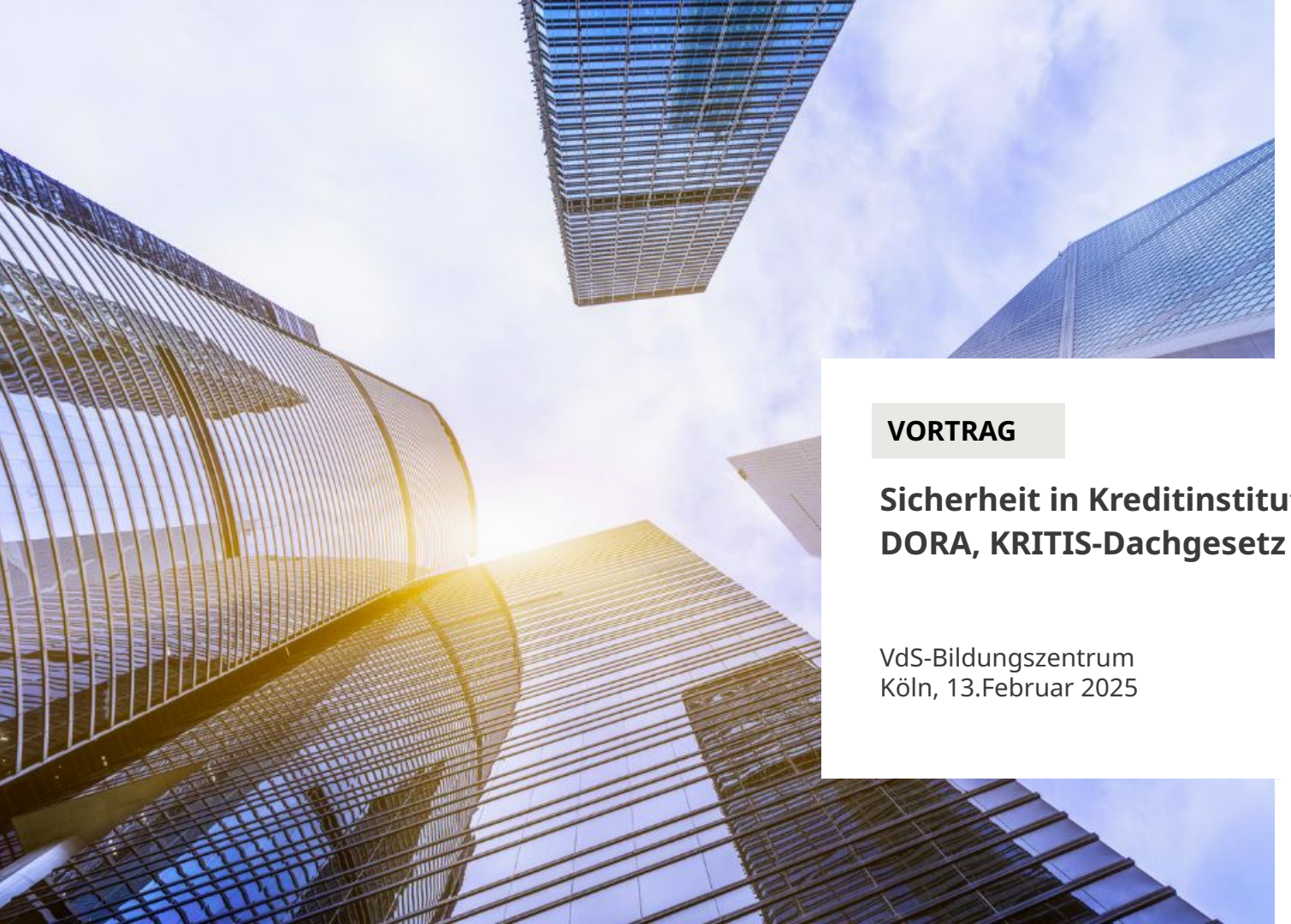


CONCEPTURE
GRUPPE | IHR ERFOLG. GESICHERT

VdS

VORTRAG

Sicherheit in Kreditinstituten- DORA, KRITIS-Dachgesetz und NIS2

VdS-Bildungszentrum
Köln, 13.Februar 2025

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

UNSERE MISSION SEIT 2001

Wir sichern Erfolge.

UNSERE SERVICES

SECURITY COMPLIANCE

Security Compliance ist der Schlüssel, um Unternehmen **zukunftssicher** aufzustellen, indem wir **Strukturen und Prozesse stärken** und Ihre **Krisenresilienz** entscheidend **erhöhen**.

PHYSICAL SECURITY

Wir entwickeln **maßgeschneiderte Sicherheitskonzepte** – von der Ausschreibung über die Fachplanung der Sicherheitstechnik bis hin zur Bauleitung – um Ihre **Widerstandsfähigkeit gegenüber physischen Bedrohungen** zu stärken.

CYBER SECURITY

Wir entwickeln maßgeschneiderte Lösungen und setzen **modernste Technologien** ein, um Ihre Systeme effektiv gegen komplexe Cyberbedrohungen abzusichern und zu gewährleisten, dass sie die **Chancen der Digitalisierung sicher für Ihr Unternehmen nutzen.**

Ihr Referent

Holger Berens

- 35 Jahre Erfahrung im Compliance und Sicherheitsmanagements
- Managing Partner bei Concepture
- Vorstandsvorsitzender des Bundesverbandes für den Schutz kritischer Infrastrukturen (BSKI)
- externer CISO von mehreren internationalen Konzernen für den EMEA-Bereich
- externer IKT-Beauftragter
- Autor von Fachbüchern sowie gefragter Experte der Medien im Bereich Compliance und Security.

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

Ziel des Vortrags🎯

1. Grundlagenverständnis Informationssicherheit
2. Grundlagenwissen zu den Schnittstellen NIS2/Kritis-Dachgesetz
3. Anleitung zur Umsetzung der IKT-Risikoanforderungen
4. Effektive Drittanbieter-Kontrolle und Governance
5. Rollen und Verantwortlichkeiten
6. Handlungsplan

ZIELE

Schnittstellen

DORA sieht IKT-Risikomanagement vor. Daher stellt sich die Frage, wie das Verhältnis zwischen DORA und den Vorgaben der EU zur Sicherheit von Kritis zu bewerten ist.

IKT-Risikomanagement

Das Ziel des IKT-Risikomanagements ist es, die Betriebskontinuität zu sichern und die Resilienz gegenüber IT-bezogenen Risiken wie Cyberangriffen, Systemausfällen und Datenverlusten zu erhöhen.

Organisation

Governance bezieht sich auf die Struktur, Prozesse und Verantwortlichkeiten innerhalb eines Unternehmens, die gewährleisten sollen, dass die Anforderungen an das IKT-Risikomanagement und die operationelle Resilienz effektiv umgesetzt werden

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

IT-Sicherheitsgesetz 1.0 Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG: Verpflichtet Betreiber Kritischer Infrastrukturen IT angemessen abzusichern und diese Sicherheit überprüfen zu lassen.

Neue Rechtssetzung durch die EU

NIS 2 & RCE (Resilience of Critical Entities) (Umsetzung bis 17. Oktober 2024)

Neue Sektoren: z. B. öffentliche Verwaltung, Weltraum, ForschungseinrichtungenEinführung „size-cap rule"

DORA (Digital Operational Resilience Act) VO und RL (Anwendung / Umsetzung bis 17.1.2025)

BSI-Kritisverordnung
Definition Sektoren:
Schwellenwerte (Bedeutung des Versorgungsgrads)

Umsetzungsfristen

2015

2016

2017

Umsetzungsgesetz NIS 1
Neu: Regelungen für Anbieter Digitaler Dienste

2021

2022/23

IT-Sicherheitsgesetz 2.0
Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a)
Neuer Sektor – Siedlungsabfallentsorgung, Selbsterklärung zur IT-Sicherheit Unternehmen im besonderen öffentlichen Interesse (§ 8f)

2024

2025

2025/26

jetzt

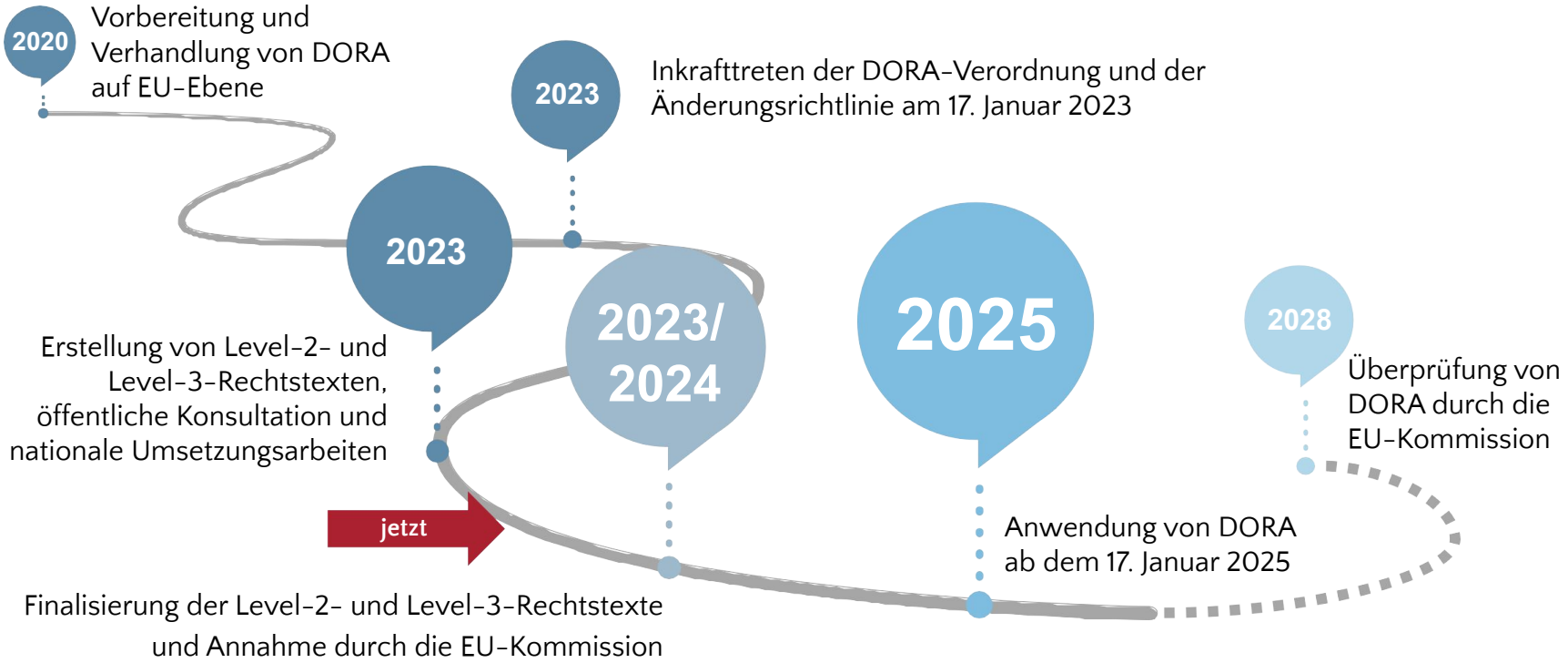
Inkrafttreten
BISG 3.0
KRITIS-Dachgesetz

Der Cyber Resilience Act („CRA")

wurde am 20.11.2024 im Amtsblatt veröffentlicht und tritt am 09.12.2024 in Kraft.

Vergangenes, aktuelles und nächste Schritte

BaFin



EINFÜHRUNG INFORMATIONSSICHERHEIT

IKT-Sicherheit:

Meint Schutz von IKT-Systemen (Informations- und Kommunikationssysteme) gegen eine Vielzahl verschiedener Gefahren und Angriffe.

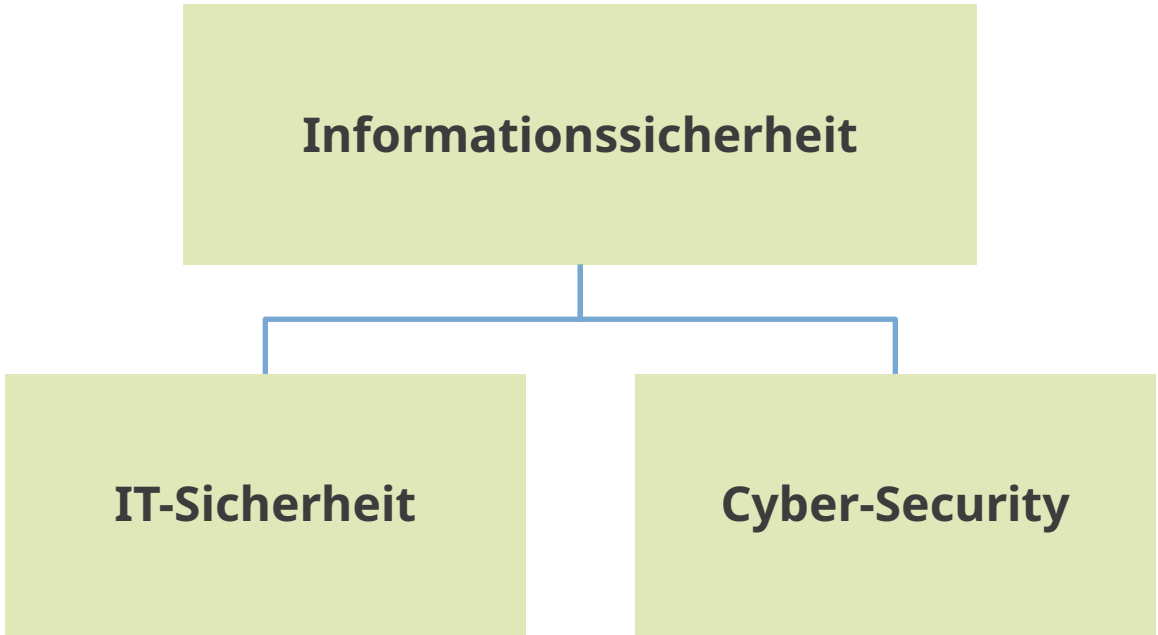
EINFÜHRUNG INFORMATIONSSICHERHEIT

Cyber Security – Internetsicherheit:
Internetsicherheit meint den Schutz von Internetbasierten Systemen und Anwendungen und von Systemen, die mit dem Internet verbunden sind, z.B. auch Browser-Sicherheit, gegen Gefahren aus beliebigen Netzwerken (in der Regel dem Internet...)

EINFÜHRUNG INFORMATIONSSICHERHEIT

Informationssicherheit:
Schutz von Daten und Informationen jeglicher Art in jeglicher Form, z.B. Datenträger, Kommunikationsdaten, Daten in flüchtigen Speichern (PC-RAM, Netzwerkkomponenten), papiergebundene Daten, Mikrofiche, Filme, Sprachaufzeichnungen, Texte und Bilder auf Flip Charts, und nicht zuletzt das Wissen eines Menschen selbst (Gehirn).

EINFÜHRUNG INFORMATIONSSICHERHEIT



EINFÜHRUNG INFORMATIONSSICHERHEIT

Hauptschutzziele der Informationssicherheit:

C-I-A

CONFIDENTIALITY	Vertraulichkeit
INTEGRITY	Integrität
AVAILABILITY	Verfügbarkeit

Sicherheitsbetrachtungen müssen sich mindestens auf diese drei Schutzziele beziehen, Maßnahmen müssen diese gewährleisten.

EINFÜHRUNG INFORMATIONSSICHERHEIT

Neben den drei IT-Schutzzielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“, bildet „**Authentizität**“ eines der erweiterten Schutzziele des DORA.

Oft wird dieses als übergeordnetes Ziel angesehen, da die anderen Schutzziele ohne Wert wären, wenn nicht gesichert ist, dass der Kommunikationspartner auch tatsächlich seiner Identität gerecht wird.

EINFÜHRUNG INFORMATIONSSICHERHEIT

Gemäß Art. 1 DORA werden einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die wesentlich sind festgelegt.

Es geht also **primär** um **IKT-Sicherheit**.

EINFÜHRUNG INFORMATIONSSICHERHEIT

Damit umfasst DORA grundsätzlich **nicht** die **Informationssicherheit**, obwohl in den ersten Entwürfen ein ISMS gefordert war.

Das hat **Auswirkungen auf Governance und Strategie**.

EINFÜHRUNG INFORMATIONSSICHERHEIT

DORA fokussiert auf

- IKT-Risikomanagement
- Meldung von schwerwiegenden IKT- Vorfällen
- Digitale Betriebsstabilität und ihre Prüfung durch bedrohungsorientierte Penetrationstests
- Steuerung der IKT- Drittanbieter

Das sind wesentliche Elemente eines ISMS, die zu ihrer Umsetzung Vorarbeiten und ergänzender Arbeiten bedürfen.

EINFÜHRUNG INFORMATIONSSICHERHEIT

DORA verlangt **implizit ein umgesetztes ISMS**, ohne es explizit im Gesetzestext zu nennen.

§ 25a KWG gibt vor, wie ein Institut personell und technisch-organisatorisch ausgestattet sein muss.

Ebenfalls muss ein angemessenes Notfallkonzept bzw. Risikomanagement – insbesondere für IT-Systeme – vorliegen.

EINFÜHRUNG INFORMATIONSSICHERHEIT

MaRisk als Verwaltungsvorschrift zur Umsetzung der aufsichtsrechtlichen Anforderungen, werden durch BAIT, VAIT etc. konkretisiert, die explizit auf Informationssicherheit gerichtet sind.

Mit Ablauf des 16. Januar 2025 sind Institute, die ab dem 17. Januar 2025 ein Risikomanagement für die Informations- und Kommunikationstechnologie (IKT) nach Artikel 5 bis 15 oder Artikel 16 Digital Operational Resilience Act (DORA) betreiben müssen, aus dem Anwenderkreis der BAIT ausgenommen.

EINFÜHRUNG INFORMATIONSSICHERHEIT

Zudem hebt die BaFin Kapitel 11 der BAIT auf. Die aktualisierten BAIT sind auf der Website der BaFin zu finden.

Durch das Finanzmarktdigitalisierungsgesetz (FinmadiG) wurde § 1a Absatz 2 Kreditwesengesetz neu gefasst, wonach ab dem 1. Januar 2027 weitere Institute DORA anwenden müssen.

Mit Ablauf des 31. Dezember 2026 werden die BAIT daher vollständig aufgehoben.

Zwischenfazit

DORA ist als EU-VO geltendes, unmittelbar **zwingendes „Gesetz“**.

Damit ist es **lex specialis** im Bereich Finanzsektor bezüglich IKT-Sicherheit.

Das Spezialitätsprinzip geht aber nur so weit, wie die Regelungen greifen.

Das bedeutet, dass NIS2 (?), KRITIS-Dachgesetz auch zusätzlich gelten, wenn DORA hier keine Regelungen vorsieht.

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

VERHÄLTNIS ZU NIS2

Es gibt zwei sogenannte EU-Richtlinien, die in nationales Recht umgesetzt werden müssen:

EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie *Naturgefahren*, *Terroranschläge* oder *Sabotage* zu stärken.

EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

Die NIS2-Richtlinie verpflichtet die Unternehmen, die in den Anwendungsbereich fallen, IT-, Cyber- und Informationssicherheit einzuführen.

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

VERHÄLTNIS ZU NIS2

EU Richtlinien müssen in den Mitgliedstaaten in nationales Recht umgesetzt werden.

Die Umsetzungsfrist für NIS2 und CER war der 17.10.2024.

In Deutschland sind das für:

NIS2 › BSIG 3.0/ITSiG 3.0

CER › KRITIS-Dachgesetz

Die EU Kommission hat ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, da diese Richtlinien nicht fristgerecht umgesetzt wurden.

VERHÄLTNIS ZU NIS2

Wegen der Neuwahlen im Februar ist nicht damit zu rechnen, dass noch im 1. Quartal 2025 die Umsetzungsgesetze in Kraft treten.

Ein genaues Datum kann nicht prognostiziert werden.

Die wesentlichen Anforderungen stehen mit den jeweiligen Entwürfen jedoch fest.

Das bedeutet, dass die Unternehmen, die in den Anwendungsbereich fallen, jetzt schon wissen, welche Maßnahmen implementiert werden müssen.

VERHÄLTNIS ZU NIS2

Damit stellt sich die Frage, ob neben DORA auch NIS2 und/oder Kritis-Dachgesetz gelten.

Der Anwendungsbereich der sogenannte NIS2 Richtlinie orientiert sich nicht an Schwellenwerten.

Maßgeblich ist die size-cap-rule, also die Größe des Unternehmens. Hinzukommen muss, dass das Unternehmen in einem der Sektoren tätig ist.

VERHÄLTNIS ZU NIS2

Folgende Unternehmensgrößen sind zu unterscheiden:

Besonders wichtige Einrichtungen

Dies sind zunächst die Betreiber kritischer Anlagen. (§ 28 V)
Es ändert sich im Grunde hier nicht viel. Die bisherige Logik von Kritis-Sektoren, kritischen Dienstleistungen und die Anlagen mit Schwellenwerten bleibt erhalten.

VERHÄLTNIS ZU NIS2

Besonders wichtige Einrichtungen

Neben den KRITIS-Betreibern sind dies Großunternehmen aus den Sektoren in NIS2-Anlage 1 und einige Unternehmen unabhängig ihrer Größe und KRITIS-Betreiber.

Dies sind Unternehmen ab 250 MA oder einem Umsatz von 50 Mio. und 42 Mio. Bilanz.

Hier sind nicht mehr die Schwellenwerte entscheidend, sondern “nur” die Tätigkeit in einem der Sektoren der **Anlage 1**.

VERHÄLTNIS ZU NIS2

Wichtige Einrichtungen

Dies sind Unternehmen ab 50 Mitarbeitern

oder

einem Umsatz und Bilanz über 10 Millionen,

die in den Sektoren der **Anlage 1** und Anlage 2 tätig sind.

VERHÄLTNIS ZU NIS2

ANHANG I

SEKTOREN MIT HOHER KRITIKALITÄT

3.	Bankwesen		Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([15])
4.	Finanzmarktinf-rastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([16])
			— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([17])

Finanzunternehmen, die unter die DORA-Verordnung der EU fallen, können per Definition keine NIS2-Einrichtung werden und erhalten daher keine NIS2-Pflichten. Diese Unternehmen werden über DORA reguliert und nicht von NIS2. DORA auferlegt ihnen ähnliche, teils deutlich detailliertere Pflichten, die betroffene Unternehmen ab Januar 2025 anwenden müssen.

Quelle: https://www.openkritis.de/it-sicherheitsgesetz/sektor_finanz-versicherungswesen.html#nis2

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

VERGLEICH ISO 27001/27002

Eine detaillierte **Vergleichsanalyse zwischen DORA und den beiden aktuellen ISO-Standards ISO/IEC 27001:2022 und ISO/IEC 27002:2022** zeigt sowohl inhaltliche Übereinstimmungen als auch spezifische Unterschiede.

Die Analyse konzentriert sich auf zentrale Themen wie Risikomanagement, Vorfallreaktion, Drittanbieter-Management und kontinuierliche Verbesserung und stellt heraus, wie DORA auf diese Anforderungen eingeht und welche zusätzlichen Details ISO 27001 und ISO 27002 bieten.

VERGLEICH ISO 27001/27002

DORA und ISO/IEC 27001:2022 sowie ISO/IEC 27002:2022 zeigen erhebliche **Überschneidungen in der Sicherstellung von Informationssicherheit und IKT-Resilienz**, jedoch mit unterschiedlichen Schwerpunkten.

Während DORA speziell auf den Finanzsektor ausgerichtet ist und die operationelle Resilienz betont, bieten ISO 27001 und ISO 27002 umfassende Leitlinien für das allgemeine Informationssicherheits-Management und die spezifische Implementierung von Sicherheitsmaßnahmen.

VERGLEICH ISO 27001/27002

Zusammen bieten sie eine synergetische Grundlage, wobei DORA für Finanzunternehmen den regulatorischen Rahmen vorgibt und ISO 27001 und ISO 27002 detaillierte Umsetzungsrichtlinien und operative Maßnahmen bieten

Es macht daher Sinn mit der Umsetzung und Implementierung der ISO-Normen zu starten.

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Regierungsentwurf von November 2024 “Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen ”

§ 2 Begriffsbestimmungen
Im Sinne dieses Gesetzes ist
1. **„Betreiber kritischer Anlagen“** eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt; ……..

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Regierungsentwurf von November 2024 “Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen ”

§ 2 Begriffsbestimmungen
Im Sinne dieses Gesetzes ist
1. **„Betreiber kritischer Anlagen“** eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt; ……..

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

§ 7 Sektor Finanz- und Versicherungswesen (Kritis-VO)
(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Finanz- und Versicherungswesen kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Bargeldversorgung;
2. der kartengestützte Zahlungsverkehr;
3. der konventionelle Zahlungsverkehr;
4. der Handel mit Wertpapieren und Derivaten sowie die Verrechnung und
5. die Abwicklung von Wertpapier- und Derivatgeschäften;
6. Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende.

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Maßgeblich sind die in der Kritis-VO vorgegebenen Schwellenwerte:

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Bargeldversorgung**		
1.1	Autorisierung einer Abhebung		
1.1.1	Autorisierungssystem	Anzahl der Transaktionen/ Jahr	15 000 000
1.1.2	System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers	Anzahl der Transaktionen/ Jahr	15 000 000
1.2	Einbringen in den Zahlungsverkehr		
1.2.1	System zur Aufbereitung durch den Geldautomatenbetreiber	Anzahl der Transaktionen/ Jahr	15 000 000
1.2.2	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/ Jahr	18 000 000
1.2.3	Clearing-System	Anzahl der Transaktionen/ Jahr	18 000 000
1.2.4	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	18 000 000
1.3	Belastung Kundenkonto		
1.3.1	Kontoführungssystem	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung verbuchten Transaktionen	15 000 000
1.4	Bargeldlogistik		
1.4.1	Cash Center	Anzahl bearbeiteter Banknoten/Jahr	93 500 000
1.4.2	IT-System für das Cash Management	Anzahl bearbeiteter Banknoten/Jahr	93 500 000

2	**Kartengestützter Zahlungsverkehr**		
2.1	Autorisierung		
2.1.1	Autorisierungssystem	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung autorisierten Transaktionen	21 500 000
2.1.2	System zur Anbindung an ein Autorisierungssystem aus Sicht des Terminalbetreibers	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung autorisierten Transaktionen	21 500 000
2.2	Einbringen in den Zahlungsverkehr		
2.2.1	System zur Aufbereitung durch den POS-Terminalbetreiber	Anzahl der Transaktionen/ Jahr	21 500 000
2.2.2	System zur Annahme der POS-Transaktionsdaten beim Zahlungsdienstleister des Zahlungsempfängers	Anzahl der Transaktionen/ Jahr	21 500 000
2.2.3	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/ Jahr	18 000 000
2.2.4	Clearing-System	Anzahl der Transaktionen/ Jahr	18 000 000
2.2.5	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	18 000 000
2.3	Belastung auf dem Konto des Zahlers und Gutschrift auf dem Konto des Zahlungsempfängers		
2.3.1	Kontoführungssystem	Anzahl der in diesem System bei der Erbringung der jeweiligen kritischen Dienstleistung verbuchten Transaktionen	21 500 000

3	**Konventioneller Zahlungsverkehr**		
3.1	Annahme einer Überweisung oder Lastschrift		
3.1.1	System zur Annahme einer Überweisung oder Lastschrift	Anzahl der Transaktionen/ Jahr	100 000 000
3.2	Einbringen in den Zahlungsverkehr		
3.2.1	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/ Jahr	100 000 000
3.2.2	Clearing-System	Anzahl der Transaktionen/ Jahr	100 000 000
3.2.3	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	100 000 000
3.3	Belastung und Gutschrift auf Kundenkonten		
3.3.1	Kontoführungssystem	Anzahl der Transaktionen/ Jahr	100 000 000

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Wenn also ein Institut die Schwellenwerte erreicht, ist das Kritis-Dachgesetz parallel zu DORA anzuwenden und umzusetzen.

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Nach § 2 wird Resilienz wie folgt definiert:

„Resilienz“ die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen; …

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- Vorsorge: Präventionsmaßnahmen gegen Vorfälle, Disaster und Klimawandel
- Physische Sicherheit: Absicherung der ihrer Liegenschaften und Kritischen Infrastruktur mit physischen Schutzmaßnahmen, Perimeterüberwachung, Detektion und Zutrittskontrolle
- Krisen: Risiko- und Krisenmanagement zur Bewältigung von Krisen, mit definierten Prozeduren, Protokollen und Alarmierung

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- Wiederherstellung: Business Continuity Management (BCM) und Maßnahmen zur Wiederherstellung nach Vorfällen — inkl. alternative Lieferketten
- Personal: Sicherheitsmanagement und besondere personelle Sicherheit, Zutrittskontrolle, Sicherheitsüberprüfung, einschließlich externem Personal und Dienstleistern
- Awareness: Beim Personal über die Resilienz-Maßnahmen

VERHÄLTNIS ZUM KRITIS-DACHGESETZ

Folgende Mindestmaßnahmen stehen fest:

- nationale Risikobewertungen,
- betreiberseitige Risikobewertungen,
- Erstellung von Resilienzplänen durch die Betreiber,
- Erarbeitung branchenspezifischer Schutzstandards durch die zuständigen Verbände sowie
- Äquivalenzprüfungen durch die fachlich zuständigen Behörden.
- Die zentralen Betreiberpflichten zu Risikoanalysen und Risikobewertungen, Resilienzmaßnahmen, Nachweispflichten und für das Meldewesen treten am 17.07.2026 in Kraft?

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

EINFÜHRUNG DORA

DORA zielt darauf ab, die **operationale Resilienz von Finanzunternehmen in der EU zu stärken**, indem Anforderungen an das Risikomanagement für Informations- und Kommunikationstechnologie (IKT) eingeführt werden.

DORA fokussiert auf die Sicherstellung der Widerstandsfähigkeit gegen IT-Risiken sowie die Regulierung von Drittanbietern.

EINFÜHRUNG DORA

„Digitale operationale Resilienz“ ist die Fähigkeit eines Finanzunternehmens, seine operative **Integrität** und **Betriebszuverlässigkeit aufzubauen**, zu **gewährleisten** und zu **überprüfen**, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die **Sicherheit der Netzwerk- und Informationssysteme** zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die **kontinuierliche Erbringung** von Finanzdienstleistungen und deren **Qualität**, einschließlich bei **Störungen**, zu unterstützen.

EINFÜHRUNG DORA

DORA gilt für eine breite Gruppe von Unternehmen im Finanzsektor, wie in Artikel 2 dargelegt. Dazu gehören u.a.:

- Kreditinstitute
- Versicherungsunternehmen
- Wertpapierfirmen
- Zahlungsinstitute
- Investmentfirmen und -fonds
- Krypto-Asset-Dienstleister
- Anbieter von Dienstleistungen im Bereich der Cloud-Computing, Datenanalyse, Zahlungsvorgänge oder Kreditvermittlung.

EINFÜHRUNG DORA

Neben den **Finanzunternehmen** erstreckt sich der Geltungsbereich von DORA gemäß Artikel 28 auch auf **Drittanbieter kritischer IKT-Dienstleistungen**.

Dies betrifft insbesondere Anbieter von Cloud-Computing, Software- und Datenanalysetools sowie Anbieter von IT-Infrastruktur.

DORA verlangt von diesen Anbietern ein hohes Maß an Cybersicherheit, um potenzielle Schwachstellen in den ausgelagerten IT-Systemen der Finanzunternehmen zu minimieren.

EINFÜHRUNG DORA

Damit gilt die Verordnung auch für ein breites Spektrum von Drittdienstleistern, sodass insbesondere auch Cloud-Service-Provider, Softwareanbieter, Datenanalysedienste und Rechenzentren miteingeschlossen sind. Explizit erfasst werden Anbieter, welche Zahlungen abwickeln oder Zahlungsinfrastrukturen betreiben.

Einem besonders **strikten Überwachungsregime** sind solche **IKT-Drittdienstleister** unterworfen, die von DORA als „kritisch“ eingestuft werden.

Wesentliche Elemente in DORA

BaFin

IKT-Risikomanagement

- **Governance und Organisation**
- **IKT-Risikomanagement-rahmen**
- **IKT -Systeme, -Protokolle und -Tools**
- **Lernprozesse und Weiterentwicklung**
- **Kommunikation**

IKT-Drittparteirisikomanagement

- **Allgemeine Prinzipien** (u. a. Informationsregister über IKT- Drittpartei Vertragsbeziehungen, Mitteilungen an die Aufsichtsbehörden, und Mindestvertragsbestandteile)

EU-Überwachungsrahmenwerk

- Überwachung von **kritischen IKT-Drittdienstleistern**

IKT-Vorfallmeldewesen

- Festlegung von **Definitionen** IKT-bezogener Vorfällen
- **Klassifikationskriterien** von IKT-bezogenen Vorfällen
- **Meldeprozess,** Berichtswesen von IKT-bezogenen Vorfällen und Cyberbedrohungen

Testen der digitalen operationalen Resilienz

- **Basistests**
- Gesamter Finanzsektor
- Schwachstellen Scans, Quellcode Tests,

TLPT

- **Fortgeschrittene Tests**
- TLP T: Threat Led Penetration Tests
- Nur „systemrelevante" Finanzunternehmen mit hohem IKT-Reifegrad
- TIBER-EU als „Blaupause"

Information Sharing & Cyberübungen

- Freiwilliger **Austausch von Informationen und Erkenntnissen** zwischen Finanzunternehmen zur Verbesserung der „Situational Awareness"
- Sektorübergreifende **Krisenmanagement- und Notfallübungen** mit Cyberbezug zur Verbesserung der Kommunikation und Stärkung der Resilienz im Finanzsektor

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

GOVERNANCE & ORGANISATION

Art. 5 des DORA definiert Anforderungen an die **Governance** und **Organisation**, um sicherzustellen, dass Institute effektiv mit IKT-Risiken umgehen und ihre operationelle Resilienz sicherstellen können.

Die Geschäftsleitung trägt die **Verantwortung** für die IKT-Risikomanagementstrategie.

Sicherstellung einer umfassenden und **wirksamen Governance-Struktur** zur Überwachung und Steuerung aller IKT-Risiken.

Aktive **Kontrolle** und **Steuerung** der **Strategie** zur Risikominimierung und Resilienz.

RISIKOMANAGEMENT

Gemäß Art. 16 DORA gelten für kleine und nicht verflochtene Wertpapierfirmen und für ausgenommene Institute die Art. 5 - 15 DORA nicht.

Betrachtet man aber den sogenannten **“vereinfachten IKT-Risikomanagementrahmen”** genauer, macht es Sinn, dennoch die Vorgaben der Art. 5 - 15 DORA entsprechend anzuwenden.

RISIKOMANAGEMENT

Art. 6 beschreibt detailliert die Anforderungen an den IKT-Risikomanagementrahmen (Informations- und Kommunikationstechnologie-Risikomanagement) für Finanzunternehmen, einschließlich Wertpapierunternehmen.

Ziel ist es, sicherzustellen, dass Unternehmen robuste Prozesse und Strukturen implementieren, um IKT-Risiken effektiv zu identifizieren, zu bewerten, zu steuern und zu überwachen.

AGENDA

1 ÜBER UNS

2 ZIEL DES VORTRAGS

3 EINFÜHRUNG INFORMATIONS-SICHERHEIT

4 VERHÄLTNIS ZU NIS 2

5 VERGLEICH ISO 27001/27002

6 VERHÄLTNIS ZUM KRITIS-DACHGESETZ

7 EINFÜHRUNG DORA

8 GOVERNANCE & ORGANISATION

9 SCHLÜSSEL-KOMPONENTEN DORA COMPLIANCE

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

IKT-Risikomanagement

Implementierung eines **umfassenden IKT-Risikomanagements** zur Identifikation, Bewertung und Minderung von Risiken.

Regelmäßige **Überprüfung** von Systemen, Prozessen und Mitarbeitern, um Schwachstellen zu erkennen.

Strategien zur Steuerung von operationellen, Cyber- und Drittanbieterrisiken.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Operative Resilienz

Festlegung von **Maßnahmen** zur Sicherstellung der **Geschäftskontinuität** bei IKT-Störungen.

Definition kritischer Geschäftsprozesse und IKT-Ressourcen.

Regelmäßige **Tests** zur Resilienzprüfung und Anpassung der Strategien basierend auf Testergebnissen.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

IKT-Vorfallberichterstattung

Einrichtung von **Meldeverfahren** für interne und externe Stakeholder.

Klare **Klassifikation** und **Priorisierung** von Vorfällen.

Meldung **erheblicher Vorfälle** an **nationale und EU-Behörden** innerhalb vorgegebener Fristen.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Vorfallreaktion und Wiederherstellung

Entwicklung eines **Vorfallreaktions- und Wiederherstellungsplans** zur Bewältigung von IKT-Störungen.

Festlegung von Rollen, Verantwortlichkeiten und Kommunikationswegen im Ernstfall.

Regelmäßige **Tests und Validierungen** der Wiederherstellungspläne

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Risikobewertung von Drittanbietern

Regelmäßige **Risikobewertungen** externer IKT-Dienstleister.

Verankerung von Resilienz- und Kontinuitätsanforderungen in **Verträgen**.

Kontinuierliches **Monitoring** und Risikomanagement von Drittanbietern

SCHLÜSSELKOMPONENTEN COMPLIANCE

Testen und Prüfen der IKT-Systeme

Regelmäßige **Resilienztests** und Audits zur **Schwachstellenidentifikation**.

Einsatz fortschrittlicher Methoden wie **Penetrationstests** und Red-Team-Übungen.

Dokumentation und Analyse der Testergebnisse zur **Anpassung der Strategien**.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Informationsaustausch

Teilnahme an Informationsaustauschen innerhalb des Finanzsektors.

Zusammenarbeit mit anderen Finanzunternehmen und relevanten Stakeholdern.

Austausch von Bedrohungsinformationen und **Best Practices**.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Governance und Aufsicht

Sicherstellung der Aufsicht durch das Management über IKT-Risiken und **Resilienzstrategien**.

Zuweisung klarer Rollen und Verantwortlichkeiten für IKT-Risiken.

Regelmäßige **Überwachung** der DORA-Compliance.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Compliance und Berichterstattung

Dokumentation aller IKT-Risikomanagementpraktiken und -strategien.

Regelmäßige **Berichterstattung** an **interne Kontrollinstanzen** und gegebenenfalls an Behörden.

Mechanismen zur **Compliance-Überwachung** und Berichterstattung.

SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

Kontinuierliche Verbesserung und Schulung

Regelmäßige **Überprüfung** und Anpassung der IKT-Risikomanagementstrategien.

Schulungsprogramme zur Sensibilisierung der Mitarbeiter für Cyber-Resilienz.

Fortlaufende Bewertung regulatorischer Änderungen und technischer Neuerungen.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt:
Holger Berens

holger.berens@bski.de
h.berens@concepture.de