Armodiotita
Beratungs-GmbH

CONSULTING UNION
The Origin of Excellence

D igital
O perational
R esilience
A ct

Verordnung über digitale operationale Resilienz im Finanzsektor

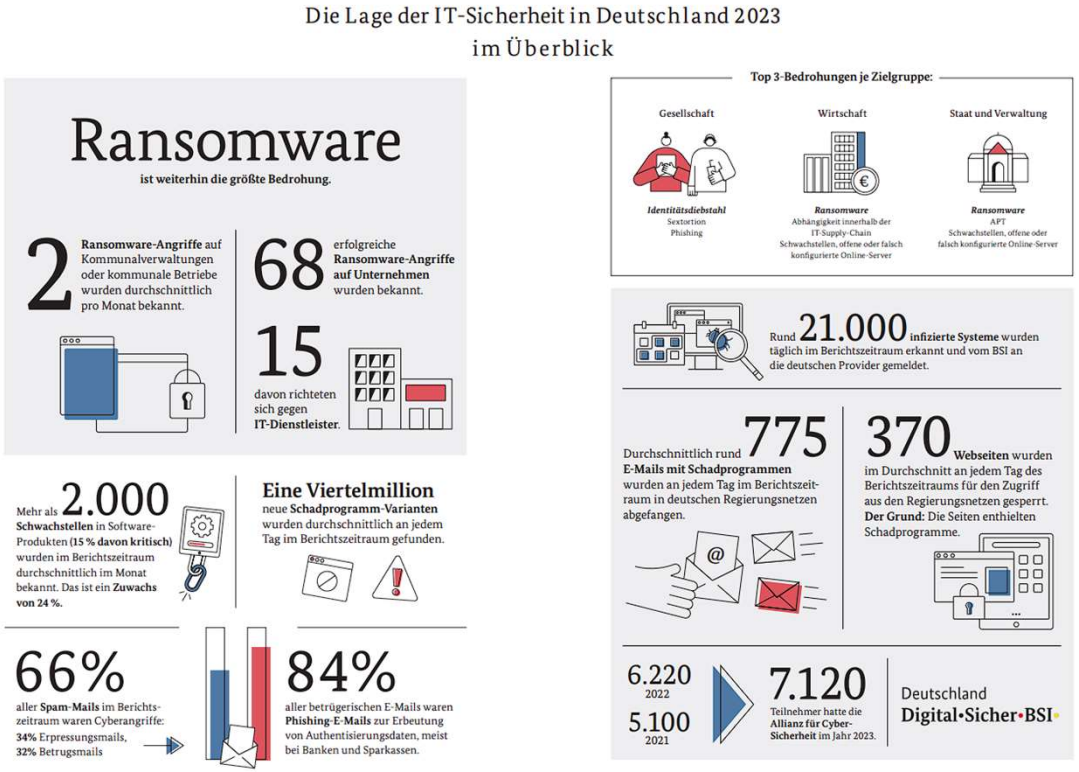
VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG)

Lagebericht des BSI zur IT-Sicherheit in Deutschland 2023

Armodiotita Beratungs-GmbH

CONSULTING UNION The Origin of Excellence

IT-Sicherheitslage spitzt sich zu
Insgesamt spitzte sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Im Berichtszeitraum wurde – wie schon im Vorjahr – eine hohe Bedrohung durch Cybercrime beobachtet. Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine.



Quelle: BSI - Die Lage der IT-Sicherheit in Deutschland (bund.de)

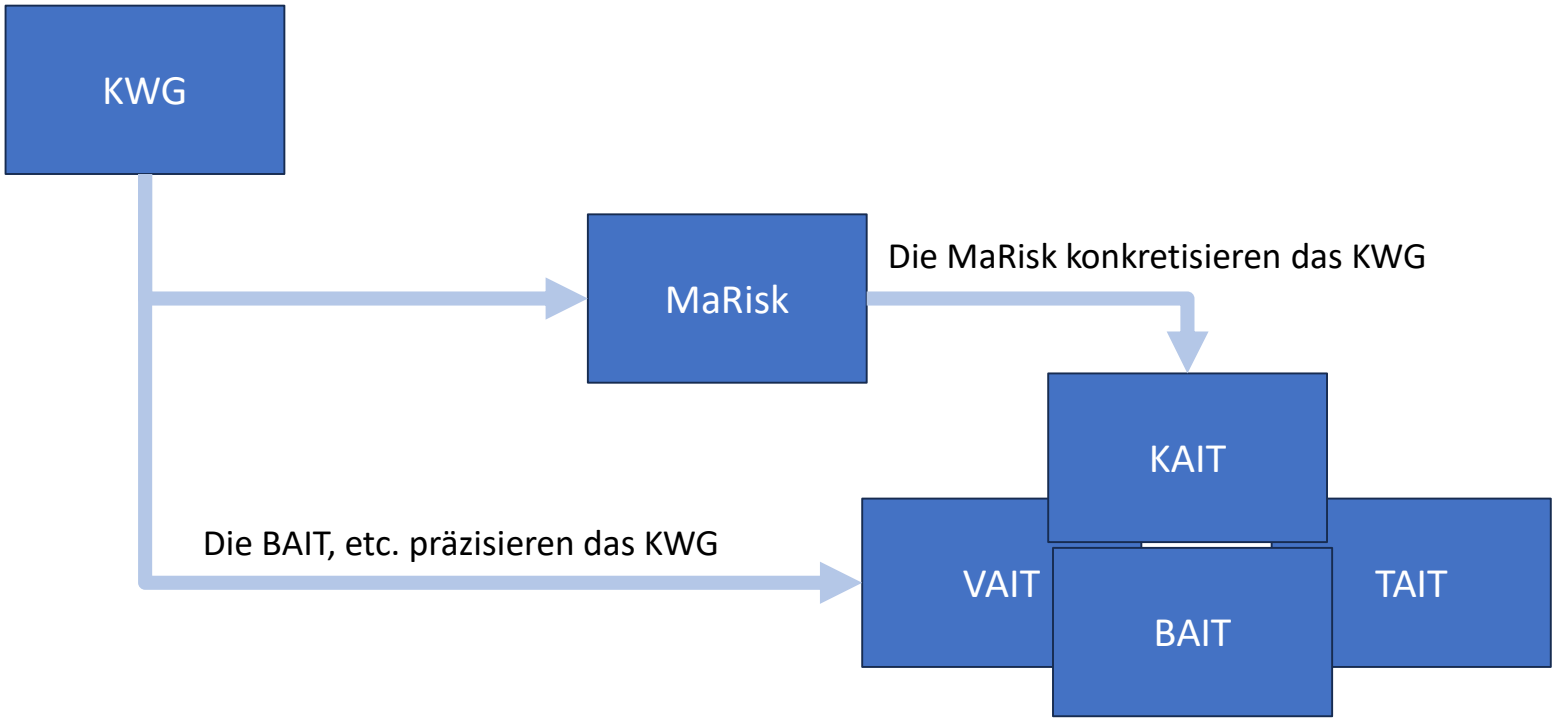
Ausgewählte IT-Sicherheitsvorfälle 2023 in Deutschland (Stand 19. September)

Armodiotita Beratungs-GmbH

CONSULTING UNION The Origin of Excellence

Datum	Vorfall	Unternehmen/Stadt/Land
September	DDoS-Angriff auf die Website der **Finanzmarktaufsicht** in Deutschland	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) - Bonn, Nordrhein-Westfalen, Deutschland
Juni	Cyberangriff auf ein **Leasingunternehmen** in Deutschland	Deutsche Leasing - Bad Homburg vor der Höhe, Hessen, Deutschland
Mai	Dienstleister für **Kundenkontakt-Management** aus Deutschland von Cyberangriff betroffen (Datenleck trifft auch Kunden der ING, Commerzbank/Comdirect, Deutsche Bank, Post-Bank, Sparda Bank, Provinzial Versicherungsgruppe, Bayern-Versicherung Lebensversicherung AG)	Majorel Deutschland - Gütersloh, Nordrhein-Westfalen, Deutschland (Kreis Gütersloh)
Mai	Cyberangriff auf ein Rechenzentrumsanbieter in Deutschland	Mivitec - München, Bayern, Deutschland
April	Einbrecher stehlen Festplatten bei einem **Versicherungsunternehmen** in Deutschland	Condor Versicherung - Hamburg, Deutschland
April	Cyberangriff auf einen IT-Dienstleister in Deutschland	Bitmarck - Essen, Nordrhein-Westfalen, Deutschland
März	Cyberangriff auf einen IT-Dienstleister in Deutschland	Materna SE - Dortmund, Nordrhein-Westfalen, Deutschland
März	Verkauf von **Prepaid-Karten** in Deutschland von Cyberangriff auf IT-Dienstleister betroffen	Vodafone Callya - Deutschland
März	Cyberangriff auf einen IT-Dienstleister in Nordrhein-Westfalen	Neuhaus Gruppe - Hamm, Nordrhein-Westfalen, Deutschland
Februar	Cyberangriff auf den Betreiber einer **Versicherungsplattform** in Deutschland	Smart InsurTech AG - Berlin, Deutschland
Januar	Unbefugter Zugriff bei einem IT-Dienstleister in Deutschland	Bitmarck - Essen, Nordrhein-Westfalen, Deutschland
Januar	Cyberangriff auf einen IT-Dienstleister in Deutschland	Adesso SE - Dortmund, Nordrhein-Westfalen, Deutschland

Der bisherige Rechtsraum im Finanzsektor



Quelle: Tomislav Maksimovic • Holger Biernat | Bankaufsichtliche Anforderungen an die IT (BAIT); Konzepte zur Implementierung der neuen Vorgaben | Springer Gabler | ISBN 978-3-658-25225-0, ISBN 978-3-658-25226-7 (eBook)

Erweiterung des Rechtsraumes: Verordnung (EU) 2022/2554

Armodiotita Beratungs-GmbH

CONSULTING UNION The Origin of Excellence

Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die
digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen
(EG) Nr. 1060/2009,
(EU) Nr. 648/2012,
(EU) Nr. 600/2014,
(EU) Nr. 909/2014 und
(EU) 2016/1011 (Text von Bedeutung für den EWR)
PE/41/2022/INIT

Quelle: *https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0001.01.DEU&toc=OJ%3AL%3A2022%3A333%3AFULL*

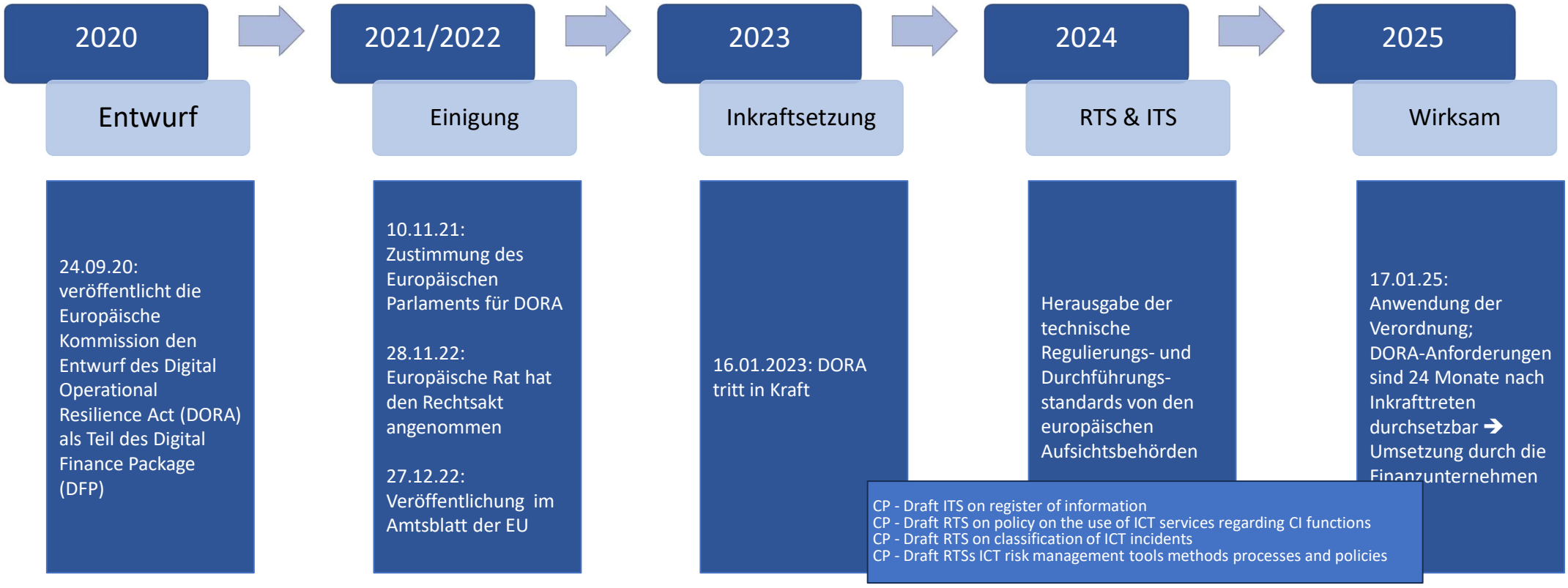
Statement der BaFin

Grenzüberschreitende Probleme?
Grenzüberschreitende Lösungen – durch DORA:

„… DORA stärkt mit der sektorübergreifenden Vereinheitlichung von Anforderungen die Cyber-Sicherheit der Finanzunternehmen. Dieser Ansatz ist für die deutsche Finanzbranche und ihre Aufsicht nicht grundsätzlich neu. Das zeigen ihre Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) sowie die damit verwandten Rundschreiben für andere Sektoren: die Bankaufsichtlichen, Kapitalverwaltungsaufsichtlichen und Zahlungsdiensteaufsichtlichen Anforderungen an die IT – kurz: BAIT, KAIT und ZAIT.

Damit keine Dopplungen in der Regulierung entstehen, werden die bestehenden Leitlinien der drei europäischen Aufsichtsbehörden zur Informationssicherheit im Finanzsektor an DORA angepasst. …“

Zeitkorridor - DORA



Regulatory Technical Standards (**RTS**) and Implementing Technical Standards (**ITS**)

Die Kernziele von DORA

Armodiotita Beratungs-GmbH

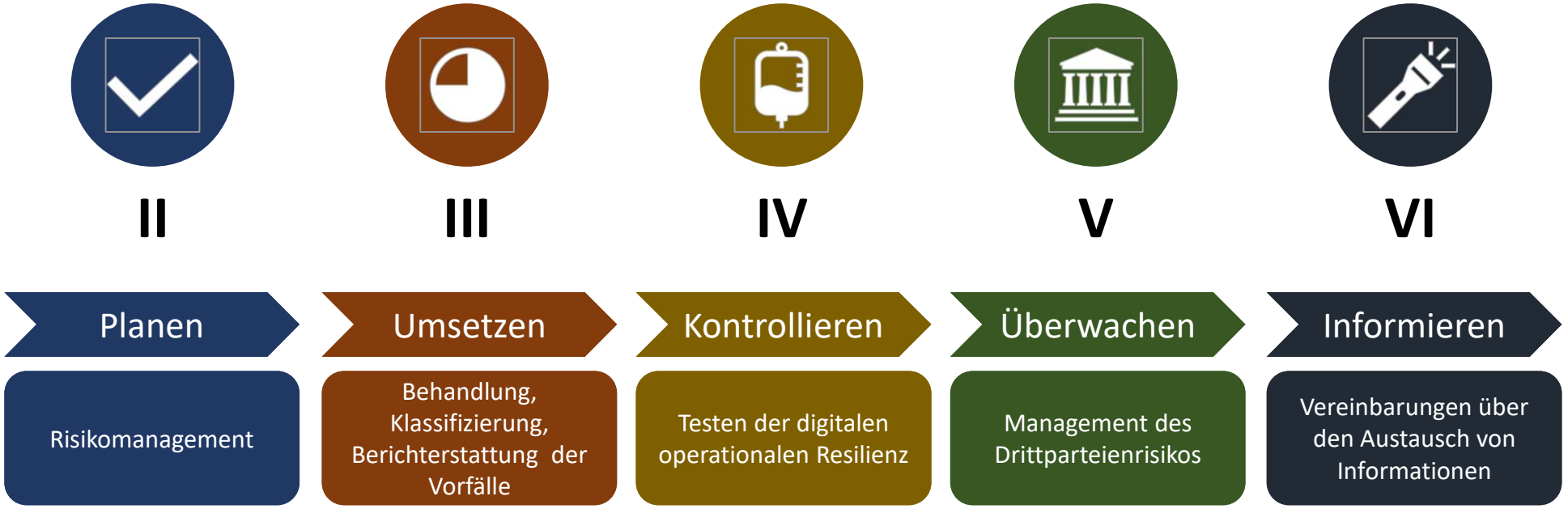
CONSULTING UNION The Origin of Excellence

1. Sie haben Kenntnis über ihre Daten, Systeme, Prozesse entsprechend der Kritikalität ihrer Geschäftsstrategie
2. Sie haben Strategien, Prozesse, Organisationen, Budget, um die formulierten Ziele zu dokumentieren, umsetzen, prüfen und testen zu können.
3. Ihre Organisation ist sich der Aufgaben und Verantwortungen über alle Ebenen bekannt und hat dafür das benötige Wissen und Qualifikationen
4. Dies gilt ebenso für wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.

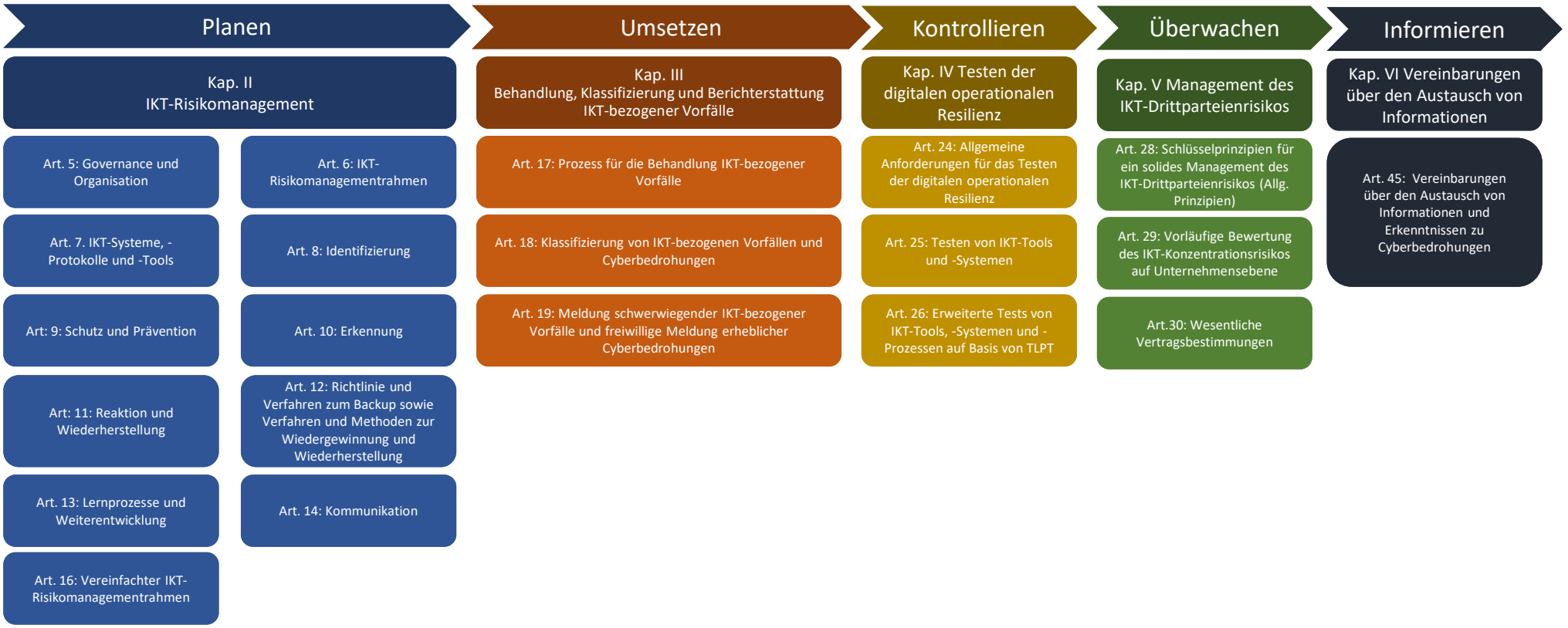
Die 5 für die Umsetzung relevanten ITK-Schwerpunkte

Armodiotita Beratungs-GmbH

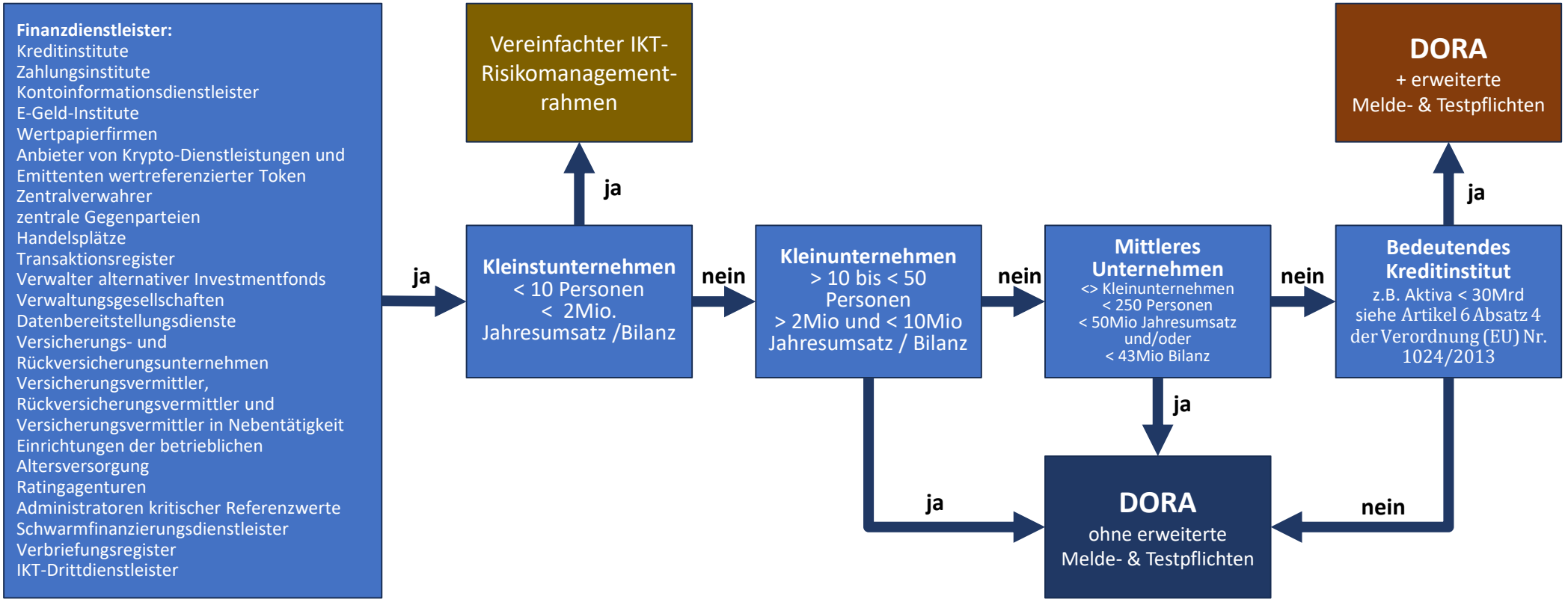
CONSULTING UNION The Origin of Excellence



DORA – Landkarte der relevanten Bausteine



Wer ist von DORA betroffen?



Die besondere Verantwortlichkeit der Unternehmensleitung

Armodiotita Beratungs-GmbH

CONSULTING UNION The Origin of Excellence

- Risikotoleranz des Unternehmens ist von ihr festgelegt
- Rollen und Verantwortlichkeiten mit ITK-Bezug sind definiert
- Business Continuity- und Desaster Recovery-Plänen sind verabschiedet
- Audit-Pläne sind frei gegeben
- Angemessene Budgets sind vergeben
- Über Geschäfte mit Drittparteien und Störfälle muss die Unternehmensleitung ausreichend informiert sein/werden.

Notwendige Aufgaben

Armodiotita Beratungs-GmbH

CONSULTING UNION The Origin of Excellence

1. Prüfen der Relevanz für das Unternehmen
2. Ermitteln des Unternehmensreifegrades, z.B. mittels Quick-Check, externen Auditoren, …
3. Klassifizierung, Gewichtung eventueller Lücken und offener Aufgaben
4. Planung des zu erzielenden Reifegrades, entsprechend der Wichtigkeit und Dringlichkeit
5. Planung der Aktivitäten in Form von Projekten (zielorientiert, terminiert, budgetiert)

Wo steht Ihr Unternehmen?
DORA-Quickcheck zeigt den Reifegrad

Armodiotita Beratungs-GmbH

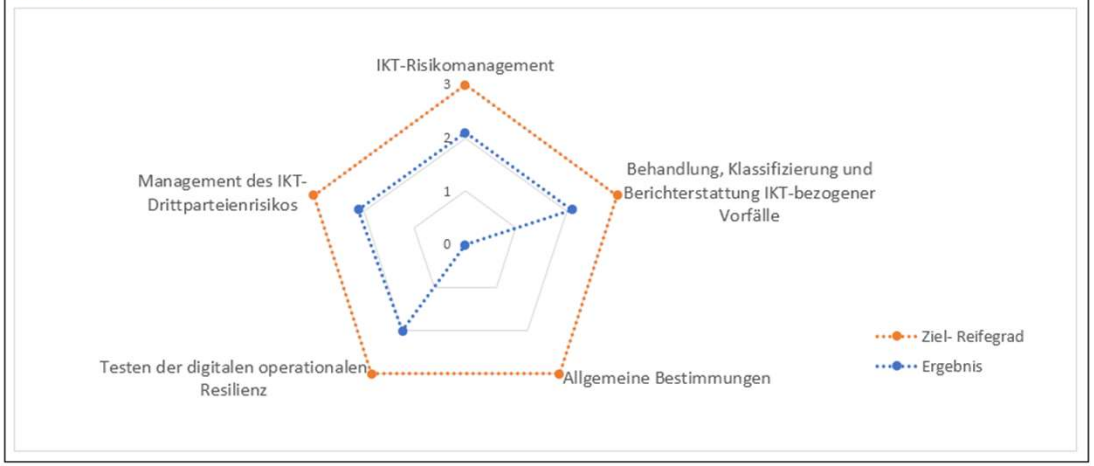
CONSULTING UNION The Origin of Excellence

DORA Assessment

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 14. Dezember 2022
über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG)

Firma:	0		
Datum:	00.01.1900		
Ergebnis mit Kürzung auf Zielreifegrad:	0,00	Maximal erreichbar:	0,00

Ergebnis je Kapitel (relevanz):



Beispiel: Schnelle Reifegradbestimmung mit übersichtlichem Management Report

DORA - Quickcheck - Kapitel
Ergebnisse

Ergebnis mit Kürzung auf Zielreifegrad:	0,00	Maximal erreichbar:	3,00

Details:

Nr.	Kapitel	Ziel-Reifegrad	Ergebnis
DORA-II.I...	IKT-Risikomanagement	3	2
DORA-III....	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	3	2
DORA-III....	Allgemeine Bestimmungen	3	0
DORA-IV. ...	Testen der digitalen operationalen Resilienz	3	2
DORA-V.I...	Management des IKT-Drittparteienrisikos	3	2

Methode: Vergleich von 279 ausgewählten DORA-Themen
- basierend auf DORA Controls
- bewertet nach SPICE ISO 15504

Wo steht Ihr Unternehmen?
DORA-Quickcheck zeigt den Reifegrad

Armodiotita Beratungs-GmbH

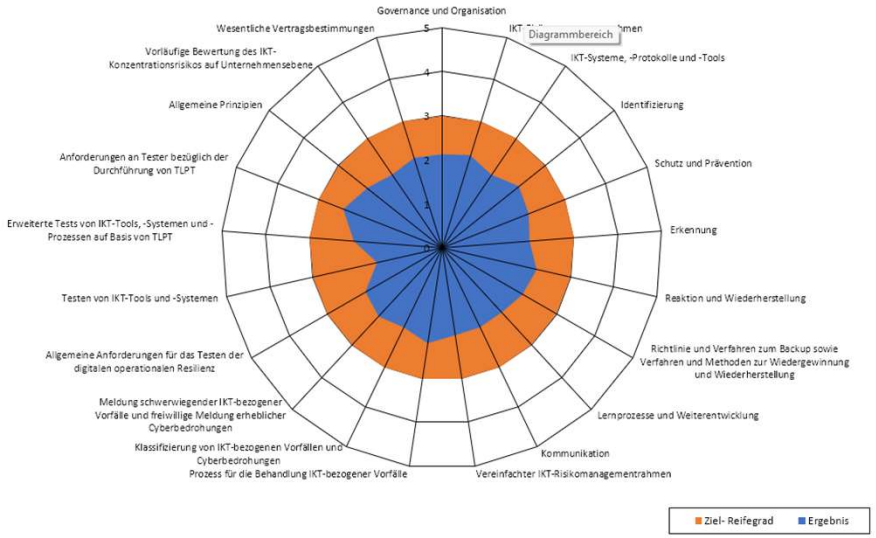
CONSULTING UNION The Origin of Excellence

DORA Assessment

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 14. Dezember 2022
über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG)

Firma:	0		
Datum:	00.01.1900		
Ergebnis mit Kürzung auf Zielreifegrad:	0,00	**Maximal erreichbar:**	0,00

Ergebnis je Artikel (relevanz):



Beispiel: Schnelle Reifegradbestimmung mit detailliertem Management Report

DORA - Quickcheck - Artikel
Ergebnisse

Ergebnis mit Kürzung auf Zielreifegrad:	0,00	**Maximal erreichbar:**	3,00

Details:

Nr.	Kapitel	Artikel	Ziel-Reifegrad	Ergebnis
DORA-II.I.5..	IKT-Risikomanagement	Governance und Organisation	3	2
DORA-II.II.6..	IKT-Risikomanagement	IKT-Risikomanagementrahmen	3	2
DORA-II.II.7..	IKT-Risikomanagement	IKT-Systeme, -Protokolle und -Tools	3	2
DORA-II.II.8..	IKT-Risikomanagement	Identifizierung	3	2
DORA-II.II.9..	IKT-Risikomanagement	Schutz und Prävention	3	2
DORA-II.II.10..	IKT-Risikomanagement	Erkennung	3	2
DORA-II.II.11..	IKT-Risikomanagement	Reaktion und Wiederherstellung	3	2
DORA-II.II.12..	IKT-Risikomanagement	Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung	3	2
DORA-II.II.13..	IKT-Risikomanagement	Lernprozesse und Weiterentwicklung	3	2
DORA-II.II.14..	IKT-Risikomanagement	Kommunikation	3	2
DORA-II.II.16..	IKT-Risikomanagement	Vereinfachter IKT-Risikomanagementrahmen	3	2
DORA-III. .17..	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	Prozess für die Behandlung IKT-bezogener Vorfälle	3	2
DORA-III. .18..	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen	3	2
DORA-III. .19..	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	3	2
DORA-IV. .24..	Testen der digitalen operationalen Resilienz	Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz	3	2
DORA-IV. .25..	Testen der digitalen operationalen Resilienz	Testen von IKT-Tools und -Systemen	3	2
DORA-IV. .26..	Testen der digitalen operationalen Resilienz	Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT	3	2
DORA-IV. .27..	Testen der digitalen operationalen Resilienz	Anforderungen an Tester bezüglich der Durchführung von TLPT	3	2
DORA-V.I.28..	Management des IKT-Drittparteienrisikos	Allgemeine Prinzipien	3	2
DORA-V.I.29..	Management des IKT-Drittparteienrisikos	Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene	3	2
DORA-V.I.30..	Management des IKT-Drittparteienrisikos	Wesentliche Vertragsbestimmungen	3	2

Methode: Vergleich von 279 ausgewählten DORA-Themen
- basierend auf DORA Controls
- bewertet nach SPICE ISO 15504

Kontakt

Armodiotita Beratungs-GmbH
Kaiser-Friedrich-Promenade 14
61348 Bad Homburg v.H.

E-Mail: info@armodiotita.de

Armodiotita steht für **Kompetenz**, in Verbeugung vor den Ursprüngen der Demokratie in Griechenland, dem griechischem Wort **Αρμοδιότητα.**

Consulting Union eG
Hauptstraße 223
65760 Eschborn

E-Mail: info@consulting-union.de

Unser Motto **„Gemeinschaft schafft Mehrwert“ !**