Webinar

15.November 2024 08:30 – 09:30 Uhr

Last Call for DORA – Fit für 2025

GSK STOCKMANN

Severn make change work

Dr. Markus Escher
Rechtsanwalt, Partner
GSK Stockmann

Christian Moerler
Geschäftsführer
Severn Consultancy

Norman Nehls
Partner
Severn Consultancy

In bewegten Zeiten sind wenige Dinge wirklich sicher … eines ist aber gewiss: die **Anwendung des Digital Operational Resiliance Act (DORA) ab 17. Januar 2025**

+++ Eilmeldung aus Berlin +++
Der Bundespräsident installiert erfahrenen Interimsmanager als Übergangskanzler.
Der Auftrag: „Lass das mal den Papa machen“.

Quelle: LinkedIn, 14.11.2024

GSK STOCKMANN

Severn make change work

Auf dem Weg zur DORA Readiness

Severn make change work

GSK STOCKMANN

Late Starter

- Wichtige Hinweise zur weiteren Priorisierung
- Profitieren von konkreten Anwendungserfahrungen

On the way

- Bewertung des bisherigen Fortschritts
- Fokussierung auf DORA-Anwendung ab Januar 2025

Nearly Finisher

- Optimierung der Prüfungsfestigkeit
- Stabilisierung der DORA-Anwendung ab Januar 2025

Ihre Experten für DORA:

Dr. Markus Escher
Partner
GSK Stockmann

Karl-Scharnagl-Ring 8
80539 München
markus.escher@gsk.de

Schwerpunkte

- Bank-, Zahlungs- und Wertpapier,-aufsichts sowie Investmentrecht
- Regulierung elektronischer Zahlungsdienste nach ZAG, MaRisk, BAIT/ZAIT

Christian Moerler
Geschäftsführer
Severn Consultancy

Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
christian.moerler@severn.de

Schwerpunkte

- IT-Strategie, IT-Management
- Begleitung KWG 44er Prüfungen
- Regulatorik-Experte
- Training und Coaching

Norman Nehls
Partner
Severn Consultancy

Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
norman.nehls@severn.de

Schwerpunkte

- IT-Management, IT-Compliance
- Wertpapiergeschäft
- IT-Prüfung, IT-Regulatorik
- Leiter DORA Competence Center

GSK STOCKMANN

Severn make change work

Agenda

1 Neues aus der Regulatorik

FinMaDiG, RTS Sub-Dienstleistung, ITS-Informationsregister, Streit EU-KOM / ESAs zu Informationsregister, BaFin-Praxis zu IKT-Diensten

2 DORA (non) Compliance per Januar 2025

Priorisierung der DORA Vorgaben, Risikobewertung einer teilweisen Erfüllung, Handlungsempfehlungen

3 DORA Best-Practices für ausgewählte Themen

DOR-Strategie & Governance, IKT-Risikomanagementrahmen, IKT-Vorfallmanagement, IKT-Drittparteienrisiken

4 Q & A

Severn
make change work

GSK
STOCKMANN

DORA Update

Neues aus der Regulatorik

RA Dr. Markus Escher
GSK Stockmann

Legislatives Trauerspiel Deutschland und Ausblicke (1)

1 DORA und das Ampel-Aus – Kommt das Finanzmarktdigitalisierungsgesetz ?

- FinMaDiG noch nicht vom Bundestag verabschiedet
- Droht Diskontinuität für ca. ein Jahr ?
- Ohne FinaMaDiG fehlen wichtige DORA-Regelungen, können aber teilweise durch „KWG-Allgemein“ ersetzt werden

FinMaDiG Entwurf	Regelung ohne FinMaDiG	KWG Allgemein und DORA ?
Förderbanken werden als DORA FU fingiert	DORA-in scope, soweit „KI“, da nicht ausgenommen	Ja, wie bisher Institutsaufsicht
Leasingunternehmen werden tw. als DORA FU fingiert	DORA nicht anwendbar, da nicht „hineinfingiert“	Allg. Institutsaufsicht ohne DORA
BaFin / EZB / Bundesbank zuständige Behörden	**Keine Behördenzuständigkeit für DORA**	Allg. KWG-Zuständigkeit, § 6 KWG
BaFin mit DORA-Spezialbefugnissen, § 47a KWG-E	**Keine DORA-Spezialbefugnisse für BaFin**	Allg. Aufsicht, § 25a und 6 (2), (3) KWG

Legislatives Trauerspiel Deutschland und Ausblicke (2)

1 DORA und das Ampel-Aus – Kommt das Finanzmarktdigitalisierungsgesetz ? (2)

FinMaDiG Entwurf	Regelung ohne FinMaDiG	KWG Allgemein und DORA ?
Mandat Abschlussprüfer zu spezifischen DORA Prüfungen	Kein spezifisches Mandat, aber auch bisher erst ab 2025	Ja, wie bisher Prüfmandat § 29 KWG
Spezifische DORA Owi -Jahresbericht 28 (3) DORA -Anzeige neue DDL Verträge	Keine spezifischen DORA OWi	Allg. KWG OWi
DORA Internet-Pranger, § 60c KWG-E	Kein DORA-Internet Pranger	Allg. KWG-Internet Pranger; 3 60b KWG

- Für DORA würde einiges fehlen, aber mit KWG-Generalbefugnissen könnte dies weitgehend durch die BaFin abgedeckt werden
- Diskontinuität droht bis Abschluss neues Gesetzgebungsverfahren / FinMaDiG „2.0“ mit neuer Bundesregierung

Legislatives Trauerspiel EU und Ausblicke

3 DORA und (rechtliche) RTS / ITS – Was gilt ab 17.01.2025 ?

- ITS Informationsregister von EU Kommission zurückgewiesen
- RTS „Subdienstleister“ im Risiko, ebenfalls zurückgewiesen zu werden

RTS / ITS	Wirkung 17.1.2025	Kommentar
Art. 15 IKT RM	In Kraft, EU-VO 2024/1774	
Art. 28 (9) ITS Informationsregister	Offen nur LEI <> EU ID, ggf. nicht in Kraft	Sonstige Vorgaben sollten berücksichtigt werden, auch wenn noch nicht in Kraft
Art. 28 (10) DDL RM	In Kraft, EU-VO 2024/1773	
Art. 30 (5) RTS Subdienstleister	**Offen**	- SubDL Feststellung nutzbar, „if **effectively underpins**“ ICT-services - Sonstige Anforderungen noch nicht umsetzbar

Tatbestand IKT-Dienstleistung und sonstige Leistungen (1)

1 Können Finanzdienstleistungen IKT-Dienstleistungen sein ?

- Aktueller Klarstellungsversuch der EBF gegenüber ESAs
- Vgl. bereits ErwGrd 7 ITS-E Register of Information; ESA Dry Run FAQ No. 75

2 BaFin - Prüfmaßstab

- BaFin-Prüfmaßstab eng am rechtlichen Tatbestand nach Art. 3 (21) DORA Könnte Auslegung bei gemischttypischen Leistungen (zB Business Process Outsourcing, Call-Centerfunktionen) erleichtern

Tatbestand IKT-Dienstleistung und sonstige Leistungen (2)

BaFin-Prüfmaßstab eng am rechtlichen Tatbestand nach Art. 3 (21) DORA

Liegt eine Dienstleistung vor?	Abgrenzung zu Werk- und Lizenzverträgen BaFin: Berücksichtigung auch von Pflege-/Wartungsleistungen als Dienstleistung Zahlungssysteme ?
Liegt ein digitaler Dienst und/oder ein Datendienst vor?	Abgrenzung zu rein operationellen Diensten (z.B. Interne Revision, Rechtsberatung)
Erfolgt die Bereitstellung der Dienstleistung über ein IKT-System?	Ggf. künftig wichtiges Kriterium zur Abgrenzung gemischt typischer Verträge (zB Callcenter) / Problem Erwgrd 7 ITS RoI, aber FAQ 75 DryRun
Soll die Dienstleistung von internen oder externen Nutzern verwendet werden?	Ggf. für Abgrenzung Projektarbeiten relevant

Tatbestand IKT-Dienstleistung und sonstige Leistungen (3)

BaFin-Prüfmaßstab eng am rechtlichen Tatbestand nach Art. 3 (21) DORA

Ist eine dauerhafte Bereitstellung der Dienstleistung vorgesehen?

→ Abgrenzung zu Projekten, Erstellung, Beratung <> aber exzessive Liste Annex III / ITS RoI; bisher „Annex III: indikativ“

Ist die Dienstleistung zur Ausübung der Geschäftstätigkeit erforderlich?

→ Bemerkenswerte Abgrenzung der BaFin, die sich dem Art. 3 Nr. 21 nicht unmittelbar entnehmen lässt (aber Art. 3 Nr. 1, 28 (1))

Erfolgt die Bereitstellung der Dienstleistung durch einen Drittdienstleister?

→ Art. 3 Nr. 19 bezieht sich auf „Unternehmen“, um als IKT-Drittdienstleister zu gelten.

↓

IKT-Drittdienstleistung im Sinne der DORA

EU Q&A Hilfen

1 Neue DORA joint ESA Q&A

- Über EIOPA ist konsolidierte Datenbank für joint ESA Q&A abrufbar (=EIOPA, ESMA, EBA Q&A zu DORA)
- Bisherige Q&A Antworten kaum hilfreich
- Q&A DORA EIOPA 2749 DORA 005: Betonung „kritischer Funktionen“ nach Art. 2 Nr. 35 BRRD
  https://www.eiopa.europa.eu/about/governance-structure/joint-committee/joint-qas_en#list-of-published-joint-qas

2 Bemerkenswert: ESA information register dry run Q&A

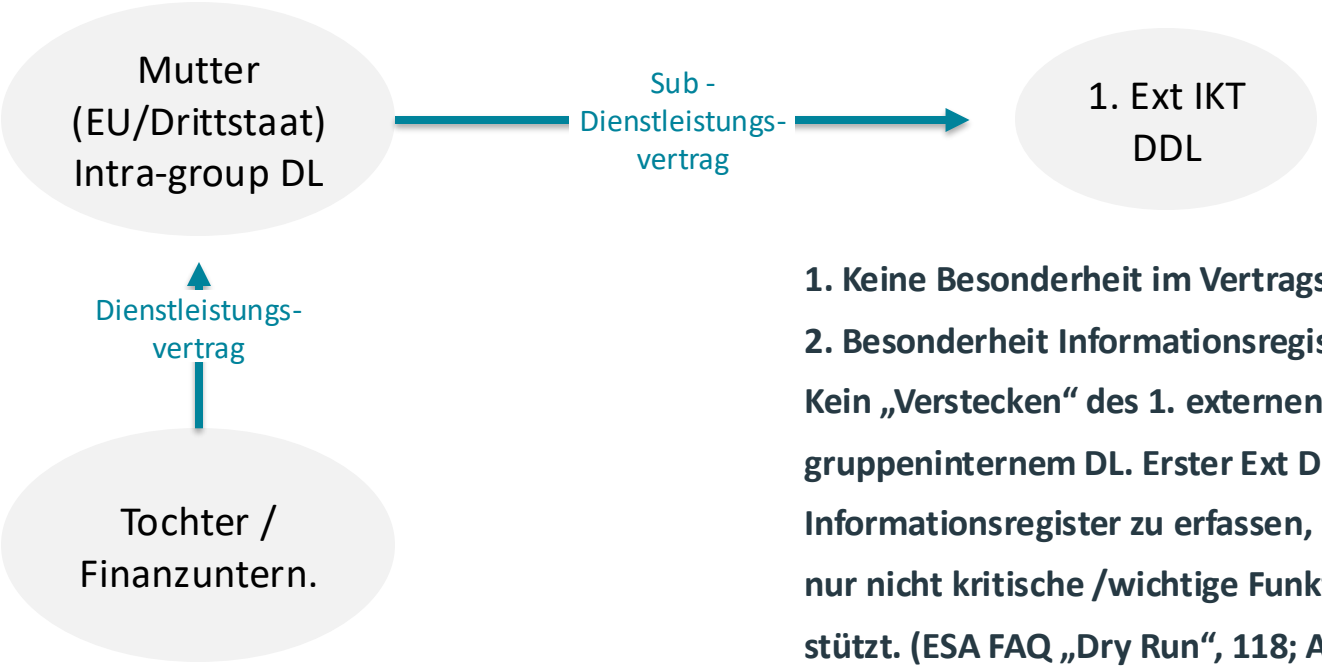
- Im Umfeld der information register dry run im Sommer 2024 wurden „ESA dry run Q&A“ erstellt, die nach BaFin Aussage weiterhin valide und wichtig bleiben
- Update 29.7.24: https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

Q&A Hilfen (2)

2 Bemerkenswert: ESA information register dry run Q&A

Dry Run Q&A	Thema	Ergebnis
118 zu Art. 2 ITS-E	Erfassung von SubDL im Informationsregister bei intra-group Dienstleistern	Bei Erhalt von IKT-DL von einem intra group DL ist durch diesen für Zwecke des Informationsregister „transparent“ durchzuschauen, um den „ersten „direct ICT third-party service provider“ festzustellen, **der im IR für nicht-kritische und kritische Funktionen zu erfassen ist.**

Intra-group / extra group (Sub-) Dienstleister



1. Keine Besonderheit im Vertragsmanagement

2. Besonderheit Informationsregister:

Kein „Verstecken“ des 1. externen DDL hinter gruppeninternem DL. Erster Ext DDL ist stets in Informationsregister zu erfassen, auch wenn er nur nicht kritische /wichtige Funktionen unter-stützt. (ESA FAQ „Dry Run“, 118; Art. 2 (1) a und ErwG 5 ITS RoI)

Vertragsanpassungen IKT-Drittdienstleistungen und Implementierungsplan

- neue verpflichtende Vertragsinhalte für alle IKT-Drittdienstleistungen, umfassende Geltung für Vertragsanforderungen auch in der Gruppe
- neue Anforderungen zur Form der Verträge über DDL (Art. 30 (1) DORA)
- **Implementierungszeitplan** und Vorgaben zur Vertragsanpassung beachten (Art. 3 (1) RTS TPP Pol), bzw. „planen“, falls Vertragsanpassung noch nicht vollständig
- Ex-ante Risikobewertung und Due Diligence auch für bereits aktive Verträge nachzuholen, hier ggf. Vorteile für gruppeninterne Dienstleister

Severn
make change work

GSK
STOCKMANN

DORA Update

DORA (non) Compliance

Christian Moerler | Geschäftsführer
Severn Consultancy GmbH

Was bedeutet eigentlich „DORA-ready“?

Wesentliche Gestaltungselemente der DORA-Compliance

Resilienz Strategie

„Kritische“ oder wichtige“ Funktionen (CIF)

„Risikoappetit“ und „Risikotoleranzschwelle“

Anweisungswesen (1. und 2. Verteidigungslinie)

DORA-Funktionen (IKT-Risiko Mgmt & Drittparteien)

Verfahren & Systeme (z.B. InfoSec, Incident, Testing, etc)

Drittparteien-Management (Verträge, Überwachung)

Internes Kontrollsystem (auf Verfahren, Prozesse, Systeme)

IKT-Risikoprozess (Identifikation, Risikobewertung, Erkenntnistransfer auf Verfahren und Systeme!)

Self-Assessment Rahmen (zur jährlichen oder ad-hoc Standortbestimmung)

Prüfstufen der Compliance-Bewertung

Design Effektivität

- Erscheint die Lösung grundsätzlich „angemessen“ und „proportional“ ?

Operationale Wirksamkeit

- Erbringt die Lösung in der Praxis nachhaltig die beabsichtigten „Resultate“ ?

Was bedeutet eigentlich „DORA-ready“?

Severn make change work

GSK STOCKMANN

Wesentliche Gestaltungselemente der DORA-Compliance

Risikoorientierung in der Implementierung per 17. Januar 2025

Resilienz Strategie	Unabdingbar, „Arbeitsprobe der Geschäftsleitung“
„Kritische“ oder wichtige“ Funktionen (CIF) / „Risikoappetit“ und „Risikotoleranzschwelle“	Unabdingbar, elementare Rahmensetzungen (Proportionalität)
Anweisungswesen (1. und 2. Verteidigungslinie)	Richtlinien (2. VL) zuerst, Dokumente der 1. VL nachrangig
DORA-Funktionen (IKT-Risiko Mgmt & Drittparteien)	Unabdingbar, da strukturelle Verantwortung der Geschäftsleitung
Verfahren & Systeme (z.B. InfoSec, Incident, Testing, etc)	Vollständigkeit der Basisverfahren (inkl. SIEM!), IKT-Assets zu CIF zuordnen, Incident-Klassifizierung und Meldeprozess unabdingbar
Drittparteien-Management (Verträge, Überwachung)	Basisverfahren Informationsregister (mit Upload), Verträge zu CIF zuordnen, Master-Vertragsklauseln, Verhandlungen gestartet
Internes Kontrollsystem (auf Verfahren, Prozesse, Systeme)	Fokus auf Definition von Kontrollhandlungen auf Ebene der 2. VL, Kontrollen auf Ebene der 1. VL nachrangig
IKT-Risikoprozess (Identifikation, Risikobewertung, Erkenntnistransfer auf Verfahren und Systeme!)	Etablierung des neuen! „holistischen“ IKT-Risiko-Assessment Verfahrens unabdingbar > „Airbag“ gegen Perfektionszwang
Self-Assessment Rahmen (zur jährlichen oder ad-hoc Standortbestimmung)	Prozess (inkl. Reporting) muss etabliert sein > wirkt auf Verantwortung der Geschäftsleitung

Handlungsempfehlungen für die „heiße Phase“

- ✔ **Inkraftsetzungsplan** für „genehmigungspflichtige“ Artefakte durch die Geschäftsleitung (z.B. DOR-Strategie, CIF, Richtlinien, Risikotoleranz, etc.)
  → Letzte Sitzung der Geschäftsleitungen ist oft spätestens Mitte Dezember.

- ✔ Frühzeitige Abstimmung mit **Jahresabschlussprüfer**, welche Aspekte der „DORA-Readiness“ er im Jahresabschlussprüfungsbericht 2024 erwähnen und auch vorher prüfen möchte (inkl. Evidenzen)

  → Typisches Prüfthema: DORA Gap Analyse und davon abgeleitete Planung der Implementierung“
  „Wie stellt das Institut vollständige Berücksichtigung/Abdeckung aller Anforderungen sicher?“

- ✔ Durchführung einer **Analyse**, welche der Anforderungen auf welchem **Reifegrad** umgesetzt sind.

- ✔ **Risikobewertung** der Abweichung und Ableitung eines operativen **Umsetzungsplans.** Verabschiedung des Plans auf Ebene der Geschäftsleitung (Temporäre Risikoakzeptanz).

- ✔ Information über Analyse und Umsetzungsplan an **Aufsichtsrat.**

Severn
make change work

GSK
STOCKMANN

DORA Update

DORA Best-Practices

Norman Nehls | Partner
Severn Consultancy GmbH

Strategie und Goverance für eine resiliente Organisation

Inhalte einer angemessenen DOR-Strategie (…in der dargelegt wird, wie der Rahmen umgesetzt wird)

- **Präambel:**
  - Commitment und Verantwortung der Geschäftsleitung
- **Grundlagen für das IKT-Risikomanagement:**
  - Anforderungen aus der Geschäftsstrategie (Strategische Ausrichtung und IT-Nutzungsgrad)
  - Geschäftsprozess-Modell mit Kennzeichnung wichtiger oder kritischer Geschäftsfunktionen
  - Erläuterung des Schutzbedarfskonzepts
  - Funktionsweise und Instrumente der Informationsklassifizierung und der Strukturanalyse
  - Funktionsweise und Instrumente des IKT-Assetmanagement
  - Vorhandene IKT-Drittanbieter und ermittelter Vernetzungsgrad
  - Verfahren und Prozesse zur Erkennung und Bewertung von Bedrohungen
- **Elemente des IKT-Risikomanagementrahmens:**
  - Überblicksdiagramm mit Vernetzung der Elemente
  - Beschreibung der einzelnen Komponenten des IKT-Risikomanagementrahmens (Elemente und Vernetzung sowie „externe“ Schnittstellen)
  - Beschreibung der Prozesse zur Ermittlung der Risikotoleranz auf Basis des IKT-Risikoprofils und der Verbindung zur Risikostrategie
- **Governance und Policies:**
  - Darstellung der Resilienz-bezogenen Governance-Strukturen (Rollen, Funktionen, Gremien)
  - Resilienz-bezogenen Dokumentenpyramide (schriftlich fixierte Ordnung)
  - Einbindungskonzept des Leitungsorgans in das IKT-Risikomanagement
- **Informationssicherheit:**
  - Ziele der Informationssicherheit
  - Beschreibung von Leistungsindikatoren zur Messung der Wirksamkeit der Informationssicherheit sowie Risikokennzahlen
  - Beschreibung der operativen Instrumente der Informationssicherheit (Maßnahmen zur Gewährleistung der Schutzziele/Sollmaßnahmen)
- **IKT-Referenzarchitektur:**
  - Ist- und Soll IKT-Architektur
  - Transition und Zwischenschritte mit Reifegrad Bewertung der IKT-Sicherheit
- **Ressourcen-Management:**
  - Beschreibung der Verfahren und Prozesse zur Ermittlung des quantitativen und qualitativen Ressourcenbedarfs für IKT-Sicherheit
  - Beschreibung der Überleitung des Ressourcenbedarfs in die Budgetplanung, -entscheidung und Mittelallokation

Strategie und Goverance für eine resiliente Organisation

Severn make change work

GSK STOCKMANN

Inhalte einer angemessenen DOR-Strategie (…in der dargelegt wird, wie der Rahmen umgesetzt wird)

- **Testen der digitalen operationalen Resilienz:**
  - Beschreibung des Testprogramms mit seinen Komponenten, Verfahren und Prozessen, einschließlich Penetrationstests
  - Steuerung der Umsetzung von Maßnahmen aus den Ergebnissen von Tests
- **IKT-Risikomanagement:**
  - Beschreibung der Risikoanalyseverfahren und Prozesse
- **IKT-Vorfallsmanagement:**
  - Beschreibung der Verfahren und Prozesse für das IKT-Vorfallsmanagement, einschließlich die Reaktionspläne
  - Beschreibung und Ermittlung der Auswirkungstoleranz für IKT-Störungen
  - Verfahren der Kommunikation und Koordination bei IKT-Vorfällen (Verweis auf Kommunikationsstrategie)
  - Meldeverfahren für IKT-Vorfälle (intern, extern)
- **Business Continuity und Disaster Recovery:**
  - Beschreibung der Instrumente, die sicherstellen, dass kritische Geschäftsprozesse im Falle eines Cyber-Angriffs oder einer anderen Störung aufrechterhalten werden können.
  - Beschreibung der Verfahren und Prozesse des ITSCM sowie der Wiederanlaufszenarien
- **Assurance der IKT-Sicherheit:**
  - Beschreibung der Verfahren und Instrumente zur Aufrechterhaltung eines hohen Niveaus an IKT-Sicherheit
  - Konzept der drei Verteidigungslinien
  - IKS-Kontrollsystem für die IKT-Sicherheit
  - Auditierung
- **IKT-Drittanbieter-Management:**
  - Bewertung des Vernetzungsgrades und der Drittanbieter-bezogenen IKT-Risikoposition
  - Beschreibung der Verfahren und Prozesse für das IKT-Drittanbieter-Management
- **Aktueller Stand der IKT-Resilienz:**
  - Dashboard mit Auflistung aller IKT-Resilienz-bezogenen Leistungsindikatoren
  - Abgleich mit Zielgrössen
  - Strategische Maßnahmenableitung und Überführung in die operative Umsetzungsplanung
- **Fortbildung und Bewusstseinsbildung:**
  - Beschreibung der Verfahren für Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter
  - Beschreibung der Verfahren zur Befähigung des Leitungsorgans zur Beurteilung von IKT-Risiken
- **Regelmäßige Überprüfung und Anpassung:**
  - Beschreibung der Prozesse und Verantwortlichkeiten für die laufende Überprüfung und Anpassung der digitalen Resilienz Strategie, um sicherzustellen, dass sie aktuell bleibt und sich an die sich ständig ändernde Cyber-Bedrohungslandschaft anpasst.

Strategie und Goverance für eine resiliente Organisation

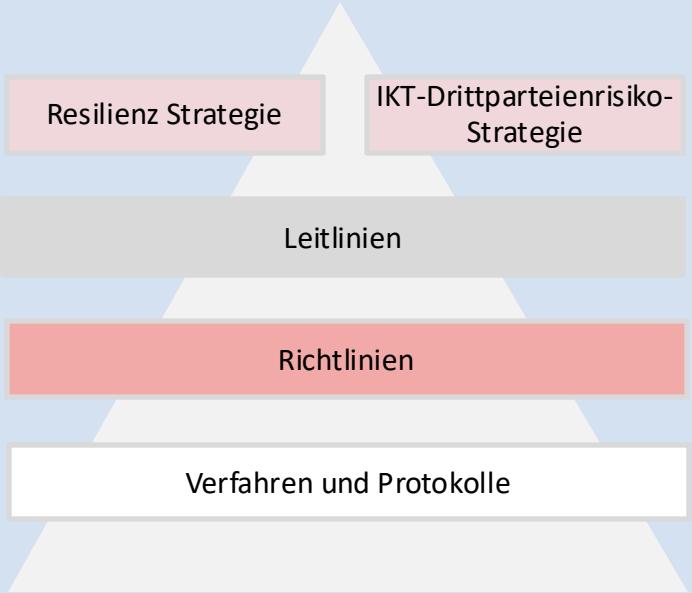
Exemplarisch

Einbindungskonzept der Geschäftsleitung / Makro- und Mikropflichten gem. Artikel 5 (2)

Geschäftsleitung	Design	Approve	Control	Review	Responsibility	Involved board members	Instruments applied	SFO /Documentation references	Primary supplying unit	Supplied documents (evidence)	Created documents (evidence)
DORA Artikel											
Governance											
Definition of legal entity specific tolerance level for ICT-Risk (derived from corporate risk appetite)	Be involved in conceptual methodological discussions, Act as steering committee member and influence scope by decision making, challenge proposals for tolerance level, ensure consistency between reality and historic Oprisk data and new proposal, review and challenge decision request	Unconditional approval of decision request in full board meeting, ensure unanimous decision. Obtain approval from supervisory board.	Quarterly review of ICT-Risk data (quantitative view) to validate ongoing adequacy of ICT Risk tolerance level as part of overall Op Risk capital allocation. In case of deviations, trigger review activity	Ad-hoc (event driven) or at least annual review of actual losses due to ICT Risk events versus planned ICT-Risk tolerance level versus the defined impact tolerance for ICT disruptions. Upon deviations, trigger update of relevant parameters (Risk appetite, risk tolerance level, impact tolerance)	CRO for adequacy and integrity of methodology incl. implementation / CIO for proposal of ICT Risk tolerance level and definition of impact tolerance, implementation of adequate downstream ICT-measures to stay within limits, monitoring of events and losses, notification about deviations / Full board for decision on methodology and concrete parameters (also updates, corrections)	CRO, CIO, Full board	Design: Project meetings (incl. Minutes), Fachkonzept, Steering Committee Meetings / Approve: Steering Committee Meetings, Decision request, full board meeting, SupBo meeting / Control: Quarterly ICT-risk report, discussion in board meeting / Review: Annual ICT-Risk report, overall Op Risk report, ad-hoc Prüfauftrag when needed	Risk strategy, DOR-strategy, ICT-Risk policy, ICT-Risk tolerance level procedure, Geschäftsverteilungsplan, Gremienplanung, etc.	ICT-Risk Managemem t function, corporate risk function (OpRisk)	Design: Fachkonzept, Risk data (actual) / Approval: Decision request, Risk data for risk appetite, Op Risk capital allocation, ICT losses / Control: Quarterly ICT-Risk report / Review: Annual ICT-Risk report	Design: Minutes of relevant project meetings and steering committee decisions / Approval: Accepted and agreed decision request / Control: Minutes of board meeting with results of discussion of Quarterly ICT-Risk report / Review: Minutes of board meeting with results of discussion of Annual ICT-Risk report
.....											
ICT-Risk Management Framework											
...											

DORA fordert einen umfassenden und gut dokumentierten IKT-Risikomanagementrahmen um ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten

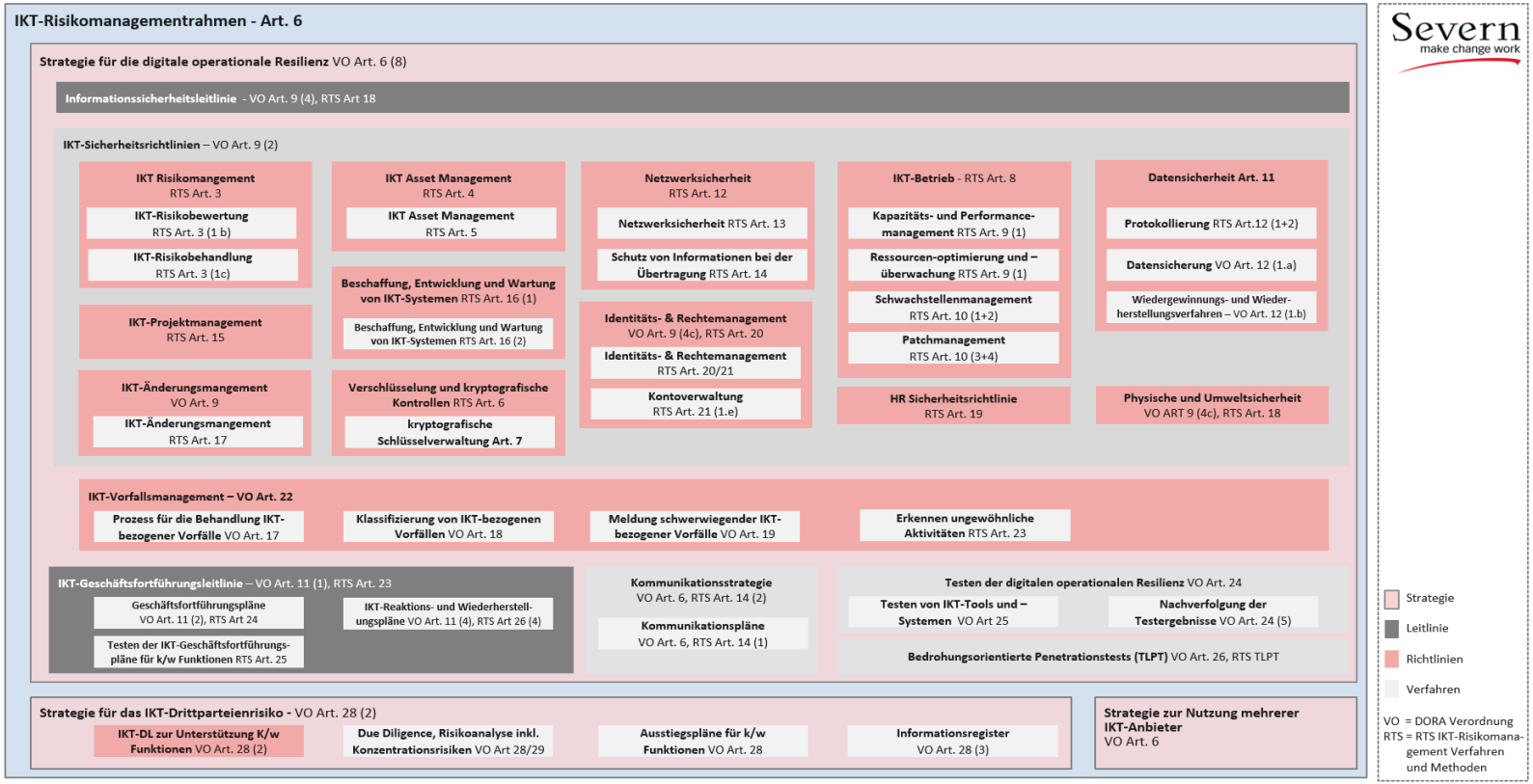
IKT-Risikomanagementrahmen – DORA VO Art. 6



Für eine „DORA-Readiness“ werden folgende Punkte erfüllt:

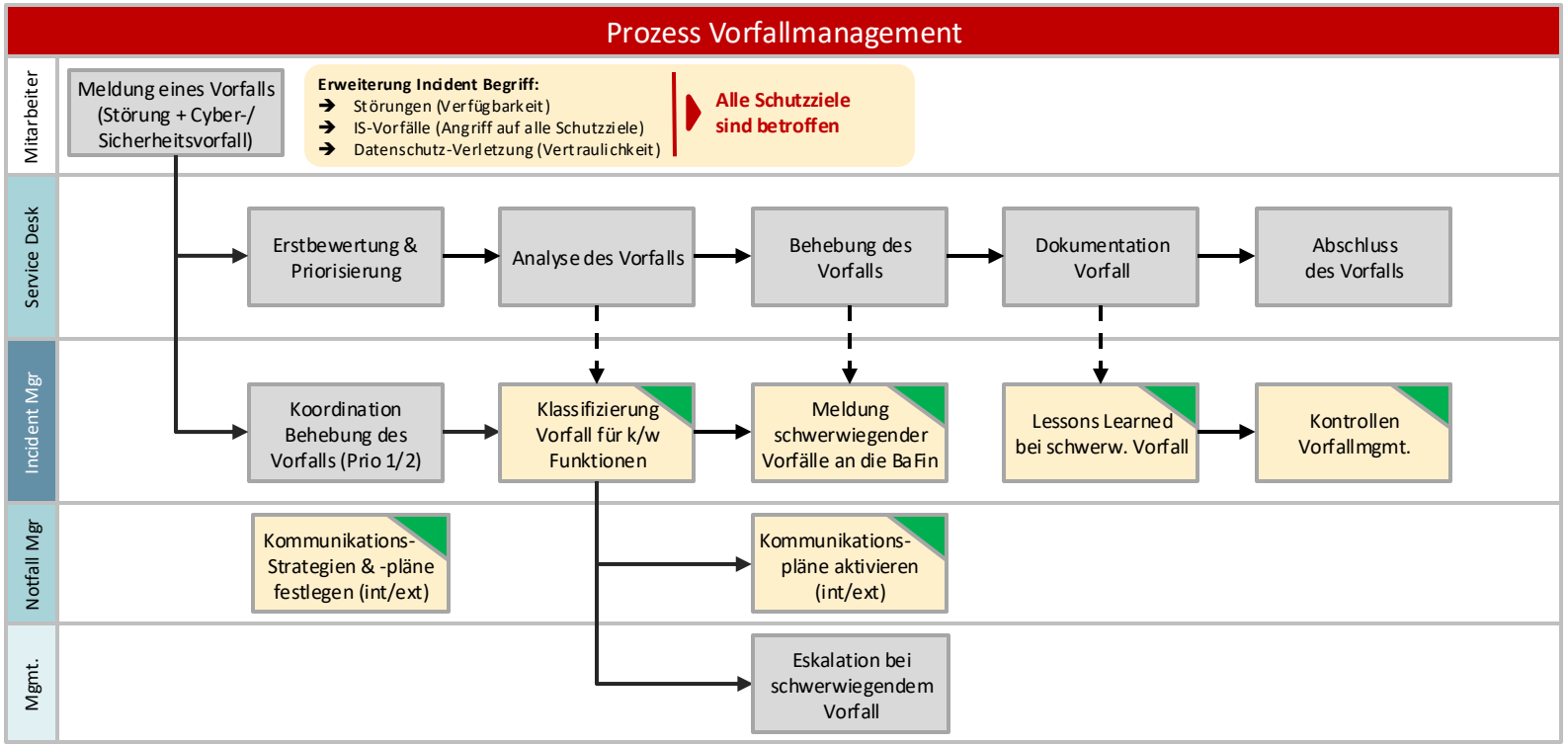
- ✔ **Ein institutsspezifischen IKT-Risikomanagementrahmen** ist festgelegt
  Hinweis: Mapping von sfO-Dokumenten teilweise möglich
- ✔ Ein **IKT-Risikomanagementprozess** ist etabliert, um Bedrohungen und IKT-Risiken aus nicht vollständig umgesetzten Anforderungen zu bewerten
- ✔ Ein **Umsetzungsplan** zur vollständigen Erfüllung der Anforderungen u.a. an Schutz und Prävention ist definiert
- ✔ Ein Prozess ist definiert, um den **IKT-Risiko-managementrahmen jährlich zu überprüfen und kontinuierlich zu verbessern**
  Hinweis: Berichtspflicht an die Aufsicht auf Verlangen (DORA RTS IKT-RM Art. 27)

DORA fordert einen umfassenden und gut dokumentierten IKT-Risikomanagementrahmen um ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten



!

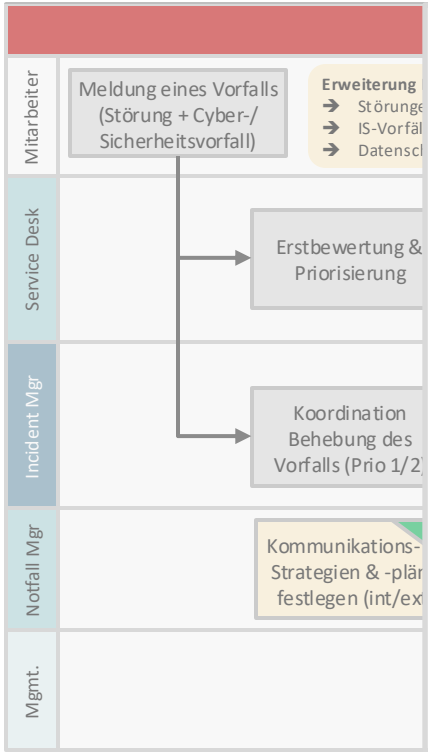
IKT-Vorfälle stehen ab Januar 2025 im besonderen Fokus der Finanzaufsicht



!

Neu mit DORA

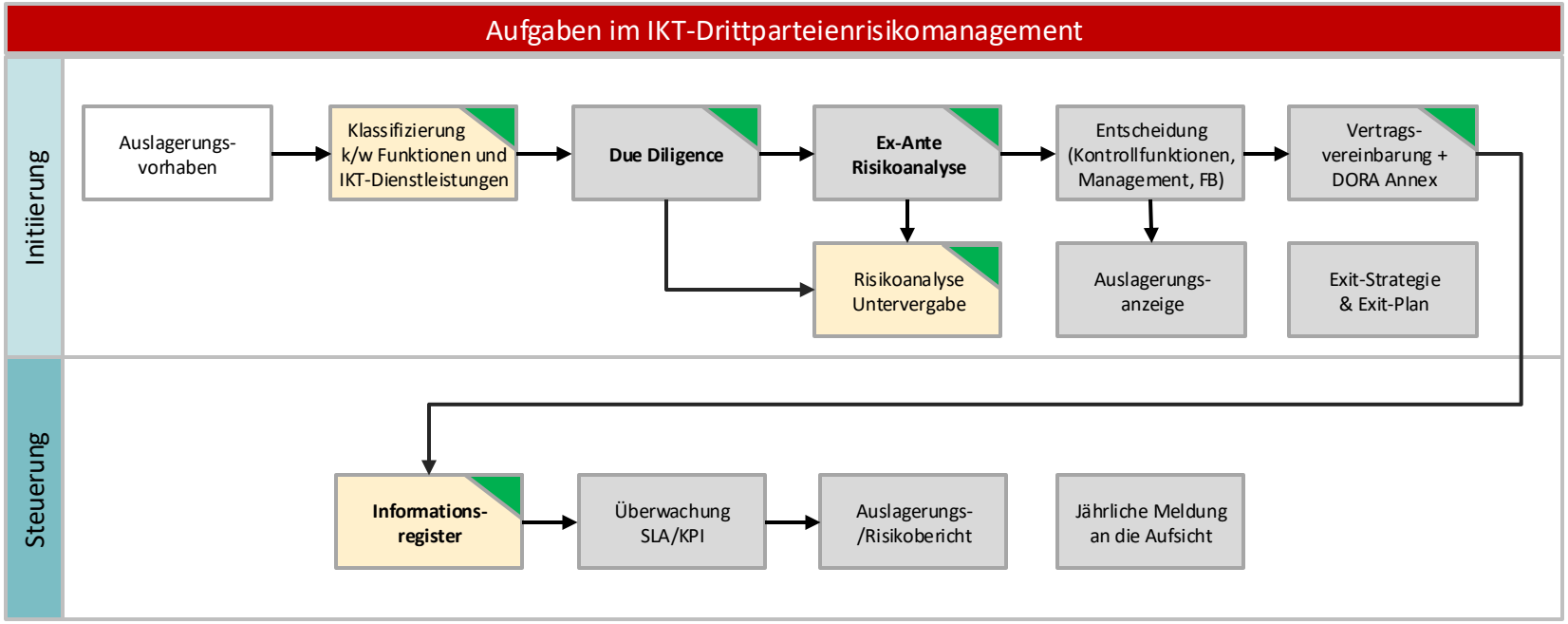
IKT-Vorfälle stehen ab Januar 2025 im besonderen Fokus der Finanzaufsicht



Für eine „DORA-Readiness“ werden folgende Punkte erfüllt:

- ✔ **kritische/wichtige Funktionen** und die unterstützenden Assets kennen
- ✔ Vorfälle jeder Art (Störungen, IS-Vorfall …) lassen sich gemäß der **DORA-Kriterien klassifizieren** (Vorüberlegung: Bewertbarkeit der Kriterien)
- ✔ **Meldepflichten** werden zeitgerecht und qualitativ vollständig erfüllt
  Erstmeldung (zeitkritisch); Zwischenberichte (ggf. mehrfach); Abschlussbericht (aufwändig) Hinweis: Vereinfachung der Meldefristen beachten
- ✔ Registrierung im **MVP-Portal** der BaFin wurde vorgenommen
- ✔ Eine **Verprobung** (Dry-Run) zu Rollen und Aufgaben im IKT-Vorfallmanagement wurde durchgeführt und Prozesse ggf. adjustiert
  Hinweis: Zuständigkeiten klären und Ansprechpartnerlisten bereitstellen
- ✔ **Kommunikationsstrategie und -pläne (je Szenario) sind definiert und abgestimmt** und Rollen für die interne und externe Kommunikation sind festgelegt

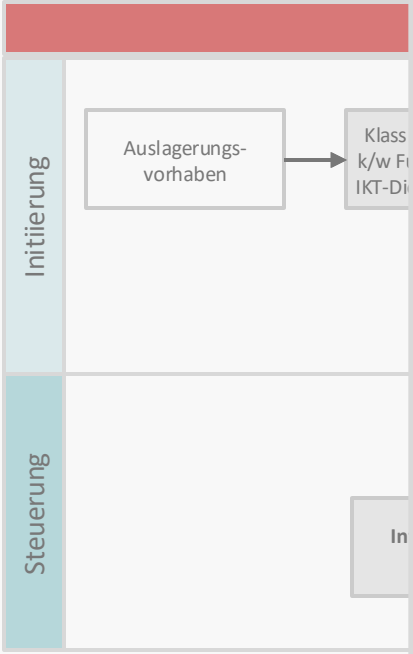
Erweiterte Pflichten an die Steuerung und Kontrolle von IKT-Drittparteienrisiken sind ab Januar einzuhalten



!

Neu bzw. erweitert mit DORA

Erweiterte Pflichten an die Steuerung und Kontrolle von IKT-Drittparteienrisiken sind ab Januar einzuhalten



Für eine „DORA-Readiness“ werden folgende Punkte erfüllt:

- ✔ **kritische/wichtige Funktionen** und die unterstützenden IKT-Drittdienstleister kennen
- ✔ **Strategie zum Drittparteienrisiko** und Anweisungen/Prozesse sind intern freigegeben
- ✔ **Due-Diligence** und **Risikoanalyse** sind um die DORA-Vorgaben erweitert
  Hinweis: Für Bestandsverträge erfolgt die Aktualisierung im Regelturnus
- ✔ Alle Weiterverlagerungen (Untervergabe) für IKT-Dienstleister, die kritische/wichtige Funktionen unterstützen sind erhoben
  Hinweis: entscheidend für die Aufnahme sind materielle Weiterverlagerungen
- ✔ DORA-konforme **Vertrags-Annexe** (für kritische/wichtige und einfache Funktionen) sind erstellt und einen **risikobasierten Abarbeitungsplan** für die Vertragsanpassungen mit IKT-Drittdienstleistern ist definiert
- ✔ Die Registrierung im **MVP-Portal** der BaFin wurde vorgenommen (Frist: 18.10.2024)
- ✔ Eine initiale Befüllung des **Informationsregisters** ist erfolgt und ein **Pflegeprozess** für die laufende Aktualisierung der Vertragsdaten (inklusive Kontrollen) ist definiert

Severn
make change work

GSK
STOCKMANN

DORA-Workshop

Q&A

Ihre Referenten / Kontakt

Dr. Markus Escher
Partner
GSK Stockmann

Karl-Scharnagl-Ring 8
80539 München
markus.escher@gsk.de

Schwerpunkte

- Bank-, Zahlungs- und Wertpapier,-aufsichts sowie Investmentrecht
- Regulierung elektronischer Zahlungsdienste nach ZAG, MaRisk, BAIT/ZAIT

Christian Moerler
Geschäftsführer
Severn Consultancy

Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
christian.moerler@severn.de

Schwerpunkte

- IT-Strategie, IT-Management
- Begleitung KWG 44er Prüfungen
- Regulatorik-Experte
- Training und Coaching

Norman Nehls
Partner
Severn Consultancy

Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
norman.nehls@severn.de

Schwerpunkte

- IT-Management, IT-Compliance
- Wertpapiergeschäft
- IT-Prüfung, IT-Regulatorik
- Leiter DORA Competence Center

Severn
make change work

GSK
STOCKMANN