaustausch und Zusammenarbeit zwischen der federführenden Überwachungsbehörde, den nationalen Aufsichtsbehörden und den NIS2-Behörden





DORA-Inhalte und Fokusthemen für IKT-Drittdienstleister

ANFORDERUNGEN AN DIE IT-GOVERNANCE UND IT-RISIKOMANAGEMENT

ANFORDERUNGEN AN IKT-GOVERNANCE UND IKT-RISIKOMANAGEMENT

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



ANFORDERUNGEN AN IKT-GOVERNANCE UND IKT-RISIKOMANAGEMENT – RELEVANZ FÜR IKT-DRITTDIENSTLEISTER

Die Einhaltung der Vorgaben muss sich in Verträgen mit IKT-Drittdienstleistern widerspiegeln.

IKT-Systeme, -Protokolle und –Instrumente – Identifizierung und Verzeichnis

(Art 7 und 8 DORA)

- Alle IKT-gestützten Unternehmensfunktionen, Rollen und Zuständigkeiten; IKT-Ressourcen und Rollen und Abhängigkeiten (hinsichtlich ihrer IKT-Risiken) sind zu ermitteln, klassifizieren und dokumentieren Überprüfung der Klassifizierung mindestens einmal jährlich
- Ermittlung aller kritischen IKT-Ressourcen (auch an externen Standorten)
- Ermittlung und Dokumentation aller Prozesse iZm IKT-Drittanbietern

Reaktion und Wiederherstellung - BCM

(Art 11 DORA)

- IKT-Strategie und Pläne zur Fortführung der Geschäftstätigkeit (eigenständiges Konzept im Rahmen der allgemeinen Strategie zur Fortführung der Geschäftstätigkeit); Business Impact-Analyse (BIA)
- IKT-Drittdienstleister sind in BCM; Plänen zu berücksichtigen
- Im Rahmen der Tests der BCM Pläne sind IKT-Drittdienstleister zu berücksichtigen

ANFORDERUNGEN AN IKT-GOVERNANCE UND IKT-RISIKOMANAGEMENT – RELEVANZ FÜR IKT-DRITTDIENSTLEISTER



Die Einhaltung der Vorgaben muss sich in Verträgen mit IKT-Drittdienstleistern widerspiegeln.

Beschaffung, Entwicklung und Wartung von IKT-Systemen

(Art 16 RTS 2024/1774)

- Sicherheitsanforderungen und Governance vertraglich sicherstellen
- Tests, Codeprüfungen und Sicherheitsanalysen ermöglichen
- Integrität des Quellcodes und sicherer Umgang mit Daten gewährleisten

Richtlinien für Personal- und Sicherheitsrichtlinien

(Art 19 RTS 2024/1774)

- Verpflichtung zur Einhaltung der IKT-Sicherheitsvorgaben
- Einbindung in Melde- und Eskalationsprozesse
- Geregelte Beendigung von Zugriffsrechten und Rückgabe von Assets

BEHANDLUNG, KLASSIFIZIERUNG UND BERICHTERSTATTUNG IKT-BEZOGENER VORFÄLLE

WAS IST DIE MELDEVERPFLICHTUNG SCHWERWIEGENDER IKT-BEZOGENER VORFÄLLE?

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

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

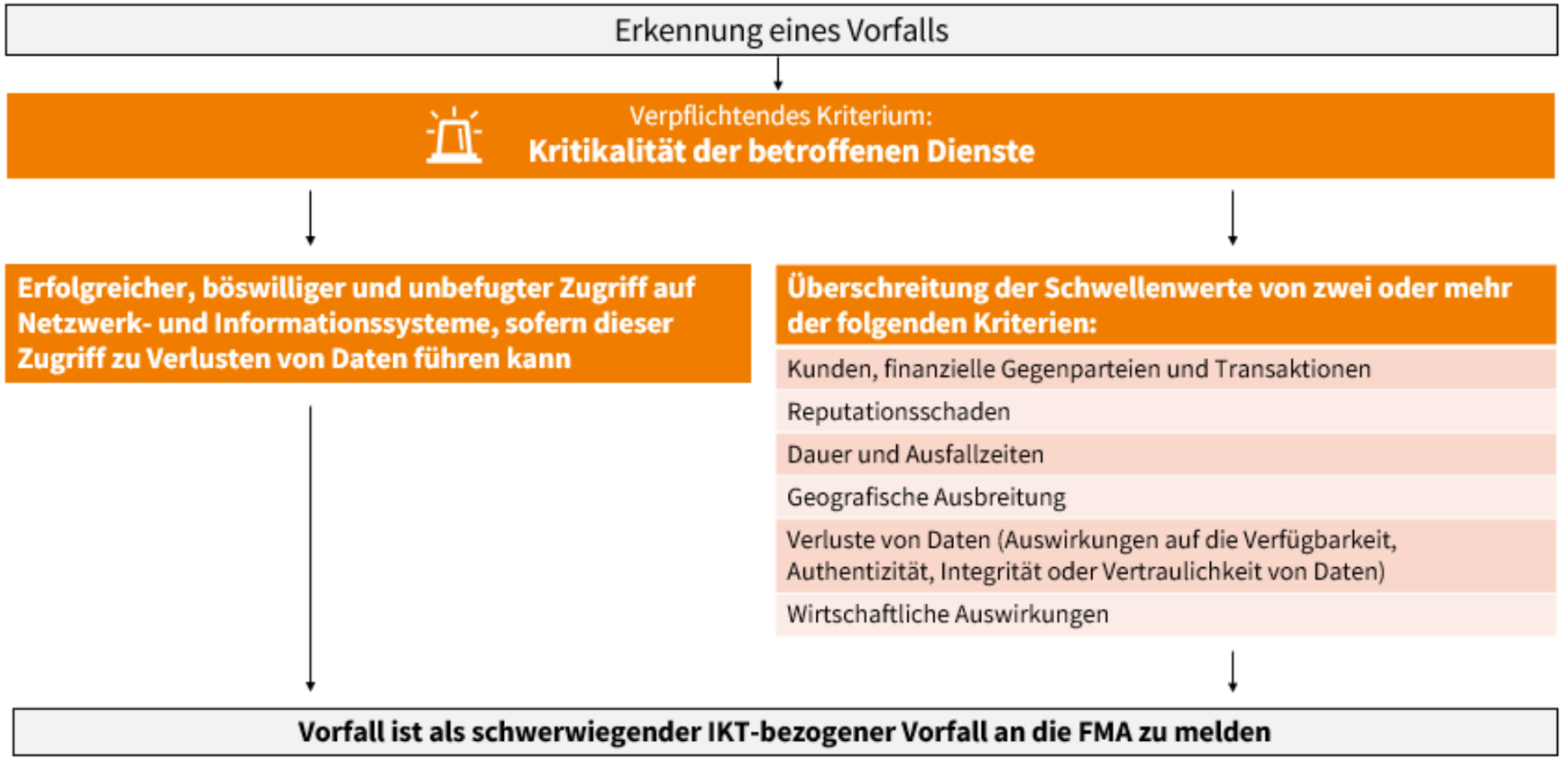
Freiwillige Meldung erheblicher Cyberbedrohungen

(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

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
  - Automatische Plausibilisierung beim Upload
  - 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

- Auf der FMA Homepage zum Thema IKT-bezogene Vorfälle finden Sie unter “Fragen und Antworten“ Meldehinweise
- **Weiter zu aktuellen Auswertungen!**

SCHWERWIEGENDE IKT-BEZOGENE VORFÄLLE

Anzahl der an die FMA gemeldeten Vorfälle
Jahr 2025 und Jahr 2026

Erstmeldungen (alle Sektoren)	2025	**2026**	Q1 2026	Q2 2026	Q3 2026	Q4 2026
Anzahl gemeldete Vorfälle	128	**116**	**31**	**49**	**35**	**79**
davon als nicht schwerwiegend reklassifiziert	25	15	5	4	6	8
Gesamt	103	**171**	**26**	**45**	**29**	**71**

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

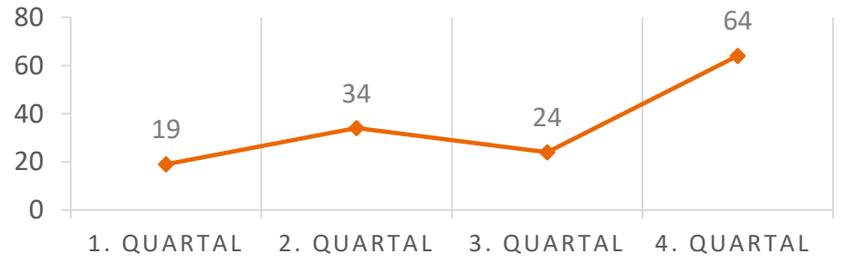
Aufstellung nach Sektoren
2026

Erstmeldungen nach Sektoren	Q1 2026	Q2 2026	Q3 2026	Q4 2026
Bankensektor	**22**	**37**	**21**	**44**
Versicherungs-, Pensionskassen- und Vorsorgekassensektor	1	4	1	8
Wertpapiersektor	3	4	7	33
Gesamt	**26**	**45**	**29**	**71**

Stand 17.11.2026

SCHWERWIEGENDE IKT-BEZOGENE VORFÄLLE

URSPRUNG IKT-DRITTDIENSTLEISTER 2026



Ursachen lt. Abschlussmeldung (Mehrfachnennung möglich)	2025	**2026**	Q1 2026	Q2 2026	Q3 2026
Böswillige Handlungen	**23**	8	1	3	4
Prozessversagen	**17**	13	4	7	2
Systemversagen/-störung	**47**	**52**	**18**	**27**	**7**
Menschliches Versagen	**8**	8	3	3	2
Externes Ereignis	**24**	36	4	15	17

Wesentliche Erkenntnisse

77 %

der im Jahr 2026 (Q1 bis Q3) gemeldeten DORA-Vorfälle gehen auf IKT-Drittdienstleister zurück

→ Stärkung des IKT-Drittparteienrisikomanagements bleibt prioritär

→ Systemversagen/-störungen bleiben wichtigste Vorfallsursache

DIE MITWIRKUNG VON IKT-DRITTANBIETERN BEI THREAT-LED PENETRATION TESTING (TLPT)

TIBER UND TLPT | NOCH ZWEI AKRONYME, DIE MAN KENNEN MUSS (?)

TIBER: „Threat-Intel Based Ethical Red Teaming“

Das **TIBER-EU Rahmenwerk** wurde 2018 eingeführt und in Österreich 2023 umgesetzt, 2025 erfolgte eine Anpassung an DORA

TLPT : „Threat–led Penetration Testing“

- Gemäß DORA seit 2025 **verpflichtend** für **systemrelevante Finanzunternehmen**
- Durchführung auf **Basis** von **TIBER-EU**

Zielsetzung: Stärkung der Cyberresilienz des Finanzsektors

TLPT bildet einen Rahmen, der **Taktiken, Techniken und Verfahren realer Angreifer nachbildet** und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten Red-Team-Test (simulierte **Angriffe „ethischer Hacker:innen“** bzw. „Red-Team“) auf die **kritischen IKT-Systeme im Echtzeitbetrieb** ermöglicht.

Wesentliche Merkmale von TLPT (erweiterte Tests)

- Von verpflichteten Finanzunternehmen **alle drei Jahre** durchzuführen
- Als **ergänzendes Mittel** zum klassischen Testprogramm (z.B. Pentests), nicht als Ersatz
- **Einbindung** von externen **IKT-Drittanbieter (IKT-TPP)**, bei Auslagerung relevanter Funktionen
- **Hohe Anforderungen** an externe (im Ausnahmefall auch interne) Red Teams
- **Begleitung** der Tests durch **Test Manger (TM)** eines TIBER Cyber Teams (TCT, in Österreich das **TCT-AT der OeNB**), um die **regelkonforme Durchführung** sicherzustellen und zu bestätigen.

TPP: Third Party Provider

TIBER-EU UND DIE FÜR AT RELEVANTEN IMPLEMENTIERUNGEN

TIBER-EU

- TIBER-EU bietet das Rahmenwerk, bestehend aus verpflichtenden und optionalen Anforderungen
- Alle wesentlichen und verpflichtenden Bestandteile eines TIBER Tests sind in TIBER-EU vorgeschrieben
- Implementierungen fokussieren sich auf optionale und nationale (insbes. institutionelle) Besonderheiten

TIBER-EU ist somit unmittelbar anwendbar!

TIBER-EU SSM

Signifikante Kreditinstitute
Aufsichtsbehörde **EZB**

TIBER-AT

Alle anderen AT-Finanzunternehmen
Aufsichtsbehörde **FMA**

MITWIRKUNGSPFLICHT VON IKT-TPP BEI TLPT | WAS BEDEUTET DAS KONKRET?

Gesetzliche Grundlage für die Mitwirkung von IKT-TPP bei TLPT ist Art. 30 (3) lit. d DORA

Werden IKT-Dienstleistungen zur **Unterstützung kritischer oder wichtiger Funktionen** in Anspruch genommen, so haben die **vertraglichen Vereinbarungen** zu beinhalten, dass der **IKT-TPP verpflichtet** ist, sich an den **TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken**.

Wie läuft die Involvierung prozessual ab?

- Der **Control Team Lead (CTL)** des Finanzunternehmens **evaluiert** im Rahmen der Einrichtung des Control Teams (CT) die **Einbindung von IKT-TPP** auf Basis des Scopes und der Szenarien.
- Ebenso evaluiert das CT bei der **Vorbereitung von Hilfestellungen** für das Red-Team („Leg-ups“) die Einbindung von IKT-TPP.
- Erst **nach Validierung durch die Test Manager** (TM) des TCT-AT wird **IKT-TPP eingebunden**.

Bedenkliche Vertragsbestandteile

- **Mitwirkungspflicht** kann **kein Recht** für den IKT-TPP beinhalten auf
  - **Einbindung** in das CT oder auch nur
  - **Information** über einen TLPT

  Diese **Entscheidung** liegt immer beim **CTL,** gefolgt von der **Validierung** durch die **TM**.
- **Keine** verpflichtende **Abtretung** bestimmter **Entscheidungen** des CTL an IKT-TPP, z.B:
  - **Auswahl Szenarien** oder **TLPT-Provider**
  - **Aussetzung** oder **Abbruch** eines **TLPT**

UMFRAGE 2 - JETZT ABSTIMMEN UNTER…

menti.com

4832 7457

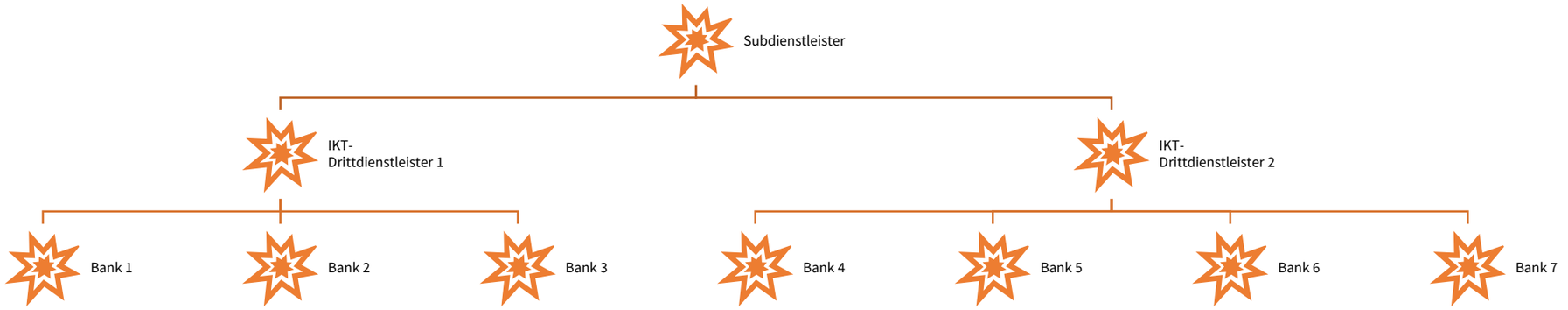


MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

IKT-DRITTPARTEIENRISIKOMANAGEMENT AUS SICHT DES FINANZINSTITUTS

- **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 Überwachung:** Nur durch gutes Management und Transparenz der IKT-Dienstleister 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.
- ➢ **Meldung an FMA durch Finanzinstitute in diesem Fall notwendig**.

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

IKT-DRITTPARTEIENRISIKOMANAGEMENT AUS SICHT DER IKT-PROVIDER

Finanzinstitute **dürfen keine Verträge eingehen**, die Mindestvertragsinhalte laut Art. 30 DORA nicht erfüllen. **Das ist nicht verhandelbar.**

„Kritische oder wichtige Funktionen“, wie im Art. 30 (3) DORA genannt, beziehen sich **immer auf das Finanzinstitut**, nicht auf die IKT-Dienstleistung

Finanzinstitute müssen die Eignung eines Dienstleisters immer individuell überprüfen. **Es gibt daher kein „DORA-Zertifikat“**, aber Zertifizierungen sind trotzdem hilfreich.

Bei Bedarf kann die FMA **direkt Informationen von Drittanbietern einfordern** und die Kundeninformation kontrollieren. Auch Vor-Ort Prüfungen werden durchgeführt.

Versäumnisse bei IKT-Providern **erfüllen die Definition von Cyberbedrohungen** und können durch die Aufsicht kommuniziert werden.

Die DORA-Anforderungen sind geltendes Recht. IKT-Provider, die diese Anforderungen nicht erfüllen können oder wollen, sind für den Einsatz im Finanzsektor nicht geeignet. Das gilt auch für Subdienstleister.

IKT-DRITTPARTEIENRISIKOMANAGEMENT AUS SICHT DER IKT-PROVIDER

Anforderung

- DORA-Mindestvertragsinhalte (Art. 30 DORA)
  - Absatz 2 beschreibt Vereinbarungen, die in ALLEN Verträgen enthalten sein müssen
  - Absatz 3 jene, die ZUSÄTZLICH enthalten sein müssen, die kritische oder wichtige Funktionen des Finanzinstituts unterstützen.
- Subdienstleister
  - Müssen dem Finanzinstitut bekannt gemacht werden.
  - Müssen ebenso transparent mit dem FI und der Aufsicht zusammenarbeiten.
- Zusammenarbeit mit der Aufsicht

Lösung

- Zwei Vertragstemplates vorbereiten:
  - Eines für alle IKT-Dienstleistungen, die an Finanzinstitute angeboten werden
  - Eines für jene DL, die kritische oder wichtige Funktionen eines Finanzinstituts unterstützen
- DORA-Mindestvertragsinhalte auch für Subdienstleister nutzen
  - Anzahl und Tiefe der Subdienstleisterketten minimieren.
  - Dienstleister außerhalb der EU bedeuten höheren Aufwand.
- IKT-Provider sind verpflichtet der Aufsicht Auskunft zu geben bis hin zu Vor-Ort-Prüfungen bei Subdienstleistern
  - Aufsicht kann u.a. Cyberbedrohungen kommunizieren.
  - Austausch mit NIS2 Behörde ist bereits aktiv.

IKT-DRITTPARTEIENRISIKOMANAGEMENT AUS SICHT DER IKT-PROVIDER

Anforderung

- Audits und regelmäßige Informationserhebungen
  - Sind ein wesentlicher Teil des IKT-Drittparteienrisikomanagements
  - Können an unabhängige Dritte übertragen werden (Art. 30 (3) letzter Satz)
- Incidenthandling

Lösung

- Proaktiv Kunden, die an gemeinsamen Audits interessiert sind, unterstützen.
  - Proaktiv Kunden mit DORA-relevanten Informationen versorgen, um Fragebögen zu minimieren.
  - Zertifizierungen mit jenen Hintergrundinformationen an Kunden zugänglich machen, die sie benötigen (z.B. Statement of Applicability, Scope, Abweichungsanalyse und Mängelverfolgungsdokumentation)
- Kommunikationspläne und Kanäle für Incidents vorbereiten und Kunden vorab informieren.
  - Finanzinstitute müssen Erstreport unverzüglich mit dem **FMA-Template** melden. Teilen Sie die benötigten Informationen Ihren Kunden proaktiv mit.
  - Template ist online unter: https://webhost.fma.gv.at/IncomingPlattform/api/HelpFilesApi/700

KONKRETE CYBERBEDROHUNG: SOFTWAREENTWICKLER IM FOKUS

Softwareentwickler:innen und in der Softwareentwicklung genutzte Werkzeuge werden zunehmend Angriffsziele von Cyberattacken

Warum?

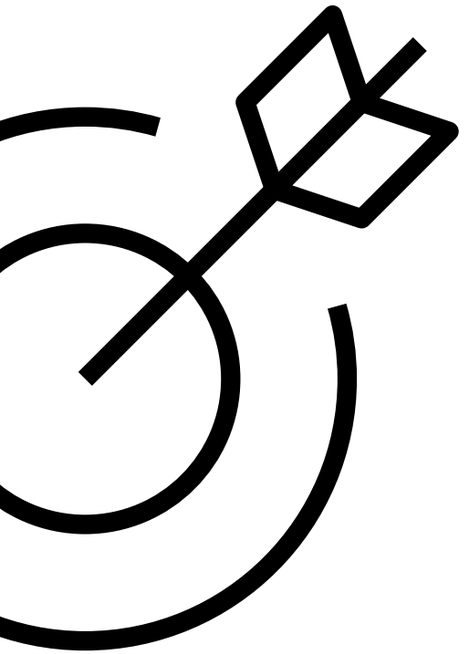
- Angriff auf Binance als global öffentlichkeitswirksamster Vorfall, aber es existieren auch ähnlich gelagerte Angriffsmuster in dem österreichischen Finanzsektor und bei IKT-Drittdienstleistern

Was?

- Softwareentwickler:innen erhalten Jobangebote, die über verschiedene Umwege zur Installation von Malware führen.
- Gängige Tools zur Softwareentwicklung werden systematisch z.B. durch Add-Ins kompromittiert.
- Es wird systematisch versucht, Quellcode aus vertraulichen Git-Repositories zu stehlen.

Gegenmaßnahmen

- Keine lokalen Administrationsrechte für Softwareentwickler, Git-Repositories kritisch reviewen, in Pentest-Scope aufnehmen.
- Keine individuelle, ungeprüfte Installation von Add-Ins über öffentliche Stores.
- Aufklärung und Schulungen der Mitarbeiter:innen, bezüglich missbräuchlichen Jobangeboten und den Risiken, Freelancer unbedingt inkludieren.



Erfahrungen aus der direkten Prüfung von IKT-Drittdienstleistern nach DORA

POTENTIELLE PRÜFMODULE UND INHALTE

IKT-Sicherheitsrisiken

- Funktionstrennung, Richtlinien, Awareness-Maßnahmen
- Überprüfung der organisatorischen und technischen Sicherheitsmaßnahmen
- Behandlung von Sicherheitsvorfällen

IKT-Änderungsrisiken

- Prüfung der Implementierung von Systemen sowie der Entwicklung und Beschaffung von Software
- Change-, Release-, Deployment- und Konfigurations-Mgmt.
- Einbindung der unabhängigen Kontrollfunktion und der damit verbundenen Aktivitäten

IKT-Systeme

- Ganzheitliche Prüfung eines Systems oder Projekts
- Prüfung aller relevanten IT-Aspekte; z.B. Organisation, Beschaffung, Entwicklung, Betrieb, IKT-Sicherheit



PRO Direkte Dienstleisterprüfung

→ Frühzeitige Identifikation von Konzentrationsrisiken

→ Direkte Beurteilung wesentlicher Sicherheits- und Resilienz-Maßnahmen

→ Effiziente Prüfung standardisierter Shared-Services

→ Erhöhter sektoraler Erkenntnisgewinn

ERKENNTNISSE AUS BISHERIGEN DIREKTEN UND INDIREKTEN IKT-DRITTDIENSTLEISTERPRÜFUNGEN

- **Governance Schwachstellen** sowie im Bereich des Risikomanagements und der Kontrollsysteme
- **Defizite bei Informationssicherheit**, Berechtigungsmanagement und Funktionstrennung
- **Erhöhte Cyber- und Betriebsrisiken** durch offene Schwachstellen, technische Altlasten
- **Mängel in Softwareentwicklung**, teilweise aufgrund unzureichender Toolunterstützung und Automatisierung.
- **Unklare Verantwortlichkeiten** und Schnittstellen zwischen IKT-Drittdienstleistern und KIs
- **Unzureichende Notfallvorsorge** sowie Defizite im Krisen- und Business-Continuity-Management



KRITISCHE FESTSTELLUNGEN BEI IKT-DRITTDIENSTLEISTERN MIT UNMITTELBAREM HANDLUNGSBEDARF

- **Wiederholte Verzögerungen** bei Softwareentwicklungs- und Implementierungsprojekten
- **Wiederkehrende Serviceunterbrechungen** als Hinweis auf Schwächen in der operativen Resilienz
- **Erhöhte Fluktuation** von Schlüsselpersonal, insbesondere in Informationssicherheitsfunktionen
- **Wiederholte Nichteinhaltung** vereinbarter Service Level Agreements (**SLAs**)
- **Häufige Notfalländerungen** oder ungeplante Produktivsetzungen
- Anhaltender **Rückstand** bei der Behebung kritischer Schwachstellen sowie überfälliger **Sicherheitsupdates**



Q&A



UMFRAGE 3 - JETZT ABSTIMMEN UNTER…

menti.com

2480 3349



AKTUELLE DORA-INFORMATIONEN

Startseite > DORA – Digitale operationale Resilienz im Finanzsektor > DORA – FMA-Aktivitäten

DORA – 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.

Dialoge und Veranstaltungen

FMA/OeNB-DORA-Dialog: KI-basierte Schwachstellensuche und -ausnutzung 02.06.2026

FMA/OeNB-DORA-Dialog: Ein Jahr DORA – Highlights, Herausforderungen & Way Forward 18.02.2026

Veröffentlichung der Dialogunterlagen auf der FMA-DORA-Website

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz

OESTERREICHISCHE NATIONALBANK

EUROSYSTEM