Deloitte.

Das zweite „DORA“-Ergänzungspaket

Aufsichtliche Erwartungen zur Anforderungserfüllung zur digitalen operationellen Resilienz

Wien, 19. Jänner 2024

Spielregeln / Organisatorisches

Ihr Mikrofon ist standardmäßig deaktiviert.

Ebenso ist die Video-Funktion deaktiviert.

Fragen können gerne jederzeit mittels Q&A-Funktion gestellt werden. Für die Beantwortung Ihrer Fragen nehmen wir uns am Ende des Vortrags 10-15 Minuten Zeit.

Die Unterlage zum Vortrag wird im Nachgang an die Teilnehmerinnen und Teilnehmer versandt.

Die Veranstaltung wird aufgezeichnet. Diese kann auf Anfrage unter attechcompliance@deloitte.com gerne zur Verfügung gestellt werden.

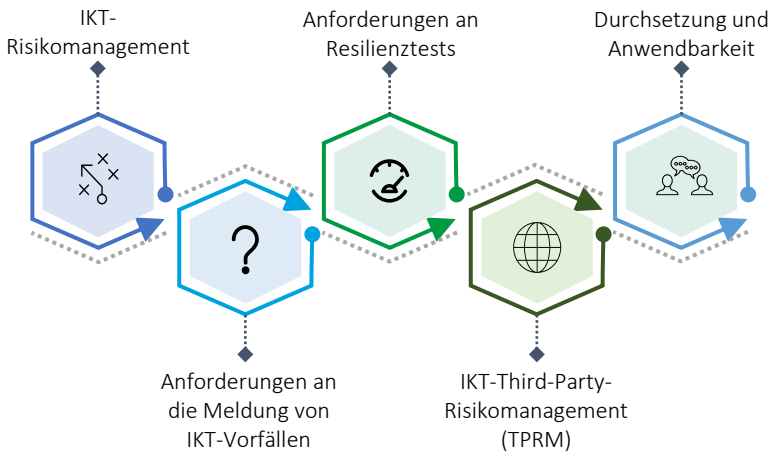
Agenda

Überblick zum EU Digital Operational Resilience Act (DORA)

Überblick zum EU Digital Operational Resilience Act (DORA)

Die Umsetzung der DORA erfordert ein Zusammenspiel zwischen Risiko-, Cyber-, Drittanbieter- und Resilienzmanagement

EU DORA legt einen einheitlichen Anforderungskatalog für ein breites Spektrum von Unternehmen in der EU in den Bereichen Cyber- und IKT-Risikomanagement:



Erster Entwurf von DORA
Europäische Kommission 24.09.20

Erörterung mit dem Rat der EU
04.06.21

Annahme durch den Rat der EU
28.11.22, nachdem das EU-Parlament am 10.11.23 für die Annahme gestimmt hat

Inkrafttreten
Veröffentlichung im Amtsblatt der EU am 27.12.22; Inkrafttreten am 16.01.23

12-18 Monate nach Inkrafttreten
Teil 1 der Level-2-Vorschriften am 19.06.23, Teil 2 am 8.12.23 als Entwurf veröffentlicht
Zeitplan für finale Level-2-Regelungen:
Teil 1 für Ende Q1 2024 erwartet
Teil 2 für Q2/Q3 2024 erwartet

24 Monate nach Inkrafttreten
Die verpflichtende Anwendung beginnt am 17.01.25 nach Ablauf der Umsetzungsfrist

Die wichtigsten Informationen zu EU DORA:

- EU-VO 2022/2554 („**DORA**“) ist am **16. Jänner 2023** offiziell in Kraft getreten. Aufgrund des Umsetzungszeitraums von **24 Monaten** müssen Finanzinstitute bis **17. Jänner 2025** mit den Anforderungen konform sein.
- Die Anforderungen von DORA an das IKT-Risikomanagement stehen weitgehend im Einklang mit den Leitlinien der EBA für IKT-Sicherheit und Risikomanagement (2019) und der EIOPA für IKT-Sicherheit und -Governance (2020), aber ihre neue Verbindlichkeit durch die Aufnahme in das Primärrecht wird die aufsichtliche Kontrolle, mit der die Unternehmen rechnen müssen, intensivieren.
- Neben den bereits bekannten technischen Standards und geplanten delegierten Rechtsakten wird durch ein Mandat der ESAs erwartet, dass weitere Regelungen für einzelne Industriezweige folgen.
- Die ESAs wurden beauftragt, gemeinsam in zwei Phasen **13 ergänzende technische Standards** zu entwickeln. **Teil 1** der technischen Standards, für den von 19. Juni 2023 bis 11. September 2023 eine öffentliche Konsultation stattgefunden hat, wurde am 17. Jänner 2024 in einem finalen Entwurf veröffentlicht. Mit einer Verabschiedung ist in den nächsten beiden Monaten zu rechnen.
- Der kürzlich veröffentlichte **Teil 2** (öffentliche Konsultation laufend seit 8. Dezember 2023 bis 4. März 2024) umfasst Folgendes:
    - RTS on threat-led penetration testing (TLPT)
    - RTS on subcontracting of critical or important functions
    - RTS and ITS on content, timelines and templates on incident reporting
    - GL on aggregated costs and losses from major incidents
    - GL on oversight cooperation between ESAs and competent authorities
    - RTS on oversight harmonization

WICHTIG: Angegebene Bezeichnungen entsprechen dem Originaltext (Englisch) der bisher bekannten Veröffentlichungen. Deutschsprachige Bezeichnungen / Versionen sind aktuell nicht verfügbar und werden erwartet. Die nachfolgenden deutschen Bezeichnungen in der Präsentation sind Übersetzungen aus der offiziellen englischen Version.

RTS zur Präzisierung von Aspekten des Threat Led Penetration Testing (TLPT)

RTS zur Präzisierung von Aspekten des Threat Led Penetration Testing (TLPT) (Art. 26 Abs. 11)

Überblick und Ansätze des Entwurfs

Wesentliche Aspekte

Finanzunternehmen, die aus IKT-Perspektive ausgereift genug und von gewisser systemischer Relevanz sind, führen mind. alle 3 Jahre anhand von TLPT erweiterte Tests durch (Art. 26). Art. 26 Abs. 11 mandatiert die ESAs im Einvernehmen mit der EZB und im Einklang mit dem TIBER-EU-Rahmen weitere Präzisierungen im Hinblick auf Finanzunternehmen, die einen TLPT durchführen müssen, den Einsatz interner Tester, Umfang, Testmethodik und Testkonzept für jede Phase, Ergebnisse / Abschluss sowie die aufsichtliche Zusammenarbeit zu erarbeiten.

- **DORA als EU-Verordnung vs. freiwilliger TIBER-EU-Rahmen**: der RTS steht größtenteils im Einklang mit dem TIBER-EU-Rahmen ➔ sofern DORA jedoch zusätzliche TLPT-Anforderungen vorsieht, müssen diese einbezogen werden; TIBER-EU sowie seine nationalen Umsetzungen stellen nur zusätzliche Leitlinien zu DORA, jedoch keinen Ersatz für den RTS dar
- **Wesentliche Unterschiede** zum TIBER-EU Rahmen:
  - **TLPT-Behörde**: DORA erlaubt die Ernennung einer einzigen Behörde, die mit allen TLPT-Aufgaben/Zuständigkeiten betraut wird, von denen sie einige/alle Aufgaben an eine andere zuständige nationale Behörde delegieren kann (Art. 26 Abs. 10) ➔ jeder Mitgliedstaat kann daher andere Aufgabenaufteilung auf die Behörden vornehmen (im RTS einheitlich die **„TLPT“ Behörden**)
  - **EZB**: Für Kreditinstitute gem. Art. 6 Abs. 4 EU-VO 1024/2013 ist die EZB mit allen TLPT-Aufgaben/Zuständigkeiten betraut; auch diese kann von Art. 26 Abs. 10 Gebrauch machen und Aufgaben/Zuständigkeiten delegieren
  - **Interne Tester**: DORA erlaubt unter besonderen Umständen den Einsatz interner Tester (diese Möglichkeit wird auch bei einer künftigen Überarbeitung des TIBER-EU-Rahmens erwartet)
  - **Purple Team-Übung**: unter DORA ist die Kollaboration zwischen rotem und blauem Team verpflichtend
  - Kleinere Details in der operativen Durchführung
  - EU-weite Anerkennung von Testergebnissen
- **Branchenunabhängigkeit**: Methodik/Verfahren des TLPT enthalten keine sektor- oder unternehmensspezifischen Anforderungen

Inhaltsverzeichnis

RTS zur Präzisierung von Aspekten des Threat Led Penetration Testing (TLPT) (Art. 26 Abs. 11)

Detailinformationen

Wesentliche Aspekte

Identifizierung von Finanzunternehmen

Art. 2 RTS

Zweistufiger Ansatz:
1. Festlegung spezifischer **Kriterien** und **Schwellenwerte** (Abs. 1): global oder systemisch wichtige Finanzinstitute; Zahlungsinstitute mit Zahlungstransaktionen von über 120 Mrd. EUR in den letzten 2 Jahren; Elektronische Geldinstitute mit Transaktionsvolumen von über 120 Mrd. EUR; Zentralverwahrer, zentrale Gegenparteien; Handelsplätze mit national höchstem Marktanteil oder auf EU-Ebene über 5%; Vers.- und Rückvers. unter bestimmten Kriterien

2. Flexibilität der TLPT-Behörde, weitere Unternehmen zu identifizieren (Abs. 3) oder bei fehlender Systemrelevanz und IKT-Reife von der Verpflichtung auszunehmen (Abs. 2)
Auch die Zugehörigkeit zu einer Unternehmensgruppe wird berücksichtigt

Testmethodik

Art. 3 - 5 RTS

Ähnlich zu TIBER-EU, Einbindung von 5 Stakeholdern:
- **TLPT Cyber Team:** Personal innerhalb der TLPT-Behörde, operative Betreuung
- **Control Team** (White Team): zentraler Ansprechpartner und Entscheidungsträger im getesteten Unternehmen, Monitoring und Risikomanagement
- **Blue Team**: Cyberabwehr, alle Mitarbeiter im Unternehmen außerhalb Control Team, nicht informiert
- **Threat Intelligence-Anbieter:** erstellt Angriffsszenarien, sammelt unternehmensspezifische Bedrohungsinformationen
- **Tester (Red Team)**: führen Angriffsszenarien durch; DORA erlaubt auch interne Prüfer

➔ **Risikomanagement** (Art. 5) muss in jeder Phase gewährleistet sein, verantwortlich ist das Unternehmen

Testprozess

Art. 6 - 10 RTS

Ähnlich zu TIBER-EU, 3 Phasen:
- **Vorbereitungsphase**: Frequenzfestlegung, Scoping, Beschaffung von Dienstleister und Testern
- **Testphase**: Sammlung von Informationen, (mind.) 12-wöchiger Red Team Test
- **Abschlussphase**: Berichterstellung & Feedback, Purple-Team-Übung (Wiederholung der defensiven und offensiven Aktionen), zusammenfassender Testbericht & Maßnahmenplan (Art. 10) an TLPT-Behörde (stellt anschließend Bescheinigung aus)

Bündeltests (Art. 26 Abs. 4): hierzu definiert der RTS **besondere Anforderungen** hins. Maßnahmenplan (Art. 10), Zusammenarbeit mit TLPT-Behörden (Art. 14 Abs. 2) und Bescheinigung (Art. 15 Abs. 5)

Interne Tester

Art. 11 RTS

DORA-Anforderungen in Art. 27 Abs. 1, Art. 26 Abs. 8 und Art. 27 Abs 2
RTS bringt **weitere Schutzmaßnahmen** für **interne Tester** und deren Einsatz:
a) Richtlinie für das Management von internen Testern in TLPTs
- Internes Testteam soll aus Testleiter und 2 Mitgliedern bestehen; Beschränkungen in Bezug auf deren Beschäftigungsdauer (2 Jahre)
- Schulungsanforderungen

b) Festlegung von Maßnahmen zur Sicherstellung, dass Einsatz keine neg. Auswirkungen auf Bewältigung IKT-bezogener Vorfälle hat
c) Festlegung von Maßnahmen, sodass interne Tester ausreichend Ressourcen und Fähigkeiten haben
- Erwähnung des Einsatzes in allen TLPT-Dokumenten (zB Red Team Test)
- Mitarbeiter von konzerninternen IKT-Drittdienstleistern gelten ebenfalls als interne Tester

EU-weite aufsichtliche Zusammenarbeit

Art. 12 RTS

Für europaweite Finanzunternehmen muss flexible Durchführung des TLPT möglich sein;
RTS deckt jene Fälle ab, in denen Zusammenarbeit zwischen Behörden aus verschiedenen Mitgliedstaaten (MS) erforderlich ist:
1) Unternehmen, die DL im Rahmen des freien DL-Verkehrs oder über eine Zweigniederlassung in anderen MS erbringen ➔ TLPT-Behörde des Herkunfts-MS muss TLPT-Behörden in Aufnahme-MS ermitteln, kontaktieren und Grad der Beteiligung am TLPT erfragen.

2) TLPT-Behörden beschließen, gemeinsame TLPT für mehrere Unternehmen mit Ansässigkeit in verschiedenen MS, aber einer Gruppenzugehörigkeit zu organisieren ➔ TLPT-Behörden vereinbaren untereinander, wer TLPT leiten soll

RTS zur Präzisierung von Aspekten der Subauslagerung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen

RTS zur Präzisierung von Aspekten der Subauslagerung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen (Art. 30 Abs. 5)

Wesentliche Aspekte

Art. 30 Abs. 2 lit. a erfordert eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Dienstleister bereitstellen muss. Dabei ist anzugeben, ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische und wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist und falls ja, welche Bedingungen hierfür gelten. Art. 30 Abs. 5 mandatiert die ESAs, hierfür eine entsprechende Präzisierung auszuarbeiten.

- Der RTS-Entwurf behandelt folgende Bereiche entlang des **Vertrags-Lifecycle**:
  - Ex-ante Risikoanalysen (bevor die IKT-Dienstleistungen vergeben werden dürfen)
  - Vertragsinhalte & laufende Leistungserbringung
  - Überwachung (insbesondere Subauslagerungsketten) & Audit
  - Unterrichtung über wesentliche Änderungen
  - Beendigung der vertraglichen Vereinbarung

- **Gruppeninterne IKT-Subdienstleister:** es gelten die gleichen Anforderungen wie für externe IKT-Drittdienstleister, wenngleich die Risiken unterschiedlich sind
- **Verantwortung**:
  - das Mutterunternehmen ist verantwortlich, dass die (zulässige) Subauslagerung in den Tochterunternehmen kohärent und auf allen relevanten Ebenen angemessen umgesetzt ist (Art. 3)
  - setzt der IKT-Drittdienstleister selbst Subdienstleister ein, bleibt die Verantwortung für Risikomanagement und Einhaltung rechtlicher Vorschriften beim Finanzinstitut und dessen Leitungsorganen
- **Implementierung geeigneter Verfahren**: einschlägige Risiken, die sich auf die Erbringung von IKT-Diensten auswirken können, müssen gemäß den vertraglichen Vereinbarungen behandelt werden können
- **Anwendung**: Der RTS ist gemeinsam mit DORA, dem RTS zur Spezifizierung der Outsourcing-Policy für IKT-Dienste, dem RTS zum Risikomanagementrahmenwerk sowie dem ITS zum Informationsregister zu lesen

1. Ist die Subauslagerung der kritischen und wichtigen Funktion zulässig?

2. Falls ja, welche Bedingungen gelten?

Inhaltsverzeichnis

RTS zur Präzisierung von Aspekten der Subauslagerung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen (Art. 30 Abs. 5)

Wesentliche Aspekte

Mindestumfang der Risikoanalyse in Bezug auf den Einsatz von Subdienstleistern (Art. 3):

- Bewertung der Fähigkeit des IKT-Drittdienstleisters, eigene Subdienstleister auszuwählen und zu beurteilen; Sicherstellung der Teilnahme an operationalem Berichtswesen und Tests
- Einbeziehung des Finanzunternehmens in relevante Subauslagerungsentscheidungen des IKT-Drittdienstleisters
- Gewährleistung der Replizierung wesentlicher Klauseln in den Subauslagerungsvereinbarungen des IKT-Drittdienstleisters
- Gewährleistung, dass IKT-Drittdienstleister als auch Finanzunternehmen selbst über Fähigkeiten, Fachkenntnisse, finanzielle, personelle und technische Ressourcen und Informationssicherheitsstandards, Organisationsstruktur, Meldeverfahren, etc. zur (direkten) Überwachung der Subdienstleister verfügen
- Beurteilung der Auswirkungen bei Ausfall von Subdienstleistern auf die digitale op. Resilienz und finanzielle Solidität
- Berücksichtigung von Risiken, die mit dem Standort der Subdienstleister des IKT-Drittdienstleisters verbunden sind
- Beurteilung von Konzentrationsrisiken
- Prüfung von etwaigen Hindernissen in Bezug auf die Ausübung von Audit-, Informations- und Zugangsrechten

Beschreibung und Bedingungen, unter denen kritische und wichtige IKT-Dienste an Subdienstleister vergeben werden können (zu spezifizierende Vertragsinhalte) (Art. 4)

- Verpflichtende Überwachung aller untervergebener kritischer und wichtiger IKT-Dienste durch den IKT-Drittdienstleister
- Festlegung der Überwachungs- und Berichtspflichten des IKT-Drittdienstleisters
- Bewertung aller Risiken, einschließlich IKT-Risiken durch den IKT-Drittdienstleister, hinsichtlich des Standortes seiner Subdienstleister / der Leistungserbringung
- Standort der Datenverarbeitung und -speicherung
- Spezifizierung der Überwachungs- und Berichtspflichten des Subdienstleisters ggü. IKT-Drittdienstleister/FU
- Sicherstellung der kontinuierlichen Bereitstellung kritischer und wichtiger IKT-Dienste durch den IKT-Drittdienstleister, auch bei Ausfall von Subdienstleistern
- Reaktion auf Vorfälle und BCM-Pläne des IKT-Drittdienstleisters
- Sicherstellung der IKT-Sicherheitsstandards, Audit- und Zugangsrechte sowie Kündigungsrechte

RTS zur Präzisierung von Aspekten der Subauslagerung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen (Art. 30 Abs. 5)

Wesentliche Aspekte

Überwachung der gesamten IKT-Subauslagerungskette (Art. 5)

- Wird eine kritische oder wichtige Funktion an einen IKT-Drittdienstleister ausgelagert, muss das Finanzunternehmen die **gesamte IKT-Subauslagerungskette** (auch) auf Basis der vom IKT-Drittdienstleister bereitgestellten Informationen überwachen und dokumentieren (siehe **Informationsregister** Art. 28 Abs. 3 und 9)
- Zudem müssen die Bedingungen für Vergabe von Subaufträgen durch den IKT-Drittdienstleister überwacht werden; ggf. durch Überprüfung von dessen Vertragsunterlagen mit den Subdienstleistern

Sonstiges

- Bei **wesentlichen Änderungen der Subauslagerung** (Art. 6) muss das Finanzunternehmen vom IKT-Drittdienstleister rechtzeitig informiert werden, um eine erneute Risikoanalyse vornehmen zu können, insbesondere wenn die Gefahr besteht, dass vertragliche Vereinbarungen durch ihn nicht mehr eingehalten werden können
- Das Finanzunternehmen muss den IKT-Drittdienstleister verpflichten, die wesentlichen Änderungen erst dann durchzuführen, wenn sie von ihm **genehmigt** wurden; zudem können Änderungsvorschläge eingebracht werden
- Sollte der IKT-Drittdienstleister trotz Widerspruch oder ohne Zustimmung des Finanzunternehmens Änderungen an den Subauslagerungsvereinbarungen vornehmen, so besteht, unbeschadet der Beendigungsklauseln, das Recht, den Vertrag mit dem IKT-Drittdienstleister zu **kündigen** (Art. 7)
- Gleiches gilt, wenn die Subauslagerung an einen Dienstleister erfolgt, die nach der vertraglichen Vereinbarung nicht hätte erfolgen dürfen

RTS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen

RTS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen (Art. 20 lit. a)

Überblick

Wesentliche Aspekte

- DORA hat zum Ziel, das Meldewesen für IKT-Vorfälle und erhebliche Cyberbedrohungen in der EU zu harmonisieren
- Der RTS- als auch der ITS-Entwurf (Art. 20 lit. b) berücksichtigen das Prinzip der **Verhältnismäßigkeit,** im Sinne der Kohärenz wurden die **Fristen** für die Meldung von Vorfällen an die EU-VO 2022/2555 („**NIS 2**“) angeglichen
- Der **Inhalt der Meldung über schwerwiegende IKT-Vorfälle** wurde präzisiert, eine detaillierte Beschreibung der Informationsarten und Anweisungen zum Ausfüllen der Meldung finden sich im Anhang zum ITS
- Insgesamt sind **101 Datenpunkte** umfasst, die folgende Themen umfassen:
  - Allgemeine Informationen des Finanzunternehmens
  - Auswirkungen des Vorfalls
  - Erfüllte Klassifizierungskriterien
  - Umgang mit dem Vorgang
  - Ursache des Vorfalls
  - Maßnahmen zur künftigen Prävention

Im Sinne der Verhältnismäßigkeit sind nur etwa **46%** der Datenfelder **obligatorisch**, die übrigen sind bedingt, abhängig von Art und Beschaffenheit des Vorfalls

Ein Großteil der Informationen ist erst in der Zwischen- bzw. Abschlussmeldung (z.B. Ursachenanalyse, Maßnahmen) zu berichten (insb. für kleine Unternehmen ein Vorteil)

- Für den **Inhalt der (freiwilligen) Meldung erheblicher Cyberbedrohungen** wird eine kurze und einfache Vorlage bereitgestellt, die nur die wichtigsten Datenfelder umfasst, die größtenteils bedingt sind
- Sofern die **Fristen** nicht eingehalten werden können, gewährt Art. 4 ITS Flexibilität ➔ die Finanzinstitute müssen dafür die zuständigen Behörden umgehend informieren und die Gründe der Verzögerung erläutern
- **Kleine Unternehmen**, die als unbedeutend eingestuft werden und wo der Vorfall keine systemischen oder grenzüberschreitenden Auswirkungen hat, müssen keine Zwischen- und Abschlussmeldung während des **Wochenendes oder an Feiertagen** vornehmen ➔ hier kann die Meldung in der ersten Stunde des Werktags danach erfolgen (Art. 6 Abs. 2 und 3 RTS)

Mit der Einrichtung von Verfahren zur Identifikation und Meldung schwerwiegender IKT-Vorfälle sollte bereits jetzt gestartet werden

Inhalte des RTS:

a) **Allgemeine Meldeerfordernisse** und **Inhalt** der Meldung über **schwerwiegende IKT-Vorfälle**

b) **Fristen** für die Erst-, Zwischen- und Abschlussmeldung

c) **Inhalt** der Meldung erheblicher **Cyberbedrohungen**

Inhaltsverzeichnis

RTS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen (Art. 20 lit. a)

Fristen und Inhalt der Meldung über schwerwiegende IKT-Vorfälle

Fristen

Art. 6 (1) lit. a RTS

Erstmeldung

So früh wie möglich **innerhalb 4h ab Klassifizierung als schwerwiegend**; nicht später als **24h** ab Kenntnisnahme

Art. 6 (1) lit. b RTS

Zwischenmeldung

Innerhalb von **72h ab Klassifizierung als schwerwiegend**, oder bereits früher, wenn folgende **Auslöser** erfüllt sind:

- Der normale Geschäftsbetrieb ist wiederhergestellt
- Status des ursprünglichen Vorfalls hat sich wesentlich geändert (Art. 19 Abs. 4)
- Veränderte Handhabung des Vorfalls aufgrund neuer Informationen (Art. 19 Abs. 4)

Eine **Aktualisierung** der Zwischenmeldung ist erforderlich:

- sofern eine relevante Statusaktualisierung verfügbar ist (Art. 19 Abs. 4)
- auf Verlangen der zuständigen Behörden (Art. 19 Abs. 4)

Art. 6 (1) lit. c RTS

Abschlussmeldung

Spätestens **1 Monat (30 Tage) ab Klassifizierung als schwerwiegend**

*Inhalt**

Art. 2 RTS **Allgemeine Informationen**

Art der Meldung, Name, Art und LEI des Finanzunternehmens; Kontaktdaten der verantwortlichen Person im Institut oder eines Dritten, der im Namen des Finanzinstituts meldet; ggf. Angabe des Mutternunternehmens der Gruppe; Währung

Art. 3 RTS

Datum und Uhrzeit der Kenntnisnahme und Klassifizierung des Vorfalls; Klassifizierungskriterien, die die Meldung ausgelöst haben; potentiell betroffene Mitgliedsstaaten, Informationen über den Ursprung; (potentielle) Auswirkungen auf andere FI/Drittdienstleister; wiederkehrender Vorfall (?), Angaben zur Aktivierung des BCM-Plans

Art. 4 RTS

Datum/Uhrzeit des Eintritts; Datum/Uhrzeit der Wiederherstellung des Geschäftsbetriebs; Referenzcode; Art des Vorfalls; Informationen über die Klassifizierungskriterien; Informationen, wie der Vorfall entdeckt wurde; (potentielle) Auswirkungen auf andere Finanzunternehmen/Drittdienstleister; betroffene Funktionsbereiche/Geschäftsprozesse; betroffene Infrastrukturkomponenten; Angaben zur Kommunikation mit Kunden/Finanzpartnern; ggf. Information über die Meldung an Strafverfolgungs- und andere Behörden; wiederkehrender Vorfall / früherer Vorfall (?); temporäre Maßnahmen; Angabe, ob der Vorfall von Drittdienstleister oder einem anderen FI ausgeht; ggf. ausgenutzte Schwachstellen / Indikatoren für Kompromittierung

Art. 5 RTS

Datum/Uhrzeit der endgültigen Behebung; Angabe zu direkten und indirekten Kosten und Verlusten und finanzieller Erholung; Angaben zur Unfähigkeit gesetzl. Anforderungen zu erfüllen; Angaben zur Verletzung vertraglicher Vereinbarungen/SLAs; Angaben zu Maßnahmen und Aktionen zur Behebung sowie zusätzliche Kontrollen, um derartige Vorfälle künftig zu verhindern; sonstige relevante Informationen; ggf. Neueinstufung in einen nicht-schwerwiegenden Vorfall

* Detailausführungen finden sich in Anhang II des ITS zur Festlegung eines Standardformats für die Meldung schwerwiegender IKT-Vorfälle

RTS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen (Art. 20 lit. a)

Inhalt der (freiwilligen) Meldung erheblicher Cyberbedrohungen

Bei **erheblichen Cyberbedrohungen** wurde der **freiwillige Charakter** der Meldung berücksichtigt, die Vorlage ist daher einfach und kurz gehalten, um zur Einmeldung zu motivieren:

INHALT*

Art. 7 RTS

- **Datum / Uhrzeit der Kenntnisnahme der Cyberbedrohung**
- **Beschreibung der erheblichen Cyberbedrohung**
- **Information über potentielle Auswirkungen**
- **Klassifizierungskriterien für potentielle Vorfälle**
- **Status der Cyberbedrohung**
- **Maßnahmen, die ergriffen wurden, um die Verwirklichung der Bedrohung zu verhindern**
- **Benachrichtigung anderer Beteiligter**
- **Indikatoren für eine Kompromittierung**

* Detailausführungen finden sich in Anhang IV des ITS zur Festlegung eines Standardformats für die Meldung schwerwiegender IKT-Vorfälle

ITS zur Festlegung eines Standardformats für die Meldung von schwerwiegenden IKT-Vorfällen

ITS zur Festlegung eines Standardformats für die Meldung schwerwiegender IKT-Vorfälle (Art. 20 lit. b)

Überblick

Wesentliche Aspekte

- Erst-, Zwischen- und Abschlussmeldung sind in **einer gesamthaften Vorlage** (Anhang I) abgedeckt
- Der Anhang II des ITS-Entwurfs enthält **Datenglossare, Charakteristiken der Datenfelder sowie Anweisungen**, wie die jeweiligen Vorlagen zur Meldung schwerwiegender IKT-Vorfälle (siehe Grafiken unten) und erheblicher Cyberbedrohungen auszufüllen sind
- Beim Ausfüllen der jeweils nächsten Meldung sollen Informationen der vorherigen, falls relevant, aktualisiert werden
- Die Meldung soll zudem grundsätzlich auf **Einzelbasis** (und nicht auf konsolidierter Ebene) erfolgen
- Sofern mehrere Finanzunternehmen einer Unternehmensgruppe die Meldung über schwerwiegende IKT-Vorfälle an Drittdienstleister auslagern (Art. 19 Abs. 5), so kann der Drittdienstleister nach Vereinbarung zwischen dem Finanzunternehmen und der zuständigen Behörde einen **einzigen Bericht auf nationaler Ebene** für die von derselben zuständigen Behörde beaufsichtigten Finanzinstitute erstellen
- Für Fälle, in denen der Vorfall schnell genug erkannt, bewertet und gelöst wurde, können alle Meldungen mit einer Vorlage **in einer einzigen Übermittlung** erfolgen

ANNEX I

Templates for the reporting of major incidents

Number of field	Data field	
	General information about the financial entity	
1.1	Type of report	
1.2	Name of the entity submitting the report	
1.3	LEI of the entity submitting the report	
1.4	Type of the entity submitting the report	
1.5	Name of the financial entity affected	
1.6	Type of financial entity affected	
1.7	LEI code of the financial entity affected	
1.8	Primary contact person name	
1.9	Primary contact person email	
1.10	Primary contact person telephone	
1.11	Second contact person name	
1.12	Secondary contact person email	
1.13	Second contact person telephone	
1.14	Name of the ultimate parent undertaking	
1.15	LEI code of the ultimate parent undertaking	
1.16	Name of affected third party providers	
1.17	LEI code of affected third party providers	
1.18	Reporting currency	
	Content of the initial notification	
2.1	Date and time of detection of the incident	

ANNEX II

Data glossary and instructions for the reporting of major incidents

Data field	Description	Instructions	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
General information about the financial entity						
1.1. Type of report	Indicate the type of incident notification or report being submitted to the competent authority.		Yes	Yes	Yes	Choice: a) initial notification b) intermediate report c) final report
1.2. Name of the entity submitting the report	Full legal name of the entity submitting the report		Yes	Yes	Yes	Alphanumeric
1.3. LEI of the entity submitting the report	Legal Entity Identifier (LEI) of the entity submitting the report assigned in accordance with the International Organisation for Standardisation. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.		Yes	Yes	Yes	Alphanumeric
1.4. Type of the entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report		Yes	Yes	Yes	Choice (multiselect) from the pre-defined list of DORA financial entities.

Als Beispiel: das in der Standardvorlage für die Meldung schwerwiegende IKT-Vorfälle (Anhang 1) auszufüllende Datenfeld „1.1 Type of report" wird in Anhang II näher konkretisiert

Inhalte des ITS:

a) Standardformulare und Vorlagen zur Meldung von schwerwiegenden IKT-Vorfällen und erheblichen Cyberbedrohungen

b) Meldeerfordernisse

Inhaltsverzeichnis

GL für die Schätzung der aggregierten Kosten und Verluste verursacht durch schwerwiegende IKT-Vorfälle

GL für die Schätzung der aggregierten Kosten und Verluste durch schwerwiegende IKT-Vorfälle

Ziel ist eine höhere Vergleichbarkeit durch einen einheitlichen Bewertungsansatz quer über die DORA-Mandate

Wesentliche Aspekte

Finanzunternehmen (ausgenommen Kleinstunternehmen) müssen auf Anfrage den zuständigen Behörden die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-Vorfälle verursacht wurden, melden (Art. 11 Abs. 10), Art. 11 Abs. 11 mandatiert die ESAs, dafür eine entsprechende Richtlinie auszuarbeiten

Einheitlicher Bewertungsansatz

Die GL empfiehlt einen einheitlichen Bewertungsansatz der Brutto-/Nettokosten und -verluste folgender **DORA-Mandate:**

- RTS zur Bewertung und Klassifizierung von IKT-Vorfällen (Art. 18 Abs. 3)
- RTS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen sowie ITS zur Festlegung eines Standardformats (Art. 20)
- GL für die Schätzung der aggregierten Kosten und Verluste durch schwerwiegende IKT-Vorfälle (Art. 11 Abs. 11)

➔ Die GL schafft keinen neuen Bewertungsansatz, sondern berücksichtigt jene in den anderen beiden RTS

Geschäftsjahr

Art. 11 Abs. 10 macht keine Angaben zu Start- und Endzeitpunkt des einjährigen Referenzzeitraums; die ESAs erachten das **Geschäftsjahr** des Finanzunternehmens als sinnvollste Variante, da die Schätzung auf der Grundlage der verfügbaren Zahlen aus den validieren Jahresabschlüssen basieren kann

Schwerwiegende IKT-Vorfälle mit Abschlussmeldung

Einbezogen werden sollen nur als **schwerwiegend** klassifizierte IKT-Vorfälle, für die eine **Abschlussmeldung** (Art. 19 Abs. 4 lit. c)

- im aktuellen Geschäftsjahr oder
- in einem vergangenen Geschäftsjahr erfolgt ist, wenn dies einen Einfluss auf die Kosten und Verluste des aktuellen Geschäftsjahres hat (Hinweis: Stichtag für die Einbeziehung des IKT-Vorfalls ist die Einreichung der Abschlussmeldung)

Aufschlüsselung der Positionen

Eine **Aufschlüsselung** der Bruttokosten und -verluste, der finanziellen Erholungen und der Nettokosten und -verluste nach schwerwiegenden IKT-Vorfällen soll den zuständigen Behörden den Vergleich der Kosten- und Verlustentwicklung der Finanzinstitute über die Jahre und die Nachvollziehbarkeit der Zahlen gewährleisten

GL für die Schätzung der aggregierten Kosten und Verluste durch schwerwiegende IKT-Vorfälle

Ziel ist eine höhere Vergleichbarkeit durch einen einheitlichen Bewertungsansatz quer über die DORA-Mandate

Wesentliche Aspekte

Die DORA-Mandate verfolgen **unterschiedliche Zwecke,** bauen jedoch nach dem „**Schichtprinzip**“ aufeinander auf:

Einheitlicher Bewertungsansatz

Annex: Reporting template for gross and net costs and losses in an accounting year

Name of the financial entity					
Start and end date of accounting year of the financial entity					
Reporting currency					
Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the accounting year	Recoveries of the incident in the accounting year	Net costs and losses of the incident in the accounting year
1					
2					
...					
Aggregated annual costs and losses	----------	----------			

1

RTS zur Bewertung und Klassifizierung von IKT-Vorfällen

- Mitunter ein Kriterium für die Einstufung des Vorfalls als schwerwiegend ist die potentielle wirtschaftliche Auswirkung (Schwellenwert 100.000 EUR)
- Angabe der Kosten / Verluste auf **Bruttobasis**, da kurz nach dem Vorfall die finanzielle Erholung noch nicht abschätzbar ist
- **Art. 7 Abs. 1 und Abs 2. RTS** definieren die Arten von Kosten, die berücksichtigt werden sollen; dabei sind nur jene relevant, die über die gewöhnliche Geschäftstätigkeit hinausgehen

2

RTS und ITS zur Präzisierung der Meldung von schwerwiegenden IKT-Vorfällen

- Erfordern die Einschätzung des **materialistischen Schadens**
- Neben den Brutto- **müssen auch die Nettokosten und -verluste** unter Berücksichtigung der **finanziellen Erholung** (siehe Anhang II, Reihe 4.24 des ITS) berichtet werden, da bei Vorlage des **Abschlussberichts** (Art. 19 Abs. 4 lit. c) Bruttozahlen allein ein verzerrtes Bild der finanziellen Auswirkungen geben könnten

3

GL für die Schätzung der aggregierten Kosten und Verluste durch schwerwiegende IKT-Vorfälle

- Zusammenfassung **aller** geschätzten Kosten und Verluste von schwerwiegenden IKT-Vorfällen innerhalb eines Geschäftsjahres
- Die Schätzung basiert auf der Klassifizierung von IKT-Vorfällen als schwerwiegend und der anschließenden Bewertung der wirtschaftlichen Auswirkung (als Nettokosten und -verluste)

RTS und GL mit Fokus auf den Aufsichtsrahmen

GL für die Kooperation zwischen den ESAs und den zuständigen Behörden hinsichtlich der Struktur der Überwachung von IKT-Drittdienstleister (Art. 32 Abs. 7)

Wesentliche Aspekte

Art. 32 Abs 7 mandatiert die ESAs, Leitlinien für die Zusammenarbeit zwischen den ESAs und den zuständigen Behörden zu erstellen, die detaillierte Verfahren und Bedingungen für die Zuweisung und Ausführung von Aufgaben zwischen zuständigen Behörden und den ESA sowie die Einzelheiten zum Austausch von Informationen regeln, die zuständige Behörden benötigen, um die Weiterbehandlung der in Art. 35 Abs. 1 lit. d genannten Empfehlungen zu gewährleisten, die an kritische IKT-Drittdienstleister gerichtet werden.

1 Allgemeine Erwägungen
Themen wie Sprache, Kommunikationsmittel, Kontaktstellen, Meinungsverschiedenheiten

2 Benennung kritischer IKT-Drittdienstleister
Informationsaustausch zwischen der FÜ, den zuständigen Behörden und dem Aufsichtsforum im Zusammenhang mit der Benennung kritischer IKT-Drittdienstleister

3 Aufsichtstätigkeiten
Verfahren und Informationsaustausch im Zusammenhang mit dem jährlichen Aufsichtsplan, allgemeine Untersuchungen und Vor-Ort-Prüfungen sowie Maßnahmen der zuständigen Behörde in Bezug auf kritische IKT-Drittdienstleister im Einvernehmen mit der FÜ

4 Weiterverfolgung der Empfehlungen
Informationsaustausch zwischen der FÜ und den zuständigen Behörden, um die Weiterverfolgung der Empfehlungen und der Entscheidung der zuständigen Behörden, von den Finanzunternehmen zu verlangen, ihren IKT-Drittdienstleistervertrag auszusetzen/zu kündigen, zu gewährleisten

- **Aufsichtliche Zusammenarbeit**: die GL behandelt nur die Zusammenarbeit zwischen ESAs und den zuständigen Behörden
- **Ziel:** kohärenter und koordinierter Ansatz im Rahmen der Aufsichtstätigkeiten, um Doppelarbeit und Überschneidungen bei der Durchführung von Maßnahmen zur Überwachung zu vermeiden

RTS zur Präzisierung der Durchführung der Überwachung von IKT-Drittdienstleistern (Art. 41)

Überblick

Wesentliche Aspekte

Mit DORA wurde ein europaweiter Aufsichtsrahmen für kritische IKT-Drittdienstleister geschaffen. Art. 41 mandatiert die ESAs, über den Gemeinsamen Ausschuss die Struktur des Überwachungsrahmens für kritische IKT-Drittdienstleister, Art und Umfang der Informationen sowie Berichtsinhalte zu spezifizieren.

- Hauptziel des Entwurfs ist die **Harmonisierung der Anforderungen** in allen Vorschriften und die Einführung **effizienter Aufsichtsbedingungen** für kritische IKT-Drittdienstleister, Finanzunternehmen und Aufsichtsbehörden in der gesamten EU
- Dieses Mandat wird in **zwei verschiedene RTS** aufgeteilt: Jener des gemeinsamen Untersuchungsteams (Art. 41 Abs. 1 lit. c) wird nach einem anderen Zeitplan und unter Einbeziehung der kürzlich eingerichteten High Level Group on Dora („**HLGO**“) gesondert spezifiziert werden
- Die **federführenden Überwachungsbehörde (FÜ)** hat umfassende Befugnisse in Bezug auf IKT-Drittdienstleister, so z.B. die Möglichkeit, von diesen alle relevanten Informationen und Unterlagen anzufordern, als auch nach Art. 35 Abs. 1 lit. c Berichte hins. der durch den IKT-Drittdienstleister ergriffenen Maßnahmen anzufordern. Diese Berichte sollen aus **Zwischen- und Abschlussberichten** bestehen (inkl. Fortschritt und belegenden Dokumenten)

➢ Bzgl. der Folgemaßnahmen zu den Empfehlungen haben die FÜ und die zuständigen Behörden eine sich **ergänzende Verantwortung**:

- ➢ **Zuständige Behörden** ➔ verantwortlich für die Weiterverfolgung der in den Empfehlungen der FÜ aufgezeigten Risiken bei den durch sie beaufsichtigten Finanzunternehmen
- ➢ **FÜ** ➔ zuständig für die Überwachung der Umsetzung der an die IKT-Drittdienstleister gerichteten Empfehlungen

Bei **schwerwiegenden Risiken**, die eine große Anzahl von Finanzunternehmen in mehreren EU-Mitgliedstaaten betreffen, sollten die zuständigen Behörden auf Ersuchen relevante Informationen über ihre Bewertung der festgestellten Risiken mit der FÜ teilen

1. (vorliegender) RTS
(Art. 41 lit. a, b, d)
➔ direkte Auswirkungen auf **Finanzunternehmen** und **kritische IKT-Drittdienstleister**

2. (erwarteter) RTS
(Art. 41 lit. c)
➔ Anforderungen, die von den **zuständigen Behörden** in Bezug auf das gemeinsame Untersuchungsteam zu befolgen sind

Inhaltsverzeichnis

RTS zur Präzisierung der Durchführung der Überwachung von IKT-Drittdienstleistern (Art. 41)

Die Inhalte des Art. 41 Abs. 1

Wesentliche Aspekte

lit. a

Informationen für einen freiwilligen Antrag nach Art. 31 Abs. 11

Einstufung als **kritischer** IKT-Drittdienstleister entweder durch ESA über Benennungsverfahren nach Art. 31 Abs. 1 lit. a oder über freiwilligen Antrag gem. Abs. 11; der Antrag muss vollständig ausgefüllt sein, da er ansonsten zurückgewiesen wird

➔ **Art. 1 RTS** enthält **abschließende Aufzählung von Informationen**, die der Antrag enthalten muss

lit. b

Inhalt, Struktur und Format der Informationen nach Art. 35 Abs. 1, einschl. der Vorlage für die Bereitstellung von Informationen zu Unteraufträgen

Die FÜ kann alle zur Erfüllung ihrer Aufgaben erforderlichen Informationen vom IKT-Drittdienstleister anfordern

➔ **Art. 3 RTS** regelt den **Inhalt** dieser Informationen

➔ **Art. 4 RTS** bezieht sich auf Art. 35 Abs. 1 lit. c (Bericht über ergriffene Maßnahmen) und ermächtigt die FÜ, Zwischenberichte (inkl. Umsetzungsfortschritt, Belegen) sowie Abschlussberichte zu verlangen

➔ **Art. 5 RTS** regelt **Struktur und Format** der Übermittlung der Informationen (auf Englisch) in Art. 3 RTS

➔ **Art. 6 RTS** bezieht sich auf Informationen zu Subauslagerungen, ein entsprechendes Muster findet sich in **Anhang I**

lit. c

Kriterien für die Zusammensetzung des gemeinsamen Untersuchungsteams

➔ wird in einem separaten **zweiten RTS** geregelt

lit. d

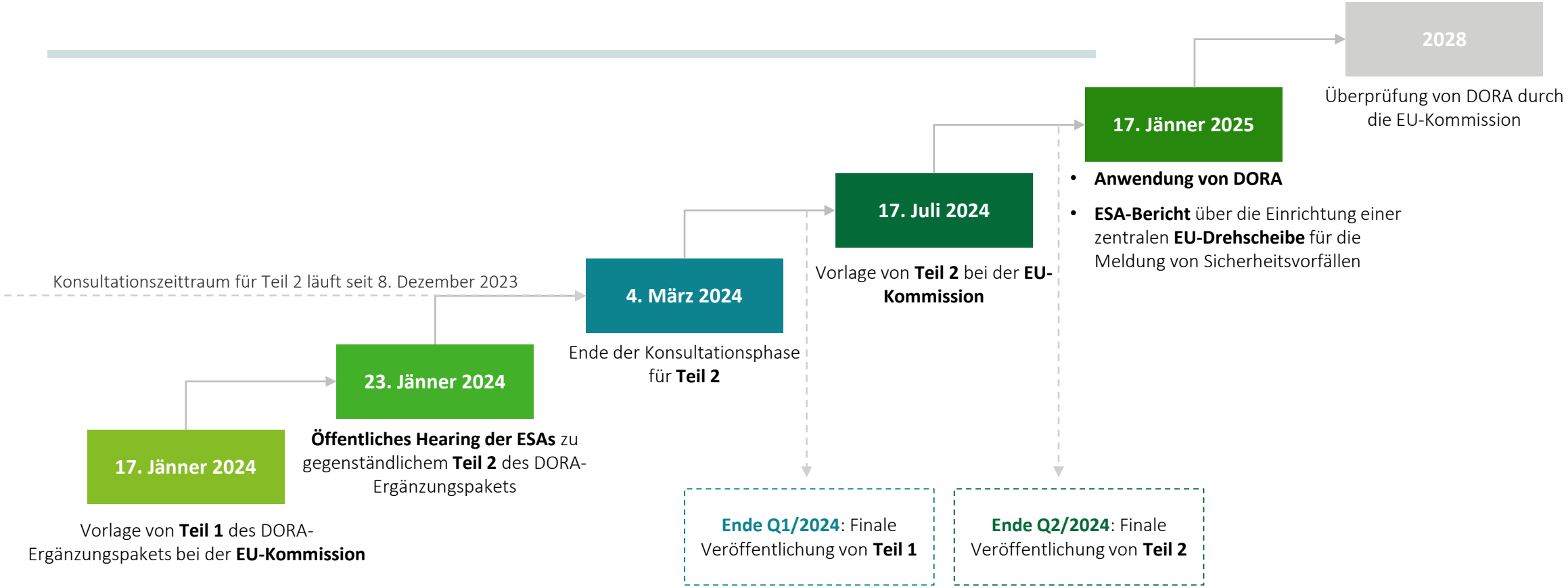
Einzelheiten der Bewertung der Maßnahmen nach Art. 42 Abs. 3

➔ **Art. 7 RTS** legt die Erfordernisse fest, anhand derer die zuständigen Behörden die Maßnahmen der IKT-Drittdienstleister (auf Grundlage der Empfehlungen der FÜ) bewerten, sie befolgen dabei einen risikobasierten Ansatz und den Grundsatz der Verhältnismäßigkeit

Ausblick

Nächste Schritte: Wie geht es weiter?

Zeitplan



- RTS zum Risikomanagementrahmenwerk und RTS zur Vereinfachung für kleine Institute
- RTS zur Bewertung und Klassifizierung von IKT-Vorfällen
- RTS zur Spezifizierung der Outsourcing-Policy für IKT-Dienste
- ITS zum Informationsregister für ausgelagerte bzw. extern beauftragte IKT-Dienste

Ansprechpartner

Deloitte – Audit and Assurance | TechCompliance & Payments | Risk Advisory

Bleiben wir in Kontakt

Alexander Ruzicka
Partner | Audit and Assurance
Specialized Controls Assurance

Tel: +43 1 537 00 7950
Mobil: +43 664 80 537 7950
aruzicka@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Thomas John
Senior Manager | Audit and Assurance
TechCompliance & Payments

Tel: +43 1 537 00 3723
Mobil: +43 664 80 537 3723
tjohn@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Julia Kitzmüller
Manager | Audit and Assurance
TechCompliance & Payments

Tel: +43 1 537 00 3779
Mobil: +43 664 80 537 3779
jkitzmueller@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Bei Fragen oder Anliegen zu den präsentierten Sachverhalten oder damit in Verbindung stehenden Themenbereichen kontaktieren Sie gerne auch unser TechCompliance Team unter

AT TechCompliance
(attechcompliance@deloitte.com)

Deloitte.

Backup

Finalentwurf des 1. DORA-Ergänzungspakets vom 17.01.2024

Überblick zu Änderungen

Wesentliche Aspekte

1. RTS zur Klassifizierung von schwerwiegenden IKT-Vorfällen

- **Änderung im Klassifizierungsansatz**:
  Das Klassifizierungskriterium "kritische Dienste betroffen" ist zwingende Voraussetzung für die Einstufung eines Vorfalls als schwerwiegend. Zusätzlich muss/müssen
  - ein böswilliger unbefugter Zugriff auf Netz- und Informationssysteme im Rahmen des Kriteriums "**Datenverlust**" festgestellt werden oder
  - die Schwellenwerte von **zwei weiteren Kriterien** überschritten werden (siehe Grafik)
- **Vereinfachung der Klassifizierungskriterien und Anpassung Schwellenwerte**: Spezifizierungen/Änderungen in den Kriterien "betroffene Kunden“ (z.B. Schwellenwert von 50.000 auf 100.000 angehoben), „finanzielle Gegenpartei“, „Transaktionen" sowie "Datenverluste", um Verhältnismäßigkeit und sektorspezifische Fragen zu adressieren sowie um relevante Cyber-Vorfälle zu erfassen
- **Neuer Ansatz für wiederkehrende Vorfälle**: dieser konzentriert sich nun auf Vorfälle, die mindestens zweimal aufgetreten sind, dieselbe offensichtliche Ursache haben und kumulativ die Kriterien für die Klassifizierung von Vorfällen erfüllt haben. Die Bewertung der Wiederholung ist monatlich vorzunehmen.

2. RTS zur Spezifizierung der Outsourcing-Policy für IKT-Dienste

- keine wesentlichen Änderungen

3. RTS zum Risikomanagementrahmenwerk und RTS zur Vereinfachung für kleine Institute

- Stärkerer Fokus auf **Verhältnismäßigkeit** und **risikobasierten Ansatz**
- **Streichung spezifischer Artikel** (Governance, Information Security Awareness) aus den allgemeinen Anforderungen
- **Präzisierung von Bestimmungen** in Bezug auf Netzsicherheit, Verschlüsselung, Zugangskontrolle und Business Continuity
- **Umgang mit Cloud Computing**: Entscheidung auf der Grundlage der Technologieneutralität keine technologiespezifischen Anforderungen einzuführen und Anforderungen in Bezug auf IKT-Vermögenswerte oder -Dienstleistungen, die von IKT-Drittanbietern erbracht werden, allgemein festzulegen
- **Mögliche weitere Leitlinien**: Erwägung weiterer Leitlinien zu den Bereichen, die gestrichen wurden sowie zu Sicherheitsaspekten des Cloud Computing.

4. ITS zum Informationsregister für ausgelagerte bzw. extern beauftragte IKT-Dienste

- **Vereinfachung**: Informationsregister wurde gestrafft und Anzahl der Spalten (Menge an Informationen) reduziert bzw. bedingt
- **Frühere Vorlagen** zu RT.05.03 in (Allgemeine Angaben zu alternativen IKT-Drittdienstleistern) und RT.07.01 (Identifikation von IKT-Dienstleistungen) **entfernt**
- **Eine Vorlage** für Unternehmens- als auch (sub-)konsolidierte Ebene
- **Ergänzung von 3 kleinen technische Vorlagen** (die nur Schlüssel enthalten), um effiziente Verwaltung der Informationen im Informationsregister zu gewährleisten.

Klassifizierung schwerwiegender IKT-Vorfälle - Übersichtstabelle

Table 1: Overview of the classification criteria and their thresholds for major incidents under DORA as introduced in the final draft RTS

	Major ICT-related Incident or security or operational payment-related incident if critical services are affected and (i) any malicious unauthorised access to network and information systems identified, which may result to data losses or (ii) the thresholds of two additional criteria from the below are met						
	Mandatory condition	**Additional classification criteria**					
	Critical services affected	**Clients, financial counterparts and transactions**	**Data losses**	**Reputational Impact**	**Duration and Service Downtime**	**Geographical Spread**	**Economic Impact**
Materiality threshold	**The incident has had any impact on critical services**	Any of: a) **>10% of all clients** using the affected service; b) **>100 000 clients** using the **affected** service; c) **>30% of all financial counterparts** used by the FE; d) **>10%** of the daily average number of **transactions;** e) **>10%** of the daily average amount of **transactions;** f) any **identified impact on clients or financial counterpart** identified by the FE as relevant.	**Any impact on the availability, authenticity, integrity or confidentiality of data,** which has or will have an **adverse impact** on the implementation of the **business objectives** of the FE or on **meeting regulatory requirements**	Any **reputational impact set out in Article 2 a) to d)** **(overview below)**	a) **incident duration** is **longer than 24 hours;** or b) **service downtime** is **longer than 2 hours for** ICT services that support critical or important functions	**Any impact** of the incident identified in the territories of at **least two Member States**	Costs and losses incurred by the FE **exceed** or are likely to exceed **€100 000** (can be based on estimates where actuals cannot be determined)
Criteria Detail	Assess if the incident : a) affects ICT services or Network and information systems that support **critical or important functions of the FE; or** b) affects financial services that require authorisation, registration or are otherwise supervised by competent authorities; or c) represents a successful, malicious and unauthorised access to the network and information systems of the financial entity.	**1. all affected clients unable to make use of the service** provided by the FE during the incident or that were **adversely impacted by the incident.** These include also third parties explicitly covered by the contractual agreement between the FE and the client as beneficiaries of the affected service. **2.** all affected **financial counterparts with contractual arrangements with the FE.** **3. relevant clients and financial counterparts** whose impact will affect the business objectives of the FE or market efficiency. **4.** all **affected transactions** with monetary amount, with one leg in the EU. (FEs can use **estimates** from comparable reference periods where actuals not available)	1. **availability** of data – data on demand rendered temporarily or permanently inaccessible or unusable; 2. **authenticity** of data – compromised trustworthiness of the source of data; 3. **integrity** of data – data inaccurate or incomplete due to non-authorised modification 4. **confidentiality** of data – data being accessed by or disclosed to unauthorised party or system.	**Reputational impact evidenced by any of the below:** **a) incident reflected in the media;** or b) received **repetitive complaints;** or c) inability **to meet regulatory requirements;** or d) **likely loss of clients or financial counterparts** with a material impact on FE's business. **Level of visibility** of the incident to be taken into account.	1. **Duration** measured from the moment an incident occurs or is detected, until it is resolved. (estimate if not yet known) 2. **Service downtime** measured from the moment service fully/ partially unavailable/ delayed to clients, financial counterparts or other internal or external users, until activities are restored to the same level before the incident.	**Assess significant** impact of the incident in **other EU Member States** on: a) **clients or financial counterparts;** b) **branches** of the FE or **other group financial entities;** (c) **Financial market infrastructures or third party providers** that may affect other FEs.	**Types of direct and indirect incurred costs** a) expropriated funds or financial assets liability, including theft; b) replacement or relocation costs; c) staff costs; d) contract non-compliance fees; e) customer redress and compensation costs; f) forgone revenues; g) communication costs; h) advisory costs. (based on available data at time of reporting)