CONCEPTURE

DORA - WAS KLEINE UNTERNEHMEN JETZT WISSEN MÜSSEN.

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

AGENDA

9 IKT Drittleister

10 GESCHÄFTSFORTFÜHRUNG (BCM)

11 VERGLEICH ISO 27001/27002 vs. BAIT

12 SCHLÜSSELKOMPONENTEN DER DORA COMPLIANCE

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

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
- Autor von Fachbüchern sowie gefragter Experte der Medien im Bereich Compliance und Security.

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

Ziel unseres Webinars 🎯

1. Grundlagenverständnis von DORA schaffen
2. Anleitung zur Umsetzung der IKT-Risikoanforderungen
3. Effektive Drittanbieter-Kontrolle und Governance
4. Rollen und Verantwortlichkeiten
5. Handlungsplan

ZIELE

Praktikabilität

DORA sieht für kleinere, nicht verbundene Wertpapierunternehmen zwar dieselben Prinzipien vor, doch können die Anforderungen in einer vereinfachten Form erfüllt werden, die sich an der Größe, Komplexität und den Risiken des Unternehmens orientiert.

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 WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

EINFÜHRUNG INFORMATIONSSICHERHEIT

IKT-Sicherheit:

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

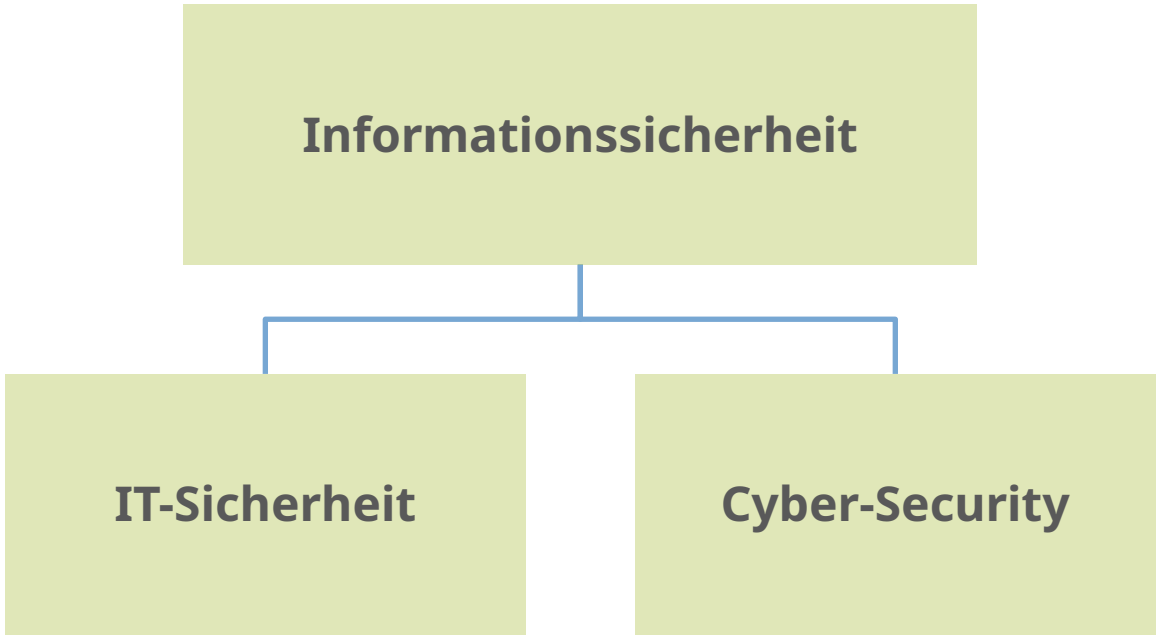
EINFÜHRUNG INFORMATIONSSICHERHEIT

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.

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, BAIT etc. auch zusätzlich gelten, wenn DORA hier keine Regelungen vorsieht.

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

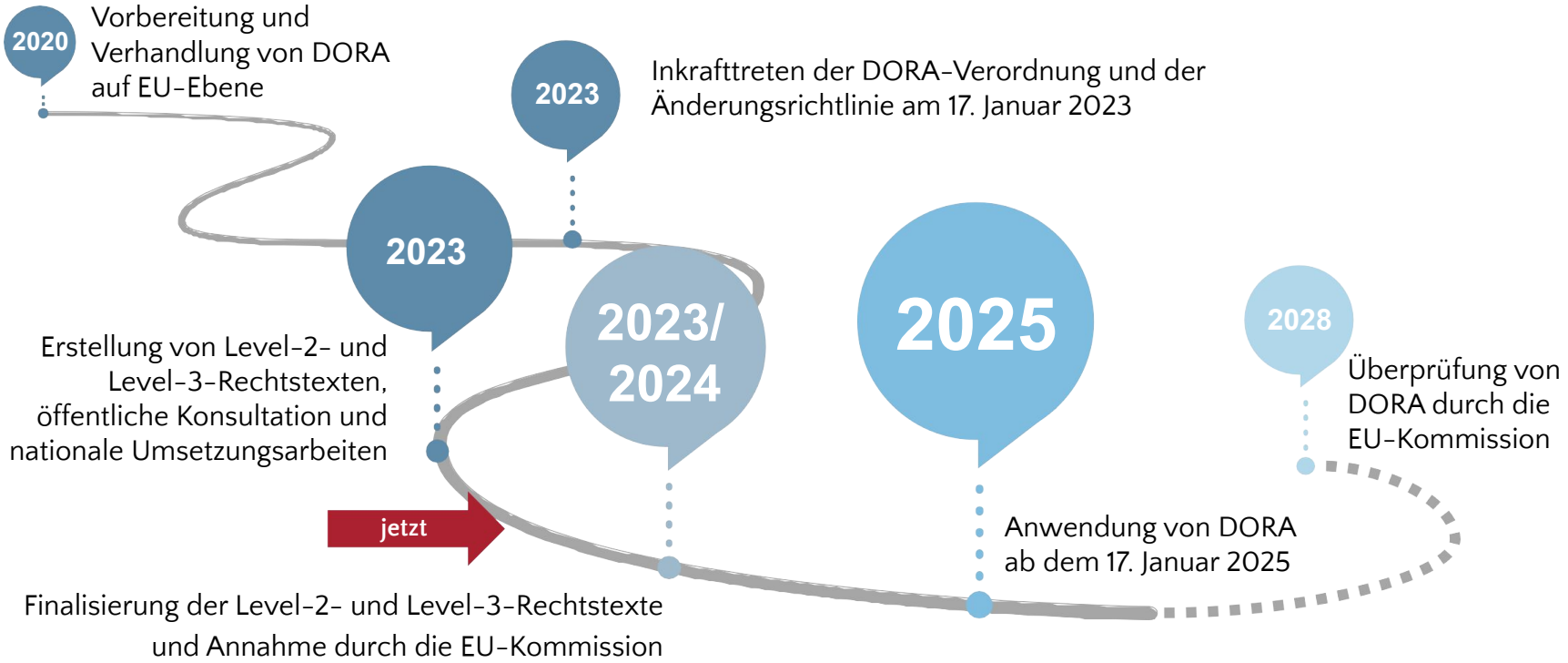
6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

Vergangenes, aktuelles und nächste Schritte

BaFin



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 ergänzt bestehende regulatorische Rahmenwerke wie BAIT und VAIT und 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-Drittparteivertragsbeziehungen, Mitteilungen an die Aufsichtsbehörden, und Mindestvertragsbestandteile)

EU-Überwachungsrahmenwerk

- Überwachung von **kritischen IKT-Drittdienstleistern**

IKT-Vorfallmeldewesen

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

Testen der digitalen operationalen Resilienz

- **Basistests**
- Gesamter Finanzsektor
- Schwachstellenscans, Quellcodetests, Performancetests etc.

TLPT

- **Fortgeschrittene Tests**
- TLPT: 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 WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

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.

Was sind die Anforderungen an Governance und Organisation? 1/7

Entwicklung einer klar definierten **IKT-Risikostrategie** und deren regelmäßige Anpassung.

Festlegung des **Risikoappetits**: Wie viel Risiko ist das Unternehmen bereit einzugehen?

Die Strategie dient als Grundlage für alle **IKT-Entscheidungen und Risikomanagementmaßnahmen**.

Was sind die Anforderungen an Governance und Organisation? 2/7

Klare Definition und Zuordnung von **Rollen und Verantwortlichkeiten** im IKT-Risikomanagement.

Etablierung einer **Hierarchie und Kommunikationsstruktur** zur effektiven Eskalation und Lösung von Risiken.

Stärkung der **Transparenz** und **Nachvollziehbarkeit** in der **Risikosteuerung**.

Was sind die Anforderungen an Governance und Organisation? 3/7

Einführung regelmäßiger **Überwachungsmechanismen** zur Risikokontrolle.

Berichterstattung an die Geschäftsleitung über den Status des IKT-Risikomanagements.

Dokumentation und Analyse von wesentlichen **IKT-Vorfällen** und getroffenen Maßnahmen.

Was sind die Anforderungen an Governance und Organisation? 4/7

Sicherstellung, dass finanzielle, personelle und technologische **Ressourcen** verfügbar sind.

Investitionen in IT-Infrastruktur, Schulungen und Risikomanagement-Tools.

Ressourcen zur Erreichung eines effektiven IKT-Risikomanagements und zur Resilienzsteigerung.

Was sind die Anforderungen an Governance und Organisation? 5/7

Sicherstellung, dass **Schlüsselmitarbeiter** über notwendige Qualifikationen verfügen.

Regelmäßige **Schulungen** zum Umgang mit IKT-Risiken und Cybersicherheit.

Förderung einer **Sicherheitskultur** im Unternehmen zur Stärkung der Resilienz.

Was sind die Anforderungen an Governance und Organisation? 6/7

Integration der IKT-Risiken in die allgemeine Unternehmensstrategie.

IKT-Risikomanagement als Bestandteil der **Entscheidungsprozesse** und der strategischen Planung.

Sicherstellung, dass alle Unternehmensbereiche auf **gemeinsame Resilienz-Ziele** hinarbeiten.

Was sind die Anforderungen an Governance und Organisation? 7/7

Regelmäßige **Überprüfung** der **Wirksamkeit** des IKT-Risikomanagements.

Ständige **Anpassung** der Sicherheitsmaßnahmen an neue Bedrohungen und Entwicklungen.

Förderung einer proaktiven Haltung zur kontinuierlichen Resilienzsteigerung

RISIKOMANAGEMENT

Gemäß Art. 16 DORA gelten für kleine und nicht verflochtene Wertpapierfirmen und für ausgenomme 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.

Was sind die Anforderungen nach Art. 6 DORA? 1/4

Regulative **Identifikation und Bewertung** von internen und externen IKT-Risiken.

Priorisierung von Risiken basierend auf deren Wahrscheinlichkeit und potenziellen Auswirkungen auf das Unternehmen.

Entwicklung präventiver und reaktiver **Maßnahmen zur Risikosteuerung**, z.B. Sicherheitsrichtlinien und technische Kontrollen.

Was sind die Anforderungen nach Art. 6 DORA? 2/4

Notfallpläne und Wiederherstellungsprozesse zur schnellen Betriebsaufnahme nach einem Vorfall.

Kontinuierliche Überwachung und Kontrolle der Maßnahmen zur Risikosteuerung.

Einsatz automatisierter Überwachungssysteme und regelmäßiger Audits zur Früherkennung von Schwachstellen.

Was sind die Anforderungen nach Art. 6 DORA? 3/4

Implementierung von **Berichts- und Eskalationsverfahren** zur schnellen Weiterleitung von Informationen.

Kritische Vorfälle und Änderungen der Risikolandschaft müssen **zeitnah gemeldet** werden.

Klare und **umfassende Dokumentation** aller IKT-Risikomanagementprozesse und -richtlinien.

Was sind die Anforderungen nach Art. 6 DORA? 4/4

Regelmäßige **Aktualisierung** und **Zugänglichmachung** der Dokumente zur **Transparenzsicherung**.

Regelmäßige **Überprüfung** und **Weiterentwicklung** des IKT-Risikomanagementrahmens.

Berücksichtigung **externer Entwicklungen** und **proaktive Reaktion** auf **neue Bedrohungen.**

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

IKT SYSTEME, PROTOKOLLE, TOOLS

Artikel 7 DORA stellt detaillierte Anforderungen an Finanzunternehmen, einschließlich Wertpapierunternehmen, für den Einsatz, die Pflege und die Sicherung ihrer IKT-Systeme, -Protokolle und -Tools.

Diese Anforderungen sollen sicherstellen, dass Unternehmen robuste Systeme betreiben, die gegen IT-Risiken resilient sind und gleichzeitig die Sicherheit und Geschäftskontinuität wahren.

Was sind die Anforderungen nach Art. 7 DORA? 1/8

Sicherstellen, dass IKT-Systeme **zuverlässig** und **belastbar** sind.

Systeme müssen **hohe Verfügbarkeit** und **Stabilität** für den täglichen Betrieb gewährleisten.

Schutz vor Bedrohungen und Belastungen durch **widerstandsfähige Systemarchitektur**.

Was sind die Anforderungen nach Art. 7 DORA? 2/8

Implementierung von **Sicherheitsprotokollen** wie Authentifizierung, Zugriffsmanagement und Verschlüsselung.

Schutz vor **unbefugtem** Zugriff, Datenverlust und **Cyberangriffen**.

Regelmäßige **Überprüfung und Aktualisierung** der Sicherheitsmaßnahmen.

Was sind die Anforderungen nach Art. 7 DORA? 3/8

Sicherstellen, dass alle IKT-Systeme regelmäßig **gewartet** und **aktualisiert** werden.

Systematisches **Patch-Management** zur Behebung von Sicherheitslücken.

Überprüfung und Anpassung von **Konfigurationen** und **Einstellungen**.

Was sind die Anforderungen nach Art. 7 DORA? 4/8

Implementierung von Überwachung und Protokollierung zur **Früherkennung** von Vorfällen.

Aufzeichnung aller relevanten Ereignisse zur **Nachverfolgbarkeit** und **Ursachenanalyse**.

Echtzeitüberwachung und sofortige Meldung von Anomalien.

Was sind die Anforderungen nach Art. 7 DORA? 5/8

Regelmäßige **Backups** aller geschäftskritischen Daten und Systeme.

Speicherung der Backups an gesicherten, separaten Standorten.

Entwicklung und **Test von Wiederherstellungsprotokollen** für schnelle Wiederaufnahme.

Was sind die Anforderungen nach Art. 7 DORA? 6/8

Regelmäßige Sicherheitsüberprüfungen und **Penetrationstests** zur Identifikation von Schwachstellen.

Sicherstellen, dass alle Sicherheitsmaßnahmen und Protokolle **wirksam** sind.

Validierung der Systeme, um den Anforderungen gerecht zu bleiben.

Was sind die Anforderungen nach Art. 7 DORA? 7/8

Sicherstellen, dass die Systeme anpassungsfähig an **neue Anforderungen** sind.

Fähigkeit zur **Skalierung** und Anpassung an wachsende Sicherheitsanforderungen.

Unterstützung der langfristigen operationellen **Resilienz** des Unternehmens.

Was sind die Anforderungen nach Art. 7 DORA? 8/8

Sicherstellen, dass **Drittanbieter-Tools** den DORA-Vorgaben entsprechen.

Sicherheitsvereinbarungen mit Drittanbietern und regelmäßige Überprüfung.

Überwachung der Einhaltung von **Datensicherheitsmaßnahmen** durch **Drittanbieter**.

AGENDA

1 ÜBER UNS

2 ZIEL DES WEBINARS

3 EINFÜHRUNG INFORMATIONSSICHERHEIT

4 EINFÜHRUNG DORA

5 GOVERNANCE & ORGANISATION

6 RISIKOMANAGEMENT

7 IKT SYSTEME, PROTOKOLLE, TOOLS

8 ERKENNUNG

ERKENNUNG

Artikel 10 des DORA beschreibt die **Anforderungen an die Erkennung von IKT-Risiken für Finanzunternehmen**.

Der Fokus liegt auf der Implementierung von Mechanismen, die sicherstellen, dass Unternehmen IT-bezogene Bedrohungen, Anomalien und Vorfälle in Echtzeit erkennen und angemessen darauf reagieren können.

Ziel ist es, die operationelle Resilienz zu stärken und sicherzustellen, dass potenzielle Risiken frühzeitig identifiziert und kontrolliert werden.

ERKENNUNG

Was sind die Anforderungen nach Art. 10 DORA? 1/8

Echtzeit-Überwachung für kritische Systeme und Infrastruktur.

Umfassende **Abdeckung** aller IT-Komponenten.

Erkennung von Bedrohungen und Anomalien in Echtzeit.

Was sind die Anforderungen nach Art. 10 DORA? 2/8

Einsatz von Intrusion Detection und Prevention Systems (IDS, IPS).

Automatisierte **Bedrohungserkennung** und Reaktion.

Frühzeitige **Erkennung** unbefugter Zugriffe und Cyberangriffe.

Was sind die Anforderungen nach Art. 10 DORA? 3/8

Festlegung von **Schwellenwerten** für ungewöhnliche Aktivitäten.

Aktivierung **automatischer Warnungen** bei Schwellenwertüberschreitung.

Direkte Benachrichtigung verantwortlicher Personen.

Was sind die Anforderungen nach Art. 10 DORA? 4/8

Protokollierung aller relevanten IT-Ereignisse und Aktivitäten.

Regelmäßige **Analyse** von Protokolldaten zur Erkennung von Mustern.

Verbesserung der **Sicherheitsstrategie** durch **Ursachenanalyse**.

Was sind die Anforderungen nach Art. 10 DORA?
5/8

Durchführung von **Penetrationstests** und **Sicherheitsaudits**.

Validierung der **Wirksamkeit** und Aktualität der Erkennungssysteme.

Anpassung und **Optimierung** zur Sicherstellung der Resilienz.

Was sind die Anforderungen nach Art. 10 DORA? 6/8

Regelmäßige **Schulungen** zur Erkennung von Sicherheitsbedrohungen.

Förderung des **Sicherheitsbewusstseins** aller Mitarbeiter.

Sicherstellung der **Reaktionsfähigkeit** bei Erkennung von Vorfällen.

Was sind die Anforderungen nach Art. 10 DORA? 7/8

Festlegung eines Verfahrens zur schnellen **Eskalation** von Vorfällen.

Meldung an das Management und an relevante Behörden bei kritischen Vorfällen.

Minimierung des Schadens durch sofortige Reaktion.

Was sind die Anforderungen nach Art. 10 DORA? 8/8

Anpassung der Erkennungssysteme an aktuelle Bedrohungen.

Proaktive Reaktion auf neue Sicherheitsanforderungen.

Sicherstellung der langfristigen operationellen **Resilienz**.

AGENDA

9 IKT Drittleister

10 GESCHÄFTSFORTFÜHRUNG (BCM)

11 VERGLEICH ISO 27001/27002 vs. BAIT

12 SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

IKT DRITTLEISTER

Artikel 28 bis 30 DORA definieren **detaillierte Anforderungen für die Verwaltung von IKT-Drittparteien**.

Diese Anforderungen sollen sicherstellen, dass Unternehmen ihre Abhängigkeit von externen IT-Dienstleistern verantwortungsvoll und risikobewusst steuern, um die operationelle Resilienz zu wahren.

Externe Anbieter, die IT-Dienstleistungen und -Infrastruktur bereitstellen, können erhebliche Risiken bergen, weshalb DORA eine proaktive Überwachung und Steuerung dieser Risiken fordert.

IKT DRITTLEISTER

Was sind die Anforderungen nach Art. 28 - 30 DORA? 1/6

Identifizierung kritischer IKT-Drittanbieter, die für den Geschäftsbetrieb relevant sind.

Bewertung des **Risikoprofils** jedes Anbieters, inkl. Sicherheitsmaßnahmen, Stabilität und Notfallpläne.

Sicherstellen, dass kritische Anbieter **Anforderungen** an die operationelle Resilienz erfüllen.

Was sind die Anforderungen nach Art. 28 - 30 DORA? 2/6

Festlegung von **Verträgen** mit Mindestanforderungen, wie Verfügbarkeit, KPIs und Sicherheitsmaßnahmen.

Recht zur **Überwachung** und **Kontrolle** der Anbieterleistungen durch Audits und Berichte.

Sicherstellung von **Notfallplänen** und **Meldepflichten** bei sicherheitsrelevanten Vorfällen.

Was sind die Anforderungen nach Art. 28 - 30 DORA? 3/6

Einrichtung eines **Systems** zur **Überwachung** der Leistungen kritischer Anbieter.

Regelmäßige **Leistungsüberprüfungen** und **Sicherheitsaudits** zur Identifikation von Schwachstellen.

Möglichkeit zur **Risikominderung** bei **Vertragsverstößen** oder Sicherheitsbedenken.

Was sind die Anforderungen nach Art. 28 - 30 DORA? 4/6

Entwicklung von **Notfallplänen** zur Sicherstellung der Dienstverfügbarkeit bei Ausfall.

Prüfung von **Alternativanbietern** zur Minimierung von Abhängigkeiten.

Proaktive Strategien zur Risikominimierung bei Nutzung externer IKT-Dienstleister.

Was sind die Anforderungen nach Art. 28 - 30 DORA? 5/6

Definition klarer **Meldepflichten** bei sicherheitsrelevanten Vorfällen.

Festlegung von **Eskalationsprozessen** für das Management und relevante Behörden.

Sicherstellen, dass Eskalationsverfahren regelmäßig **überprüft** und **angepasst** werden.

Was sind die Anforderungen nach Art. 28 - 30 DORA? 6/6

Umfassende Dokumentation aller Prozesse zur Verwaltung von Drittanbietern.

Regelmäßige **Aktualisierung** der Dokumentation für Transparenz und Nachweis gegenüber Behörden.

Sicherstellung, dass alle Schritte zur Einhaltung der DORA-Anforderungen nachvollziehbar sind.

AGENDA

9 IKT Drittleister

10 GESCHÄFTSFORTFÜHRUNG (BCM)

11 VERGLEICH ISO 27001/27002 vs. BAIT

12 SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

GESCHÄFTSFORTFÜHRUNG (BCM)

Artikel 11 des DORA beschreibt die **Anforderungen an die Reaktion und Wiederherstellung nach IKT-bezogenen Vorfällen für Finanzunternehmen**, einschließlich Wertpapierunternehmen.

Ziel ist es, sicherzustellen, dass Unternehmen auf IKT-Störungen oder Cyberangriffe schnell und effektiv reagieren können, um den Geschäftsbetrieb aufrechtzuerhalten und Schäden zu minimieren.

Die Wiederherstellung muss nach einem Vorfall so gestaltet sein, dass die operationelle Resilienz und die Sicherheit der IT-Infrastruktur gewährleistet bleiben.

GESCHÄFTSFORTFÜHRUNG (BCM)

Artikel 11 verlangt von Unternehmen, dass sie ihre **Reaktions- und Wiederherstellungspläne** regelmäßig testen und validieren, um sicherzustellen, dass sie in der Praxis effektiv sind.

Die verschiedenen Tests – Simulationen, Penetrationstests, Red-Team-Übungen, Disaster Recovery Tests, Tabletop-Übungen, Kommunikationstests und Notfallplan-Tests – helfen, Schwachstellen zu identifizieren, um im Ernstfall schnell und zuverlässig reagieren zu können.

Durch die regelmäßige Durchführung dieser Tests bleiben die Unternehmen auf dem aktuellen Stand der Bedrohungslage und gewährleisten die Resilienz ihrer IT-Systeme.

AGENDA

9 IKT Drittleister

10 GESCHÄFTSFORTFÜHRUNG (BCM)

11 VERGLEICH ISO 27001/27002 vs. BAIT

12 SCHLÜSSELKOMPONENTEN DORA COMPLIANCE

VERGLEICH ISO 27001/27002 vs. BAIT

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 vs. BAIT

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 vs. BAIT

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.

VERGLEICH ISO 27001/27002 vs. BAIT

Die Anforderungen der BAIT und VAIT gehen im Wesentlichen in den Anforderungen der DORA an den „regulären IKT-Risikomanagementrahmen“ (**Art. 5 – 15 DORA**) und an die „Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos“ **(Art. 28 - 30 DORA)** sowie der einschlägigen **Level 2-Rechtstexte** bzw. deren Entwürfe abgebildet sind auf.

Die BaFin beabsichtigt die Regelung der BAIT aufzuheben.

(BaFin: Aufsichtsmitteilung, Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement, Stand Juni 2024)

AGENDA

9 IKT Drittleister

10 GESCHÄFTSFORTFÜHRUNG (BCM)

11 VERGLEICH ISO 27001/27002 vs. BAIT

12 SCHLÜSSELKOMPONENTEN 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 DORA 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

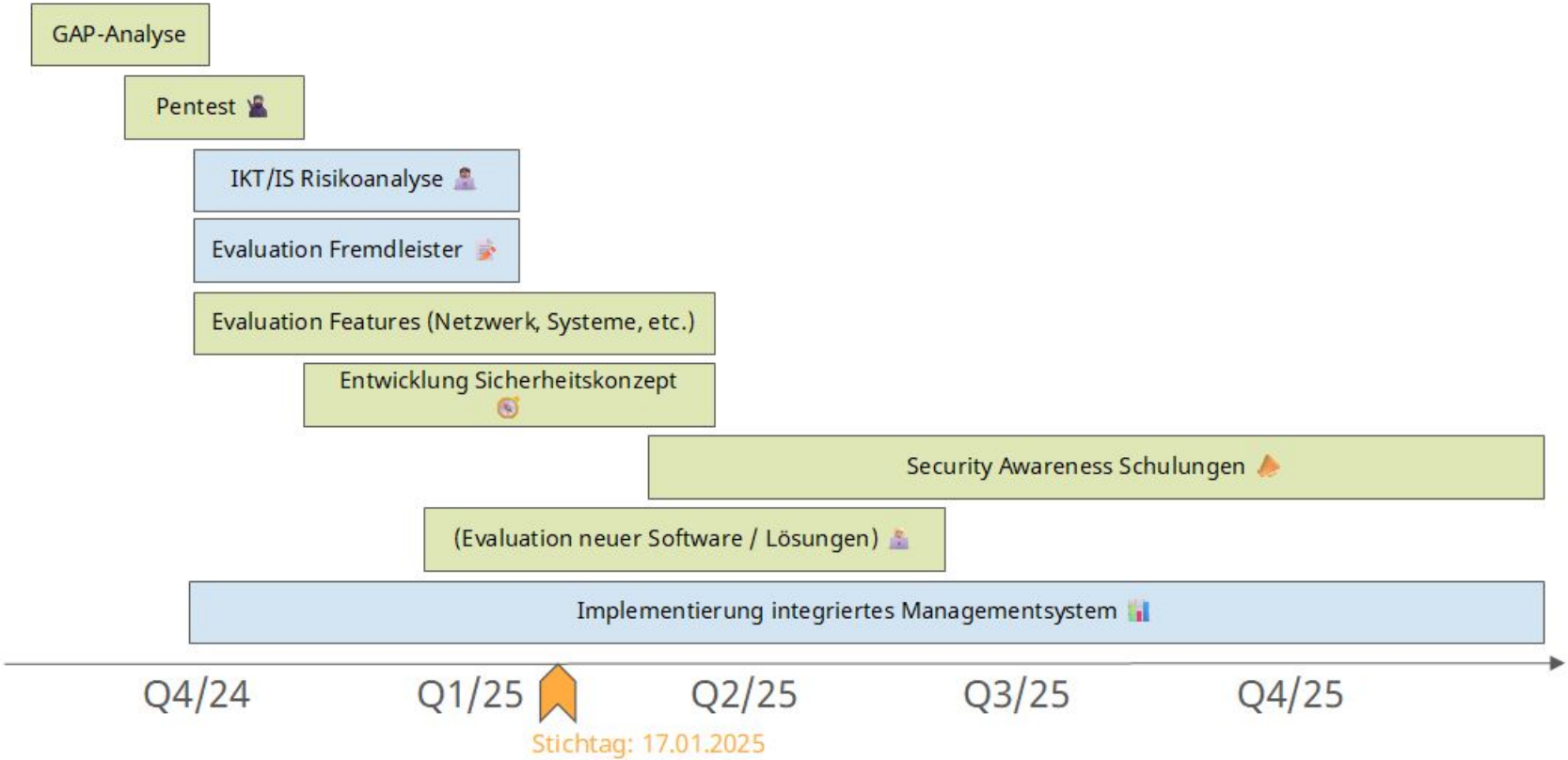
Kontinuierliche Verbesserung und Schulung

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

Schulungsprogramme zur Sensibilisierung der Mitarbeiter für Cyber-Resilienz.

Fortlaufende Bewertung regulatorischer Änderungen und technischer Neuerungen.

ROADMAP UMSETZUNG DORA COMPLIANCE



Vielen Dank!

Holger Berens
Managing Partner

h.berens@concepture.de

Manuel Bohé
CEO Concepture

m.bohe@concepture.de