IKT-Drittdienstleister - Kollateralschäden der DORA?

Know-How-To-Go

12.06.2025

Christian Friedrich

Who am I

Christian Friedrich
Senior Managing Consultant bei der HiSolutions AG

Diplom-Informatiker

13 Jahre Sicherheitsberater bei der HiSolutions AG
- Aufbau ISMS nach ISO 27001 und IT-Grundschutz
- Audit und Zertifizierung von ISMS

5 Jahre Informationssicherheitsbeauftragter der Investitionsbank Berlin
- Aufbau und Weiterentwicklung des ISMS
- Bearbeitung von aufsichtsrechtlichen Prüfungen
- Vorbereitung DORA-Umsetzung

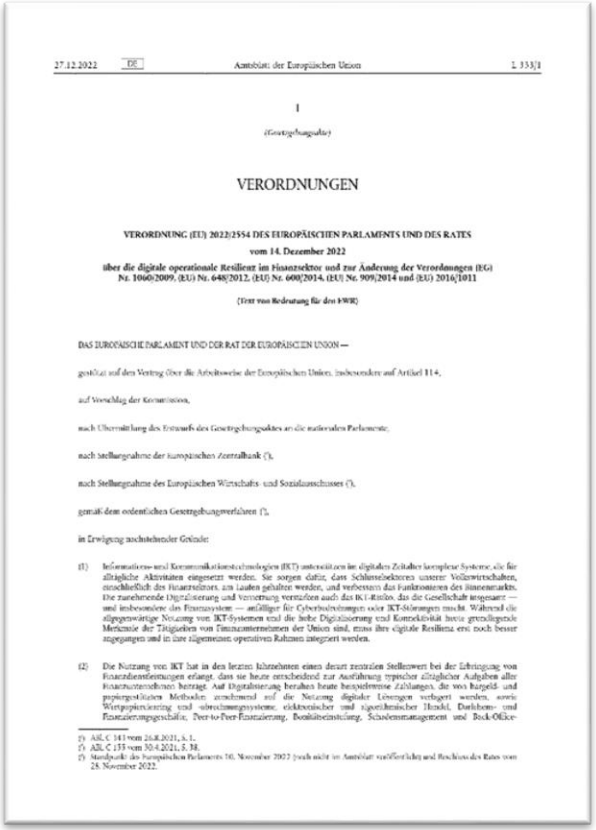
Agenda

1. DORA Grundlagen
2. Schwerpunkte
3. Auswirkungen für IKT-Drittdienstleister
4. Handlungsempfehlungen für IKT-Drittdienstleister

DORA Basiswissen

Digital Operational Resilience Act

- Gilt für alle Finanzunternehmen aus dem EWR
- Ersetzt bisherige deutsche Regelungen (BAIT, VAIT, KAIT, ZAIT)
- Regelt die digitale Widerstandsfähigkeit im EU-Finanzsektor



27.12.2022 DE Amtsblatt der Europäischen Union L 333/1

I

(Gesetzgebungsakte)

VERORDNUNGEN

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)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

gemäß dem ordentlichen Gesetzgebungsverfahren (3),

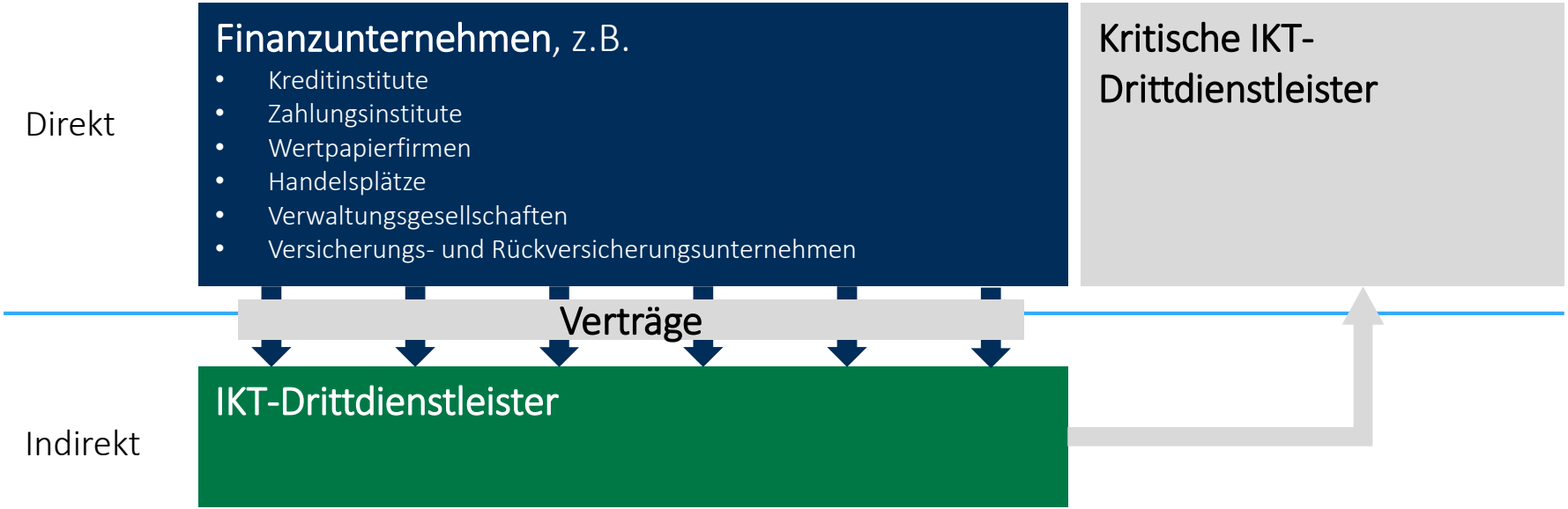
in Erwägung nachstehender Gründe:

(1) Informations- und Kommunikationstechnologien (IKT) unterstützen in digitalen Zeitalter komplexe Systeme, die für alltägliche Aktivitäten eingesetzt werden. Sie sorgen dafür, dass Schlüsselsektoren unserer Volkswirtschaften, einschließlich des Finanzsektors, am Laufen gehalten werden, und verbessern das Funktionieren des Binnenmarkts. Die zunehmende Digitalisierung und Vernetzung verstärken auch das IKT-Risiko, das die Gesellschaft insgesamt — und insbesondere das Finanzsystem — anfälliger für Cyberbedrohungen oder IKT-Störungen macht. Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale der Tätigkeiten von Finanzunternehmen der Union sind, muss ihre digitale Resilienz erst noch besser angegangen und in ihre allgemeinen operativen Rahmen integriert werden.

(2) Die Nutzung von IKT hat in den letzten Jahrzehnten einen derart zentralen Stellenwert bei der Erbringung von Finanzdienstleistungen erlangt, dass sie heute entscheidend zur Ausführung typischer alltäglicher Aufgaben aller Finanzunternehmen beiträgt. Auf Digitalisierung beruhen heute beispielsweise Zahlungen, die von Bargeld- und papiergestützten Methoden zunehmend auf die Nutzung digitaler Lösungen verlagert werden, sowie Wertpapierclearing und -abrechnungssysteme, elektronischer und algorithmischer Handel, Darlehens- und Finanzierungsgeschäfte, Peer-to-Peer-Finanzierung, Bonitätseinstufung, Schadensmanagement und Back-Office-

(1) ABl. C 343 vom 26.8.2021, S. 1.
(2) ABl. C 155 vom 30.4.2021, S. 38.
(3) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

Für wen gilt die DORA?

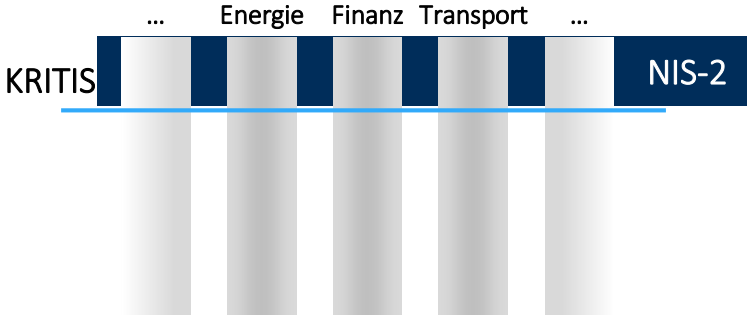


Vergleich zu NIS-2

Ziel: Verbesserung der europaweiten Cybersicherheit und Widerstandsfähigkeit gegen Cyberangriffe

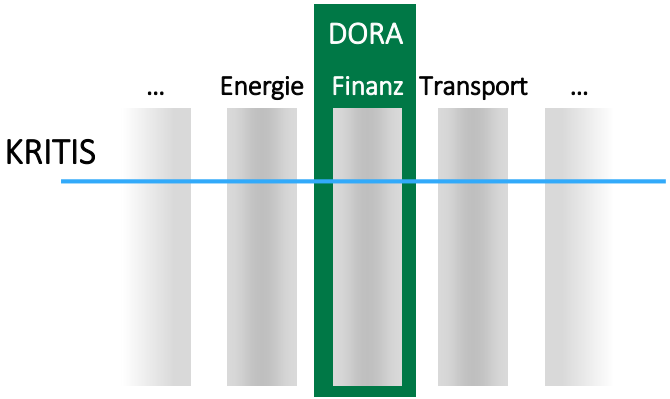
NIS-2

- EU-Richtlinie, braucht deutsches Gesetz
- In einigen Bereichen weniger konkret als DORA



DORA

- EU-Verordnung, gilt direkt
- Zusätzliche Konkretisierungen (RTS und ITS)
- „lex specialis“, ersetzt NIS-2 für Finanzunternehmen*



** Von DORA werden ggf. nicht alle Themen der NIS-2 abgedeckt, die müssen die Finanzunternehmen ggf. dann zusätzlich umgesetzt werden*

Für DORA sind weitere Vorgaben relevant

Mehrstufiges Verfahren der Rechtsakte

Stufe 1	**Basisrechtsakt** DORA EU-Verordnung 2022/2554
Stufe 2	**Technische Regulierungsstandards** Regulatorische Technische Standards (RTS) **Technische Durchführungsstandards** Implementing Technical Standards (ITS)
Stufe 3	**Leitlinien**

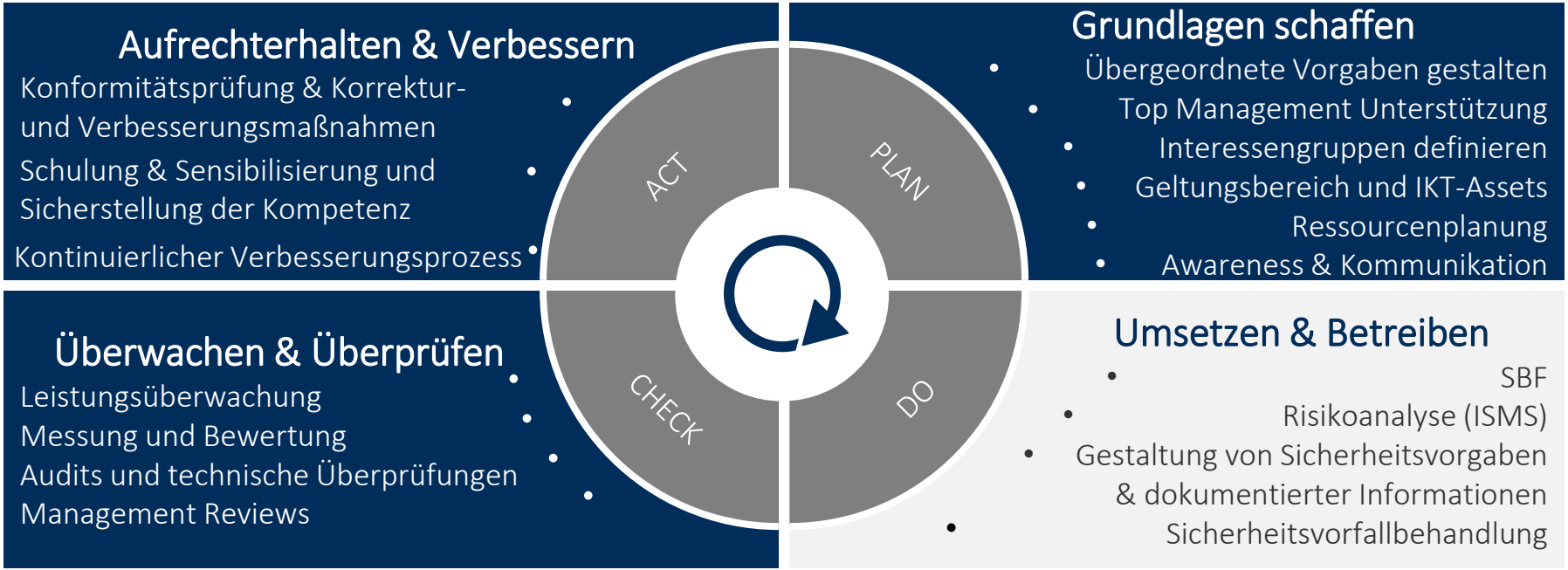
- **RTS Risikomanagementrahmen**
  (EU 2024/1774)
- **RTS Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen**
  (EU 2024/1772)
- **RTS Meldung schwerwiegender IKT-bezogener Vorfälle und Cyberbedrohungen**
  (EU 2025/301)
- **RTS Vertragliche Vereinbarungen mit IKT-Drittdienstleistern bei kritischen oder wichtigen Funktionen**
  (EU 2024/1773)
- **ITS Vorlage für Informationsregister**
  (EU 2024/1773)
- **ITS Verfahren zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls und Cyberbedrohungen**
  (EU 2025/302)
- **RTS Threat Led Penetration Testing**
  (Entwurf)
- **RTS Unterauftragsvergabe**
  (Entwurf)

Risikomanagementrahmen als Integriertes Managementsystem (IMS) (I)

**Drittparteienrisikomanagement*

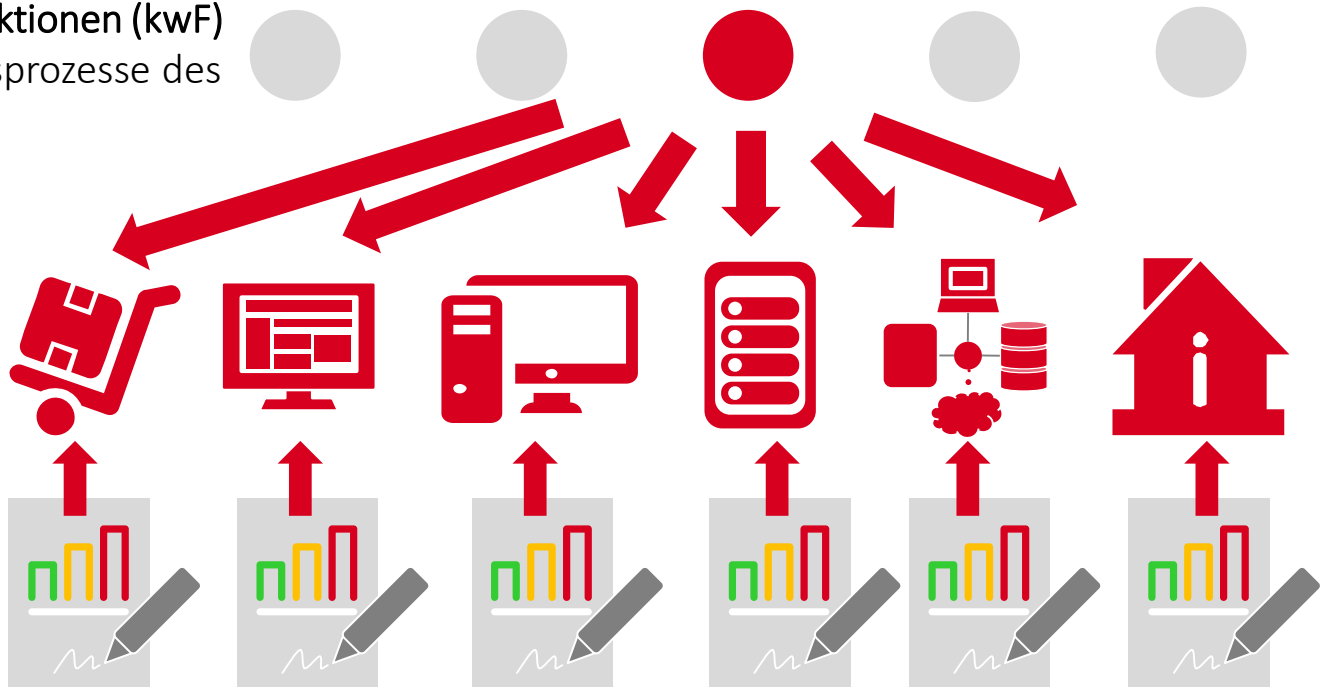
Risikomanagementrahmen als Integriertes Managementsystem (IMS) (II)

P, C und A werden übergreifend im Risikomanagementrahmen behandelt.



Identifizierung der „Kronjuwelen“

- **Kritische oder wichtige Funktionen (kwF)**
  Die elementaren Geschäftsprozesse des Finanzinstituts
- Relevante IKT-Assets und IKT-Drittdienstleister
- Risikoorientierte Vorgaben



Die Aufsicht fordert die Meldungen aller kritischen IKT-bezogenen Vorfälle

Intensive Analyse der Auswirkungen, z.B.
- Wirtschaftliche Schäden, betroffene Kunden, Reputationsschäden

Prozess zur Identifizierung von kritischen IKT-bezogenen Vorfällen (innerhalb von 24h)

→

Erstmeldung (innerhalb von 4h nach Klassifizierung oder 24h nach Meldung des IKT-Vorfalls)

→

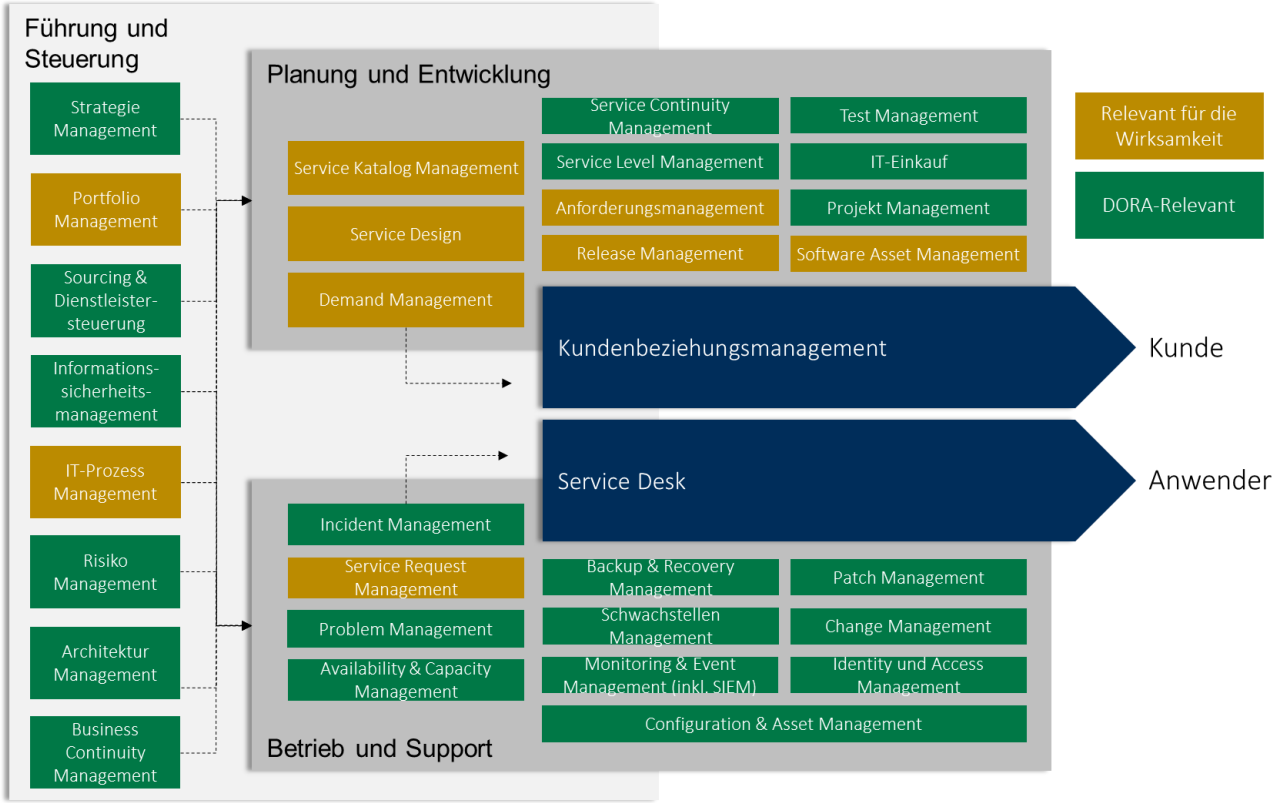
Zwischen-meldung (mind. Alle 72h oder anlass-bezogen)

→

Abschluss-meldung (30 Tage nach letzter Zwischen-meldung)

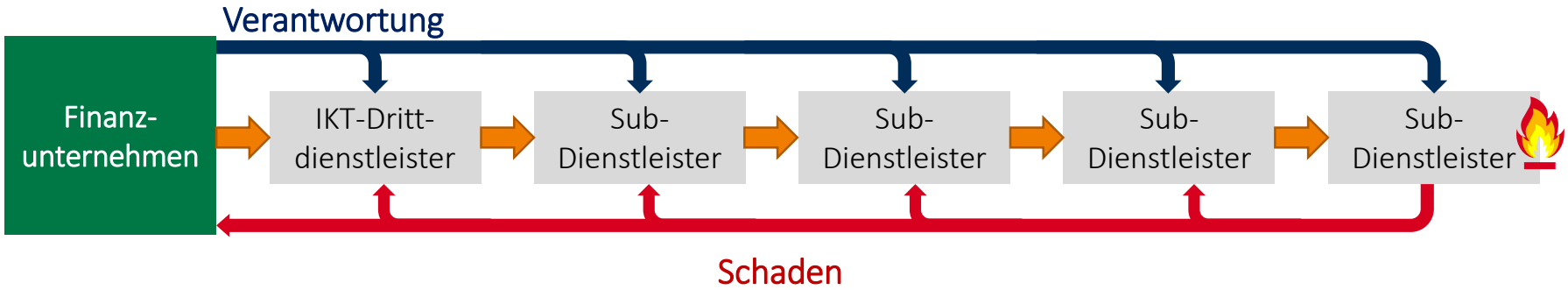
Konkretere Vorgaben für IT-Betrieb

- Fast alle IT-Prozesse betroffen
- Zum Teil sehr umfangreiche Anforderungen, bspw.:
  - Dokumentation aller Bibliotheken (SBOM)
  - Quellcodeanalyse bei Beschaffungen
  - Automatische Überwachung der Protokollierung (SIEM)



Kein Verschieben der Verantwortung auf IKT-Drittdienstleister

- Die Finanzunternehmen haben Verantwortung für den Einsatz von IKT-Drittdienstleistern
  - Risikobewertung
  - Aktive Steuerung
- Die gesamte Kette der Subdienstleister muss betrachtet werden



- Einheitliches Sicherheitsniveau in der gesamten Kette erforderlich

Fast alle Dienstleister von Finanzunternehmen sind IKT-Drittdienstleister

IKT-Drittdienstleister
Ein Unternehmen, das IKT-Dienstleistungen bereitstellt.
(EU-Verordnung 2022/2554, Art. 3)

IKT-Drittdienstleistung
Digitale Dienste, die über IKT-Systeme … dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen …
(EU-Verordnung 2022/2554, Art. 3)

Sonderfall kritische IKT-Drittdienstleister

- Beeinträchtigung hat „systemische Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen“
  EU-Verordnung 2022/2554, Art. 31

- Von der Aufsicht bestimmt und veröffentlicht (noch nicht erfolgt)
- Direkte Überwachung durch die Aufsichtsbehörden
- Gleiche Vorgaben wie Finanzinstitute

- Aufsicht kann
  - Umsetzung von Maßnahmen einfordern und
  - Nutzung dieser IKT-Drittdienstleister untersagen

Finanzinstitute setzen die Messlatte selbst …

(Mindest-)Vertragsinhalte für IKT-Drittdienstleister

(DORA Art. 30 (2))

Allgemeine Vorgaben

- Formvorschriften
- Beschreibung der IKT-Drittdienstleistung
- Datenzugriff
- Aufsicht
- Kündigung
- Standort
- IKT-Vorfall
- Schulungen

DOR‘-Vorgaben

- Informations-sicherheit *(angemessene Standards für Informations-sicherheit)*

**Digitale operative Resilienz*

… besonders hoch für IKT-Drittdienstleistern bei kwF

Zusätzlich Vertragsinhalte bei IKT-Drittdienstleistern für kwF
(DORA Art. 30 (3) und RTS Vertragsinhalte)

Allgemeine Vorgaben

- Formvorschriften
- Beschreibung der IKT-Drittdienstleistung
- Datenzugriff
- Aufsicht
- Kündigung
- Ausstieg
- Berichterstattung
- Überwachung
- Prüfrechte
- (TLPT (Pentests))*

DOR-Vorgaben

- Informationssicherheit *(die aktuellsten und höchsten Qualitätsstandards für die Informations-sicherheit)*
- Geschäftsfortführung
- Unterauftragsvergabe

*Threat-Led-Penetration-Testing, ggf. nur für große Finanzunternehmen relevant

Auswahl der DOR-Vorgaben erfolgt risikoorientiert

Kriterien für Umfang der Vorgaben

- Kritikalität der IKT-Drittdienstleistung
- Komplexität der IKT-Drittdienstleistung
- „Risikoappetit“
- Reifegrad der Organisation
- Durchsetzungsvermögen
- Wirtschaftlichkeit
- Einfluss der Aufsicht

Umfang der DOR-Vorgaben

- Allgemeine Vorgaben (Vertraulichkeitsvereinbarung, SLA)
- Allgemeine Vorgaben für einzelne Bereiche (z.B. Berechtigungsmanagement)
- Verpflichtung zur Zertifizierung
- Umfangreicher Katalog mit Vorgaben

Verträge sind gut, Kontrolle ist besser

Finanzunternehmen sind zu Kontrollen angehalten

- Vertragliche Vereinbarungen reichen nicht aus
- Es müssen bei kwF-relevanten IKT-Drittdienstleistern Prüfrechte vereinbart werden

> „uneingeschränkte Zugangs-, Inspektions- und Auditrechte“
>
> *DORA Art. 30 Abs. 3 lit. e Ziffer i*

Zertifizierungen sind nicht ausreichend

- Zertifikate reichen als Nachweis nicht aus
- Sollten sich aber risikomindernd auswirken

Die Aufsicht kann Einsicht verlangen

- Zusammenarbeit mit der Aufsicht erforderlich

IKT-Drittdienstleister mit nicht umgesetzten Vorgaben sind ein Risiko

Mängel bei der Umsetzung

- Nicht umgesetzte Vorgaben führen nicht automatisch zum Ausschluss.
- Alle nicht erfüllten Vorgaben der IKT-Drittdienstleister sind Risiken
- Risiken müssen bewertet und behandelt werden
- Akzeptanz ist auch eine Behandlung

Erfordern aktive Steuerung der Risiken

- Mindestens jährliche Neubewertung und ad-hoc
- Nachverhandlung mit IKT-Drittdienstleistern
- Dokumentation der Prüfung von Exit-Strategien
- Erhöhte Prüfaktivität

Mangelhafte IKT-Drittdienst-leister sind eine Belastung

- Die Steuerung der Risiken verursacht Aufwand für die Finanzunternehmen
- Kann zu preislichen Diskussionen führen
- Besonderes Kündigungsrecht bei Mängeln muss vereinbart werden

Handlungsempfehlungen für IKT-Drittdienstleister

- Geeignete Sicherheitsorganisation aufstellen
  - Basismaßnahmen für ISMS, BCM und DPRM etablieren
  - anerkannte Standards sollten befolgt werden (ISO 27001, ISO 22301, IT-Grundschutz)
  - Übergreifendes Risikomanagement etablieren
  - Alle Subdienstleister sollten bekannt sein und aktiv gesteuert werden
  - Ein ordentlicher IT-Betrieb mit standardisierten Prozessen sollte gelebt werden
  - Möglichkeit zur schnellen Bewertung von IKT-relevanten Vorfällen
  - Gegebenenfalls „DORA-Niveau“ als Marktvorteil nutzen

Handlungsempfehlungen für IKT-Drittdienstleister (II)

- Der Stellenwert der IKT-Drittdienstleistung sollte bekannt sein
  - Ein regelmäßiger Austausch mit dem Finanzunternehmen sollte etabliert sein
  - Die tatsächlich verarbeiteten Informationen und deren Schutzbedarf sollten bekannt werden
  - Hinterfragen, ob Risikobewertung angemessen ist
  - Insbesondere, wenn die IKT-Dienstleistung als relevant für kwF benannt ist
  - Einschätzung des Marktumfeldes kann helfen, angemessene Reaktionen zu ermitteln

Handlungsempfehlungen für IKT-Drittdienstleister (III)

- Keine „DORA-Blankochecks“
  - Nicht versprechen, eine DORA-konforme IKT-Dienstleistung anzubieten
  - Grundsätzliche zusätzliche Aufwände sollten bekannt sein und mit eingepreist werden
    - Begleitung für die Prüfungen durch Aufsicht oder Finanzunternehmen
    - Steuerung von Subdienstleistern (insbesondere Dokumentation und Prüfungen)
  - Für mögliche technische und organisatorische Zusatzleistungen sollte nachverhandelt werden

Handlungsempfehlungen für IKT-Drittdienstleister (IV)

- Entwicklung der DORA weiter verfolgen
  - Die Auslegung der DORA durch die Aufsicht ist noch nicht einheitlich
    - Finanzunternehmen legen DORA unterschiedlich streng aus
    - Nachverhandlungen aufgrund von Sonderprüfungen sind möglich
  - Mindestens zwei weitere RTS sind noch nicht final veröffentlicht
    - RTS TLPT kann bei großen Finanzunternehmen Auswirkungen haben
    - RTS Subdienstleister kann Auswirkungen haben
  - Für 2028 ist eine Überprüfung der DORA vorgesehen

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com