FMA-OeNB-DORA-Dialog:

Ein Jahr DORA – Highlights, Herausforderungen & Way Forward

Stand der Hinweise ist 20.2.2026.

FMA-Antworten sind in dieser Form dargestellt.

Die Hinweise zu den während des Webinars erhaltenen Fragen stellen keine verbindliche Auslegung und insbesondere auch keine Auslegungen im Rahmen der Fragen- und Antwort-Prozesse (Q&As) der drei Europäischen Aufsichtsbehörden (EBA – European Banking Authority, ESMA – European Securities and Markets Authority und EIOPA – European Insurance and Occupational Pensions Authority) dar. Alle Angaben erfolgen trotz sorgfältiger Bearbeitung, insbesondere hinsichtlich Aktualität, Vollständigkeit und Richtigkeit ohne Gewähr und es wird keinerlei Haftung für die Inhalte übernommen. Fragstellungen wurden gs. unformatiert übernommen.

1. In welchem Umfang sind Exit-Strategien zu testen?
   Ausstiegspläne sind im Einklang mit dem Grundsatz der Verhältnismäßigkeit des Art. 4 Abs. 2 Verordnung (EU) 2022/2554 (DORA-VO) zu testen.

2. Wie viele Prüfungen nach DORA wurden 2025 durchgeführt?
   In allen drei Sektoren wurden insgesamt 17 Vor-Ort-Prüfungen mit Schwerpunkt DORA durchgeführt.

3. Wie muss ein als kritisch designierter Dienstleister bewertet werden, wenn dieser Dienstleister keine kritische Funktion im Unternehmen bedient?
   Die Bewertung erfolgt auf Basis der Vorgaben der DORA-VO – unabhängig von der Einstufung als kritischer IKT-Dienstleister.
   Siehe dazu auch Slide 45 des Dialogs.

4. Auf welchem Weg werden die Finanzunternehmen über die Risiken informiert, die sich aus den Empfehlungen an die IKT DL ergeben?
   Sie erhalten die Informationen von den zuständigen DORA-Behörden, ggf von FMA.
   Siehe dazu Art. 42 Abs. 3 DORA-VO.

5. Könnten wir bitte auch einen Überblick der meistgenannten kritischen IKT Drittdienstleister nur für Österreich erhalten?
   Auswertungen für den österreichischen Finanzmarkt werden aufgrund der übermittelten Informationsregister erstellt.

6. Richten sich die Ersuchen/Verlangen bzw. Prüfungen, die gerade erwähnt wurden, daher ausschließlich an kritische IKT Dienstleister?
   Wenn mit der Frage der Überwachungsrahmen für kritische IKT-Drittdienstleister gemeint ist, ist klarzustellen, dass die diesbezüglich in DORA vorgesehenen Ersuchen, Informationsanforderungen sowie Prüfungs- und Untersuchungshandlungen ausschließlich gegenüber als kritisch eingestuften IKT-Drittdienstleistern (CTPPs, critical ICT third-party service providers) zur Anwendung kommen. Dies ergibt sich auch aus dem JC 2025 29 DORA Oversight Guide, der den Geltungsbereich des Oversight Frameworks ausdrücklich auf CTPPs beschränkt.

Für weiterführende Informationen zum Überwachungsrahmen verweisen wir auch auf die entsprechende Informationsseite der FMA:
https://www.fma.gv.at/querschnittsthemen/dora/dora-kritische-ikt-drittdienstleister/

7. Bzgl. den 19 kritischen IKT-Dienstleistern, liegt der Fokus konzentriert auf den festgestellten, konkreten juristischen Personen oder erfolgt eine Konzernbetrachtung (Vererbung der Kritikalität auf Töchter)?
   Gehört der IKT-Drittdienstleister zu einer Gruppe, so werden die Einstufungskriterien in Bezug auf die von der Gruppe als Ganzes bereitgestellten IKT-Dienstleistungen berücksichtigt.
   Siehe Art. 31 Abs. 3 DORA-VO. Siehe auch Frage 9.

8. Ich fände es bei der nächsten Veranstaltung sehr hilfreich, wenn auch die gesammelten Erfahrungen iZm Drittparteienmanagement stärker geteilt werden könnten – das würde aus meiner Sicht einen großen Mehrwert für alle bringen.
   Wir nehmen den Punkt gerne mit.

9. Auf welcher Ebene werden die kritischen IKT-Dienstleister überwacht? Werden österr. Tochterunternehmen von kritischen IKT-Drittdienstleistern, auch dezidiert überwacht werden (z.B. Accenture Rechenzentrum österr. Banken von FMA/OeNB im Rahmen des JET) oder findet die Überwachung lediglich auf der Ebene der Konzernspitze statt.
   Siehe Fußnote 16 von ‚Digital Operational Resilience Act (DORA): Oversight of critical third-party providers, Guide on oversight activities': The ESAs designate group structures as CTPP (i.e. focus on the parent company, with the ability to oversee all the subsidiaries providing the identified ICT services to the FEs).

10. Werden noch genaue Daten zu den Dienstleistern veröffentlicht, zB LEI?

    Ergänzung: Die Liste ist insofern unvollständig als nur die Namen genannt werden. Teilweise ist unklar welche konkrete entity gemeint ist, hier wäre die Veröffentlichung des LEI relevant.
    Wir bringen das Anliegen in relevante Gremien ein.

11. Ad Zertifizierung:
    Widerspruch! ;-) - Ein um die in ISO 27001 nicht enthaltenen DORA-Anforderungen erweitertes ISMS (zusätzliche Controls gem. 6.1.3. b) stellt sehr wohl die Erfüllung aller DORA-Anforderungen sicher, und ist damit als ausreichende Zertifizierung zu werten.
    Ebenso sind die Anforderungen von DORA auf deutlich höherer Flughöhe als die der ISO 27001 und damit ist jede DORA-Anforderung mittels direktem Mapping erfüllbar.
    Es sind jedenfalls sämtliche Zertifizierungen auf deren Scope und Inhalte zu überprüfen.
    Zertifikate sind per se keine Freibriefe.
    Die ISO/IEC 27001 bezieht sich auf das Informationssicherheitsmanagement des Unternehmens und betrifft die organisatorische Sicherheit eines Unternehmens. Hingegen gibt es auch Zertifikate, wie bspw. ISO/IEC 15408 mit denen auch Software bzw. Hardware auf Sicherheit offiziell bewertet werden.

12. ad Folie 32 und Kulturwandel:
    Nein, die Themenstellung an sich gibt es zumindest seit dem Jahr 2000 und der ISO 27001, die das Thema bereits seit Jahrzehnten enthält.
    Was Kulturwandel fördern könnte, ist direkter Druck der FMA /Aufsicht auf die kritischen IKT-Dienstleister, da kleinere Finanzinstitutionen keinerlei strategischen Druckmittel haben, Compliance zu erzwingen.
    Welche Prüfschritte bei kritischen IKT-Dienstleistern sind seitens FMA geplant?
    Ein gemeinsames Vorgehen von zuständigen DORA-Behörden und ESAs ist geplant.

13. Einen nicht vernachlässigbaren Aufwand im IKT-TPRM würde ich auch in der (korrekten) Klassifizierung der IKT-Services gem. DORA sehen und der Abstimmung bzw. vielmehr den (oft schier endlosen) Diskussionen mit den IKT-Drittdienstleistern dahingehend.

-

14. Insbesondere die Exit-Pläne (nicht bloß die Strategien) sind eine massive Herausforderung mangels echter Alternativen zu einzelnen großen Anbietern. Ein Austausch von Lösungsansätzen oder ein gesonderter Termin hierzu wäre sicher hilfreich.
    Wir nehmen das Thema gerne auf.

15. Wie kann man sich für die Übermittlung der GTL anmelden?
    Bitte wenden Sie sich an tct@oenb.at.

16. Können Sie ein paar Worte verlieren was die Überwachung der kritischen IKT-Drittdienstleistender (veröffentlicht 18.11.2025) bedeutet? Was ist für ein Finanzunternehmen zu erwarten? Gibt es Erleichterungen welche z.b. nicht mehr vom FI durchgeführt werden müssen sondern durch die Behörde direkt?
    Der neue Überwachungsrahmen wurde im Rahmen des Dialogs (ab Slide 36) adressiert.

17. Gibt es eine Übersicht, welche Informationsaustauschformate die Meldepflicht auslösen? Sind bereits Informationsveranstaltungen, die am Markt angeboten werden, zu DORA (z.B. auch von privaten Veranstaltern) erfasst? Wie hat die Meldung zu erfolgen?
    Die Meldepflicht an die FMA bezieht sich gemäß Art. 45 DORA-VO auf formelle Informationsaustauschvereinbarungen, nicht auf die Teilnahme an Newslettern oder auf informellen Austausch.

18. Haben sich die Ausführungen auf IKT-Drittdienstleister nur auf kritische IKT-Drittdienstleister bezogen oder auf alle IKT-Drittdienstleister?
    Die DORA-Vorgaben zum IKT-Drittparteienrisikomanagement gelten bezüglich aller IKT-Drittdienstleister eines Finanzunternehmens, nicht nur der kritischen IKT-Drittdienstleister.
    Zu beachten sind allenfalls spezifische DORA-Anforderungen im Hinblick auf kritische oder wichtige Funktionen eines Finanzunternehmens.

19. Ist abzusehen, dass eine Spezifizierung der Vorgaben an Tests und Testregimes gemacht wird? Die Beschreibung ist umfangreich, und für uns schwer abzuwägen hinsichtlich Methode, notwendiger Umfang ...?
    Das Programm für das Testen der digitalen operationalen Resilienz folgt einem risikobasierten Ansatz. Das jeweilige Unternehmen definiert individuell das jeweilige Testprogramm. Siehe insbesondere Art. 24 Abs. 3 DORA-VO.

20. Wie sollen Vereinbarung bzgl. Nutzung von Informationsquellen wie z.B. CERT der FMA gemeldet werden?
    Die Meldepflicht an die FMA bezieht sich gemäß Art. 45 DORA-VO auf formelle Informationsaustauschvereinbarungen, nicht die Teilnahme an Newslettern oder auf informellen Austausch.

21. Welche konkreten Kriterien machen ein Finanzunternehmen *bedeutend*? - Nur systemrelevante?
    Die Kriterien zur Identifikation bedeutender Finanzunternehmen im Kontext von bedrohungsorientierten Penetrationstests sind in Art. 26 Abs. 8 DORA-VO geregelt und werden durch Art. 2 Delegierte Verordnung (EU) 2025/1190 präzisiert.

22. Incident Klassifizierung: Beim Kriterium böswilliger Angriff auf Systeme und (möglicher) Verlust von Daten: ist mit "Verlust von Daten" (dataloss) die Verletzung von einem der Schutzbedarfe (CIAA) gemeint, oder nur das Schutzziel Vertraulichkeit?
    Der (mögliche) Verlust von Daten betrifft grundsätzlich mögliche Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten (Art 9 delVO 2024/1772). Sollte die Anforderung weiterhin unklar sein, ersuchen wir um Präzisierung oder um bilaterale Kontaktaufnahme unter dora@fma.gv.at.

23. Wie viele Meldungen wurden bislang aufgrund von Cyberangriffen auf meldepflichtige Unternehmen registriert?
    Rund 19% der eingegangenen IKT-Vorfallsmeldungen waren auf böswillige Handlungen zurückzuführen.

24. Auf welcher Grundlage wurde die Regeln zur Validierung des Informationsregister vorgenommen, wenn der EBA ITS zum RoI andere Vorgaben macht? Z.B. RT.02.02.0150 Location of the data at rest (storage) - Mandatory if 'Yes' is reported in RT.02.02.0140
    Gibt es keine Datenverarbeitung/-speicherung ist das Feld nicht verpflichtend.
    Es generiert hunderte Fehlermeldungen im Test-Upload, die Ende Jänner noch angezeigt wurden.
    Dazu ist anzuführen, dass der ITS bedauerlicherweise sich gegenüber dem Datenmodell der EBA unterscheidet. Im Datenmodell der EBA (Data Model for DORA RoI) werden die Felder B.02.02.0130, B.02.02.0150 und B.02.02.0160 als Pflichtfelder (Nullable = No) angeführt. In diesen Fällen ist bei den Auswahlfeldern ‚Not applicable' auszuwählen (siehe dazu Frequently asked question on reporting of the registers of information Nr. 59, Nr. 61 u. Nr. 63).

    Ein weiteres Pflichtfeld lt. Datenmodell der EBA ist B_04.01.0040. In diesem Fall ist ebenfalls 'Not Applicable' einzutragen (siehe dazu Frequently asked question on reporting of the registers of information Nr. 64).

25. Wir müssen das ROI dem Konzern melden und der Konzern meldet es der BAFIN aber schwerwiegende Vorfälle müssen wir der FMA melden. Wie werden hier die Information von dem ROI eingeholt?
    Ein Informationsaustausch unter den zuständigen DORA-Behörden und ESAs ist eingerichtet.

26. Wie definieren Sie eine Auffälligkeit im Fit & Proper Gespräch, der weiter nachgegangen wird?
    Gemeint war, dass wir im Vorfeld des Fit & Proper Gesprächs bei der Entscheidung, ob auch Fragen zum Themenkomplex IT-Risiko im Rahmen des Gesprächs gestellt werden, ua berücksichtigen, ob es beim Unternehmen Auffälligkeiten im Bereich IT-Risiko gab/gibt (bspw bevorstehende große IT-Projekte, Vorfälle, etc).

27. ad Folie 7: Warum nur für Führungsfunktionen mit IT-Bezug? Ein Problem der Praxis ist, dass vor allem andere Führungsfunktionen entsprechende Investitionen blockieren, weil zu wenig Verständnis für die Wichtigkeit der IT /IT-Risiken vorhanden ist.?
    Vielen Dank für den wichtigen Kommentar. Wir konzentrieren uns auf jene Führungskräfte, die einen konkreten Bezug zu IT-Risikomanagement oder zur IT-Infrastruktur haben, stellen uU aber auch bei anderen Führungskräften Fragen zum Thema IT-Risiko, wenn dies indiziert ist.

28. Fordert DORA ein IKT-Desaster Recovery oder ein ganzheitliches BCM so wie es auch im BSI 200-4 vorgesehen ist?
    Vorgaben zu Desaster Recovery und BCM sind in den DORA-Vorgaben enthalten, aber es wird auf keine konkreten Standards verwiesen.

29. Findet eine kurzfristige Prüfung durch die FMA auch an einem Wochenende statt?
    FMA-Bestätigungen zum Erhalt von scherwiegenden IKT-bezogenen Vorfällen und die Weiterleitung an die europäischen Aufsichtsbehörden erfolgen nach Einbringung, unabhängig vom Wochentag. Bei schwerwiegenden Fällen war die FMA schon bislang auch an Wochenenden verfügbar.

30. Was heißt das, "die FMA zieht Stichproben auf Richtlinien und Prozesse? Was ist hier zu erwarten?
    Sie werden demnächst dazu informiert.