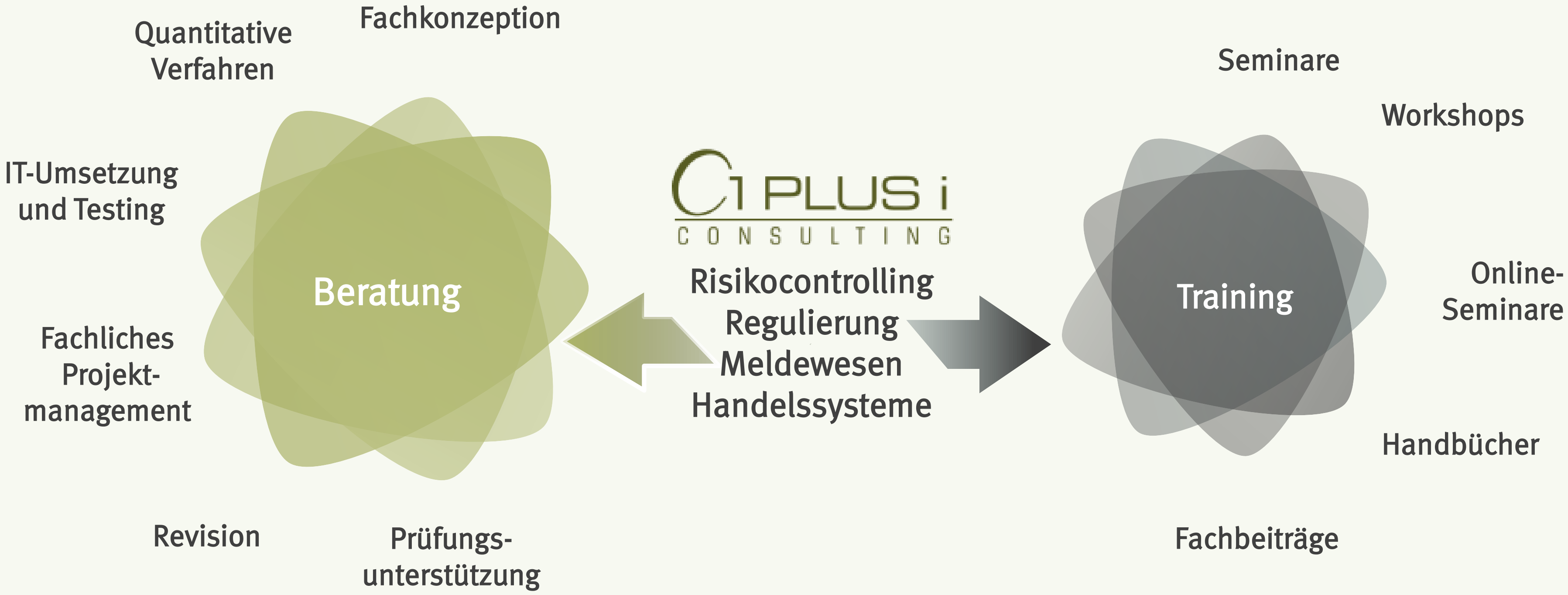
C1 PLUS i
CONSULTING

Friederike Krüsemann
Lukas Görnert

DORA: PRÜFUNG DES IKT-DRITTPARTEIENMANAGEMENTS

Kundensymposium 19. März 2026

1 PLUS I – BERATUNG UND TRAINING AUS EINER HAND



Beratung

Quantitative Verfahren

Fachkonzeption

IT-Umsetzung und Testing

Fachliches Projektmanagement

Revision

Prüfungsunterstützung

Risikocontrolling
Regulierung
Meldewesen
Handelssysteme

Training

Seminare

Workshops

Online-Seminare

Handbücher

Fachbeiträge

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
- Testmanagement
- 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!

02/2026
Thorsten Gendrisch
Henning Heuter

IRRBB UND CSRBB – EBA-BERICHT ZU MITTEL-
LANGFRISTIGEN HANDLUNGSFELDERN

EINLEITUNG

Mit der Veröffentlichung der IRRBB¹-Leitlinien 2018 und deren N
die EBA auf europäischer Ebene ein fundiertes Rahmenwerk für
Zins- und Kreditspreadrisiken geschaffen und somit eine Lücke i
der Säule I geschlossen. Gleichzeitig stehen diese Regularien ni
Vorgaben im Raum. Vielmehr stellt sich die EBA der Praxis und sie
eine ständige Weiterentwicklung und Anpassung aufgrund von
als notwendig an.

So wurden für den vorliegenden Bericht² Erkenntnisse aus den
den Meldedaten der IRRBB-Berichtspflichten und weiteren Info
Prüfungen gesammelt. Es werden daraus auch weniger konkret
Anpassungen direkt abgeleitet, als vielmehr Beobachtungen und
Betroffenen dargestellt.

¹ IRRBB steht allgemein für das Zinsänderungsrisiko im Bankbuch, was jedoch im Laufe der aufsichtlichen
verfeinert wurde.
² Quelle für weitere Aussagen dieses Fachbeitrages (ohne diese gesondert zu kennzeichnen):
https://www.eba.europa.eu/sites/default/files/2026-01/9addc5b3-7578-4002-9a8d-1f7473220a2e/Report%20on%20IRRBB%20heatmap%20implementation.pdf

---

Kerstin Eiser
Januar 2026

PARADIGMENWECHSEL UNTER HOCHDRUCK – DIE CRR
DES OPERATIONELLEN RISIKOS UND NEUERUNGEN ZU
TEN MELDESTICHTAGEN

Regulatorischer Hintergrund

Durch das Inkrafttreten der CRRIII verfolgte die europäische Ban
mentare Kehrtwende in der Behandlung des operationellen Ris
Säule I. Die Freiheit zur Wahl interner Modelle wurde durch die Pf
chen Standardansatz (SMA) zu nutzen, abgelöst. Ziel dessen war
rung des Businessindikators (Business Indicator, BI) die Vergleich
Instituten zu erhöhen und die Komplexität durch einheitliche Vo
lung zu reduzieren.[1] Diese vermeintlichen Vereinfachungen fü
Instituten zu massiven operativen Belastungen und einem tiefgrei
Datenarchitektur, u.a. zwischen den Abteilungen Finanzen und Ri
Eine große Schwierigkeit für die Institute bestand nicht allein in de
xität, sondern in den prozessualen Instabilitäten der Vorgaben d
Authority (EBA).

Das Moving-Target

Nach einer Phase umfangreicher Konsultationen und der Strei
sprünglich geplanter Entwurfs-Templates konsolidierte die EBA d
in vier verbindliche COREP-Meldebögen (C 16.01 bis C 16.04; neb
henden, je nach Größe des Instituts auch granular zu befüllenden,
rend des Prozesses gab es zahlreiche Überarbeitungen an den Ter
So wurde im Dezember 2023 die erste Roadmap veröffentlicht, a
neuen Meldebogenanforderungen und den damit verbundene
konnte. Im Juni 2024 erkannte die EBA jedoch, dass es zwischen
FINREP- und den OpRisk-Komponenten fundamentale Mapping-Pr
gen erste technische Korrekturen erfolgten. Aufgrund der nicht u
Historie, erlaubte die EBA im November 2024 Übergangslösunge

ZUSAMMENFASSUNG DES ESMA-ABSCHLUSSBERICHTS – BEDINGUNGEN FÜR DIE ERFÜLLUNG DER ANFORDERUNGEN EINES AKTIVEN KONTOS IN DER EU (AAR)

WOHER KOMMT DIE ANFORDERUNG & WAS IST DAS ZIEL?

Am 19.06.2025 veröffentlichte die ESMA ihren Abschlussbericht¹ zur Erfüllung der Bedingungen bzgl. der Anforderungen zur Führung eines aktiven Kontos in Bezug auf das Clearing von Zinsderivaten innerhalb der europäischen Union (EU). Das Active Account Requirement (AAR) ist Teil der überarbeiteten EMIR 3.0 Regelung.

In der Vergangenheit wurden einige Clearingdienste außerhalb d
temischer Bedeutung für die EU eingestuft: SwapClear von LCH Lt
EUR und polnische Zloty (PLN) lautenden Zinsderivaten sowie C
und die STIR²-Dienste von ICE Clear Europe Ltd. (ICEU), in beiden F
Produkte. Mit dem AAR führt die ESMA ein neues Gesetz ein, das
nichtfinanzielle Gegenparteien dazu verpflichtet, für einige OT
(Clearing-) Konto bei einer in der EU zugelassenen zentralen Ge
terhalten. Die EU verfolgt damit das Ziel die Abhängigkeit vo
staat-CCPs zu verringern. Die EU möchte demnach mit dem AAR
keit von Drittstaaten-CCPs, insbesondere von der LCH Ltd., verrin
könnten solche CCPs Risiken für die Stabilität in der EU darsteller
rekten europäischen Aufsicht operieren.

Ein aktives Konto bei einem EU-CCP soll sicherstellen, dass systen
jederzeit auf eine Infrastruktur innerhalb der EU zurückgreifen
scher als auch in organisatorischer Sicht. Dabei ist hervorzuheb
komplette Verlagerung aller Aktivitäten der Gegenparteien in die

¹ ESMA91-1505572268-4201 Final Report on the EMIR 3 Active Account Requirement
² Short-Term-Interest-Rate

Jetzt anmelden!

Folgen Sie uns auf LinkedIn®

AGENDA

1	Das IKT-Drittparteienmanagement
2	Historischer Kontext
3	Evolution statt Neubau
4	Das Informationsregister
5	Prüfungsrelevanz & Fragen

WARUM IKT-DRITTPARTEIENMANAGEMENT EIN KERNTHEMA IST

Ausgangslage

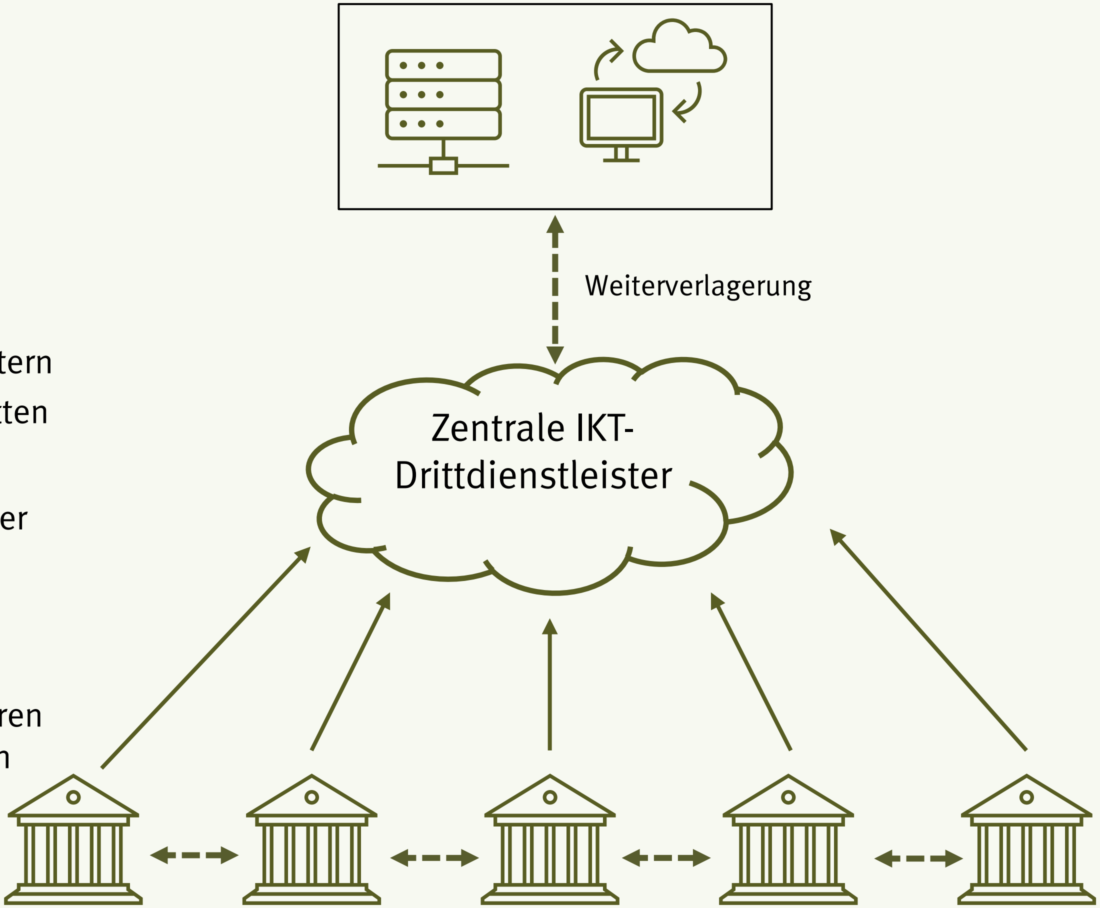
- Finanzunternehmen sind heute hochgradig abhängig von IKT-Drittparteien
- Zunehmend von:
  - Cloud-Services
  - Spezialisierten Softwareanbietern
  - Komplexen Dienstleistungsketten

Kernaussage

- Digitale Resilienz endet nicht an der Unternehmensgrenze

Praxisbezug

- Viele schwere IT-Vorfälle haben ihren Ursprung nicht im Institut, sondern bei Dienstleistern



WAS VERSTEHT MAN UNTER IKT-DRITTPARTEIENMANAGEMENT?

Begrifflichkeit

- *IKT-Drittdienstleistermanagement bezeichnet alle Governance-, Risiko- und Steuerungsprozesse, mit denen ein Finanzunternehmen die Risiken aus der Nutzung externer IKT-Dienstleistungen systematisch beherrscht (aufsichtlicher Sammelbegriff; Art. 3 ff DORA)*
- Kernpunkt: Nicht der Dienstleister steht im Fokus, sondern die digitale Abhängigkeit für die Leistungserbringung

Anwendung

- Erfasst sind alle vertraglichen IKT-Dienstleistungen, unabhängig davon, ob es sich um eine klassische Auslagerung, einen sonstigen Fremdbezug, einen Cloud-Service oder gruppeninterne IKT-Dienstleister handelt.
- Abgrenzung: DORA geht weiter als das frühere Auslagerungsverständnis unter BAIT/MaRisk

Steuerungslogik

- DORA adressiert drei zentrale Risikodimensionen
  - Abhängigkeit von einzelnen Dienstleistern
  - Konzentrationsrisiken (institutsintern & sektorweit)
  - Substituierbarkeit & EXIT-Fähigkeit
- Neue Perspektive: Risiken entstehen nicht nur im Institut, sondern in Dienstleisterketten

AGENDA

AUSGANGSPUNKT UNTER BAIT: FOKUS AUF AUSLAGERUNGEN

Bankaufsichtliche Anforderungen an die IT

Historischer Kontext

BAIT-Logik

- Schwerpunkt lag auf:
  - Wesentlichen Auslagerungen
  - IT-Sicherheit
  - Kontroll- und Zugriffsrechten

Typische BAIT-Anforderungen

- Risikoanalyse vor Auslagerung
- Auslagerungsverträge mit Mindestinhalten
- Überwachungs- und Prüfungsrechte
- EXIT-Regelungen (oft abstrakt)

Begrenzung

- Fokus auf Einzelinstitut
- Kein systemischer Blick auf Konzentrationsrisiken
- Unterschiedliche Auslegungen je Institut

GRENZEN DES BAIT-ANSATZES

Typische Schwächen:

- Nicht auslagerungsrelevante IT-Dienstleistungen oft nicht erfasst
- Komplexe Sub-Dienstleisterketten, die unzureichend transparent sind
- Cloud-Risiken nur teilweise abgebildet

Erkenntnis der Aufsicht:

- Einzelne Institute waren regelkonform, das Gesamtsystem war jedoch verwundbar

PARADIGMENWECHSEL DURCH DORA

- **Was DORA grundlegend ändert**
  - Einheitlicher EU-weiter Rahmen
  - Erweiterung von „Auslagerungsmanagement“ zu IKT-Drittparteienmanagement
  - Fokus auf:
    - Kritische / wichtige Funktionen
    - Abhängigkeiten
    - Konzentrations- und Substitutionsrisiken

- **Kernaussage:**
  - DORA fragt nicht nur:

    „Ist der Vertrag korrekt“, sondern

    „Was passiert, wenn der Dienstleister ausfällt?“

AGENDA

EVOLUTION STATT NEUBAU

- **Kaum ein Institut startet bei DORA „auf der grünen Wiese“**
- **Typischer Ausgangspunkt:**
  - Auslagerungsrichtlinie gem. BAIT / MaRisk ist vorhanden
  - Dienstleisterinventar ist vorhanden
  - Vertragsstandards sind entwickelt und kommen in der Praxis zur Anwendung
  - Es bestehen Risikoanalysen für wesentliche Auslagerungen

- **DORA-Logik:**
  - Aus dem Auslagerungsmanagement wird ein IKT-Drittparteienmanagement mit End-to-End-Steuerung

- **DORA-Zielbild:**
  - Es wird eine vollständige Transparenz über alle IKT-Drittparteien hergestellt
  - Es erfolgt eine Bewertung entlang der Kritikalität, der Abhängigkeit, der Konzentration und der Substituierbarkeit
  - Es erfordert eine aktive Management-Steuerung, nicht nur die Dokumentation

WAS MAN AUS BAIT-STRUKTUREN GUT WEITERVERWENDEN KANN

	BAIT-Baustein	Weiterverwendung unter DORA
1.	Auslagerungsrichtlinie	...dient als Basis für DORA-Strategie
2.	Risikoanalyse vor Auslagerung	... die Methodik ist weiter nutzbar
3.	Vertragsmindestinhalte	Ausgangspunkt für DORA-Verträge
4.	Dienstleisterliste	Basis für Informationsregister
5.	Prüf- und Zugriffsrechte	Weiterhin zwingend
6.	EXIT-Regelungen	Müssen konkretisiert und getestet werden

BAIT liefert die Struktur, DORA liefert die Tiefe und den Umfang !

Typische BAIT-Lücken aus DORA-Sicht:
- Fokus nur auf wesentliche Auslagerungen
- Sonstige IKT-Dienstleister oft nicht erfasst und nicht risikobewertet
- Keine systematische Betrachtung von Konzentrationsrisiken und Substituierbarkeit

AUFBAU: DORA-KONFORMES IKT-DRITTPARTEIENMANAGEMENT

Schritt 1

Scope erweitern (zentraler DORA-Schritt)

- Erfassung aller IKT-Dienstleistungen, nicht nur Auslagerungen
- Inkl. Cloud, SaaS, gruppeninterne IT und sonstiger Fremdbezug
- Ergebnis: vollständiges IKT-Drittparteieninventar

Schritt 2

Kritikalität neu bewerten

- BAIT: Wesentlichkeit der Auslagerung
- DORA: Unterstützt die Dienstleistung eine kritische oder wichtige Funktion?
- Neu: Kritikalität = Geschäftsauswirkung, nicht Vertragskonform

Schritt 3

Integration ins IKT-Risikomanagement

- IKT-Drittparteienrisiken sind Teil des IKT-Gesamtrisikoprofils
- Erforderlich sind:
  - Einheitliche Methoden,
  - Konsolidierte Reporting,
  - Verbindung zu Incident Managment & Resilienztests

AUFBAU: DORA-KONFORMES IKT-DRITTPARTEIENMANAGEMENT

Schritt 4

Governance & Management-Einbindung aufbauen

- Leitungsorgan muss eine Strategie erarbeiten und genehmigen, den Risikoappetit setzen sowie Entscheidungen über die Akzeptanz von Restrisiken treffen.
- Praktische Ergänzungen: klare Eskalationsschwellen, dokumentierte Managemententscheidungen und regelmäßiges Vorstandsreportings

Schritt 5

Vertragsmanagement erweitern

- Regelungen treffen zu Informationspflichten bei Incidents, Sub-Outsourcing, EXIT-Tests und Datenlokation sowie Zugriffsrechte
- Standardverträge oft nicht ausreichend → Zusatzvereinbarungen erforderlich; dokumentierte Risikoakzeptanz

Schritt 6

Konzentrations- & Substitutionsrisiken bewerten

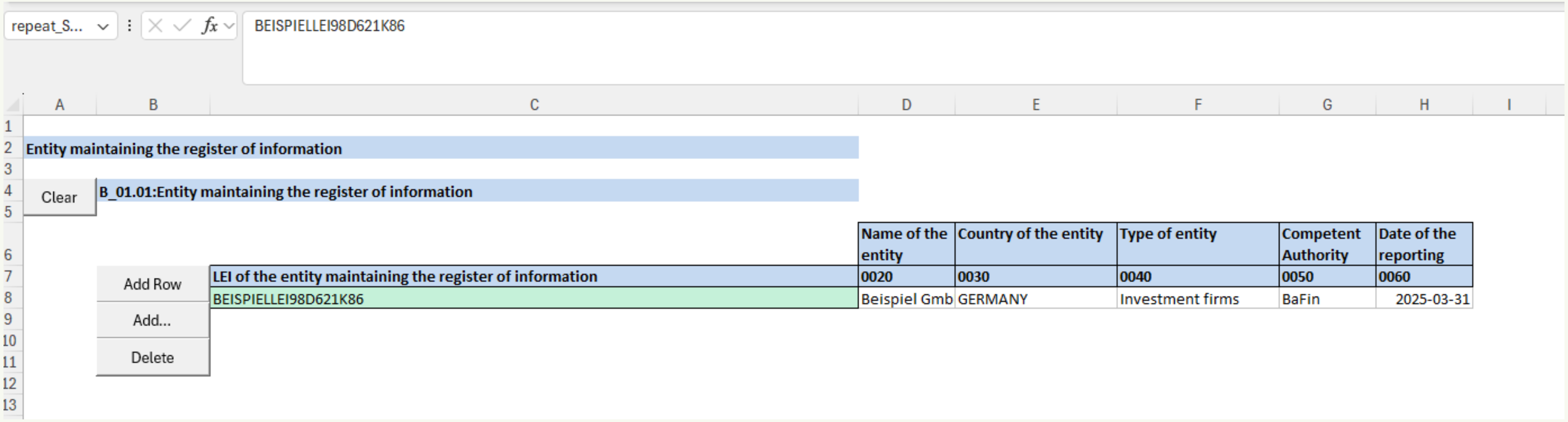
- Bewertung erfolgt einzelinstitutsbezogen & sektorweit (über das Informationsregister)
- Konkret: Welche kritischen Funktionen hängen:
    - Von einem Anbieter
    - Von einer Technologie
    - Von einer Region ab?

AUFBAU: DORA-KONFORMES IKT-DRITTPARTEIENMANAGEMENT

Schritt 7

Informationsregister aufbauen

- Register ist kein Nebenprodukt
- Zentrale Datenquelle für die Aufsicht, die Prüfung und Managemententscheidungen
- In der Praxis kommen die Daten aus unterschiedlichen Bereichen
  - Einkauf,
  - IT,
  - Auslagerungsmanagement,
  - Risikomanagement



BEISPIELLEI98D621K86

Entity maintaining the register of information

B_01.01:Entity maintaining the register of information

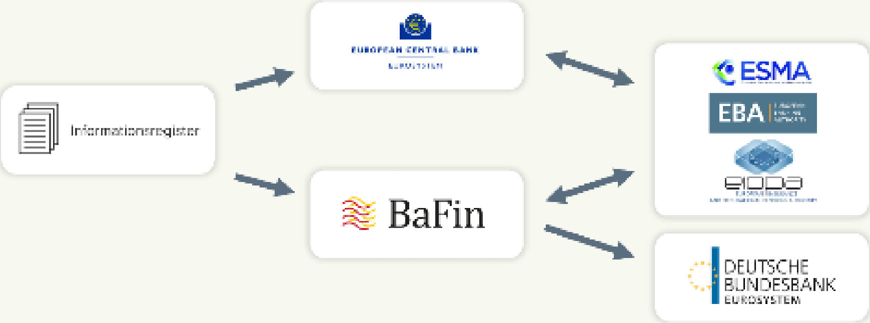
	Name of the entity	Country of the entity	Type of entity	Competent Authority	Date of the reporting
LEI of the entity maintaining the register of information	0020	0030	0040	0050	0060
BEISPIELLEI98D621K86	Beispiel Gmb	GERMANY	Investment firms	BaFin	2025-03-31

AGENDA

DAS INFORMATIONSREGISTER

- **Verpflichtung zur Einreichung gem. Art. 28 Abs. 3 DORA**
  - Implementierung eines umfassenden IKT-Drittparteienrisikomanagements
  - Berücksichtigung von Kritikalität der unterstützenden Funktionen, Substituierbarkeit der Dienstleister, Abhängigkeiten innerhalb von IKT-Dienstleistungsketten
  - Laufende Überwachung während des gesamten Vertragslebenszyklus

- **Jährliche Einreichung an BaFin bzw. EBA**
- **Datengrundlage für**
  - Identifikation kritischer IKT-Drittdienstleister (CCTPs)
  - EU-weite Konzentrationsanalyse
  - Überwachungsrahmen der ESAs



DAS INFORMATIONSREGISTER

Single Source of Truth für alle IKT-Dienstleisterbeziehungen

Steuerung & Governance

- Transparenz über IKT-Abhängigkeiten
- Identifikation von Konzentrations- & Substitutionsrisiken
- Grundlage für Management-Entscheidungen & IT-Strategie
- Input für IKT-Risikomanagement & Auslagerungssteuerung

Aufsicht & Prüfung

- Basis für Identifikation kritischer IKT-Drittdienstleister
- Zentrale Prüfungsunterlage (§ 44 KWG / JAP)
- Konsistente Datengrundlage für BaFin & ESAs
- Erwartung: vollständig, aktuell, prüfungssicher

Ohne belastbares Informationsregister ist DORA-Compliance nicht prüffähig

IKT-DRITTDIENSTLEISTUNG & ABGRENZUNG ZU AUSLAGERUNGEN

- **Jede vertragliche Nutzung von IKT-Dienstleistungen**
- **Umfasst auch:**
  - Microsoft 365
  - Lizenzmodelle mit Update-Service
  - Webhoster
  - SaaS-Lösungen
- **Aussagen wie „Wir haben keine IKT-Drittdienstleister“ sind faktisch kaum haltbar**
  - 2026 ist kein Einreichen einer Leermeldung des Informationsregisters möglich

- **IKT-Auslagerungen sind nur eine Teilmenge**
- **Register umfasst:**
  - Wesentliche & nicht wesentliche IKT-Dienstleistungen
  - Gruppendienstleistungen
  - Interne & externe Vertragsketten
- **Praxisbeispiel:**
  Interner IT-Dienstleister + dessen Subunternehmer müssen transparent sein.

INFORMATIONSREGISTER: AUFBAU UND WEITERENTWICKLUNG

- **Aufbauanforderungen**
  - Vollständige Erfassung aller IKT-Dienstleistungen (nicht nur klassische Auslagerungen)
  - Klare Zuordnung hinsichtlich
    - Was ist eine unterstützende Funktion?
    - Was ist eine kritische/nicht kritische Funktion?
    - Vertrags- & Dienstleistungsketten (inkl. Sub-Dienstleister)
  - Nutzung der Standardvorlagen gem. ITS (strukturierte Datenlogik)
  - Konsistenz zu Auslagerungsregister, Vertragsdaten und Funktionslandkarte / BIA
- **Weiterentwicklung**
  - Laufende Pflege, kein statisches Register
  - Aktualisierung bei neuen / geänderten Verträgen, Rezertifizierung von Funktionen und Wechsel von (Sub)-Dienstleistern
  - Einbettung in Change- & Vendor-Management sowie Risiko- & Kontrollprozesse

Projektarbeit

Produktion

DAS EBA DATENMODELL (DPM-LOGIK)

- **Das Informationsregister folgt dem EBA Data Point Model (DPM). Das bedeutet:**
  - Tabellen stehen in logischer Beziehung zueinander
  - Felder sind technisch verknüpft
  - IDs und Referenzen müssen konsistent sein
- **Aggregationen müssen rechnerisch nachvollziehbar sein**

- **Beispiel aus der Praxis:**
  - In Tabelle 02.01_0050 werden Kosten auf Vertragsebene erfasst
  - In Tabelle 05.01_0100 werden Kosten auf Dienstleisterebene aggregiert
  - → Stimmen diese Werte nicht überein, entsteht ein Validierungsfehler.

Das Register muss nicht nur vollständig, sondern auch datenlogisch konsistent sein.
Institute sollten das DPM verstehen und nicht nur die Excel-Vorlage befüllen.

IDENTIFIKATOREN KORREKT VERWENDEN (LEI, EUID & CO.)

- **IKT-Drittdienstleister müssen eindeutig identifizierbar sein.**
- **Grundsatz:**
  - EU-Unternehmen → EUID
  - Finanzinstitute → LEI
  - Nicht-EU-Dienstleister ohne LEI → alternative ID gemäß EBA-Vorgaben
- **Typische Fehler:**
  - Abweichende Schreibweisen
  - Unterschiedliche IDs für denselben Dienstleister
  - Fehlende Synchronisation zwischen Tabellen
- **EU-Datenbanken enthalten bis ca. 2028 noch Inkonsistenzen**
  - False Positives bei EUID sind möglich
  - Diese sind intern zu dokumentieren – nicht zwingend meldepflichtig
- **Empfehlung:**
  Ein zentrales ID-Governance-Konzept für Drittparteien etablieren.

TYPISCHE VALIDIERUNGSFEHLER UND IHRE FOLGEN

Häufige Fehlerquellen:

- Duplikate desselben Vertrags
- Inkonsistente Kostenangaben
- Unplausible oder „runde“ Fantasiekosten
- Unvollständige Verknüpfung von Vertrags- und Dienstleistertabellen
- Strukturveränderung der Excel-Vorlage
- Copy-Paste mit Formatübernahme

Konsequenz:

- Datei wird technisch als „nicht nutzbar“ eingestuft
- Neueinreichung erforderlich
- Bei behebbaren Fehlern → möglicher Verstoß gegen Art. 28 Abs. 3 DORA

Datenqualität ist mittlerweile ein aufsichtliches Qualitätskriterium.

ERWARTUNGSHALTUNG DER AUFSICHT

- **Das Informationsregister als Governance-Indikator**

- **Zentrale Botschaften:**
    - Keine regulatorischen Erleichterungen vor 2028
    - Fehlerbereinigung ist verpflichtend
    - Register wird aktiv ausgewertet
    - Konzentrationsrisiken stehen im Fokus
- **Das Register ist:**
    - Grundlage für CCTP-Identifikation
    - Bestandteil des europäischen Überwachungsrahmens
    - Indikator für Reifegrad im Third-Party-Risk-Management

- **Strategisch bedeutet das:**
  Das Register ist ein Spiegelbild der organisatorischen Steuerungsqualität.

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

EBA | EUROPEAN BANKING AUTHORITY

HANDLUNGSEMPFEHLUNGEN

- Vollständige Inventarisierung aller IKT-Drittdienstleistungen
- Klare Definition eines Register-Owners (z. B. IKT-TPRM-Funktion)
- Zentrale Pflege von Drittparteien-IDs
- Automatisierte Konsistenzprüfungen vor Einreichung
- Nachvollziehbare Kostenaggregation
- Dokumentation von Validierungsprotokollen
- Regelmäßige Überprüfung der KWF-Einstufung

Das Informationsregister ist kein Excel-Projekt. Es ist ein struktureller Baustein der digitalen operationalen Resilienz.

LISTE KRITISCHER IKT-DRITTDIENSTLEISTER (CCTPS)

- Accenture plc
- Amazon web Services
- EMEA Sarl
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation (IBM)
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited

BEOBACHTUNGEN DER BAFIN AUS 2025

- System zum Einreichen des Informationsregisters war stabil
- In Deutschland wurde eine hohe Datenqualität erreicht – nur 2% der Einreichungen wurden aufgrund schwerwiegender Fehler zurückgewiesen
- Die Vorlage der BaFin erleichterte das Erreichen der Datenqualität
- Bearbeitung des Einreichungssystems im laufenden Prozess führte teilweise zu falschen Fehlermeldungen
- Oftmals wurden mehrere Einreichungen für ein fehlerfreies Informationsregister genutzt
- Konsequenzen für 2026
    - Erweiterte Hilfestellung durch die BaFin bei Fehlermeldungen
    - Fehlermeldungen immer hinterfragen und sollten nicht beachtet werden, falls die Eingabe nachweislich korrekt ist – gut dokumentieren!
    - Datenmodell wurde nicht angepasst – nur inhaltliche Änderungen notwendig, keine technischen
    - Leermeldungen sind nicht möglich

Quelle: BaFin-Veranstaltung "Informationsregister", 24.2.2026

AGENDA

TYPISCHE PRÜFUNGSFESTSTELLUNGEN & ERFOLGSFAKTOREN

Häufige Feststellungen:

- IKT-Dienstleistungen nicht vollständig erfasst
- Unklare Abgrenzung von Auslagerungen vs. IKT-Dienstleistung
- Fehlende oder nicht schlüssige Exit- oder Substitutionsfähigkeit
- Konzentrationsrisiken wurden nicht bewertet

Erfolgsfaktoren

- Vollständige Transparenz über das Informationsregister
- Klare Kritikalitätslogik
- Frühzeitige Vertragsprüfungen inkl. Rezertifizierung
- Enge Verzahnung mit IKT-Risikomanagement

IKT-Drittparteienmanagement ist unter DORA ein zentrales Steuerungs- und Aufsichtsthema – kein Nebenprozess

MÖGLICHE PRÜFUNGSFRAGEN

Wie ist die Risikoanalyse vor Vertragsabschluss ausgestaltet?

Wie wird sichergestellt, dass Unterauftragnehmerketten angemessen überwacht werden?

Wie sieht die Dokumentation der Exitstrategien aus?

Wie werden IKT-Konzentrationsrisiken analysiert und gesteuert?

IHR REFERENT VON 1 PLUS i

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.

IHR REFERENT 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

1 PLUS i 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