BAI – WEBINAR

DORA KOMMT – SIND SIE STARTKLAR?

Speaker:

Nicole Bittlingmayer, Partnerin Financial Services, Investment Funds & Alternative Investments, Luther Rechtsanwaltsgesellschaft mbH

Wulf Ley, Geschäftsführer, VIVACIS Consulting GmbH

Sven Bittlingmayer, Gründer und Geschäftsführer, KnowledgeRiver GmbH

Sina Nennstiel

Referentin Recht & Policy

Poppelsdorfer Allee 106
53115 Bonn
+49 (0) 228 96987-13
nennstiel@bvai.de

Speaker

Nicole Bittlingmayer

- Partnerin bei Luther im Bereich Financial Services, Investment Funds & Alternative Investments
- Mehr als 20 Jahre Erfahrung in der Beratung deutscher und internationaler Mandanten im dt. Investment- und Aufsichtsrecht

Wulf Ley

- Geschäftsführer der VIVACIS Consulting GmbH
- Schwerpunkt in der Beratung (inter-) nationaler Anbieter von offenen und geschlossenen Fonds, Banken, Wertpapierinstituten und Asset Manager

Sven Bittlingmayer

- Gründer und Geschäftsführer von KnowledgeRiver GmbH
- Verantwortlicher insbesondere für den Bereich IT-Richtlinien-Konformität
- Fast 25 Jahre Erfahrung in IT-Umgebungen von Unternehmen

Agenda

- Eröffnungsworte
- Legal Wrap-Up: DORA im Überblick
- DORA-Grundkonformität: Scoping, Gap-Analyse, Umsetzung
- DORA im Regelbetrieb: DORA-Compliance-Beauftragter und -Plattform
- Q&A

Anstehende Events

BAI InnovationsDay

- 19. September 2024

BAI Real Assets Symposium

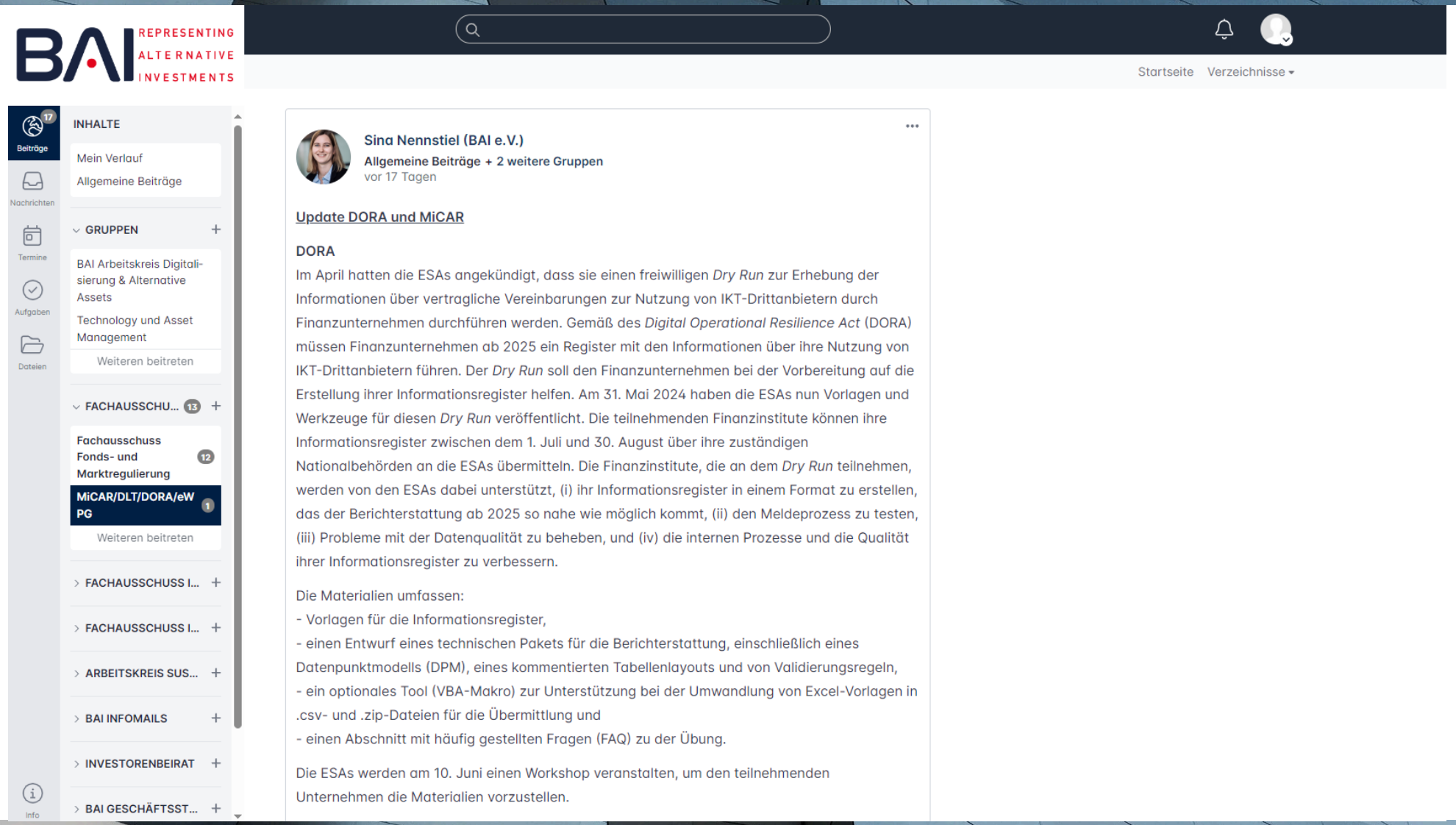
- 1. Oktober 2024

BAI Workshop Sustainable Finance & ESG

- 28. November 2024

Hier geht es direkt zum BAI-Eventkalender

BAI Mitgliederportal: https://www.mitglieder.bvai.de



Luther.

BAI Webinar

DORA kommt - sind Sie startklar?

25. Juni 2024

unyer GLOBAL ADVISORS

Der „Digital Operational Resilience Act“ unter die Lupe genommen

Kooperation

DORA ist Querschnittsthema: Legal, Business Operation, IT-Technology

Luther.

Beratung von Finanzmarktunternehmen zu sämtlichen Compliance- und Governance-Anforderungen, Risikomanagement, Begleitung regulatorischer Transformations-prozesse

Nicole Bittlingmayer
Luther Rechtsanwaltsgesellschaft mbH
Rechtsanwältin, Partnerin
T +49 69 27229 24710
nicole.bittlingmayer@luther-lawfirm.com

VIVACIS Consulting

vivacis.de | info@vivacis.de

Consultingunternehmen im Bereich Banken, Wertpapierinstitute, Kapitalverwaltungsgesell-schaften:

- Prozess-, Organisations- und Strategie-beratung sowie Umsetzung von Regulatorik
- Übernahme operativer Funktionen (Beauftragte für Compliance, Geldwäsche, Datenschutz, Risikomanagement, Informationssicherheit, Interne Revision)

Wulf Ley
VIVACIS Consulting GmbH
Geschäftsführer
T +49 6172 6875 501
wulf.ley@vivacis.de

Knowledge River
Enterprise IT Resilience Optimization

IT-Consultingunternehmen:

Datenerhebung und -Analyse zu IT-Topologie und -Konfiguration sowie Nutzung und Organisation, automatisierte Dokumentationen und Analyse-Reports unter Berücksichtigung kundenspezifischer Compliance-Anforderungen (IT-Sicherheit, Regulatorik)

Sven Bittlingmayer
KnowledgeRiver GmbH
Geschäftsführer
T +49 6134 5004869
Sven.Bittlingmayer@KnowledgeRiver.com

Cyberrisiken im Fokus der BaFin

„Die BaFin hat daher die Resilienz der großen Cloud-Dienstleister schon seit einer Weile im Blick. Eine große Chance bietet zudem DORA, der Digital Operational Resilience Act. Mit ihm wird es uns künftig leichter fallen, stärkeren Einfluss auf sie auszuüben.“

(Kurzkommentar von BaFin-Präsident Mark Branson im BaFinJournal, 5. Dezember 2023)

Gründe für DORA

Fraktionierte Geschäftsprozesse, komplexe IT-Infrastrukturen, zunehmende Digitalisierung, Nutzung von IKT- Dienstleistungen (z. B. Cloud-basierte Geschäftslösungen).

Cyberkriminelle finden neue Angriffsflächen zur Destabilisierung des Finanzmarktes.

IKT-Vorfälle führen zu Reputations-verlusten und hohen Schadenssummen bei den Betroffenen.

Keine einheitliche Regulierung/ Verwaltungspraxis zur Stabilisierung und Resilienz des Finanzmarktes auf europäischer Ebene.

Obwohl die Anzahl an Cyberattacken erheblich zugenommen hat und die gestiegenen IKT-Risiken bekannt sind, gab es auf **EU-Ebene** für Finanzunternehmen und IKT-Drittdienstleister **keine einheitlichen Regelungen zur Stabilisierung der digitalen, operationellen Resilienz**.

Die Ausgangslage für DORA

- Die **Digitalisierung**, der zunehmende **Einsatz von Cloud-basierten Geschäftslösungen** und die **Vernetzung von Daten, Objekten und Systemen** durch komplexe IT-Infrastrukturen und Geschäftsprozesse eröffnen für die Finanzbranche enorme Chancen.
- Dies birgt **unvorhersehbare Risiken** und bietet Cyberkriminellen neue Angriffsflächen. Durch steigende Cyberangriffe ist es für Finanzunternehmen – auch im Sinne ihrer Kunden – notwendiger denn je, sich auf Vorfälle vorzubereiten und **Maßnahmen zur Stärkung der Cyberresilienz** einzuführen und so ernsthafte finanzielle und reputative Schäden zu vermeiden.
- Gezielte **Cyberattacken** (z. B. Phishing) führen zu höheren Erfolgsquoten für Angreifer und **größeren Schadenssummen bei den Opfern**.
- Gesetzliche und regulatorische Vorgaben führen zur **Verschärfung der aufsichtlichen Überwachung der IT**.
- Die **Prämien für Cyber-Haftpflichtversicherungen steigen** weiter oder die Versicherer verweigern ihren Kunden die Versicherung, was die Risiken für Unternehmen erhöht. Zukünftig stehen **Reformen bei den Auszahlungen von Cyber-Versicherungen** an – dabei steigen auch die Anforderungen an proaktive Maßnahmen der Unternehmen zum Management ihres Cyberrisikos.

Ziele von DORA

- Stärkung der Widerstandsfähigkeit und Sicherheit des gesamten europäischen Finanzsektors
- Schaffung einheitlicher und konsistenter Anforderungen für den Finanzsektor in puncto Cybersicherheit, IKT-Risiken und digitale operationale Resilienz
- Berücksichtigung proportionaler Anforderungen an an Finanzsektor (Prinzip der Proportionalität)

Betroffene Akteure

EU-Finanzunternehmen*

Die Anforderungen gelten für regulierte Finanzunternehmen:

- **Kreditinstitute,**
- **Zahlungsinstitute,**
- **Kapitalverwaltungsgesellschaften,**
- **Versicherungen,**
- **Wertpapierfirmen,**

sowie weitere Unternehmen mit Finanzbezug:

- Anbieter von Krypto-Dienstleistungen,
- Ratingagenturen,
- Zentralverwahrer,
- Einrichtungen der betrieblichen Altersversorgung
- etc.

IKT-Drittdienstleister

IKT-Dienstleistungen sind „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern erbracht werden, einschließlich Diensten für die Bereitstellung, Eingabe, Speicherung und Verarbeitung von Daten und Berichterstattungsdiensten, Datenüberwachung sowie datenbasierter Dienste und Diensten für Entscheidungsunterstützung."

Damit sind jedenfalls auch Anbieter von Cloud-Diensten, Software, Datenanalyse und Rechenzentren, die von Finanzunternehmen zur Erbringung ihrer Leistungen eingesetzt werden, gemeint.

Zuständige Behörden

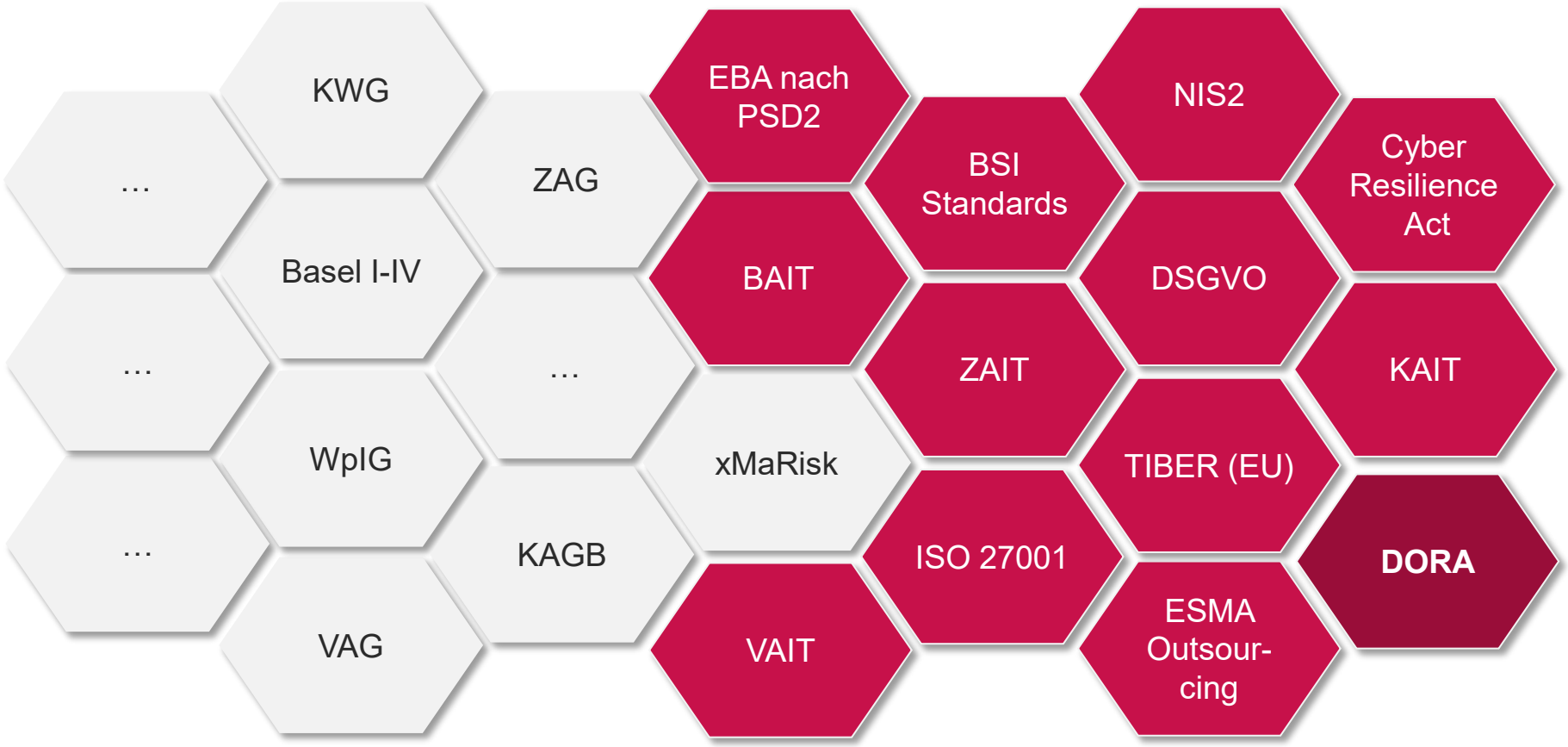
Jeweils eine der folgenden (Europäischen) Aufsichtsbehörden wird dazu ernannt, die Finanzunternehmen und ihre zugehörigen kritischen Drittanbieter (CTPP) zu kontrollieren und Standards zu gewährleisten:

- Nationale Aufsichtsbehörde (z. B. BaFin),
- Europäische Bankaufsichtsbehörde (EBA),
- Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA),
- Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA).

* Befreiungen und Erleichterungen:

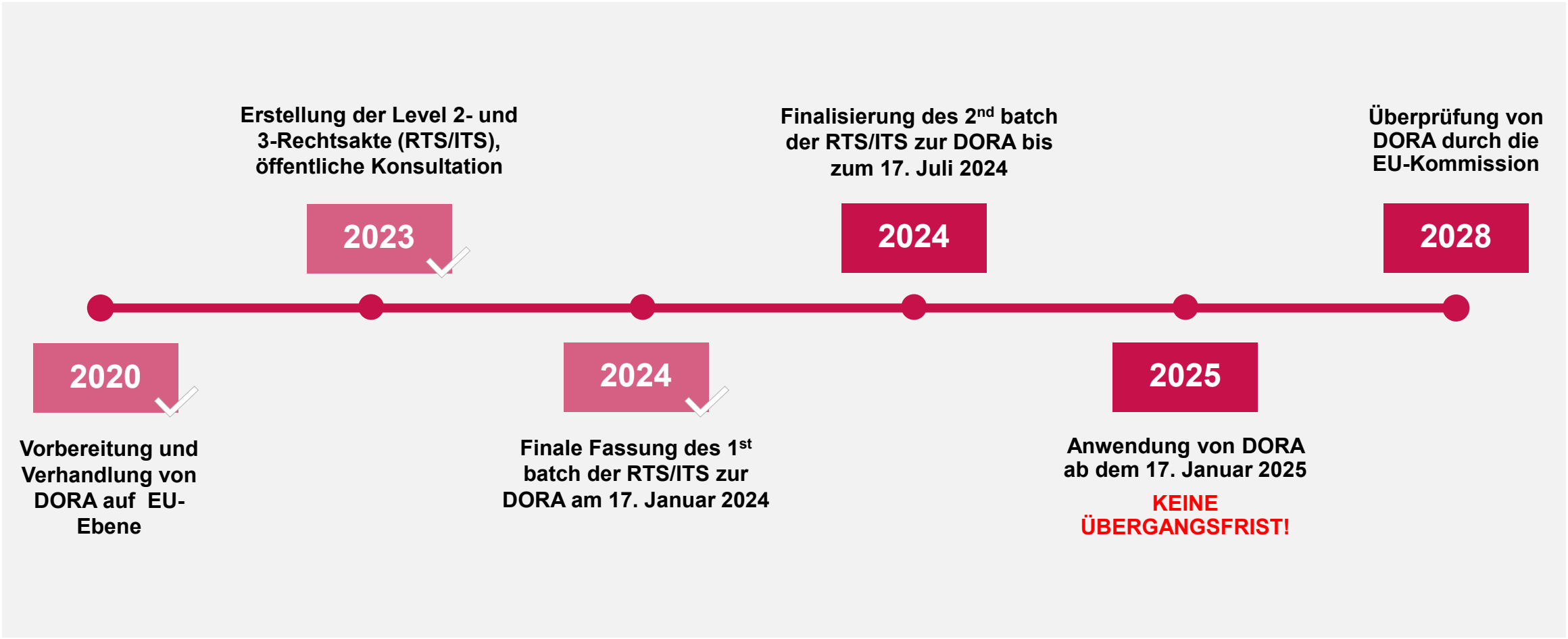
- für Kleinstunternehmen mit weniger als 10 Mitarbeitern und einem Jahresumsatz bzw. einer Bilanzsumme unter EUR 2 Mio.
- Größenabhängige Erleichterungen („Proportionalitätsgrundsatz")

Die Regelungen in DORA stehen im Kontext mit weiteren Gesetzen, FAQs, Verordnungen, Richtlinien…

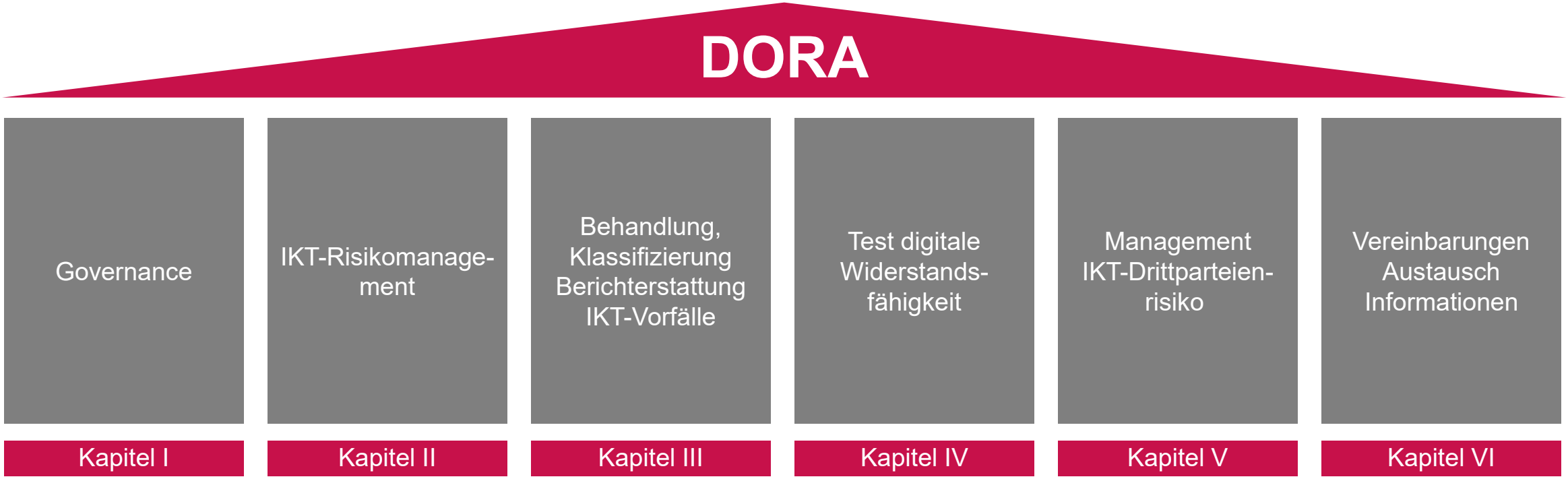


DORA fokussiert sich auf digitale Betriebsstabilität, Vorfälle und Risiken. Bei **xAIT** handelt es sich um die maßgebende nationale Richtlinien für Risikomanagement, IT Governance und Informationssicherheit, diese werden nach Information der BaFin **aufgehoben**.

Zeitschiene



Die sechs DORA-Säulen im Überblick



Die in DORA formulierten regulatorischen Anforderungen werden in 13 delegierten EU-Rechtsakte als RTS/ITS konkretisiert.

DORA erfordert interdisziplinäre Anwendungskompetenz aus tiefem juristischen Know-how, intensiver Erfahrung mit regulatorischen Transformationsprozessen, hohem Verständnis von IT-Betrieb bzw. -Management und Zusammenarbeit von Akteuren in fraktionierten, aufsichtsrechtlich geprägten Geschäftsstrukturen.

Grundsatz der Proportionalität

DORA gilt als **einheitliches Regelwerk** für den gesamten Finanzsektor

Finanzunternehmen mit **unterschiedlichen Risikoprofilen und Betriebsgrößen**

ausgewogener risikobasierter Ansatz für die Anwendung der DORA-Vorschriften

Vereinfachter Risikomanagementrahmen für bestimmte Finanzunternehmen (z.B. kleine und nicht verflochtene Wertpapierfirmen)

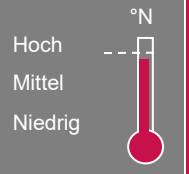
Weitreichende **Erleichterungen/Ausnahmen für Kleinstunternehmen**

Exkurs: Erste Beurteilung identifizierter Handlungsfelder

Governance

- Überprüfung, Anpassung bzw. Erstellung der Dokumentation des internen Governance- und Kontrollrahmens im Hinblick auf Cyber- und IKT-Sicherheitsrisiken (Rahmenanweisung DORA).
- Schulung und Fortbildung.
- ...

IKT-Risikomanage-ment



- Überprüfung der Dokumentation zum IKT-Risiko-managementrahmen (insb. Strategie, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle).
- Maßnahmen zur Erkennung IKT-bezogener Vorfälle.
- IKT-Notfallmanagement.
- Bereitstellung ausreichender Kapazitäten und Ressourcen.
- …

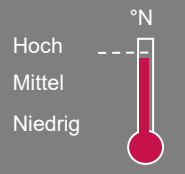
Regelungen für Tests

- Durchführung Systemtests in regelmäßigen Abständen; mindestens einmal pro Jahr.
- Automatisierte Aufbereitung Ist-Zustand IT (Topologie, Konfiguration); in verschiedenen Detailgraden unterschiedliche Bedrohungsszenarien zu berücksichtigen.
- Lösung zur teilautomatisierten Erstellung von Dokumentationen basierend auf gesammelten Daten und aufbereiteten Informationen: IT- Infrastruktur, DORA, Pen-Test-Vorbereitung und Durchführung.
- …

IKT-Berichter-stat-tung

- Definition Frühwarnindikatoren für IKT-Vorfälle.
- Implementierung Risikomanagementprozess für IKT-Vorfälle.
- Klassifizierung möglicher Vorfälle bzw. Störungen in der standardisierten Berichterstattung.
- …

Risiko-Manage-ment IKT-Dritt-anbieter



- Review Due Diligence IKT-Drittparteien (Auswahl, Geeignetheit), Prüfung (Unter-)Auslagerungsvertrags-dokumentation mit IKT-Dienstleistern.
- Anpassung/Verhandlung Verträge (unter Berück-sichtigung Mindestanforderungen sowie IT-Recht).
- Anpassung/Erstellung Auslagerungsstrategie.
- Etablierung Berichtswesen, Prüfung der Berechtigungen, auf Dokumente zuzugreifen.
- Durchführung Vor-Ort-Prüfungen; Aussprache von Empfehlungen oder Anweisungen.
- …

Informationsaus-tausch

- Erstellung Vereinbarungen zum Informationsaustausch.
- Unterstützung bei Etablierung des Informationsregisters.
- IT-gestützte Vorfallsaufbereitung.
- …

So können sie planvoll und effizient die DORA-Vorgaben umsetzen

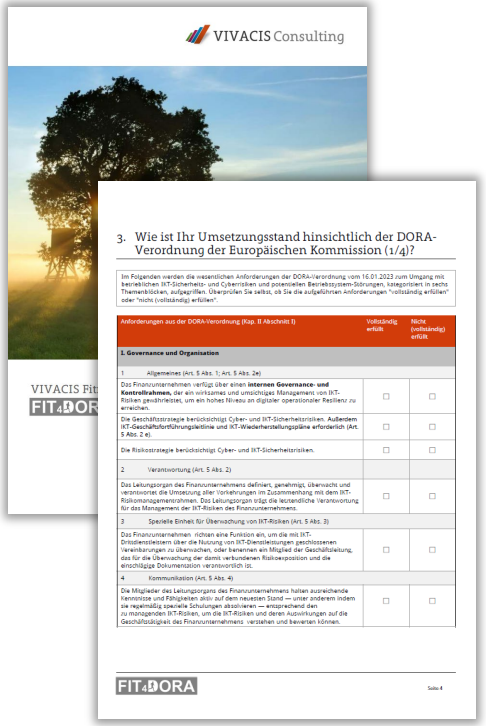
Scoping | Gap-Analyse | Priorisierung Ergebnisse & Umsetzungsplan | Umsetzung

Projekt Management (Support)

Scoping

- Klärung Geltungsbereich DORA
- Definition Parameter für die Beurteilung
  - Grad der Fertigungstiefe/ Dienstleister-struktur
  - Gesellschaftsrechtliche Ausgangslage (Gruppenzugehörigkeit/Stand Alone)
  - Bisherige regulatorische Erfahrung im Bereich IKT (des Dienstleisters)
- Festlegung Dokumentenuniversum
- Toolset zur Unterstützung: z.B. FitnessCheck DORA

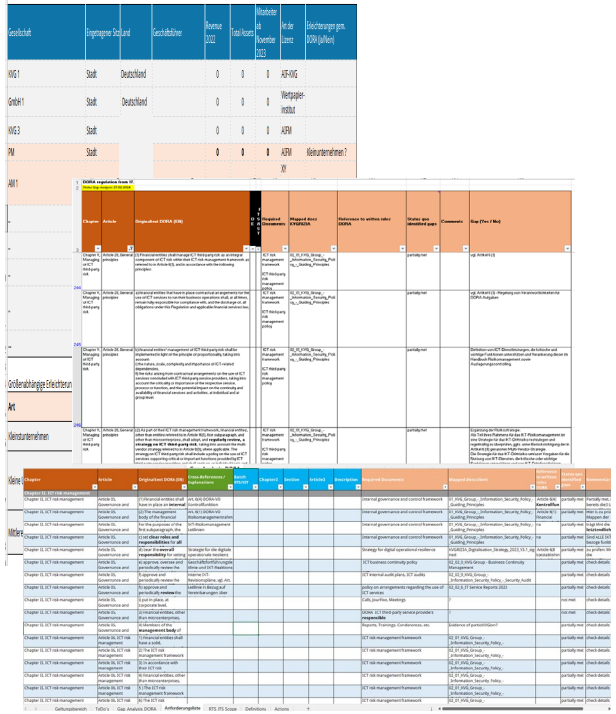
Ziel: Betroffenheitsfeststellung



Gap-Analyse

- Herausforderung Festlegung des „richtigen“ Betrachtungsniveaus (High Level vs. Detailanalyse)
- Definierte Gesellschaften nach derzeitigem Stand DORA mit aktuellem Umsetzungsstand SFO abgleichen.
- Erhebung über bereitgestellte Dokumente bzw. Durchführung von Interviews
- GAPs aufzeigen, bewerten und Handlungsmaßnahmen ableiten.
- Toolset: Excel-Tapete

Ziel: Ist-Situation strukturiert aufnehmen und Handlungsbedarf aufzeigen



Unternehmens-IT: Rückgrat und Achillesferse zugleich

BaFin: „Mit DORA [...] hat die Europäische Union eine finanzsektorweite Regulierung für die Themen **Cybersicherheit, IKT-Risiken** und **digitale operationale Resilienz** geschaffen.“

Abgeleitete IT-Anforderungen (Ausschnitt)

- **Berichtswesen** (Empfänger: Aufsichtsbehörden, Wirtschaftsprüfer und/oder unternehmensinterne Gremien)
  - Dokumentation der DORA-Konformität
  - Dokumentation von Tests und Prüfungen
  - Dokumentation des Risikomanagements (z.B. Praktiken und IKT-Drittanbieter-Risiken)
  - Dokumentation von IKT-Sicherheitsmaßnahmen
  - Handbücher wie z.B. Notfall- und Betriebshandbuch
- **Meldewesen** (Empfänger: Aufsichtsbehörden)
  - IKT-Vorfälle
  - Meldungen an das Informationsregister (z.B. Liste kritischer IKT-Drittdienstleister + Vertragsparameter)
  - Informationsaustausch zur gemeinsamen Bekämpfung von Bedrohungen
- **Prüfwesen** (Empfänger: Unternehmensinterne Gremien)
  - Penetrationstests (Achtung: adressiert nur Cybersicherheit!)
  - Backup/Restore-Tests
  - Disaster-Recovery-Tests
  - KPI-Einhaltung

PHASE 2

- **Transformation zur DORA-Konformität**
  - Schritt 1:
    Die in Phase 1 (Scoping + Gap-Analyse) erkannten Schwachstellen als „Work Items“ zeitlich und thematisch (IT, Prozesse, Recht) einordnen sowie priorisieren
  - Schritt 2:
    Teams zusammenstellen, Umsetzung planen, Projektdurchführung leiten und überwachen

Umsetzung von DORA im (IT-)Regelbetrieb

PHASE 3

- **Digitale DORA-Plattform zur Automatisierung und Zusammenarbeit**
  - (Teil-) automatisierte Sammlung bzw. Anbindung von relevanten Daten und Informationen
  - Automatisierte Erstellung von Dokumentationen basierend auf kundenspezifischen Templates
  - Plattform zur Vorbereitung, Durchführung und Dokumentation von Resilienz-Tests
  - Automatisierung des Meldewesens (beinhaltet z.B. auch Sammlung von Konfigurations- und Log-Daten zum Zeitpunkt eines IKT-Vorfalls)
  - Daten- und Kommunikationsplattform für alle Stakeholder: Mitarbeiter des Unternehmens, Informationssicherheitsbeauftragte (ISB), IT-Provider, IKT-Drittdienstleister, Juristen und Prozess-Spezialisten

- **Funktion: „DORA Compliance Officer“**
  - Zentraler Kommunikationspunkt für alle DORA-Compliance-Angelegenheiten
  - Benötigt technische Fachexpertise und sehr gute Übersicht über bestehende DORA-Anforderungen und Neuerungen
  - Weiterentwicklung von internen und externen Prozessen
  - Kontaktpflege zu allen Stakeholdern

Vielen Dank!

Luther.

Die Angaben in dieser Präsentation sind ausschließlich für die genannte Veranstaltung bestimmt. Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers. Die hier zusammengestellten Texte und Grafiken dienen allein der Darstellung im Rahmen dieser Veranstaltung und dokumentieren die Thematik ggf. nicht vollständig.

Die Präsentation stellt keine Rechts- oder Steuerberatung dar und wir haften daher nicht für den Inhalt. Diese erfolgt individuell unter Berücksichtigung der Umstände des Einzelfalls auf der Grundlage unserer Mandatsvereinbarung. Die Verteilung, Zitierung und Vervielfältigung – auch auszugsweise – des Inhalts zum Zwecke der Weitergabe an Dritte ist nur nach vorheriger Absprache gestattet.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com