DORA in der Praxis

Best-Practice-Lösungen für eine pragmatische Umsetzung

Wien, 19. Juni 2024

DORA – WAS KOMMT AUF SIE ZU?

Source: unsplash.com

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

16.01.23
Inkrafttreten

Release RTS/ITS Jan 2024

Q2/2024

Release RTS/ITS Jul 2024

17.01.25 Go Live

DORA – KERNTHEMEN

Source: Adobe Stock

- IKT-Risikomanagement
- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
- Testen der digitalen operationalen Resilienz
- Management des IKT-Drittparteienrisikos
- 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

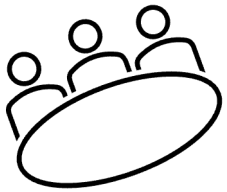
Umsetzung der neuen und erweiterten Vorgaben

Grad der notwendigen Beistellleistungen 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

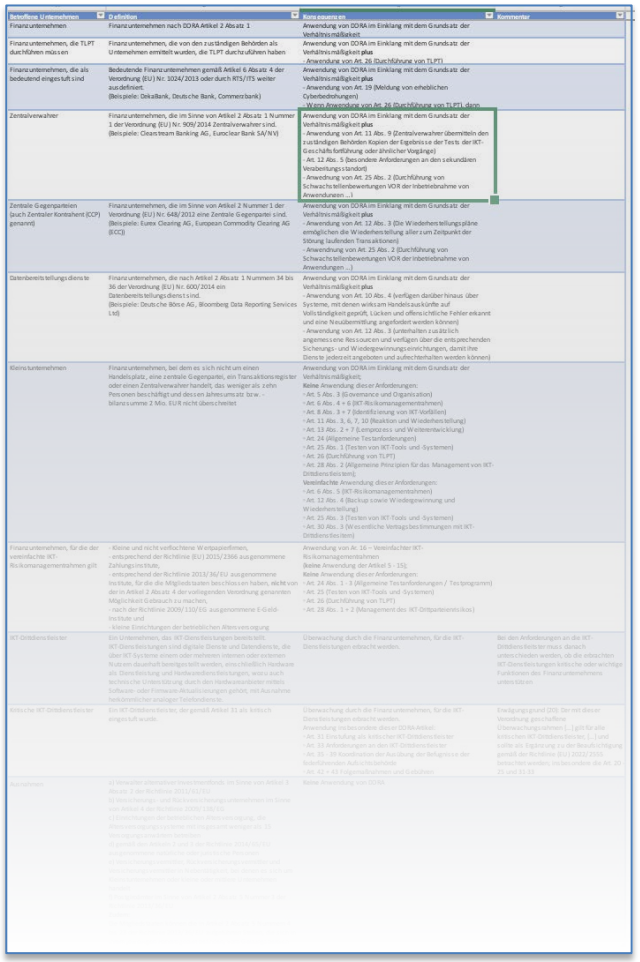
Aufbereitung der wesentliche Handlungspunkte für das Top-Management

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

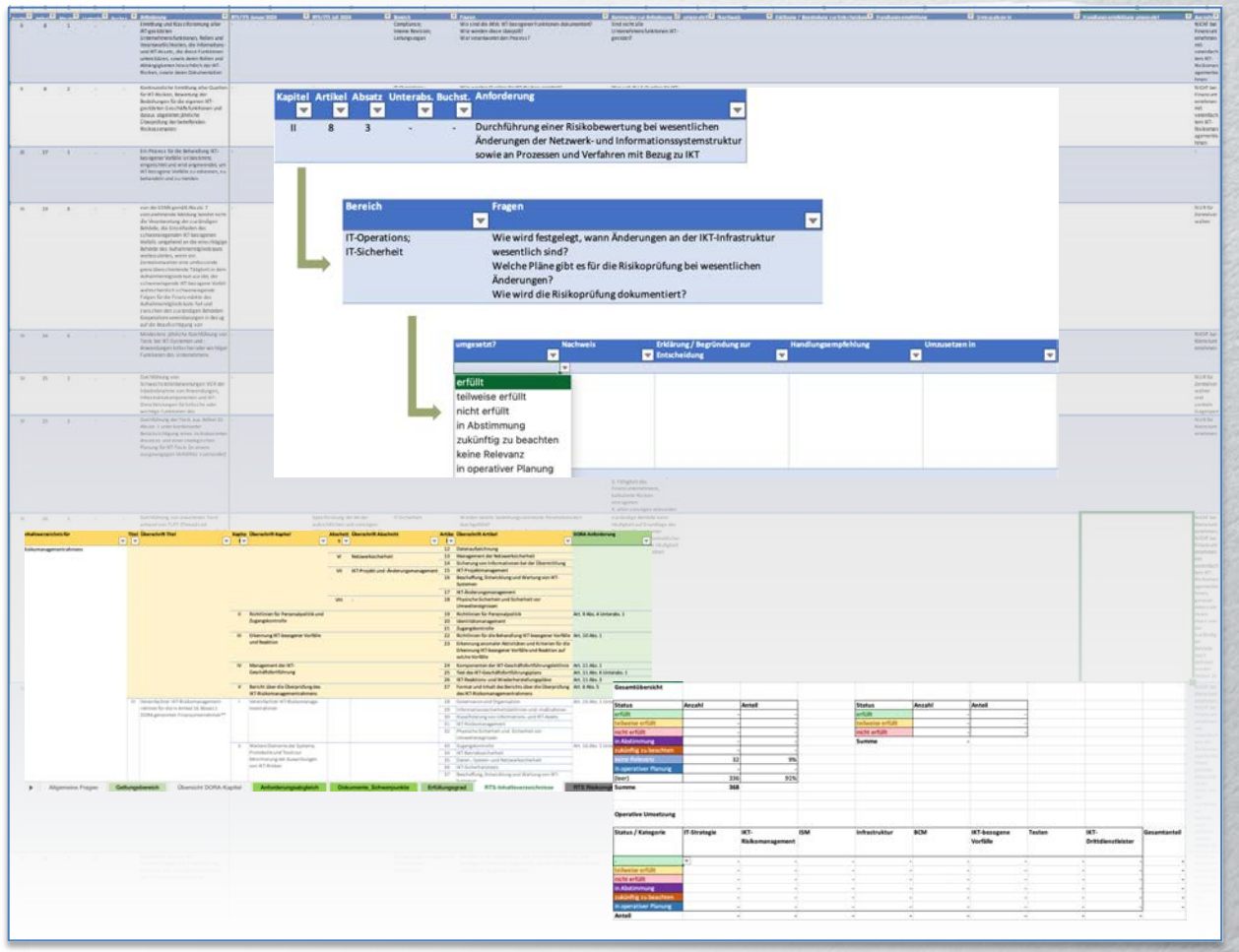
Source:
unsplash.com

DORA – GAP-ANALYSE ANFORDERUNGSTOOL (BEISPIEL)

1. Geltungsbereich



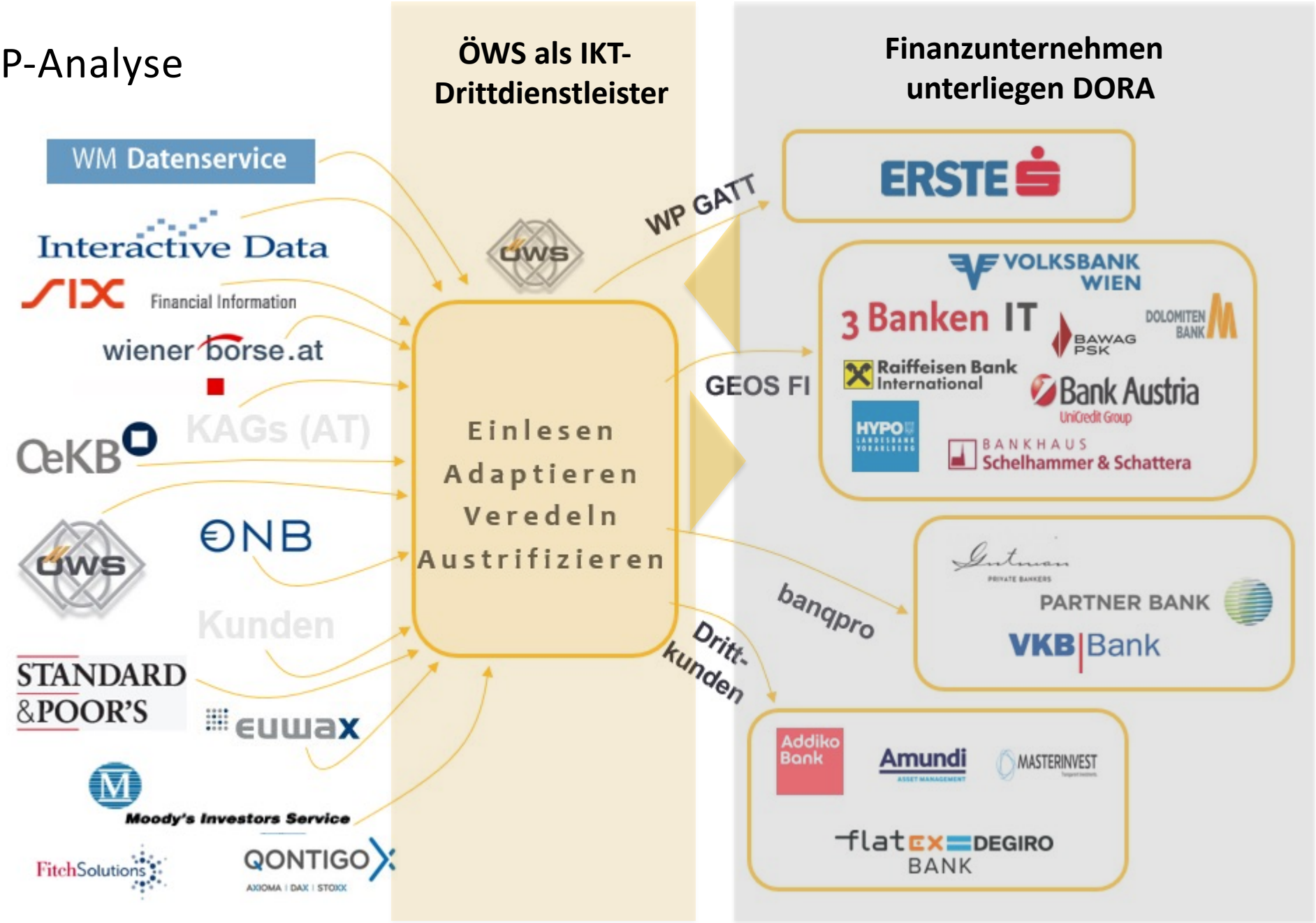
2. Anforderungsabgleich



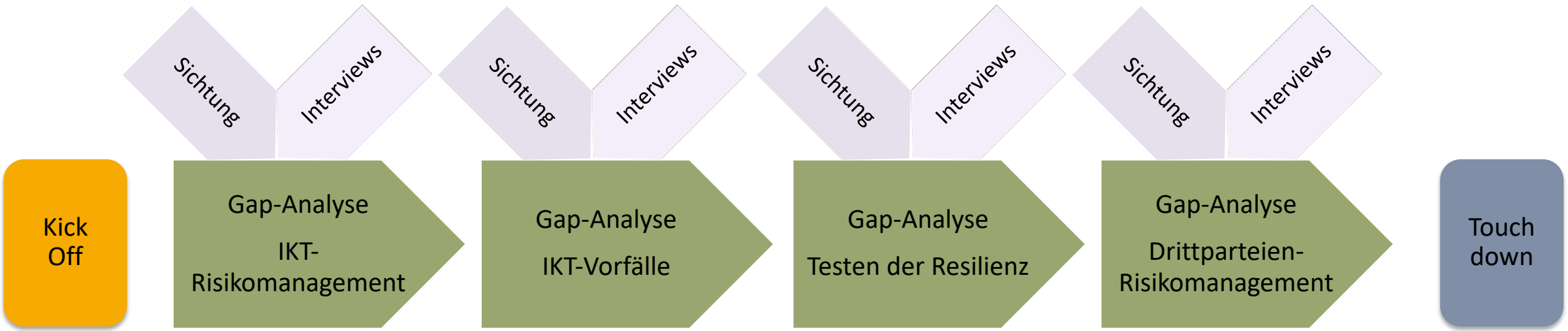
- Best Practice
- Bei mehr als 10 Kunden im Einsatz
- inkl. RTS/ITS (Level 2 - Batch 1)
- inkl. Mapping XAIT + ISO 27001/2
- Gesamtübersicht über Kapitel/Status/Kategorien
- Optional - DO IT YOUSELF

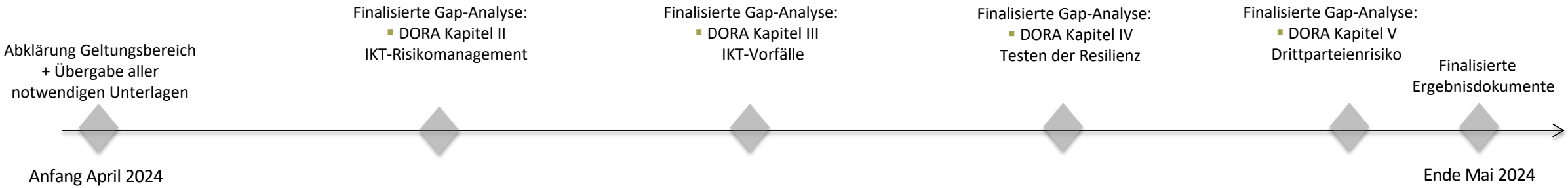
ÖWS DORA GAP-Analyse

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



Vorgehen und Zeitleiste – ÖWS DORA GAP-Analyse

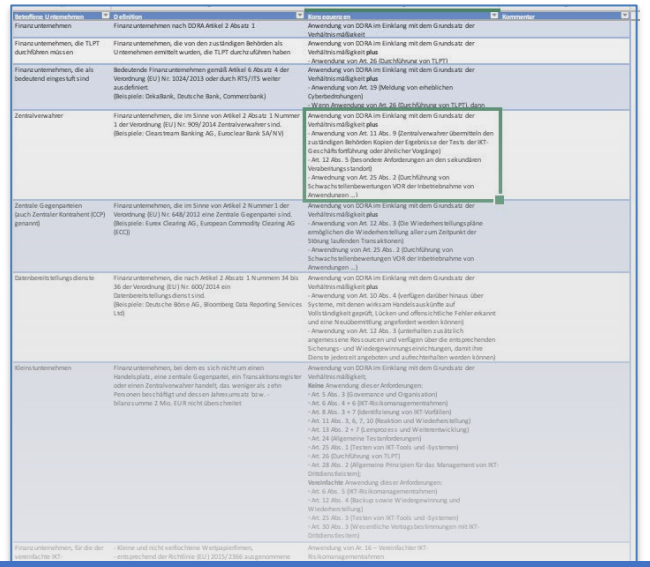




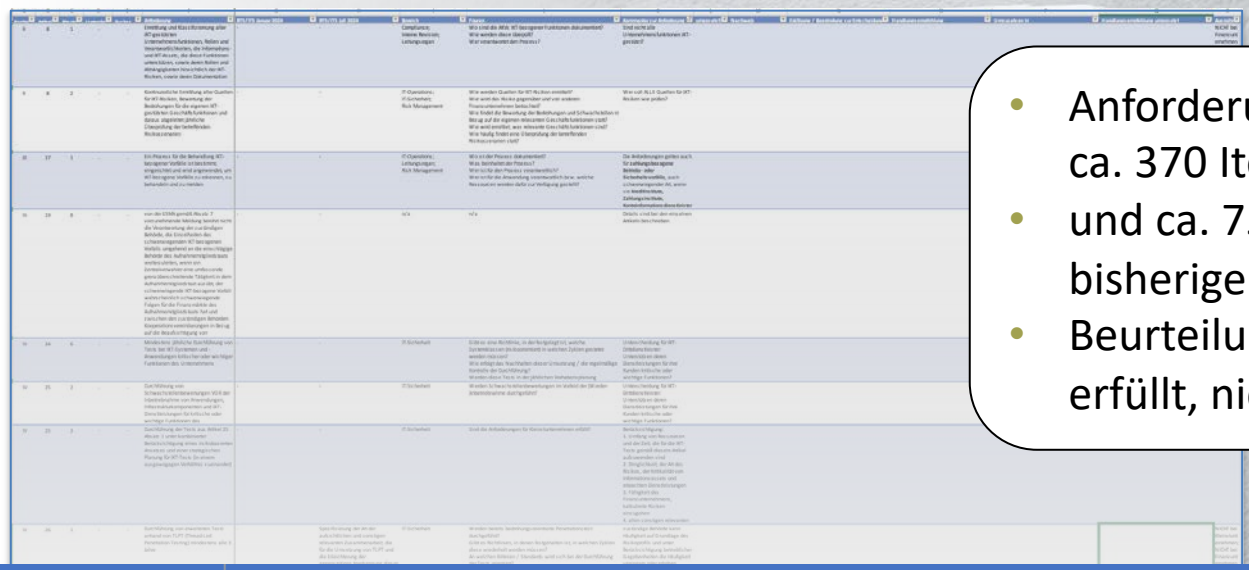
Source: unsplash.com

DORA – GAP-ANALYSE ANFORDERUNGSTOOL (BEISPIEL ÖWS)

1. Geltungsbereich



2. Anforderungsabgleich



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

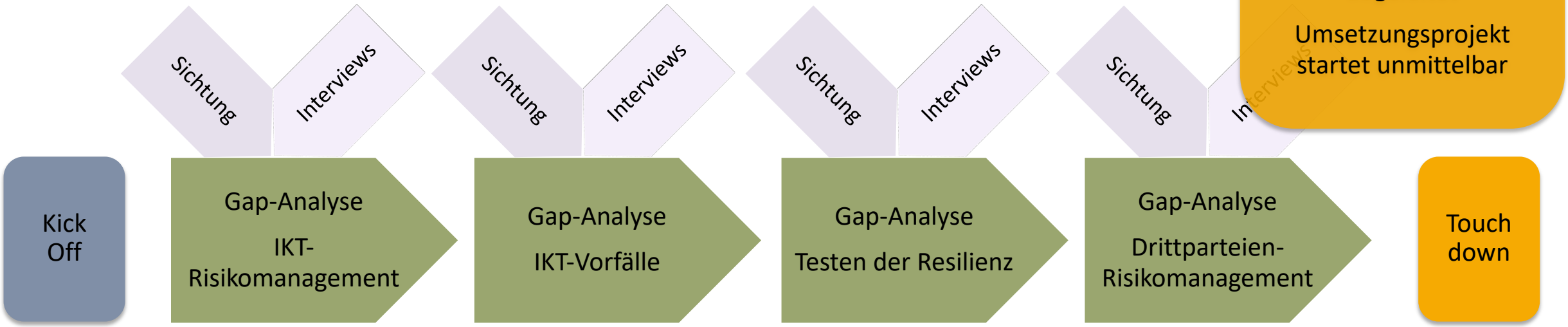
Kapitel	Artikel	Absatz	Unterabs.	Buchst.	Anforderung	Fragen	umgesetzt?	Nachweis	Erklärung / Begründung zur Entscheidung
II	7	1	-	+	IKT-Systeme sind stets auf dem neuesten Stand zu halten und …	Wie werden IKT-Systeme, -Protokolle und -Tools gemanaged?	erfüllt	Betriebshandbuch - ATT_OWS_3029_BHB: Kap. 5.1, 7.1 Stratagiepapier2023_IT-V02:	Übergeordneter Punkt, dessen Anforderungen in den Unterpunkte 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 Stratagiepapier2023_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 Stratagiepapier2023_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

GAP-Analyse abgeschlossen

Themenfelder für das Umsetzungsprojekt abgeleitet

Umsetzungsprojekt startet unmittelbar



Abklärung Geltungsbereich + Übergabe aller notwendigen Unterlagen

Finalisierte Gap-Analyse:
- DORA Kapitel II
IKT-Risikomanagement

Finalisierte Gap-Analyse:
- DORA Kapitel III
IKT-Vorfälle

Finalisierte Gap-Analyse:
- DORA Kapitel IV
Testen der Resilienz

Finalisierte Gap-Analyse:
- DORA Kapitel V
Drittparteienrisiko

Finalisierte Ergebnisdokumente

Anfang April 2024

Ende Mai 2024

CONCEDRO – ANGEBOT – „DORA-Gap-Analyse“

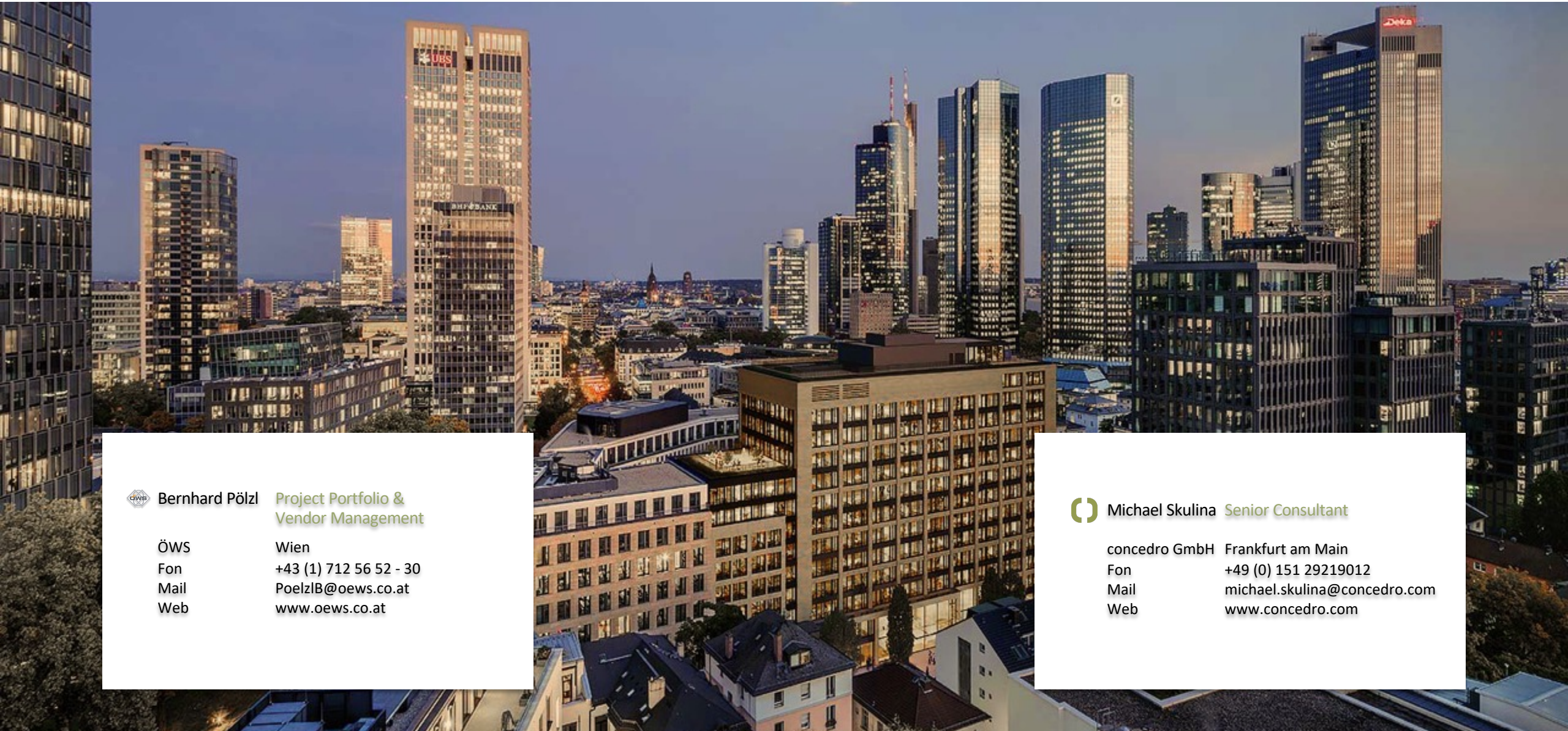
Bedürfnisse der Kunden können individuell abgebildet werden

Offering	Scope Projekt
DORA-Anforderungstool Anfrage nach einer Unterstützung für eine eigene Analyse	▪ Lieferung des DORA-Anforderungstools, inkl. struktureller und inhaltlicher Einführung ▪ Personentage-Kontingent für den Know-how Transfer
DORA-Gap-Analyse Anfrage nach einer Analyse und anschließender eigenen Umsetzung	▪ 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 Richtliniestruktur
Unterstützung DORA-Umsetzung Anfrage nach einer Analyse und darauf aufbauender Umsetzungsbegleitung	▪ 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

Babcock Pensionskasse
5 FIVE QUARTERS
FENION
SMARTBROKER+
ÖWS
INTREAL
bayerische börse

KONTAKT



Bernhard Pölzl Project Portfolio & Vendor Management

ÖWS Wien
Fon +43 (1) 712 56 52 - 30
Mail PoelzlB@oews.co.at
Web www.oews.co.at

Michael Skulina Senior Consultant

concedro GmbH Frankfurt am Main
Fon +49 (0) 151 29219012
Mail michael.skulina@concedro.com
Web www.concedro.com