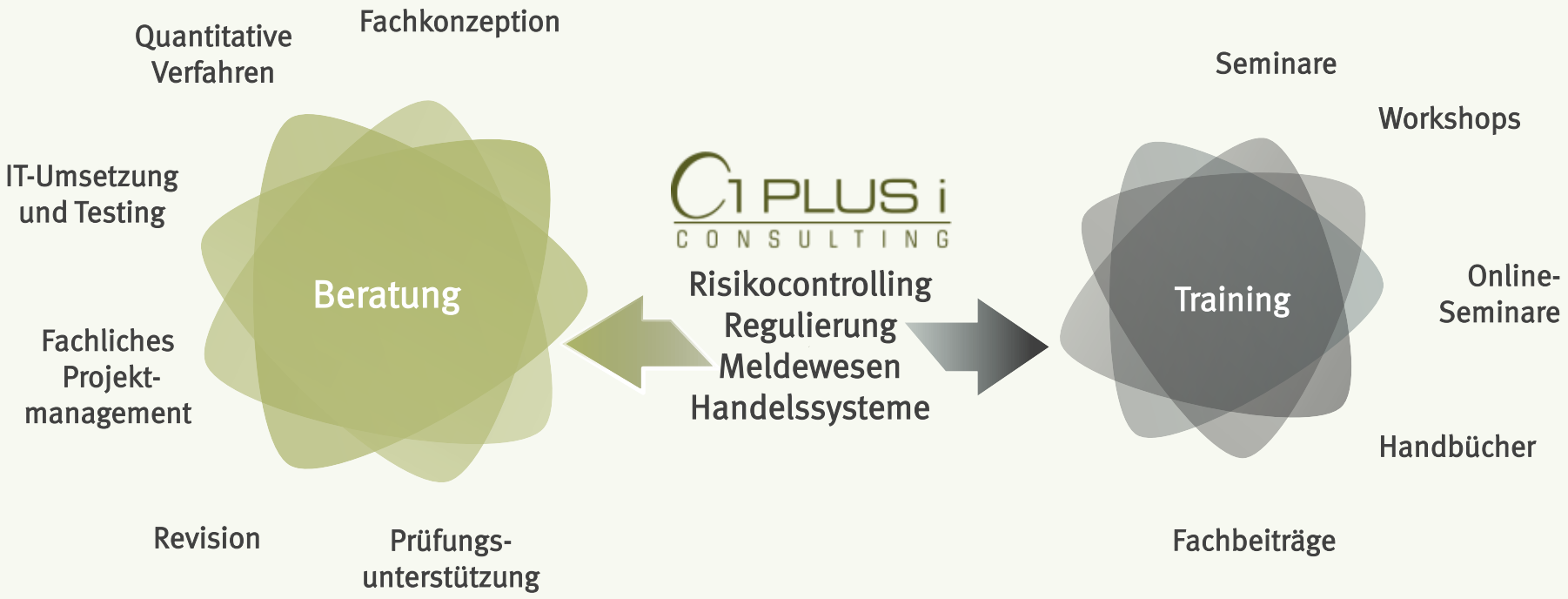
C1 PLUS i CONSULTING

Friederike Krüsemann
Lukas Görnert

DORA AUS MANAGEMENTPERSPEKTIVE

Kundensymposium 19. März 2026

1 PLUS I – BERATUNG UND TRAINING AUS EINER HAND



Mehr als 40 Mitarbeiter

Kunden: Mehr als 350 Banken, Finanzdienstleister und banknahe Rechenzentren

Seit 2003 am Markt

UNSERE BERATUNGSFELDER IM ÜBERBLICK

Regulierung & Meldewesen

- CRR
- COREP (KSA, IRBA, etc.)
- EMIR | SFTR | MMSR
- MiFID II | MiFIR
- DORA
- BRRD | SRM-VO | SAG
- Sonstiges Meldewesen
- SFDR | CSRD | ESG-Offenlegung

Risikomanagement

- SREP & MaRisk
- ICAAP & RTF
- Risikomodelle
- ESG-Risiko
- Ratingverfahren
- IRRBB & Marktrisiko
- Stresstesting
- Validierung und Modellrisiko
- ILAAP

Systeme

- Meldewesensoftware
- Handelssysteme
- Gesamtbanksteuerung
- IDV-Anwendungen
- Schnittstellen

Übergreifende Themen

- Interne Revision
- Test-management
- Fachliches Projektmanagement
- Reporting
- Künstliche Intelligenz

IMMER AUF DEM LAUFENDEN MIT 1 PLUS I

1 PLUS i FACHBEITRÄGE

Interesse an unseren regelmäßigen Fachbeiträgen? Melden Sie sich für unseren Fachbeitragsverteiler an oder folgen Sie uns auf LinkedIn!

Jetzt anmelden!

Folgen Sie uns auf LinkedIn®

AGENDA

1 **Einordnung & Zielsetzung**

2 DORA-Gesamtarchitektur und Governance

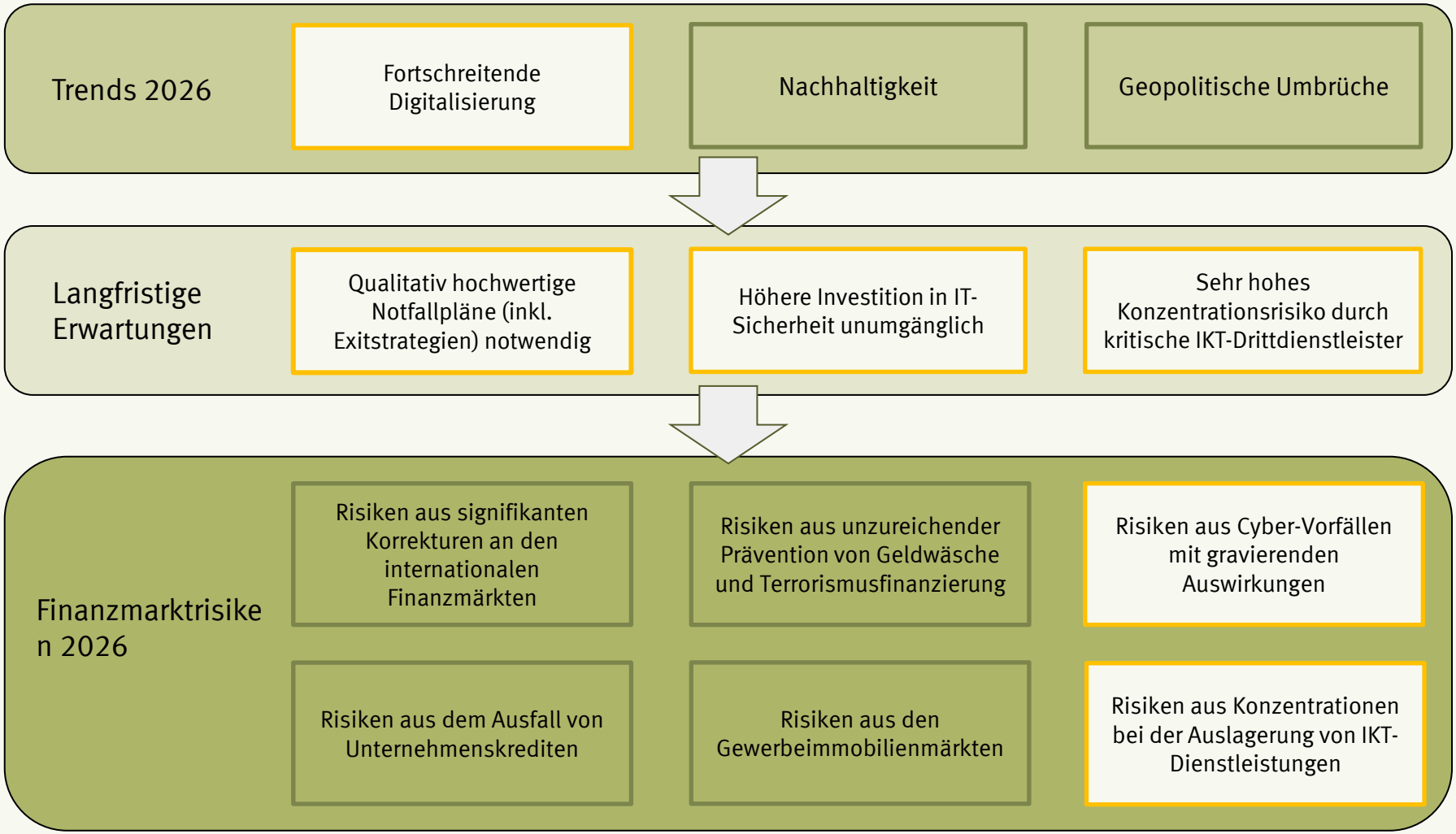
3 Schnittmengen ICAAP, XAIT & DORA

4 Abgrenzung Auslagerungen vs. IKT-Drittdienstleister

5 Berichtswesen unter DORA

6 KI und DORA

IT RISIKEN IM FOKUS DER BAFIN



ZIELE VON DORA

- Finanzsektorweite Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz
- EU-weite Harmonisierung der Regeln für das IKT-Risikomanagement
- Stärkung digitale operationale Resilienz im Finanzsektor
- Schaffung eines einheitlichen Rahmens im IKT-Risikomanagement

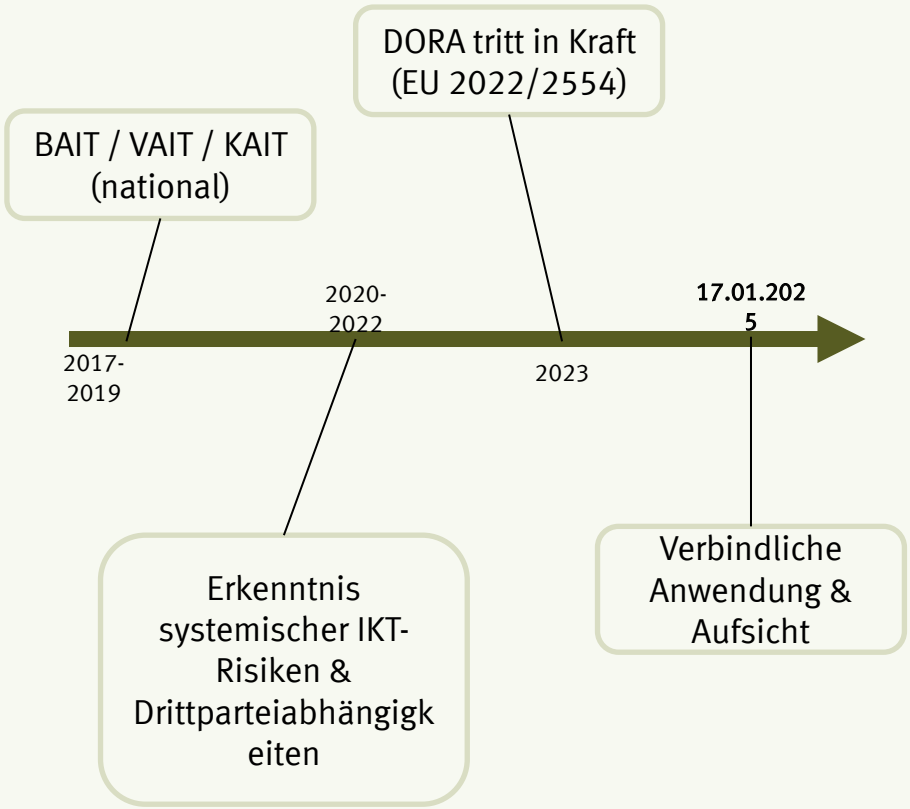
PFLICHT FÜR WEN? ART. 2: ANWENDUNGSBEREICH

DORA gilt für
(fast) Alle*

- a) Kreditinstitute
- b) Zahlungsinstitute
- c) Kontoinformationsdienstleister
- d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG
- e) Wertpapierfirmen
- f) Anbieter von Krypto-Dienstleistungen und Emittenten wertreferenzierter Token
- g) Zentralverwahrer
- h) zentrale Gegenparteien
- i) Handelsplätze
- j) Transaktionsregister
- k) Verwalter alternativer Investmentfonds
- l) Verwaltungsgesellschaften
- m) Datenbereitstellungsdienste
- n) Versicherungs- und Rückversicherungsunternehmen
- o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit
- p) Einrichtungen der betrieblichen Altersversorgung
- q) Ratingagenturen
- r) Administratoren kritischer Referenzwerte
- s) Schwarmfinanzierungsdienstleister
- t) Verbriefungsregister
- u) IKT-Drittdienstleister

* Besonderheit: FinmadiG schließt Leasinggesellschaften ab 2027 ein

REGULATORISCHER KONTEXT



- Dora ist die konsequente Weiterentwicklung der nationalen Rahmenwerke
  - BAIT (Banken)
  - VAIT (Versicherungen)
  - KAIT (Kapitalverwaltungsgesellschaften)
- DORA ist EU-weit einheitlich und unmittelbar anwendbar (Verordnung)
- Sektorübergreifend
  - Banken,
  - Versicherungen,
  - KVG,
  - Zahlungsdienstleister

DORA ersetzt xAIT nicht technisch, sondern überführt deren Kerngedanken in eine verbindliches, EU-weites Resilienzmodell – mit deutlich höheren Anforderungen an Governance, Transparenz & Steuerungsfähigkeit

AGENDA

1 Einordnung & Zielsetzung

2 **DORA-Gesamtarchitektur und Governance**

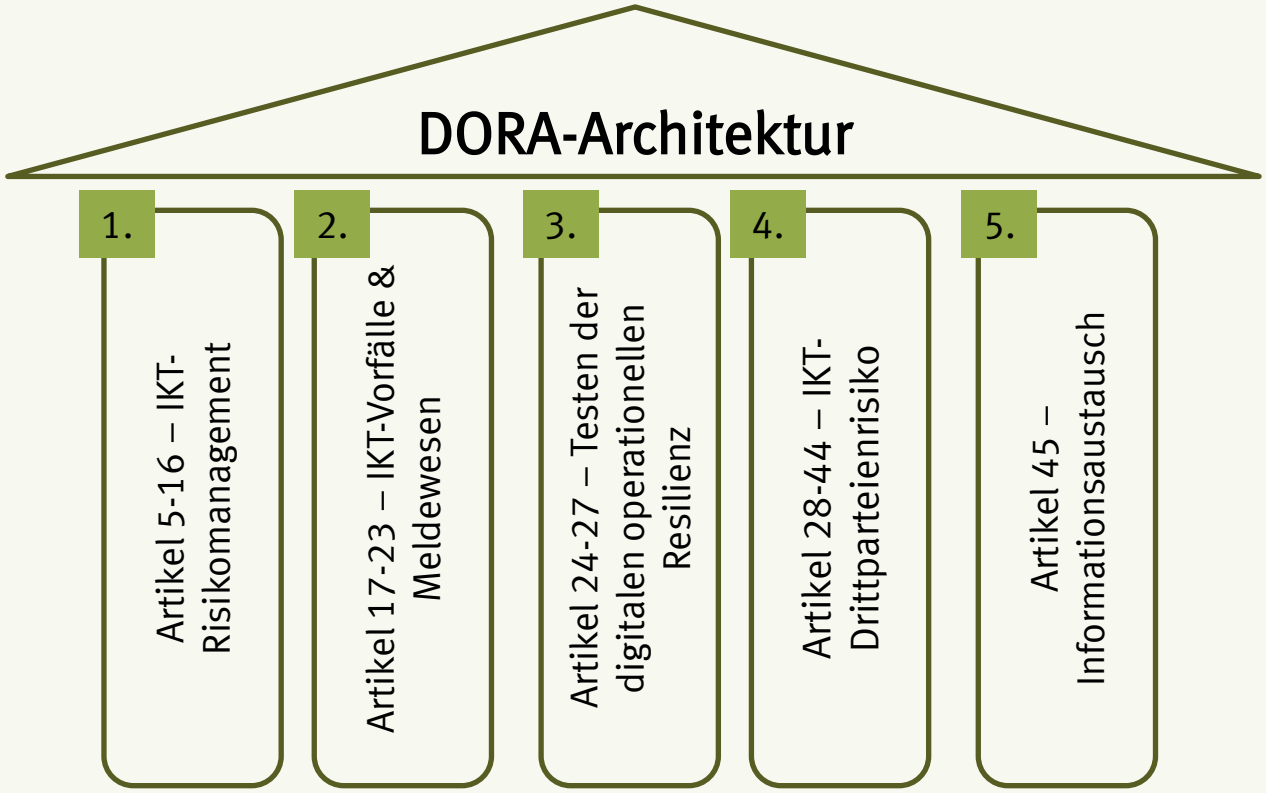
3 Schnittmengen ICAAP, XAIT & DORA

4 Abgrenzung Auslagerungen vs. IKT-Drittdienstleister

5 Berichtswesen unter DORA

6 KI und DORA

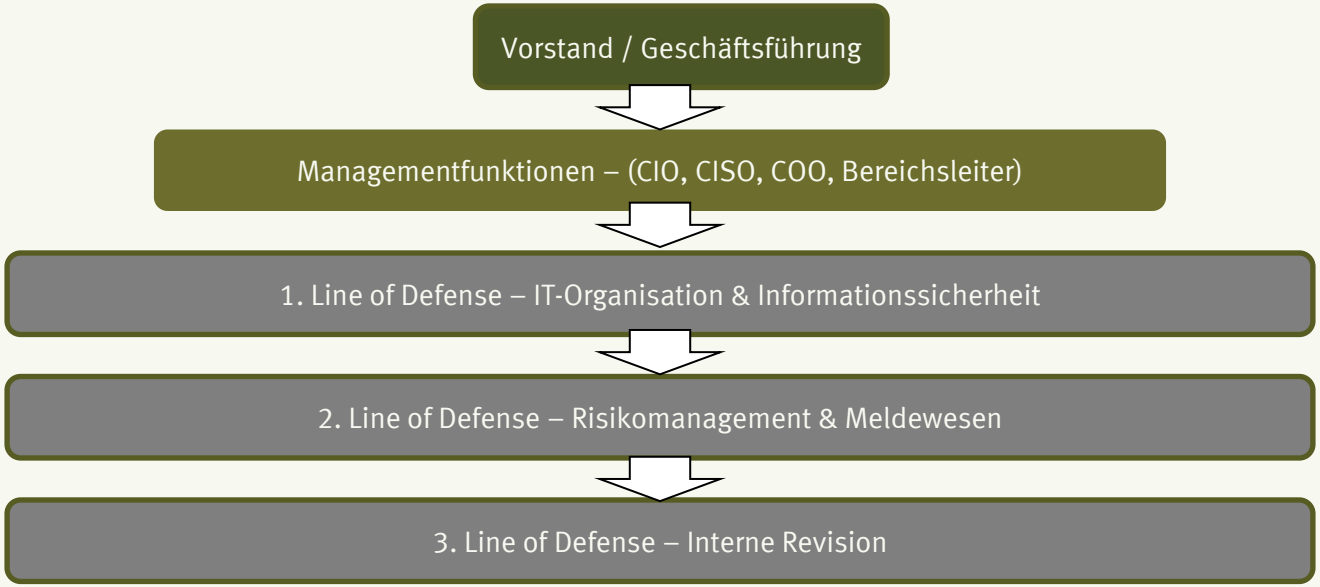
DORA IM ÜBERBLICK – DIE 5 SÄULEN DER DORA-ARCHITEKTUR



Keine Säule steht für sich alleine. Schwächen in der einen Säule untergraben die gesamte Architektur. DORA wird horizontal geprüft.

GOVERNANCE-STRUKTUR: ROLLEN UND VERANTWORTLICHKEITEN

- DORA verlangt nachvollziehbare und wirksame Governance-Architektur für IKT-Risiken
- Kernprinzipien:
  - Eindeutige Zuständigkeiten
  - Trennung von Verantwortung, Umsetzung, Kontrolle
  - Klare Eskalations- und Entscheidungswege
  - Dokumentation aller wesentlichen Rollen



GOVERNANCE-MODELL IKT-RISIKOMANAGEMENTRAHMEN

IKT-Risikomanagementrahmen

Governance

- Leitungsorgan
- Kontrollfunktion
- IKT-Risikomanagement
- Kontinuierliche Weiterentwicklung

Identifikation

- IKT-Risiken
- Geschäftsprozesse
- Information- und IT-Assets
- IKT-Drittbezüge

Prävention und Detektion

- Schutz von IT-Assets
- Erkennungsmechanismen für anormale Aktivitäten
- BCM
- IKT-Risiken im DPM
- Schulung & Sensibilisierung
- Testen der Notfall- und Krisenpläne
- Testen der digitalen operationalen Resilienz

Reaktion und Wiederherstellung

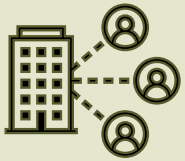
- Behandlung IKT-bezogener Vorfälle
- Geschäftsfortführung- und Reaktionspläne
- Kommunikation in Not- und Krisenfällen
- Backup und Wiederherstellung
- Exitstrategien
- Lernprozesse und Weiterentwicklung

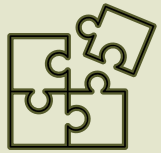
Reporting & Überwachung

- Reporting an das Leitungsorgan
- Resilienzmessung
- Überwachung technologischer Entwicklungen
- Reporting an die Aufsicht
- Meldung an die Aufsicht

IDENTIFIZIERTE HERAUSFORDERUNGEN

- Klar dokumentierte Vorgaben inkl. überprüfbarer Ziele
- Aktive Rolle des Leitungsorgans
- Ermittlung kritischer und wichtiger Funktionen
- Vollständige und aktuelle Inventare
- Klare Verantwortlichkeiten und Prozesse
- Unabhängige und wirksame IKT-Kontrollfunktionen
- Etablierung Schwachstellenmanagement
- Risikomanagement bei IKT-Drittdienstleistern
- Vollständige Anbindung an zentrales Überwachungssystem
- Klare Abläufe für Alarmbearbeitung und Eskalation
- Notfall- und Wiederherstellungspläne haben und umsetzen
- Regelmäßige Sensibilisierung von Mitarbeitenden
- Nachverfolgung von Mängeln





Quelle: BaFin Veranstaltung "Das erste Jahr DORA", Dez. 2025

MÖGLICHE PRÜFUNGSFRAGEN

Wie wird sichergestellt, dass das Leitungsorgan seine Aufgaben systematisch wahrnehmen kann?

Wie ist der Prozess, um den IKT-Risikomanagementrahmen stets aktuell und vollständig zu halten?

Wie oft wird der IKT-Risikomanagementrahmen von der internen Revision geprüft und wie werden die Prüfer zu dem Thema ausgebildet?

Wie werden die Inventare geführt?

AGENDA

1 Einordnung & Zielsetzung

2 DORA-Gesamtarchitektur und Governance

3 **Schnittmengen ICAAP, XAIT & DORA**

4 Abgrenzung Auslagerungen vs. IKT-Drittdienstleister

5 Berichtswesen unter DORA

6 KI-Agenten und DORA

SCHNITTSTELLEN ZWISCHEN DORA & ICAAP

	ICAAP Element	Beitrag des IKT-Risikomanagements
1.	Risikoinventar	Vollständige Erfassung wesentlicher IKT-Risiken
2.	Risikobewertung	Bewertung von Geschäftsunterbrechungen & Abhängigkeiten
3.	Risikoappetit	Toleranz für Ausfälle, Incidents, Abhängigkeiten
4.	Risikosteuerung	Maßnahmen zur Prävention & Resilienz
5.	Reporting	Entscheidungsrelevante Informationen für das Leitungsorgan

DORA operationalisiert den ICAAP dort, wo digitale Abhängigkeiten kritisch werden

WEITERENTWICKLUNG DER XAIT ZU DORA

1. IKT-Risikomanagementrahmen

- Vorgaben DORA-Strategie
- Einführung kritische wichtige Funktionen
- Etablierung IKT-Kontrollfunktion
- Weiterführende Vorgaben zu bspw. Schwachstellen- oder Notfallmanagement

2. IKT-bezogene Vorfälle

- Vorgaben zu Meldung und Klassifizierung von IKT-Vorfällen
- Erstellung Inventar Cyberbedrohung
- Erstellen Kommunikationsstrategie
- Vorgaben Berichterstattung

3. Management des IKT-Drittparteienrisikos

- Einführung IKT-Dienstleistungsbegriff
- Überwachungserweiterung der regulierten Dienstleistungen
- Weiterführende Vorgaben zu bspw. Due Diligence oder Konzentrationsrisiken

4. Testen der digitalen operationalen Resilienz

- Einführung TLPT
- Verpflichtendes jährliches Testen von IKT-Systemen
- Erstellen Programm für Tests

5. Informationsaustausch

- Freiwillige Vereinbarungen zum Austausch
- Implementierung von Umsetzungsstrategien

MÖGLICHE PRÜFUNGSFRAGEN

Wie sind die Verantwortlichkeiten bzgl. der Kommunikationsstrategie verteilt?

Wie werden die kritisch wichtigen Funktionen definiert?

Welche Tests führt das Institut in welchem Rhythmus durch?

Wurde eine IKT-Kontrollfunktion eingeführt und wie wird sichergestellt, dass diese unabhängig agieren kann?

AGENDA

1 Einordnung & Zielsetzung

2 DORA-Gesamtarchitektur und Governance

3 Schnittmengen ICAAP, XAIT & DORA

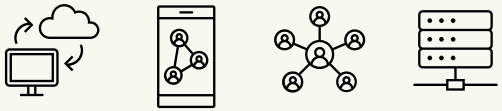
4 **Abgrenzung Auslagerungen vs. IKT-Drittdienstleister**

5 Berichtswesen unter DORA

6 KI und DORA

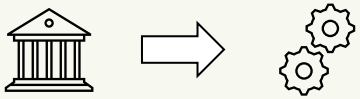
IKT-DIENSTLEISTUNG VS. AUSLAGERUNG

IKT-Dienstleistung



- jede vertragliche Nutzung von IT-/IKT-Leistungen eines Dritten
- Beispiel:
  - Cloud (AWS, Azure, etc.),
  - Software,
  - Hosting,
  - IT-Support
- Selbst Standardsoftware oder Lizenzen gelten als IKT-Dienstleistung (inkl. Updates, etc.)

Auslagerung



- Teilmenge aller IKT-Dienstleistung
- Die Funktion eines Instituts wird an einen Dritten übertragen
- Beispiel:
  - Betrieb des Kernbankensystems durch Dienstleister
  - Externe Zahlungsverkehrsabwicklung
  - Outsourcing von Backoffice-Prozessen
- Funktionsübertragung (make → buy)
- Integraler Bestandteil der Leistungserbringung
- Unterscheidung zwischen wesentlich und nicht wesentlich

DORA verschiebt die Perspektive. Der Fokus liegt nicht mehr primär auf „Auslagerung“, sondern auf IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen

AGENDA

1 Einordnung & Zielsetzung

2 DORA-Gesamtarchitektur und Governance

3 Schnittmengen ICAAP, XAIT & DORA

4 Abgrenzung Auslagerungen vs. IKT-Drittdienstleister

5 **Berichtswesen unter DORA**

6 KI und DORA

REPORTING AN DAS LEITUNGSORGAN

- **Anforderungen**
  - Regelmäßige, strukturierte Berichte
  - Fokus der Berichte auf:
    - → wesentliche Risiken
    - → Schwachstellen
    - → Abhängigkeiten
    - → Vorfälle
  - Nicht ausreichend
    - → rein technische Statusberichte
    - → Ampeln ohne Erläuterung
    - → fehlende Entscheidungsoptionen
- **Gute Praxis**
  - Berichte enthalten:
    - → Handlungsoptionen
    - → Auswirkungen
    - → Entscheidungsvorschläge

INHALT EINES BEISPIELHAFTEN BERICHTS

Management Summary
- Gesamtrisikolage (Ampel / Trend)
- Wesentliche neue oder veränderte Risiken
- Kritische Abhängigkeiten oder Vorfälle skizzieren
- Zentrale Entscheidungspunkte für das Leitungsorgan aufzeigen



Wesentliche IKT-Risiken
- Darstellung der als wesentlich eingestuften IKT-Risiken
- Betroffene kritische oder wichtige Funktionen
- Risikoeinschätzung (Eintrittswahrscheinlichkeit / Auswirkung)
- Veränderungen ggü. Vorperiode

Erkannte Schwachstellen
- Zusammenfassung identifizierter Schwachstellen
- Beschreibung Schwachstelle
- Einschätzung der potenziellen Auswirkungen
- Status der Behebung / Maßnahmenfortschritt

Abhängigkeiten zu IKT-Drittdienstleistern
- Darstellung wesentlicher Abhängigkeiten zu IKT-Drittdienstleistern
- Relevante IKT-Drittdienstleister aufzeigen
- Unterstützte Funktionen / Prozesse
- Einschätzung der Kritikalität
- Relevante Vertrags- oder Steuerungsthemen (z.B. EXIT-Fähigkeit, Auditrechte)

IKT-Vorfälle & Cyberbedrohungen
- Zusammenfassung relevanter IKT-Vorfälle im Berichtszeitraum
- Art und Ursache des Vorfalls
- Betroffene Systeme / Funktionen
- Auswirkung auf Betrieb, Kunden, Compliance
- „Lessons Learned“

Auswirkungen auf das Institut
- Verdichtete Bewertung der potenziellen oder eingetretenen Auswirkungen der Risiken, Schwachstellen und Vorfälle
- Fokus: Geschäftsfortführung, finanzielle Leistungsfähigkeit, regulatorische Compliance, Reputation & Vertrauen

Handlungsoptionen
- Beschreibung von Maßnahmen
- Zielsetzung
- Verantwortlichkeiten
- Grobe Zeitachse
- Einschätzung der Wirksamkeit

AGENDA

1 Einordnung & Zielsetzung

2 DORA-Gesamtarchitektur und Governance

3 Schnittmengen ICAAP, XAIT & DORA

4 Abgrenzung Auslagerungen vs. IKT-Drittdienstleister

5 Berichtswesen unter DORA

6 KI-Agenten und DORA

KI-SYSTEME UNTER DORA

Was ist aufsichtlich relevant?

- KI = komplexe Software,
- Datengetrieben
- Oft cloud-basiert
- Häufig durch Drittanbieter bezogen
- Oft geschäftskritisch (**kwF**)

…damit automatisch im DORA-Anwendungsbereich.

Praxisbeispiele:

- KI-gestütztes Kredit-Scoring
- LLM-basierter Kundenassistent
- Betrugserkennung

KI ist kein Sonderfall, sondern ein IKT-System mit erhöhtem Risikoprofil

KI-SYSTEME UNTER DORA – ZENTRALE IKT-RISIKODIMENSIONEN

- **Governance-Risiko**
  - Unklare Verantwortlichkeiten, fehlende Einbindung in IKT-Risikostruktur
  - Schnittstelle MaRisk AT 4 & DORA Art. 5-9
- **Entwicklungs- & Test-Risiko**
  - Keine Trennung zw. Dev- und Produktionsumgebungen
  - Unzureichende Testumgebungen (fehlende Testdaten)
  - Schnittstelle DORA Art. 10
- **Betriebsrisiko**
  - Performance-Abfall, Fehlende Fallback-Prozesse
  - API-Ausfälle
  - Schnittstelle BIA & Incident Management
- **Drittparteienrisiko**
  - Cloud-Provider, API-Abhängigkeiten, Weiterverlagerung
  - Schnittstelle Auslagerungsmanagement
- **Cyber-Risiko**
  - Prompt Injection, Data Poisoning
  - Schnittstelle ISMS / SOC SIEM
- **Datenrisiko**
  - Datenschutz & Trainingsdatenqualität
  - Schnittstelle Data-Governance & Modellvalidierung

Eine KI ist ein IKT-Asset mit Betriebs-, Cyber- und Drittparteienrisiko

SONDERFALL KI-AGENTEN: EIN GOVERNANCE-THEMA

- **KI Agenten unterscheiden i.d.R. nicht sauber zwischen:**
  - internen vs. Externen Mitarbeitern
  - Befehlen vs. Dateninput
  - vertrauenswürdig vs. potenziell manipulativ
- **Alles landet im selben Kontextfenster.**
  Für das Modell ist es semantisch gleichwertig.
- **Das ist aus Governance-Sicht ein**

Gemini

- **DORA verlangt:**
  - klare IKT-Governance-Strukturen
  - kontrollierte Vertrauens- und Sicherheitszonen
  - Schutz kritischer oder wichtiger Funktionen (kwF)
  - kontrollierten Zugriff auf Systeme, Daten und Workflows
  - nachvollziehbare Verantwortlichkeiten
- **Ein KI-Agent, der:**
  - auf Kundendaten zugreift
  - Workflows auslöst
  - Entscheidungen vorbereitet
  - Schnittstellen zu Drittanbietern nutzt
- **→ wird Teil des IKT-Risikomanagementrahmens.**

KI-AGENTEN ALS TEIL DER DORA-GOVERNANCE

Beispiel : ein KI-Agent unterstützt im Kreditprozess und darf:

- Kundendaten aus dem CRM abrufen
- Bonitätsdaten extern anfragen
- eine Vorbewertung generieren
- eine Entscheidungsempfehlung ins Kernbankensystem schreiben
- Die finale Entscheidung verbleibt beim Menschen (Human-in-the-Loop-Ansatz)

DORA-relevante Fragen:

- Ist diese Funktion kritisch oder wichtig?
- Ist das LLM ein IKT-Drittdienstleister?
- Wie wird der Agent gegen Prompt Injection abgesichert?
- Wer überwacht Fehlentscheidungen?
- Ist der Zugriff rollenbasiert begrenzt?
- Gibt es ein Exit-Szenario bei Ausfall des Anbieters?

IHR REFERENT VON 1 PLUS i

1 PLUS i CONSULTING

Lukas Görnert
M +49 172 837 911 6
Lukas.goernert@1plusi.de

Postfach 130211 T0911 – 56 79 94 99
90114 Nürnberg F0911 – 56 79 95 55 www.1plusi.de

Herr Görnert ist Senior-Berater bei 1 PLUS i und zertifizierter IT-Risk-Practitioner des ISACA Germany Chapters. Er befasst sich mit sämtlichen Fragestellungen der IT-Governance und der IT-Compliance im Kontext des Digital Operational Resilience Act (DORA) und den damit verbundenen Herausforderungen für das IT-Risikomanagement bei Banken. Er verfügt über fundierte Erfahrung im Umgang mit regulatorischen Anforderungen neuer Technologien wie künstlicher Intelligenz und Cloud-Anwendungen im Finanzsektor. Ferner ist er zertifizierter Blockchain-Experte des Blockchain-Centers der Frankfurt School of Finance & Management. In diesem Zusammenhang beschäftigt er sich mit sämtlichen Fragestellungen rund um die Themen digital Assets, Blockchain-Ökosysteme und CBDCs.

IHRE REFERENTIN VON 1 PLUS i

1 PLUS i CONSULTING

Friederike Krüsemann
M +49 163 317 5732
Friederike.kruesemann@1plusi.de

Postfach 130211 T0911 – 56 79 94 99
90114 Nürnberg F0911 – 56 79 95 55 www.1plusi.de

Friederike Krüsemann ist Beraterin bei der 1 PLUS i GmbH. Ihre Studien in Betriebswirtschaftslehre (Bachelor) und Organization Studies sowie Wirtschaftspädagogik (beides Master) in Innsbruck bereiteten sie auf ihre Position als Risikomanagerin bei der BTV Vier Länder Bank AG vor. Ihr Fokus dort lag auf nicht-finanziellen Risiken – insbesondere OP-Risk und IKS -, dem Reporting, internen Schulungen über Risikothemen und Projekt- und Prozessmanagement. Sie war außerdem bei der Einführung und Umsetzung von Basel IV beteiligt und verantwortete die Zusammenführung einzelner Risk Self Assessments.

ANGEKÜNDIGTE DORA-PRÜFUNG? KEINE PANIK!

DORA ist nach wie vor in aller Munde und mittlerweile stehen die ersten Prüfungen an. Bedingt durch wenig Prüfungspraxis ergeben sich viele Fragen:

- Ist unser Institut DORA-compliant?
- Was können wir vorbereitend auf eine DORA-Prüfung tun?
- Wie sehen DORA-Prüfungen überhaupt aus?

Die Konsequenz? Unsicherheiten, die bei Prüfungen zum Fallstrick werden können.

Profitieren Sie von unseren Prüfungserfahrungen zu DORA:

- Was ist wirklich relevant bei aufsichtlichen DORA-Prüfungen?
- Wie können wir unser Institut durch interne Prüfungen auf externe Prüfungen vorbereiten?
- Wie sieht ein adäquater Prüfungsleitfaden für unser Institut aus?
- Wie können wir als interne Revision die Fachbereiche ideal unterstützen, um DORA bestmöglich zu reviewen und zu integrieren?

Vorprüfung, interne Vorbereitung, Interview-Training? Wir haben viele Ideen und Ansätze für die DORA-Prüfungen!

MELDEN SIE SICH EINFACH BEI UNS.

Erstinformation
Kennenlernen der Rahmenbedingungen Ihres Instituts u. Abstimmung von Inhalten des Workshops

Workshop
Übersicht über Möglichkeiten der Unterstützung, Darstellung der Prüferfahrung (Institut), Skizzierung Arbeitsprogramm

Angebot für mögliche Unterstützung
Vorbereitung der Prüfung, Unterstützung während der Prüfung und bei der Bearbeitung der Feststellungen

1PLUSi CONSULTING

Henning Heuter
M 0163 – 41 75 872
henning.heuter@1plusi.de

Postfach 130211 T0911 – 56 79 94 99
90114 Nürnberg F0911 – 56 79 95 55 www.1plusi.de