



IT-Compliance Webcast für die FS Praxis

DORA:

Auf Kurs mit Umsetzung nach Augenmaß

Webcast

März 2023

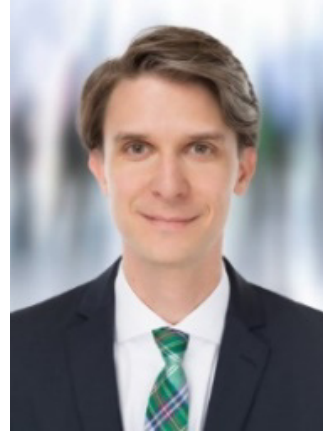


Vorstellung der Ansprechpartner:innen



Vaike Metzger

Partnerin
Financial Services



Marian Bernhard

Senior Manager
Financial Services



Caroline Sieveritz

Senior Managerin
Financial Services

Ausblick zu den Inhalten



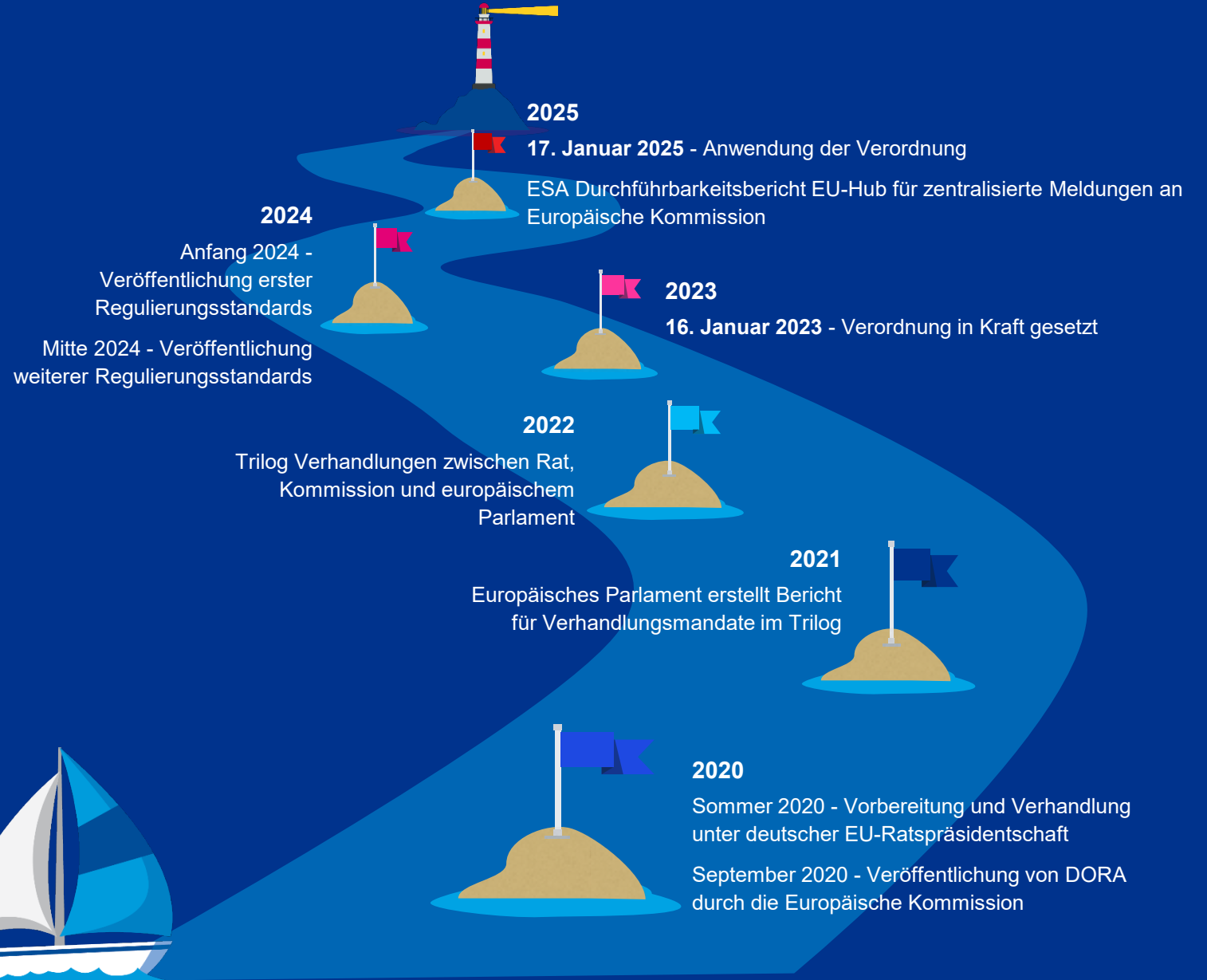
- DORA – kurz erklärt
- Regulierungsstandards
- Gap Analysen
- Hot Topics
- Zusammenfassung und Ausblick

DORA – Kurz erklärt

Die Initiative zur „Digital Operational Resilience“ wurde Ende September 2020 von der EU Kommission als Vorschlag eines Maßnahmenpakets zur weiteren Digitalisierung des Finanzsektors veröffentlicht. Das Ziel ist die Stärkung der Wettbewerbsfähigkeit, Innovation sowie Resilienz bei Cyber-Angriffen. Die DORA-Verordnung wurde am 16. Januar 2023 in Kraft gesetzt und hat eine Umsetzungsfrist für die Implementierung von zwei Jahren.

Der Vorschlag erweitert bestehende Vorschriften (MaRisk/MaGo/KAMaRisk, BAIT/VAIT/KAIT, etc.) und geht verstärkt auf Anforderungen bezüglich Cyber und weiterer digitaler Risiken ein.

Wichtige Bestandteile sind die Harmonisierung der Vorschriften für das Informations- und Kommunikationstechnologie (IKT) – Risiko-management, die Meldung und Bericht-erstellung, Test und Prüfungen sowie die Risiko-evaluierung von IKT-Drittanbietern.



Erkenntnisse aus unseren bisherigen DORA Analysen und unserer internationalen Zusammenarbeit

Stimmungsbild

Der DORA wird bei Finanzunternehmen positiv aufgenommen. Diese sehen darin eine Chance, die operationelle Resilienz zu verbessern. Erste Umsetzungsprojekte werden aufgesetzt und Implementierungsideen konkretisiert.

>30

Anzahl unserer bereits erfolgreich durchgeführten Gap Analysen und Workshops



Internationale Zusammenarbeit

Die Expertenaustausche in unseren globalen Netzwerken bieten internationale Erfahrung gepaart mit lokalen Besonderheiten



Abdeckungsgrad

Die einschlägige Regulatorik deckt einen Teil der für die Finanzunternehmen relevanten DORA Anforderungen bereits ab

~37%



Veröffentlichung der Regulierungsstandards (RTS & ITS) in den nächsten 12 bzw. 18 Monaten

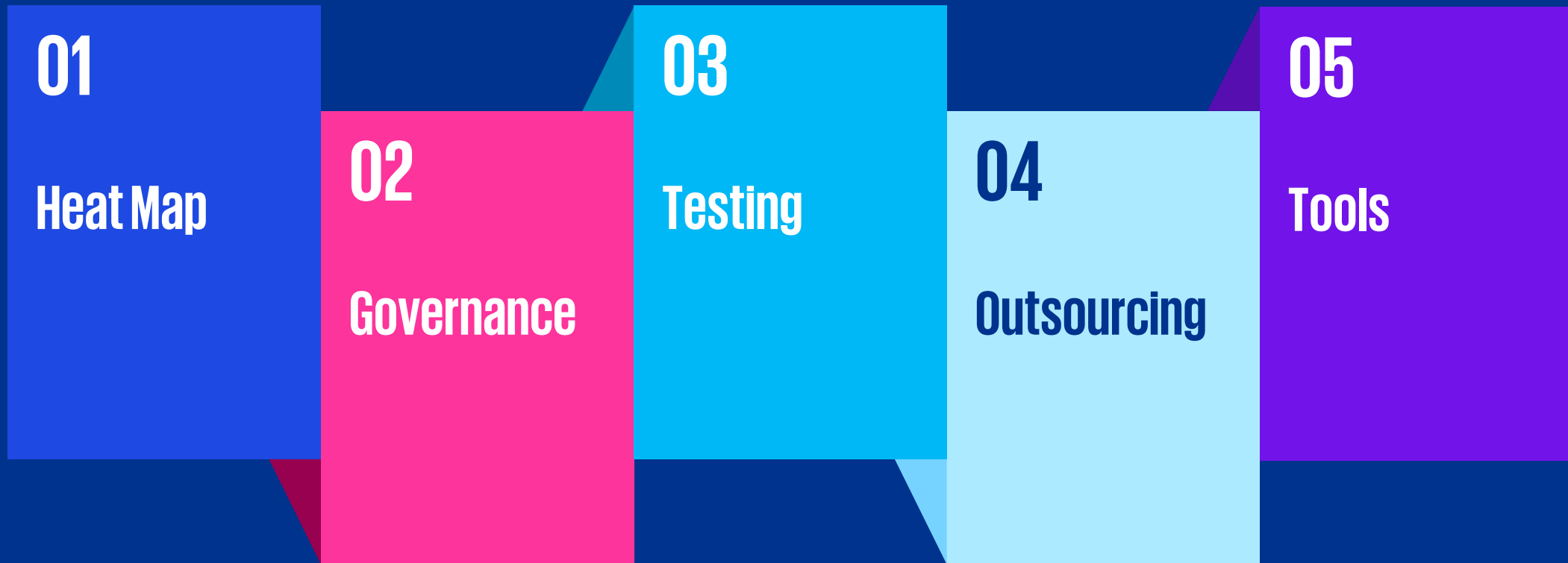


IKT-Risikomanagementrahmen (Kapitel II)	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III)	Testen der digitalen operationalen Resilienz (Kapitel IV)	Management des IKT-Drittparteirisikos (Kapitel V Sektion I)	Überwachungsrahmen (Kapitel V Sektion II)
- RTS zum IKT-Risikomanagementrahmen (Art.15) - RTS zum Vereinfachten IKT-Risikomanagementrahmen (Art.16.3) - Leitlinien für Schätzung aggregierter jährlicher Kosten und Verluste, durch schwerwiegende IKT-bezogene Vorfälle (Art.11.11)	- RTS zur Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen (Art.18.3) - RTS zum Inhalt von Meldungen über schwerwiegende IKT-bezogene Vorfälle (Art.20.a) - ITS zu den Reporting Details zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls (Art.20.b) - Durchführbarkeitsbericht Meldungs-Zentralisierung schwerwiegender IKT-bezogener Vorfälle in EU-Hub (Art.21) (17. Januar 2025)	RTS für erweiterte Tests auf Basis von Threat Led Penetration Testing TLPT (Art.26.11)	- ITS mit Standardvorlagen für Informationsregister (Art.28.9) - RTS zur Spezifizierung der Nutzung von IKT-Dienstleistungen von IKT-Drittdienstleistern (Art.28.10) - RTS zur Auftragsvergabe von Unterstützung kritischer oder wichtiger Funktionen an IKT-Drittdienstleistungen (Art.30.5)	- EBA ersucht ESAs um Stellungnahme zu Kritikalitätskriterien (Art.31.8) und Gebühren (Art.43.2) (September 2023, Rechtsakt 17. Juli 2024) - Leitlinien Zusammenarbeit ESA mit Behörden zur Aufsicht (Art.32.7) - RTS zur Harmonisierung der Überwachung (Art.41)

(RTS) Regulatory Technical Standard // Technische Regulierungsstandards
(ITS) Implementation Technical Standard // Technische Durchführungsstandards
● Grau abweichende Timeline

Hot Topics

Aus unseren durchgeführten Gap Analysen bei Finanzunternehmen unterschiedlicher Größenordnung haben sich unter anderem folgende Schwerpunkte zur Umsetzung ergeben. Die Heat Map liefert einen Überblick hierzu.



Heat Map – Aktuelle Erkenntnisse zu den Schwerpunkten der Umsetzungsbedarfe

01



Governance

-  Strategie für digitale operationale Resilienz (Art. 6)
-  Verantwortlichkeit des Leitungsorgans (Art. 5)

Management des IKT-Drittparteirisikos

-  IKT-Drittanbieterstrategie (Art. 28)
-  Vertragsergänzungen und Risikoanalyse (Art. 28, 30)
-  Informationsregister (Art. 28)
-  Ausstiegsstrategien (Art. 28, 30)

Testverfahren

-  Bedrohungsbasierte Penetrationstests (Art. 26-27)
-  Testen der digitalen operationalen Resilienz (Art. 24-25)
-  Testen der Wiederherstellungspläne (Art. 11)

IKT-bezogene Vorfälle

-  Erkennung, Klassifizierung und Berichterstattung von Vorfällen (Art. 10, Art. 17-19)
-  Reaktion auf IKT-Vorfälle (Art. 11)
-  Kommunikation (Art. 11 & 14)

Exkurs: Relevanz Kommunikation

Erhöhte Anforderungen an die Kommunikation von IKT-Vorfällen umfassen u.a. die **Etablierung einer Kommunikationsstrategie**, das regelmäßige **Testen von Kommunikationsplänen** bis hin zur vertraglichen und prozessualen **Einbeziehung von (Sub-)Dienstleister** bei relevanten IKT-Vorfällen.

DOR Governance – einheitliche und vollständige Perspektive sicherstellen

Beispiel

1. Gesamtverantwortung DORA

CRO (Chief Risk Officer)

DOR Strategie

2. Risiko Zusammenführung

Risikoarten mit Schnittstellen zur digitalen Resilienz

3. Betrachtete Komponenten im OpRisk

Operationelle Risiken

Organisation

Informationen und Informationsverarbeitung (IT)

BCM und Krisenmanagement

Management IKT-
Drittanbieter

Informationssicherheit

Methode

Human Resources

(IT) Projektmanagement

...

4. Operative Ebene

IT

Fachbereiche

Dienstleister

Umsetzung und Reporting

(strategische) Vorgaben, Methoden, Werkzeuge

Übersicht: Die Anforderungen an das Testen der digitalen operationalen Resilienz steigen

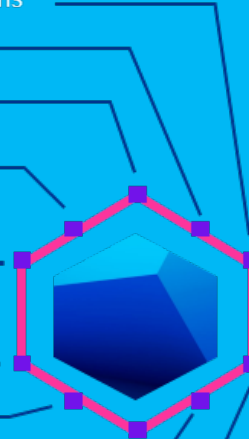
Artikel 24

Allgemeine Anforderungen

Artikel 25

Testen von IKT-Tools und -Systemen

1. Schwachstellenbewertung und -scans
2. Lückenanalysen
3. Netzwerksicherheitsbewertungen
4. Quellcodeprüfungen (soweit durchführbar)
5. Überprüfungen der physischen Sicherheit
6. Szenario-basierte Tests
7. End-to-End-Tests
8. Penetrationstests
9. Kompatibilitätstests
10. Leistungstests



Artikel 26

Erweiterte Tests



Durchzuführen, wenn seitens der Behörden gefordert (gem. Artikel 26 Abs. 8)



Schließt relevante IKT-Prozesse, -Systeme und -Technologien für kritische Funktionen sowie Dienste und Dienstleister ein



Erstellen von Berichten und Plänen mit Maßnahmen ist notwendig

Artikel 27

Anforderungen an Tester



Management des IKT-Drittparteienrisikos

Die folgenden Themen bilden aktuell den Schwerpunkt der Umsetzung:

01 | Strategie

- Eigenständiges oder integriertes Strategiedokument für das Risiko durch IKT-Drittanbieter konkretisiert durch eine Leitlinie
- Einrichtung bzw. Bündelung eines zentralen „Third Party Risk Management“

02 | Vertrag

- Sub-Contracting
- Ort der Leistungserstellung
- Unterstützung bei der Behebung von Vorfällen
- Teilnahme an Awareness-Programmen

04 | Sub-Outs.

- Bewertung der Risiken, die sich aus der Sub-Delegation / dem Sub-Outsourcing ergeben
- Erfassung im Informationsregister

03 | EXIT-Management

- Analyse von Konzentrationsrisiken sowie der Substituierbarkeit
- Erarbeitung einer ganzheitlichen integrierten (aus dem Risiko abgeleiteten) EXIT-Lösung u.a. Berücksichtigung von theoretischen Vorbereitungen für den Ernstfall und technischer Implikationen (Tests)

05 | Register

- Register über alle IKT-Drittanbieter und bzgl. der durch diese erbrachten Leistungen
- Berücksichtigung der Sub-Dienstleister bis zu Anzahl x innerhalb der Kette

Unser bewährter Ansatz zur DORA Gap Analyse

01

Kick-Off & Scoping
Scoping der relevanten Einheiten, Analyse und Verfahrensdefinition sowie Projektplanung

02

Informationen sammeln & Analyse
Vorläufige Lückenbewertungen auf der Grundlage von Schlüssel-Dokumenten, Interviews, Workshops

03

Auswertung der Analyse-Ergebnisse
Abgleich der Ergebnisse mit KPMG-Fachexperten

04

Gap Report & Implementierungsoptionen
Maßnahmenempfehlungen inkl. Heat Map zur Prioritätensetzung

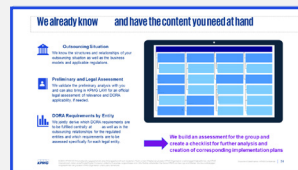
05

Fertigstellung finaler Report & Roadmap
Abschließende Abstimmung der Umsetzungspunkte, Vorstandspräsentation und Implementierungs-Roadmap

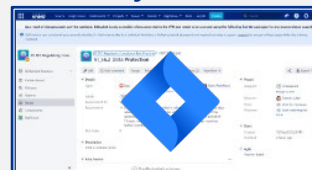
Was wir bereits mitbringen

DORA-BAIT-Mapping

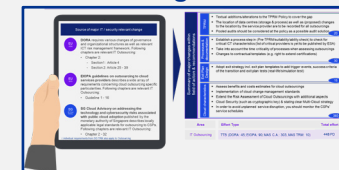
Knowledge



Tool-basierter Analyseansatz



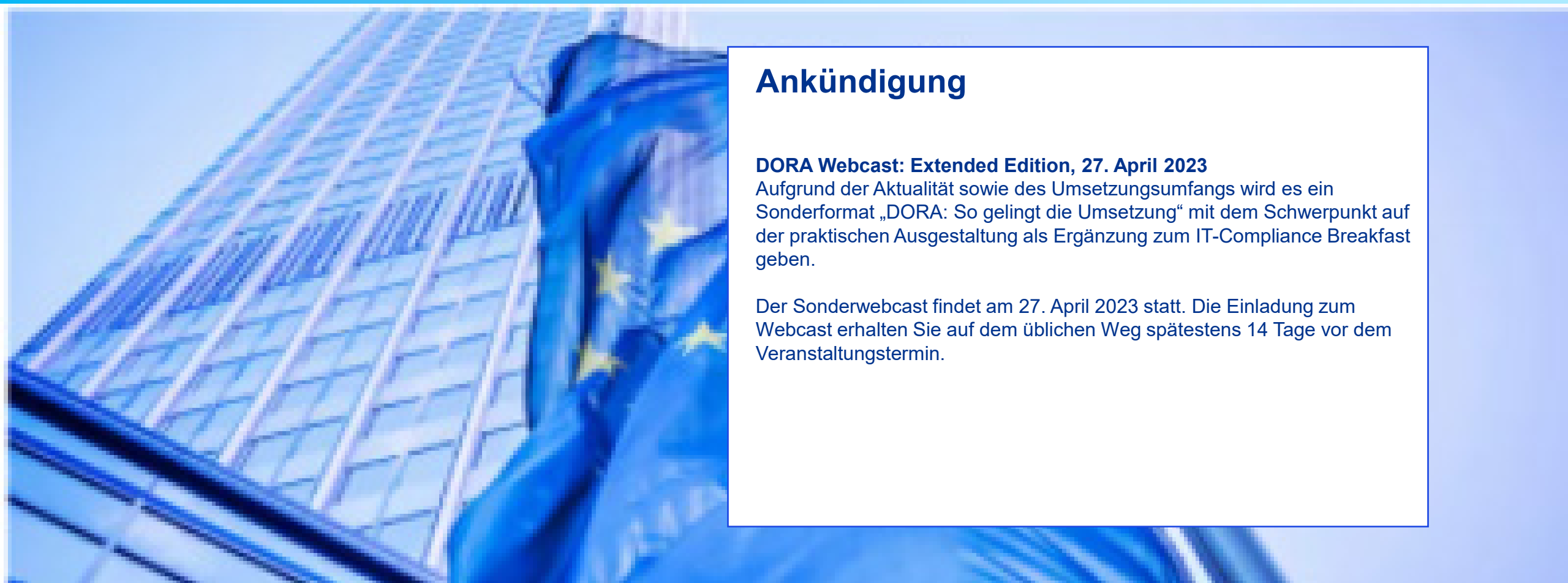
Detaillierte Präsentation der Ergebnisse



Präsentation der Gesamtergebnisse & Aktionsplan

Measure/Action Category	Description	No. of activities per category
IT	IT-related necessary	49
Doc_Change	Any changes to any IT system or environment	21
Doc_New	Changes to documentation (independent of type) required	11
Doc_Rev	New documentation (independent of type) required	11
Doc_Rev	Changes affected by the measure	85
Doc_Rev	Work-in-progress affected by the measure	33
Inventory	Any type of inventory in a sub-contractors affected by the measure	21
Process	Processes affected by the measure	89

Measure/Action Category	Required	Document	Work	Inventory	Process
IT Security / Cyber Protection (42)	41	11	43	7	39
Observation / Cloud (17)	7	8	0	3	11
SCM / Operational Resilience (26)	1	10	0	19	15
Data Privacy / Data Transfer (15)	0	0	0	0	0

The background of the slide features a low-angle, upward-looking view of a modern skyscraper with a glass facade, reflecting the sky. Overlaid on the right side of the image is the European Union flag, which is blue with a circle of twelve gold stars. The entire image has a blue color cast.

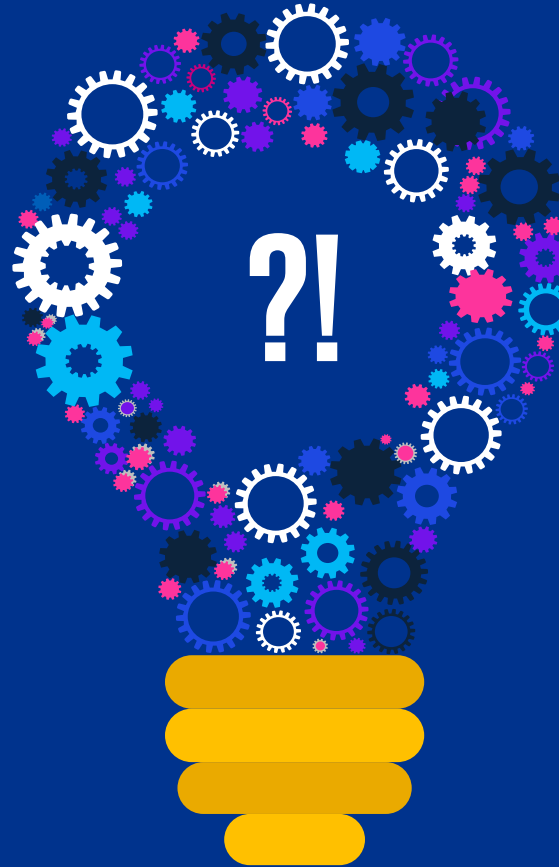
Ankündigung

DORA Webcast: Extended Edition, 27. April 2023

Aufgrund der Aktualität sowie des Umsetzungsumfangs wird es ein Sonderformat „DORA: So gelingt die Umsetzung“ mit dem Schwerpunkt auf der praktischen Ausgestaltung als Ergänzung zum IT-Compliance Breakfast geben.

Der Sonderwebcast findet am 27. April 2023 statt. Die Einladung zum Webcast erhalten Sie auf dem üblichen Weg spätestens 14 Tage vor dem Veranstaltungstermin.

Zeit für Ihre Fragen!





Vaike Metzger

Partnerin, Financial Services

T +49 172 2895793
vmetzger@kpmg.com

Marian Bernhard

Senior Manager, Financial Services

M +49 172 2858366
mbernhard@kpmg.com

Caroline Sieveritz

Senior Managerin, Financial Services

M +49 151 15423145
csieveritz@kpmg.com

KPMG AG

Wirtschaftsprüfungsgesellschaft
Ganghoferstraße 29
80339 München

KPMG AG

Wirtschaftsprüfungsgesellschaft
Nikolaus-Dürkopp-Straße 2a
33602 Bielefeld

KPMG AG

Wirtschaftsprüfungsgesellschaft
THE SQUAIRE / Am Flughafen
60549 Frankfurt am Main



kpmg.de/socialmedia

kpmg.de

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.

Document Classification: KPMG Public