



## **DORA in der Praxis**

Best-Practice-Lösungen für eine pragmatische Umsetzung

Wien, 19. Juni 2024

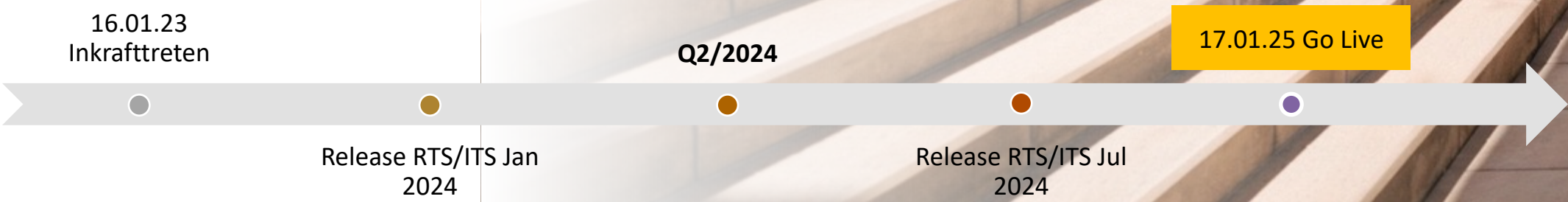
# DORA – WAS KOMMT AUF SIE ZU?

*Verordnung über die digitale  
operationale Resilienz  
im Finanzsektor*

**INHALT** – neue EU-Verordnung zur Verbesserung der Widerstandsfähigkeit des Finanzsektors gegenüber digitalen Risiken (u. a. Cyber-Risiken)

**ANSPRUCH** – Vereinheitlichung und Schärfung bestehender europäischer & nationaler Standards und Anforderungen an die Sicherheit der Informations- und Kommunikationstechnik (IKT)

**ZIEL** – detailliertes und umfassendes Rahmenwerk für die digitale Betriebsstabilität von Finanzunternehmen



# DORA – KERNTHEMEN

-  IKT-Risikomanagement
-  Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
-  Testen der digitalen operationalen Resilienz
-  Management des IKT-Drittparteiensrisikos
-  Vereinbarungen über den Austausch von Informationen

# „DORA-DREIKLANG“

Der Grad der Betroffenheit definiert den Geltungsbereich.

## GAP-ANALYSE

- Analyse Betroffenheitsgrad
- Sichtung der Richtlinien & relevanten Dokumente
- Experten-Interviews
- Analyse gegen die Anforderungen der DORA-Verordnung \*
- Ableitung von Handlungsempfehlungen
- ggf. Mapping auf Richtlinienstruktur

+ Best Practice Anforderungstool

ggf. + ISO 27001/2

**Erarbeitung der Maßnahmen zur Erreichung des Soll-Zustands**

## ANPASSUNG RICHTLINIEN

- Aufbau / Re-Organisation der Richtlinienstruktur
- inhaltlicher Aufbau der neuen Richtlinien bzw. Ergänzung bestehender Richtlinien
- Konformität mit der DORA-Verordnung (z. B. Wording, Begrifflichkeiten, Struktur)

+ Best Practice Templates

**Konzeptionierung der Richtliniendokumente und Prozesse**

## AUFSETZEN REGISTER/LISTE

- Informationsregister
- Risikoregister
- IKT-Asset-Liste
- BCM-Maßnahmenplan

## ANPASSEN ORGANISATION

- Tätigkeiten & Rollen

## PRÜFUNG VERTRÄGE

- Vertragsprüfung und -verhandlung

**Umsetzung der neuen und erweiterten Vorgaben**

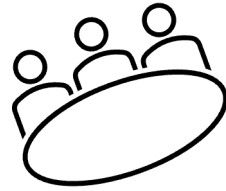
Grad der notwendigen Beistelleistungen des Kunden

\* Aufwände abhängig von der Betrachtung: Level-1-Anforderungen (nur DORA-Verordnung) oder Level-2-Anforderungen (DORA-Verordnung inkl. erster Batch RTS/ITS)

# VORGEHENSWEISE & ERGEBNISTYPEN GAP-ANALYSE



**Sichtung vorhandener Richtlinien**



**Durchführung von DORA-Interviews**



**Strukturierungsvorschlag für Richtlinien**



**Abgleich mit DORA-Anforderungen**  
(Grundlage ist die aktuelle veröffentlichte DORA-Verordnung)

**Umsetzungspunkte (Anforderungsliste) im Ampelsystem inkl. Ableitungen von Detail-Maßnahmen**

Mapping der Anforderungspunkte auf die bestehenden Richtlinien oder auf den Strukturierungsvorschlag für Richtlinien

**Aufbereitung der wesentliche Handlungspunkte für das Top-Management**

Beschreibung der Inhalte der Folgeprojekte zur Umsetzung der DORA-Konformität (in 2024) sowie der DORA-Operationalisierung (in 2025)

# DORA – GAP-ANALYSE ANFORDERUNGSTOOL (BEISPIEL)

## 1. Geltungsbereich

Bereitschaft / Unternehmen	Dynamik	Wann konkretisiert	Wann konkretisiert
Finanzunternehmen	Finanzunternehmen nach DORA Artikel 2 Absatz 1	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit
Finanzunternehmen, die TFTP durchzuführen müssen	Finanzunternehmen, die von den zuständigen Behörden als Unternehmen ermittelt wurden, die TFTP durchzuführen haben	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit
Finanzunternehmen, die als bedeutend eingestuft sind	Bedeutende Finanzunternehmen gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 504/2013 oder durch RT/ITS, weiter ausdifferenziert (Beispiele: Deutsche Bank, Commerzbank)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von Art. 19 Weidung von erheblichen Cyberbedrohungen
Zentrale Kreditgeber	Finanzunternehmen, die im Sinne von Artikel 2 Nummer 1 Nummer 1 der Verordnung (EU) Nr. 504/2013 zentrale Kreditgeber sind. (Beispiele: Clearstream Banking AG, Luxor Bank SA/NV)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von Art. 11 Absatz 3 (Zentrale Kreditgeber übermitteln den zuständigen Behörden Kopien der Ergebnisse der Tests, der ICT-Geschäftsfortführung oder ähnlicher Vorgehens)
Zentrale Gegenparteien (auch Zentraler Kontrahent (CCP) genannt)	Finanzunternehmen, die im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2013 eine Zentrale Gegenpartei sind. (Beispiele: Eurex Clearing AG, European Commodity Clearing AG)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von Art. 12 Abs. 3 (Die Wiederherstellungspläne ermöglichen die Wiederherstellung aller zum Zeitpunkt der Störung kritischen Transaktionen)
Datenbereitstellungsdienste	Finanzunternehmen, die nach Artikel 2 Absatz 1 Nummer 3a bis 3c der Verordnung (EU) Nr. 602/2014 ein Datenbereitstellungsdienst sind. (Beispiele: Deutsche Börse AG, Bloomberg Data Reporting Services Ltd)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von Art. 30 Abs. 4 (Verfahren darüber hinaus über Systeme, die Daten in einem zentralen Verzeichnis auf Vollständigkeit geprüft, Lücken und offensichtliche Fehler erkannt und eine Neubereitstellung angefordert werden können)
Einzelunternehmen	Finanzunternehmen, bei dem es sich nicht um einen Handlungszweig, eine zentrale Gegenpartei, ein Transaktionsgegner oder einen Zentralen Kontrahenten handelt, die weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. Bilanzsumme 2 Mio. EUR nicht überschreitet	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Keine Anwendung dieser Anforderungen: - Art 5 Abs. 3 (Governance und Digitalität) - Art 6 Abs. 4 (ICT-Risikomanagement) - Art 8 Abs. 3 + 7 (Berichterstattung von ICT-Vorfällen) - Art 11 Abs. 3, 5, 7, 10 (Reaktion und Wiederherstellung) - Art 13 Abs. 2 + 7 (Sensitivität und Weiterentwicklung) - Art 14 (Regelmäßige Tests/Überprüfungen) - Art 15 Abs. 1 (Testen von ICT-Tools und -Systemen) - Art 16 Abs. 2 (Allgemeine Pläne für das Management von ICT-Datenverlusten) - Nachfolgende Anwendung dieser Anforderungen: - Art 6 Abs. 5 (ICT-Risikomanagement) - Art 12 Abs. 6 (Berichtswesen/ Wiederherstellung und Wiederherstellung) - Art 20 Abs. 3 (Testen von ICT-Tools und -Systemen) - Art 30 Abs. 3 (Gründliche Vertragsüberprüfungen mit ICT-Datenverlusten)
Finanzunternehmen, für die der wesentliche ICT-Risikomanagementansatz gilt	Kleine und nicht-veflechtene Unternehmen, entsprechend der Richtlinie (EU) 2015/2366 ausgenommen Zahlvorgaben	Anwendung von Art. 16 - wesentliche ICT-Risikomanagementansätze	Keine Anwendung dieser Anforderungen: - Art 20 Abs. 1 + 3 (Allgemeine Testverfahren / Testprogramme) - Art 21 (Testen von ICT-Tools und -Systemen) - Art 29 (Durchführung von TFTP) - Art 30 Abs. 1 + 3 (Regelmäßige ICT-Datenüberprüfungen)
ICT-Dienstleister	Ein Unternehmen, das ICT-Dienstleistungen bereitstellt, über ICT-Systeme, -anwendungen, -rechner oder -netze, die für die Geschäftstätigkeit des Auftraggebers erforderlich sind, als Dienstleister und/oder als Dienstleister, wenn auch technische Unterstützung durch den Auftraggeber mittels Software- oder Hardware-Abhängigkeiten erfolgt, mit Ausnahme herkömmlicher analoger Telefonleitungen	Überwachung durch die Finanzunternehmen, für die die Dienstleistungen erbracht werden	Bei den Anforderungen an die ICT-Dienstleister muss durchzudenkt werden, ob die erbrachten ICT-Dienstleistungen kritische oder wichtige Funktionen des Finanzunternehmens unterstützen
Wesentliche ICT-Dienstleister	Ein ICT-Dienstleister, der gemäß Artikel 19 als kritisch eingestuft wurde	Überwachung durch die Finanzunternehmen, für die die Dienstleistungen erbracht werden	Überwachung gemäß DORA. Der mit dieser Überwachung einhergehende Aufwand ist geringfügig, falls ein ICT-Dienstleister als kritisch eingestuft wurde, und falls eine Ergänzung zur Berichterstattung gemäß der Richtlinie (EU) 2022/2536 betreffen werden, insbesondere die der Art. 20 und 21. 50
Finanzunternehmen	1) Bedeutende Finanzunternehmen im Sinne von Artikel 6 Absatz 4 der Richtlinie (EU) 2013/504 2) Zentraler Kreditgeber und zentrale Gegenpartei im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 504/2013 3) Zentraler Kontrahent im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2013 4) Datenbereitstellungsdienst im Sinne von Artikel 2 Absatz 1 Nummer 3a bis 3c der Verordnung (EU) Nr. 602/2014	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit

## 2. Anforderungsabgleich

The screenshot shows a complex software interface for DORA gap analysis. It features a main table with columns for 'Kapitel', 'Artikel', 'Absatz', 'Unterabs.', 'Buchst.', and 'Anforderung'. A detailed view of a requirement is shown in a pop-up window:

**Anforderung:** Durchführung einer Risikobewertung bei wesentlichen Änderungen der Netzwerk- und Informationssystemstruktur sowie an Prozessen und Verfahren mit Bezug zu ICT

**Bereich:** IT-Operations; IT-Sicherheit

**Fragen:**

- Wie wird festgelegt, wann Änderungen an der ICT-Infrastruktur wesentlich sind?
- Welche Pläne gibt es für die Risikoprüfung bei wesentlichen Änderungen?
- Wie wird die Risikoprüfung dokumentiert?

**Ergebnis:** Erfüllt teilweise erfüllt nicht erfüllt

**Erklärung / Begründung zur Entscheidung:** teilweise erfüllt nicht erfüllt in Abstimmung zukünftig zu beachten keine Relevanz in operativer Planung

Below the main table, there are several summary tables:

Ergebnisbereich	Anzahl	Anteil
Gesamt	336	95%
erfüllt	318	95%
teilweise erfüllt	18	5%
nicht erfüllt	0	0%

Operative Umsetzung:

Status / Kategorie	IT-Strategie	ICT-Risikomanagement	IRM	Infrastruktur	BCM	ICT-bezogene Vorfälle	ICT-Datenverluste	Gesamtanteil
erfüllt	1	1	1	1	1	1	1	1
teilweise erfüllt	1	1	1	1	1	1	1	1
nicht erfüllt	0	0	0	0	0	0	0	0

Best Practice

Bei mehr als 10 Kunden im Einsatz

inkl. RTS/ITS (Level 2 - Batch 1)

inkl. Mapping XAIT + ISO 27001/2

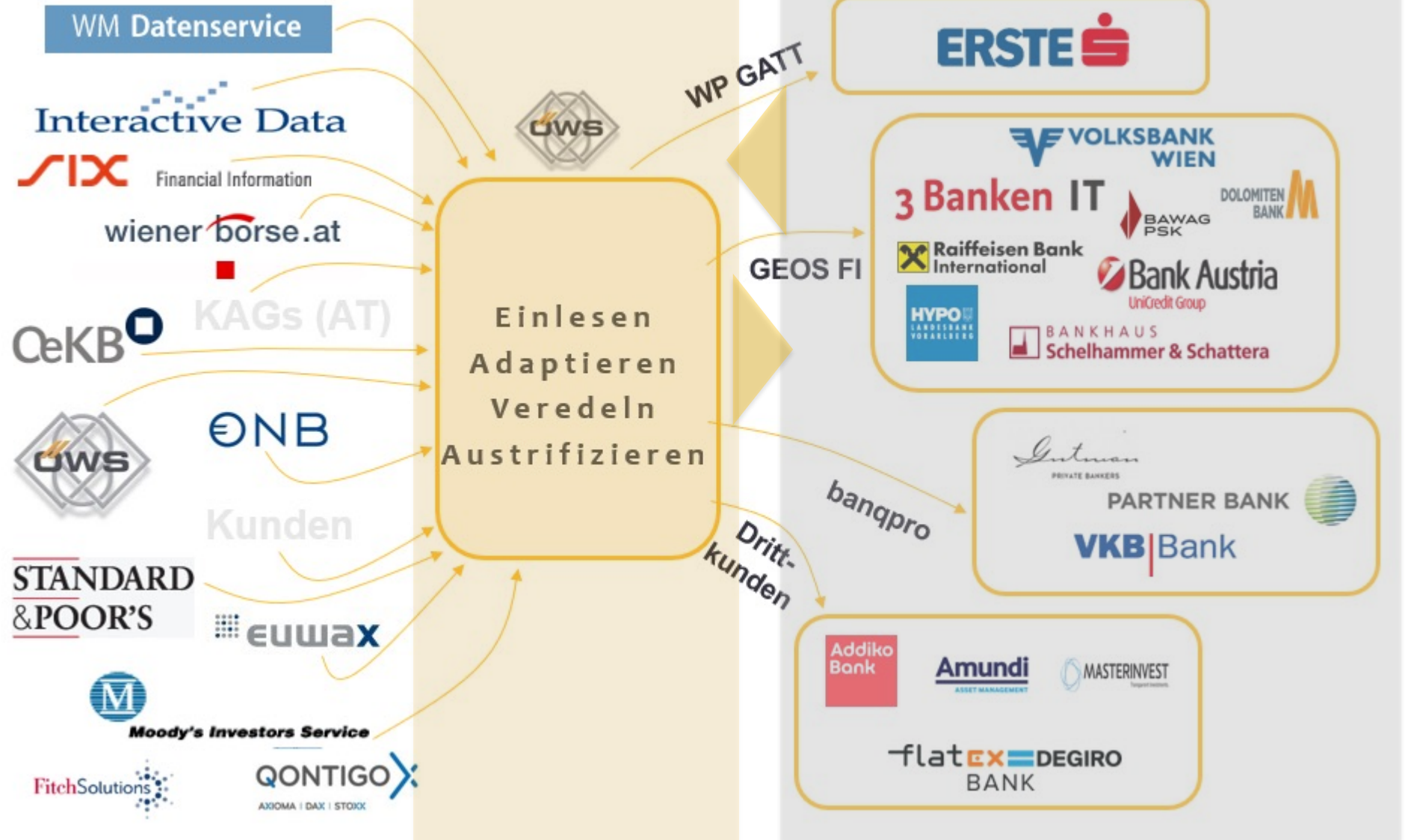
Gesamtübersicht über Kapitel/Status/Kategorien

Optional - DO IT YOURSELF



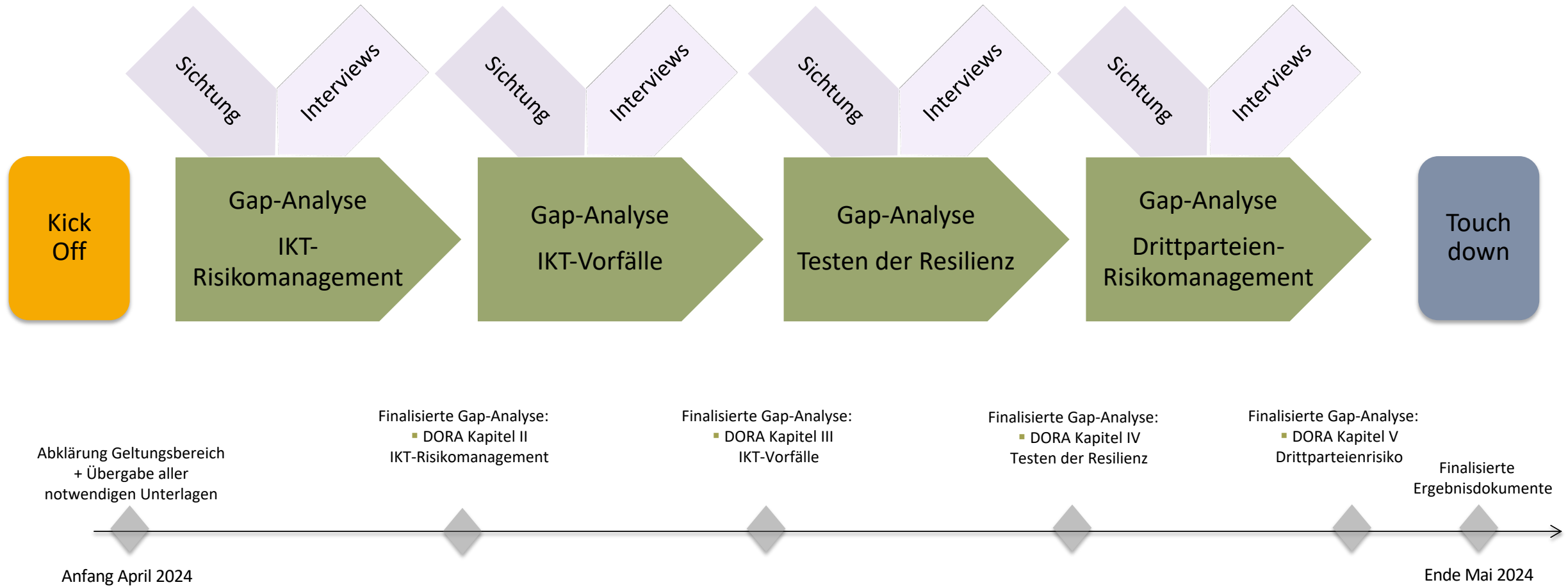
# ÖWS DORA GAP-Analyse

- Proaktive Umsetzung für unsere Kunden
- Pragmatisches und kompaktes Vorgehen
- Rechtzeitig DORA-Konformität herstellen
- GAP Analyse mit concededro für den organisatorisch-inhaltlichen Teil





# Vorgehen und Zeitleiste – ÖWS DORA GAP-Analyse





# DORA – GAP-ANALYSE ANFORDERUNGSTOOL (BEISPIEL ÖWS)

## 1. Geltungsbereich

Kategorie	System	Rechtsgrundlage
Finanzunternehmen	Finanzunternehmen nach DORA Artikel 2 Absatz 1	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit
Finanzunternehmen, die TFTP durchführen müssen	Finanzunternehmen, die von den zuständigen Behörden als Unternehmen ermittelt wurden, die TFTP durchführen haben	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit Anwendung von Art. 26 Durchföhrung von TFTP
Finanzunternehmen, die als bedeutend eingestuft sind	Bedeutende Finanzunternehmen gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 504/2013 oder durch RTSP/TS weiter ausgedefmt. (Beispiele: Deutsche Bank, Commerzbank)	Anwendung von Art. 19 Meldung von erheblichen Cyberbedrohungen Anwendung von Art. 28 Durchföhrung von TFTP
Zentraler Anbieter	Finanzunternehmen, die im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 909/2014 Zentralanbieter sind. (Beispiele: Clearstream Banking AG, Luxclear Bank SA/NV)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit plus Anwendung von Art. 11 Abs. 3 Zentralanbieter übermitteln die zuständigen Behörden Kopien der Ergebnisse der ICT-Geschäftsfortführung oder ähnlicher Vorgehenspläne Art. 22 Abs. 5 Besondere Anforderungen an den sekundären Wiederherstellungsprozess Anwendung von Art. 22 Abs. 2 Durchföhrung von Schwachstellenbewertungen VOR der Inbetriebnahme von Anwendungen (...)
Zentrale Gegenparteien	Finanzunternehmen, die im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2013 eine Zentrale Gegenpartei sind. (Beispiele: Euronext Clearing AG, Euronext Commodity Clearing AG (ECC))	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit plus Anwendung von Art. 22 Abs. 3 Die Wiederherstellungspläne ermöglichen die Wiederherstellung aller zum Zeitpunkt der Störung kritischen Transaktionen Anwendung von Art. 23 Abs. 2 Durchföhrung von Schwachstellenbewertungen VOR der Inbetriebnahme von Anwendungen (...)
Datenbereitstellungsdienste	Finanzunternehmen, die nach Artikel 2 Absatz 1 Nummer 3a bis 3c der Verordnung (EU) Nr. 602/2014 ein Datenbereitstellungsdienst sind. (Beispiele: Deutsche Börse AG, Bloomberg Data Reporting Services Ltd)	Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit plus Anwendung von Art. 30 Abs. 4 Verfügen darüber hinaus über Systeme, mit denen ein Datenanforderer Zugriff auf Informationen erhält, die für die Erfüllung der Aufgaben des Datenanforderers erforderlich sind Anwendung von Art. 32 Abs. 3 Unternehmen zu zusätzlich angemessene Ressourcen und Fähigkeiten (z.B. rechtliche, technische, Sicherheits- und Wiederherstellungsmaßnahmen, damit ihre Daten bereitgestellt und aufbewahrt werden können) Anwendung von DORA im Einklang mit dem Grundsatz der Verhältnismäßigkeit
Einzelunternehmen	Finanzunternehmen, bei dem es sich nicht um einen Handlungszweig, eine zentrale Gegenpartei, ein Transaktionsgegenüber oder einen Zentralanbieter handelt, die weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw. Bilanzsumme 2 Mio. EUR nicht übersteigt	Keine Anwendung dieser Anforderungen: - Art 5 Abs. 3 (Governance und Digitalisation) - Art 6 Abs. 4 (ICT-Risikomanagement) - Art 8 Abs. 3 (Identifizierung von ICT-Risikofaktoren) - Art 11 Abs. 3, 5, 7, 10 (Meldung von ICT-Risikofaktoren) - Art 13 Abs. 2 (IT-Service und Weiterentwicklung) - Art 24 (Regelmäßige Tests) - Art 25 Abs. 1 (Erstellen von ICT-Plänen und Systemen) - Art 26 Abs. 2 (Allgemeine Prinzipien für das Management von ICT-Drittanbietern) Wechselseitige Anwendung dieser Anforderungen: - Art 6 Abs. 5 (ICT-Risikomanagement) - Art 22 Abs. 6 (Beschwerde-Wiederherstellung und Wiederherstellung) - Art 25 Abs. 3 (Erstellen von ICT-Plänen und Systemen) - Art 30 Abs. 3 (Erweiterte Vertragsklauseln mit ICT-Drittanbietern) Anwendung von Art. 16 – Verantwortliche ICT-Risikomanagementmaßnahmen

## 2. Anforderungsabgleich

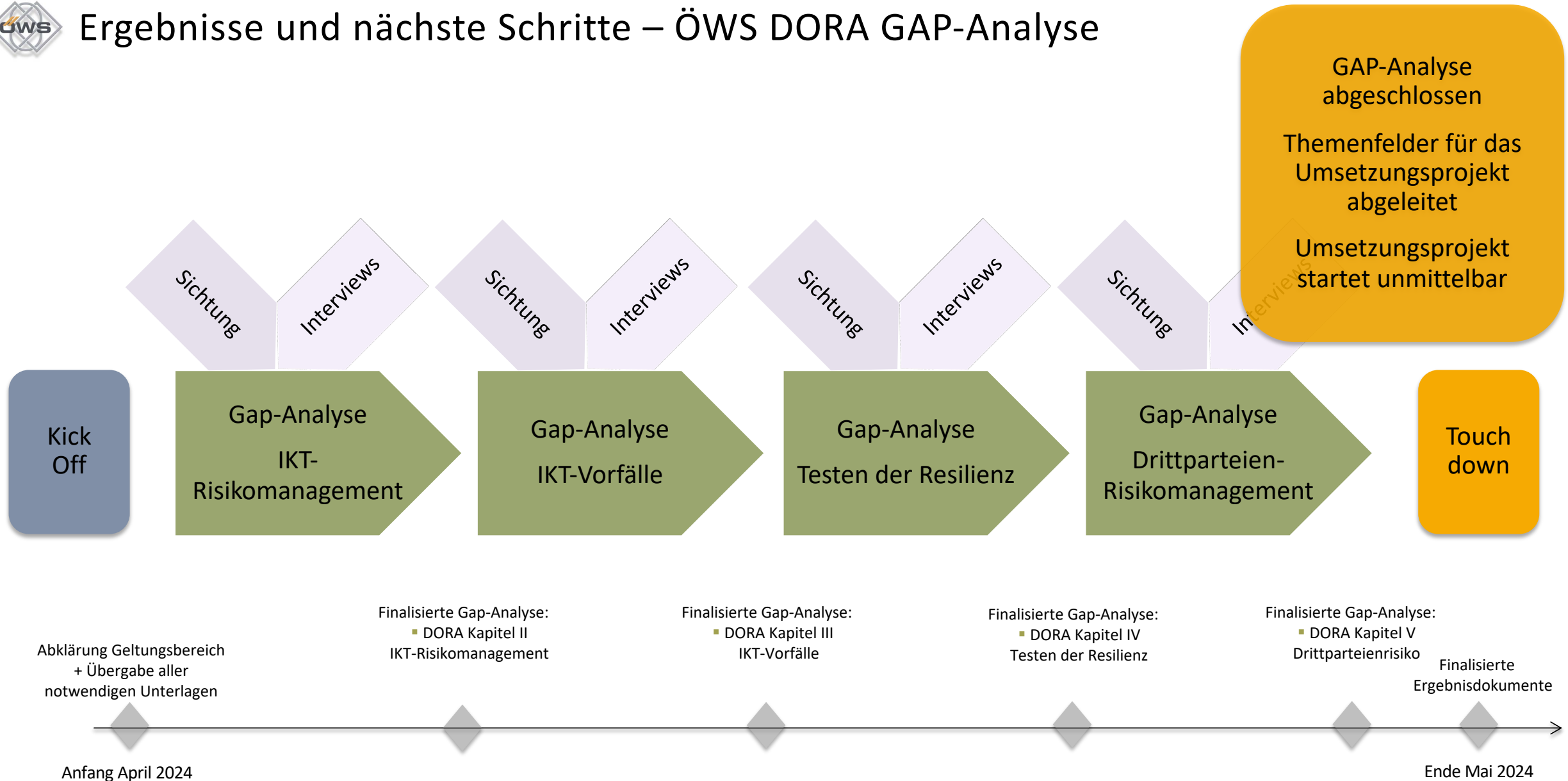
System	Anforderung	Umsetzung	Nachweis	Erklärung / Begründung zur Entscheidung
Finanzunternehmen	IKT-Systeme sind stets auf dem neuesten Stand zu halten und ...	Umsetzung durch regelmäßige Updates und Patching	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1, 7.1	Übergeordneter Punkt, dessen Anforderungen in den Unterpunkten benannt sind.
Finanzunternehmen	dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Art. 4 angemessen	Regelmäßige Tests und Überprüfungen der Systemleistung	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1	BHB beschreibt in der Service Strategy die Zukunftsfähigkeit der IT; Strategiepapier beschreibt den (historischen) Verlauf der Entwicklung der IT der ÖWS inkl. weiterem Ausblick
Finanzunternehmen	zuverlässig	Redundanz und Failover-Mechanismen	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1, 7.1	BHB beschreibt in der Service Strategy die Zukunftsfähigkeit der IT und gibt explizit die Ziele zuverlässiger IT-Systeme an; Strategiepapier beschreibt den (historischen) Verlauf der Entwicklung der IT der ÖWS inkl. weiterem Ausblick

• Anforderungstool beinhaltet ca. 370 Items (Level 1) und ca. 750 Items (Level 2 – bisherige RTS/ITS) • Beurteilung ob erfüllt, tlw. erfüllt, nicht erfüllt, etc.

Kapitel	Artikel	Absatz	Unterabs.	Buchst.	Anforderung	Fragen	umgesetzt?	Nachweis	Erklärung / Begründung zur Entscheidung
II	7	1	-	+	IKT-Systeme sind stets auf dem neuesten Stand zu halten und ...	Wie werden IKT-Systeme, -Protokolle und -Tools gemanaged?	erfüllt	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1, 7.1 Strategiepapier2023_IT-V02:	Übergeordneter Punkt, dessen Anforderungen in den Unterpunkten benannt sind.
II	7	1	-	a	dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Art. 4 angemessen	Wie wird nachgehalten, dass die Systeme die Geschäftstätigkeit angemessen unterstützen?	erfüllt	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1 Strategiepapier2023_IT-V02:	BHB beschreibt in der Service Strategy die Zukunftsfähigkeit der IT; Strategiepapier beschreibt den (historischen) Verlauf der Entwicklung der IT der ÖWS inkl. weiterem Ausblick
II	7	1	-	b	zuverlässig	Wie wird nachgehalten, dass die Systeme zuverlässig sind?	erfüllt	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1, 7.1 Strategiepapier2023_IT-V02: Kap. 1. 2. 3. 4. 5	BHB beschreibt in der Service Strategy die Zukunftsfähigkeit der IT und gibt explizit die Ziele zuverlässiger IT-Systeme an; Strategiepapier beschreibt den (historischen) Verlauf der Entwicklung der IT der ÖWS inkl. weiterem Ausblick



# Ergebnisse und nächste Schritte – ÖWS DORA GAP-Analyse



# CONCEDRO – ANGEBOT – „DORA-Gap-Analyse“

Bedürfnisse der Kunden können individuell abgebildet werden

## Offering

**DORA-Anforderungstool**  
Anfrage nach einer Unterstützung für eine eigene Analyse

**DORA-Gap-Analyse**  
Anfrage nach einer Analyse und anschließender eigenen Umsetzung

**Unterstützung DORA-Umsetzung**  
Anfrage nach einer Analyse und darauf aufbauender Umsetzungsbegleitung

## Scope Projekt

- Lieferung des DORA-Anforderungstools, inkl. struktureller und inhaltlicher Einführung
- Personentage-Kontingent für den Know-how Transfer
- Scope-Analyse des Betroffenheitsgrades
- Sichtung aller wesentlichen Richtlinien & relevanten Dokumente
- Durchführung von Experten-Interviews
- Pragmatische Analyse der aktuellen Umsetzung gegen die Anforderungen der DORA-Verordnung als IST-Aufnahme
- Ableitung von individuellen Handlungsempfehlungen
- Optional: Mapping der Detailmaßnahmen zur Richtlinienstruktur
- Umsetzung der Handlungsempfehlungen aus der vorangegangenen DORA-Gap-Analyse
- Aufbau der notwendigen Richtlinienstruktur und kundenindividuellen inhaltlichen Beschreibung
- Abstimmung der Inhalte auf die Prozesse und operativen Umsetzungsmöglichkeiten des Kunden

## Referenzen



FIVE QUARTERS



**SMARTBROKER+**



**INTREAL**





Bernhard Pölzl

Project Portfolio &  
Vendor Management

ÖWS

Fon

Mail

Web

Wien

+43 (1) 712 56 52 - 30

PoelzB@oews.co.at

[www.oews.co.at](http://www.oews.co.at)



Michael Skulina Senior Consultant

concedro GmbH Frankfurt am Main

Fon

Mail

Web

+49 (0) 151 29219012

[michael.skulina@concedro.com](mailto:michael.skulina@concedro.com)

[www.concedro.com](http://www.concedro.com)