FORUM Gesellschaft für Informations-sicherheit mbH, Dresden

Dresden, 13. Juni 2024

Henning Riediger

Aktuelle Anforderungen der Bankenaufsicht

- *Fokusthemen*
- *Fallstudien*

DISCLAIMER

- Dieser Vortrag spiegelt ausschließlich die persönliche Meinung des Referenten und nicht notwendigerweise die der Deutschen Bundesbank wieder.

Angaben zur Person

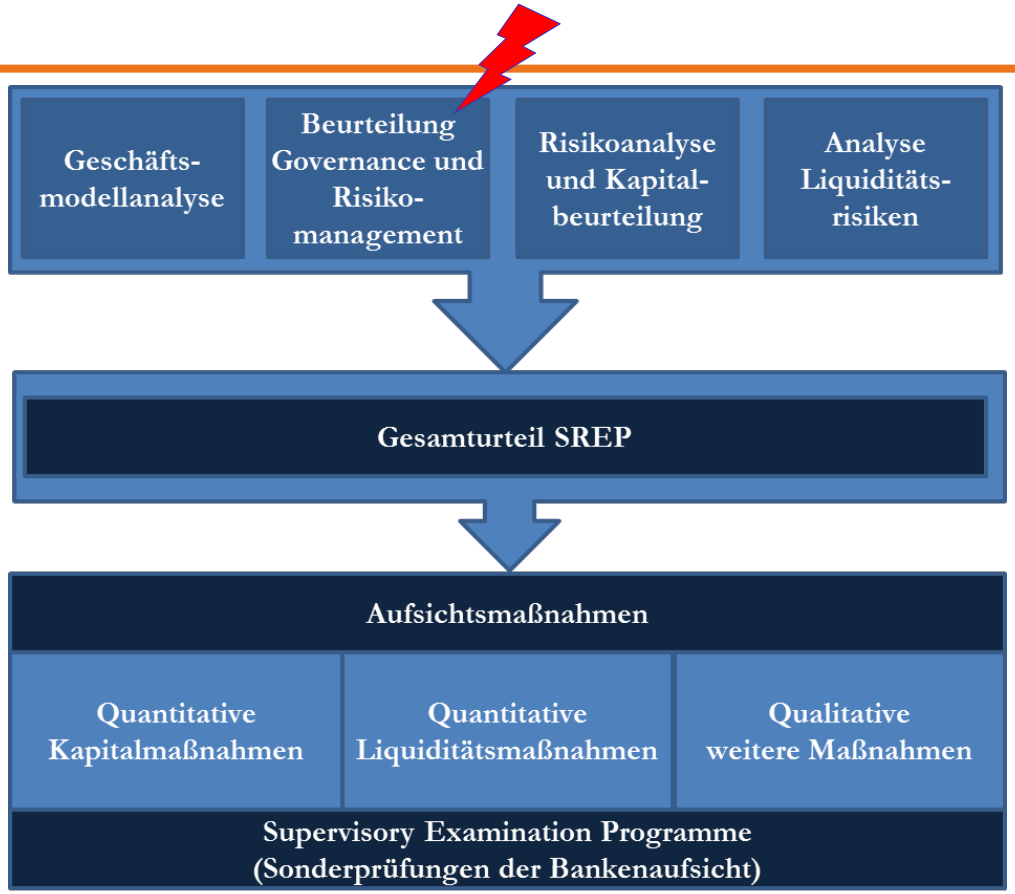
- **Henning Riediger**
  Diplom-Betriebswirt (FH)
- 2001 Deutsche Bundesbank,
  Studium an der Hochschule Hachenburg
- 2004 **Deutsche Bundesbank**
  2014 **Prüfungsleiter** im Referat
  Bankgeschäftliche Prüfungen, Hannover
- **Schwerpunkte**
  Gesamtbanksteuerung/Risiko-Controlling
  Internes Kontrollsystem
  Informationstechnologie
  Outsourcing

AGENDA

- Fokusthemen
  - IKS
  - Compliance
  - DORA / Auslagerungen
- Fallstudien
- Teilnehmer-Themen

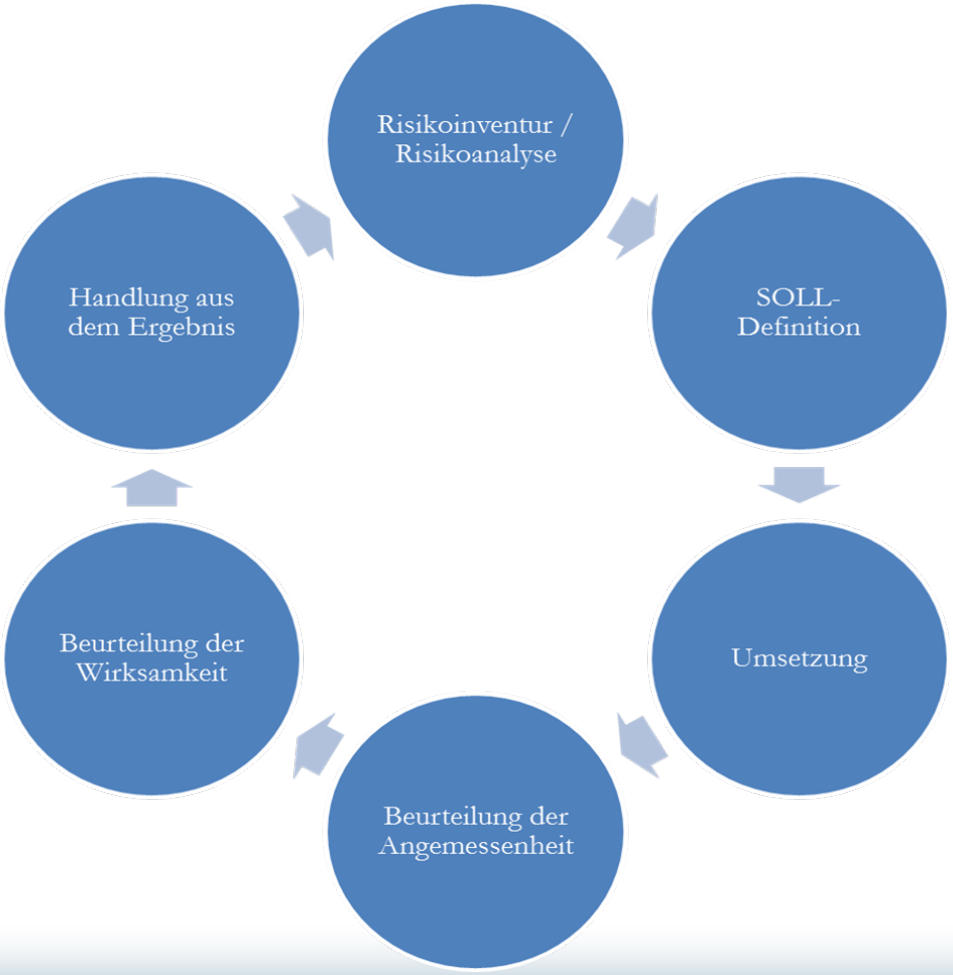
AKTUELLE AUFSICHTS-SCHWERPUNKTE

IKS – im Fokus!



- Bewertung jeweils einer Skala von 1 bis 4
- Risk Control versus Risk Level
- EK-Zuschlagsberechnung erfolgt nach einem Matrix-Ansatz
- Expertenschätzungen im Bereich Risk Control auf Basis zur Verfügung stehender Informationen

IKS – im Fokus!



Aufsichtliche Prüfgebiete

- Kontrollzweck
- Vollständigkeit versus Risiko
- **Funktionsfähigkeit**

Handlungserfordernisse

- Frequenz festlegen
- Zuständigkeiten definieren
- Berichtswege festlegen
- Toleranzen definieren
- Ergebnisse festhalten

IKS – im Fokus!

Die Geschäftsprozesse und Verfahrensweisen sind …	Wirksam	Grundsätzlich wirksam	Nicht wirksam
angemessen			
Grundsätzlich angemessen			
Nicht angemessen			

Angemessenheit = saubere Umsetzung in Art, Umfang und Vollständigkeit sowie der entsprechenden Dokumentation (sfO, policy usw.)

Wirksamkeit = Nachhaltige Einhaltung und mögliche Fehleranfälligkeit im Prozess bzw. im gelebten Tagesprozess

Compliance - im Fokus!

- Soll-Ist-Abgleich muss auch bei Tätigkeiten der Compliance-Funktion möglich sein (z. B. Vollständigkeit, Termintreue, inhaltliche Befassung usw.); Schwerpunkt hierbei auf der **Pflege des Compliance-Universums**
- „objektiv überprüfbar“ bedeutet: Nachvollziehbarkeit und Plausibilität
- **Minimalprinzip bei techn. Rechtevergabe** (insbesondere Schreibrechte)
- Zuordnung der Daten von Compliance einer entsprechend **hohen Schutzbedarfsklasse**
- Mögliche Prüfungshandlungen der Aufsicht
  - Überprüfung der Stellenbeschreibung der Compliance-Funktion
  - Einsichtnahme in die Wesentlichkeitsanalyse
  - Ausnutzung von eingeräumten Rechten (z. B. Veto-Rechte, Kontroll- und Prüfrechte)
  - Auswertungsanalyse der letzten Risikoinventur
  - Beurteilung der Initiativen der Compliance-Funktion, insbesondere Schwerpunktsetzung
  - Plausibilisierung des Risikouniversums, Abdeckung der Rechtsbereiche
  - Einbindung in Projektarbeiten
  - Durchgeführte Stichprobenprüfungen für bestimmte Rechtsbereiche; Analyse von weiteren Kontroll- und Überwachungshandlungen anhand von aussagekräftigen Arbeitsunterlagen
  - Scanning von Lücken in den Rechtsbereichen im Institut bzw. Themen ohne Zuordnung zu Kontrolleinheit
  - Auswertung der regulären Berichte und Ad-Hoc-Informationen
  - Auswertung von Abstimmungen mit anderen Kontrollbereichen bzw. Austausch mit Interner Revision

Compliance - im Fokus!

- **Kontrollhandlungen durch die Compliance-Funktion**

Compliance-Prüfungen		
Level A Prüfungen	Level B Prüfungen	Level C Prüfungen
- Plausibilitätsprüfungen -	**- Umsetzungsprüfungen -**	**- Einhaltungsprüfungen -**
Erfolgen im Rahmen der jeweiligen Normeneinwertung bzw. deren Neueinwertung durch Compliance (z. B. Relevanz- und Wesentlichkeitsprüfungen)	Erfolgen im Rahmen der Normen- bzw. Themenumsetzung und dessen Reporting für Normen von besonderer Bedeutung (z. B. Regulatorischer Zeitstrahl)	Erfolgen im Rahmen dezidierter Compliance-Prüfungen zur permanenten Normeneinhaltung (z. B. Überwachungsvermerk)

Prüfungsumfang

Prüfungsintensität

Compliance - im Fokus!

- **Auslagerung der Compliance-Aktivitäten**
  - Voll-Auslagerung aufgrund der besonderen Funktion nach MaRisk nur bei kleinen Instituten unter Umständen möglich
  - Auslagerung Compliance (auch von Teilen der besonderen Funktion) ist immer als wesentlich einzustufen
  - Immer einen Abgleich der intern vorgegebenen Aktivitäten mit den Leistungsschreinen vornehmen
  - Dient der Erkennung ob Teil- oder eine faktische Vollauslagerung vorliegt
  - Setzt klare Vorgaben für die Auslagerungsüberwachung im Bereich der Compliance-Funktion
  - Einrichtung eines Compliance-Beauftragten (analog dem Revisionsbeauftragten), welcher die Leistungserbringung und Sicherstellung der Compliance-Funktion des Instituts überwacht
  - Bei Vorliegen einer Institutsgruppe ist eine Auslagerung nur für nicht wesentliche Institute möglich

DORA

Im Zentrum der Betrachtung steht nicht der Prozess, sondern die eingesetzten **Technologien und Daten.**

- DORA soll die digitale operationale Resilienz des gesamten europäischen Finanzsektors in diesen sechs wesentlichen Bereichen stärken:
  - IKT-Risikomanagement (Kapitel II, Artikel 5 bis 16)
  - Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III, Artikel 17 bis 23)
  - Testen der digitalen operationellen Resilienz einschließlich Threat-led Penetration Testing (TLPT) (Kapitel IV, Artikel 24 bis 27)
  - Management des IKT-Drittparteirisikos (Kapitel V, Abschnitt I, Artikel 28 bis 30)
  - Überwachungsrahmen für kritische IKT-Drittdienstleister (Kapitel V, Abschnitt II, Artikel 31 bis 44)
  - Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen (Kapitel VI, Artikel 44 und Artikel Kapitel VII, Artikel 49)
- Die drei Europäischen Aufsichtsbehörden
  - die EU-Wertpapieraufsichtsbehörde (European Securities and Markets Authority – ESMA),
  - die EU-Bankenaufsichtsbehörde (European Banking Authority – EBA) und
  - die EU-Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (European Insurance and Occupational Pensions Authority – EIOPA)

  erarbeiten gemeinsam dazu technische Regulierungsstandards, Implementierungsstandards und Leitlinien, die die Anwendung von DORA in allen Sektoren weiter konkretisieren.

FINANZSEKTORÜBERGREIFEND!

DORA – Verantwortung des Managements

- Management Body (bspw. Vorstand sowie Aufsichtsräte bei Banken) trägt die Verantwortung für das IKT-Risikomanagement.
- Member des Management Bodys müssen sich aktiv bzgl. IKT-Risiken auf dem Laufenden halten und regelmäßige IKT-spezifische Weiterbildungen erhalten.
- Die Funktion der ICT risk management control function ist durch den Management Body einzurichten.
  - Aufgaben ähnlich der bekannten Informationssicherheitsbeauftragten
  - Strenge Trennung von Control Function und First Line (IT). Three-Lines-of-Defense
  - Weiterhin **starke aufsichtsrechtliche Erwartung** den ISB im eigenen Hause vorzuhalten.
- Eine formelle Dokumentation des aktuellen Stands des IKT-Risikorahmenwerks ist zu erstellen und vorzuhalten.
- FU müssen über die sie betreffenden Schwachstellen bei ihren Dienstleistern informiert werden und auch selbst ihre Schwachstellen an Kunden und Partner angemessen kommunizieren.

DORA – Detaillierte (erhöhte?) Sicherheitsanforderungen

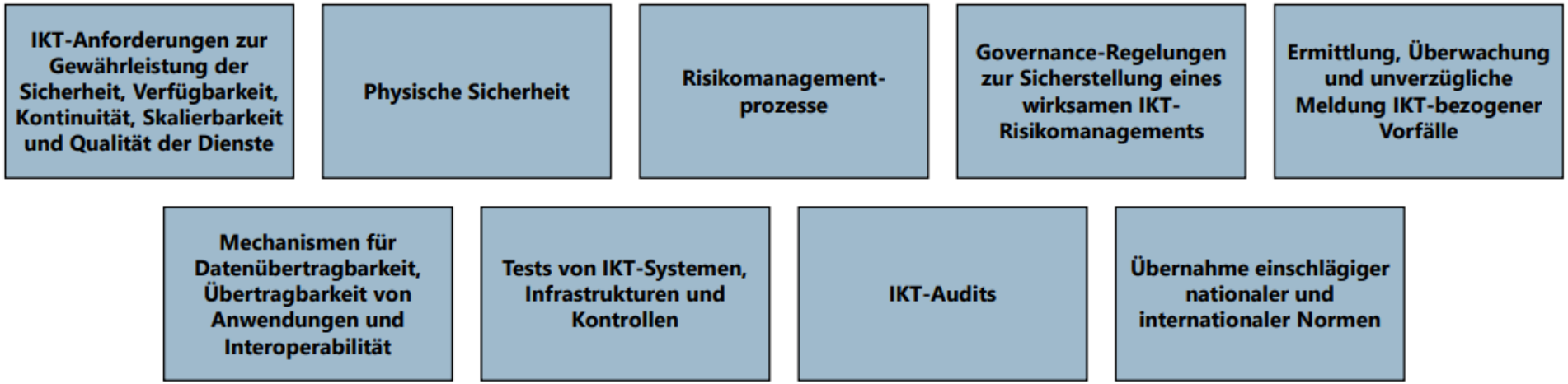
- Daten sind in allen Zuständen zu verschlüsseln (at rest, in transit & in use).
- Interner und externer Netzwerkverkehr ist zu verschlüsseln.
- Für kryptographische Schlüssel ist ein Lifecycle-Management einzurichten.
- Anforderungen an automatisierte Schwachstellenscans und die Behebung von Schwachstellen sind gestiegen.
- Automatisierte Schwachstellenscans mindestens wöchentlich.
- Lieferkettenrisiko rückt in den Fokus.
- Patches auszuspielen hat bei der Behebung von Schwachstellen die höchste Priorität.
- Sicherstellen, dass nur autorisierte Software und Speichermedien verwendet werden.
- Gewährleisten, dass die Sicherheit auch bei Home-Office und BYOD gegeben ist.
- Mitarbeiter welche Cloud-Anwendungen nutzen, müssen gesondert geschult werden, die Credentials zum Cloud-Interface sind besonders sicher zu schützen

DORA – IKT-Drittdienstleistungen

- IKT-Drittdienstleister ist ein „Unternehmen, das IKT-Dienstleistungen anbietet“ (Art. 3 Nr. 19 DORA).
- IKT-Dienstleistungen:
  - Gem. Art 3 Nr. 21 DORA handelt es sich dabei um „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste“
  - Auflistung von beispielhaften IKT-Dienstleistungen in Anhang III des Entwurfs der europäischen Aufsichtsbehörden zum IST-Informationsregister (“Implementing technical standards with regard to standard templates for the register of information”) kann indikativ herangezogen werden, um Erwartungen in Bezug auf häufig anfallende Arten von IKT-Dienstleistungen abzuschätzen.

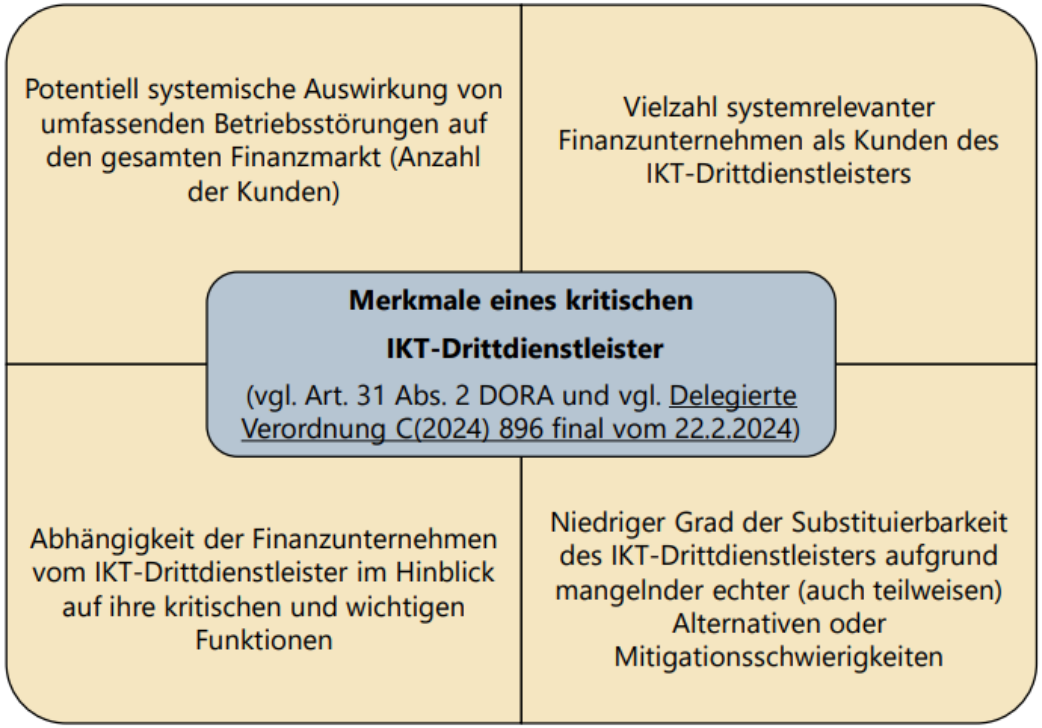
DORA – Überwachung der IKT-Drittdienstleistungen

- Neues Element der EU-Finanzregulierung stellt keine direkte Aufsicht über kritische IKT-Drittdienstleister dar (vgl. Erwägungsgrund 76 DORA).
- Die Aufsicht überwacht kritische IKT-Drittdienstleister mit Blick auf den gesamten Finanzmarkt.
- Der Überwachungsumfang der Aufsicht beschränkt sich auf (vgl. Art. 33 Abs. 3 DORA):



DORA – Kritischer IKT-Drittdienstleister

- Kritischer IKT-Drittdienstleister ist ein „IKT-Drittdienstleister, der gemäß Art. 31 DORA als kritisch eingestuft wurde“ (Art. 3 Nr. 23 DORA).
- Anbieter von Cloud-ComputingDiensten stehen im Fokus des europäischen Gesetzgebers bei der Entwicklung des Überwachungsrahmenwerks (vgl. Erwägungsgrund 20 DORA).

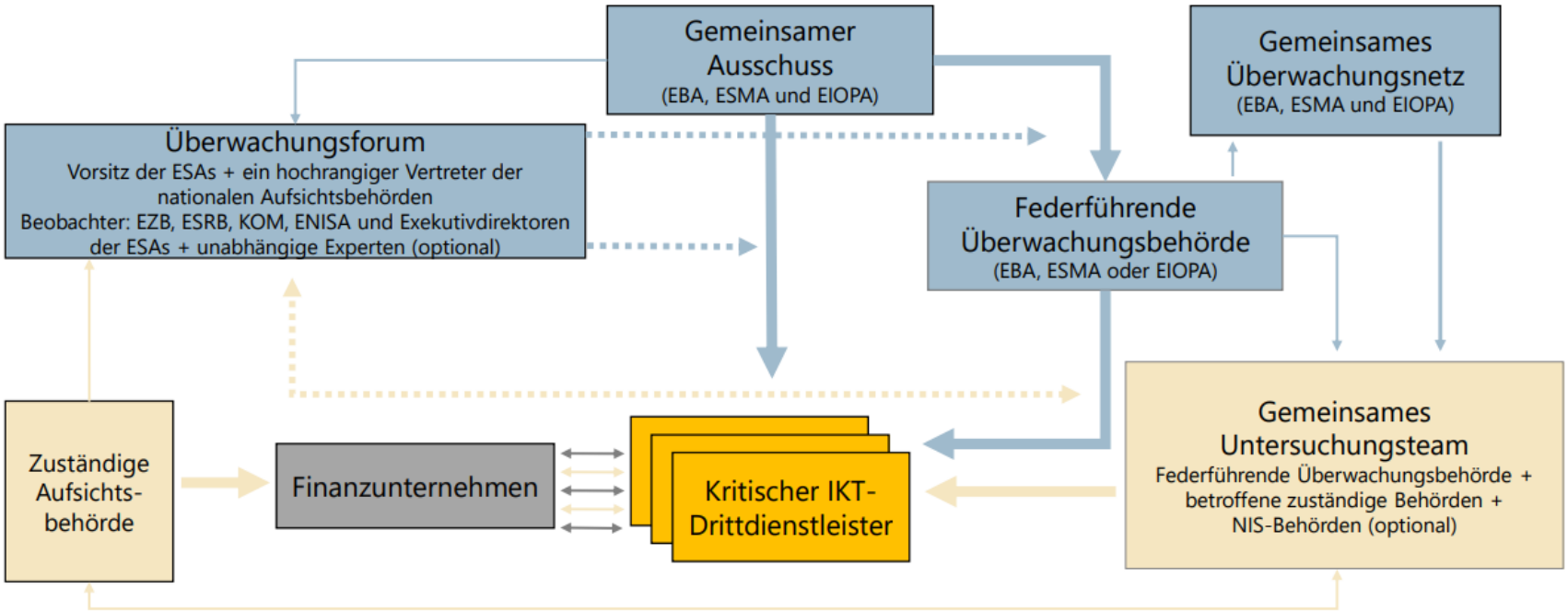


Ausnahmen:

- Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen.
- IKT-Drittdienstleister, die einem Überwachungs-rahmen zur Unterstützung des Europäischen Systems der Zentralbanken unterliegen.
- Gruppeninterne IKT-Dienstleister (vgl. Art. 3 Nr. 20 DORA)
- IKT-Drittdienstleister, die IKT-Dienstleistungen ausschließlich national für rein national tätige Finanzunternehmen bereitstellen.

DORA – Kritischer IKT-Drittdienstleister

- Überwachungsrahmenwerk



DORA – Überwachungszyklus

- Überwachungszyklus

Überwachungstätigkeiten

- Die europäischen Aufsichtsbehörden erstellen **jährlich** einen **individuellen risikobasierten Überwachungsplan (inkl. Überwachungszielen und Überwachunsgmaßnahmen)** für den kritischen IKT-Drittdienstleister.
- Die europäischen Aufsichtsbehörden haben gegenüber kritischen IKT-Drittdienstleistern die folgenden **Überwachungsbefugnisse**:
  - Anforderung von Informationen und Unterlagen
  - Durchführung von Prüfungen
  - Anforderung von Berichten zu Maßnahmen in Folge der Empfehlungen
- **Durchsetzung der Befugnisse:**
  - Verhängung von Zwangsgeldern mit Veröffentlichung
  - Täglich bis zu **1% des durchschnittlichen weltweiten Tagesumsatzes** des vergangenen Geschäftsjahres, max. 180 Tage

Empfehlungen

- Die europäischen Aufsichtsbehörden können **Empfehlungen** gegenüber dem kritischen IKT-Drittdienstleister abgeben, insb. im Hinblick auf die Anwendung von IKT-Sicherheits- und Qualitätsanforderungen oder -verfahren.
  - Kritische IKT-Drittdienstleister müssen binnen **60 Tagen** nach Erhalt der Empfehlung erklären, ob sie den Empfehlungen Folge leisten oder begründen, warum sie dies nicht tun.
  - Nicht erfolgte oder unzureichende Erklärungen werden grds. von den europäischen Aufsichtsbehörden **veröffentlicht**.
- Der kritische IKT-Drittdienstleister erstellt einen **Plan zur Mitigation der aufgezeigten Risiken** und legt auf Verlangen **Fortschrittsberichte** dazu vor.
- Die europäischen Aufsichtsbehörden können nach Abschluss der Überwachungstätigkeiten **Berichte** über die (Abhilfe-)Maßnahmen im Hinblick auf die ausgesprochenen Empfehlungen anfordern.

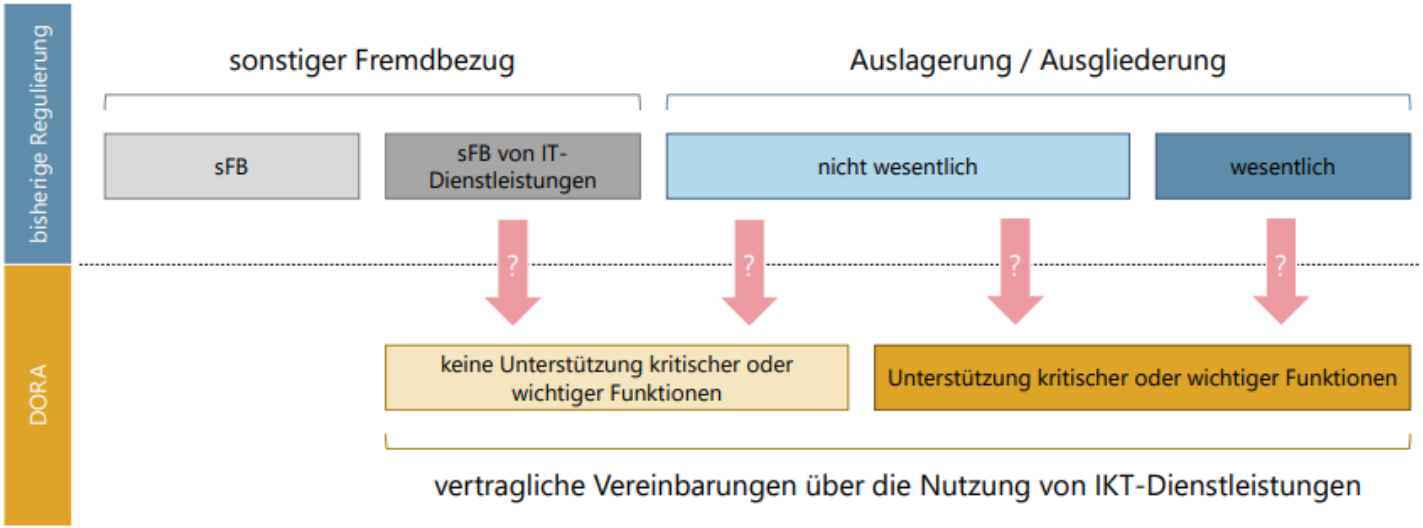
Folgemaßnahmen

- Die zuständigen Behörden prüfen **risikobasiert** und nach dem **Grundsatz der Proportionalität**, wie die Finanzunternehmen die in den Empfehlungen festgestellten **Risiken** beim kritischen IKT-Drittdienstleister zu berücksichtigen planen.
- Bei **nicht oder nicht ausreichender Berücksichtigung der Risiken** durch Finanzunternehmen, teilt die nationale Behörde ihre Einschätzung dem Finanzunternehmen mit und kann binnen 60 Tagen nach dieser Mitteilung als **letztes Mittel** von Finanzunternehmen verlangen,
  - die Nutzung des kritischen IKT-Drittdienstleisters **ganz oder teilweise zu unterbrechen**, bis die Risiken beseitigt sind, oder
  - die Verträge mit dem kritischen IKT-Drittdienstleister **ganz oder teilweise zu kündigen**.

DORA – Auslagerungsbeziehungen

- Ausgestaltung der Verträge abhängig von betroffener Funktion – Fokus auf Unterscheidung zwischen IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen und solchen, die dies nicht tun als Grundlage.
  Erster Schritt ist somit eine entsprechende Bewertung der betroffenen Funktionen. Kritisch oder wichtig sind Funktionen, wenn ihr Ausfall eine erhebliche Beeinträchtigung
  - **der finanziellen Leistungsfähigkeit,**
  - **der Geschäftsfortführung oder**
  - **regulatorischer Art**

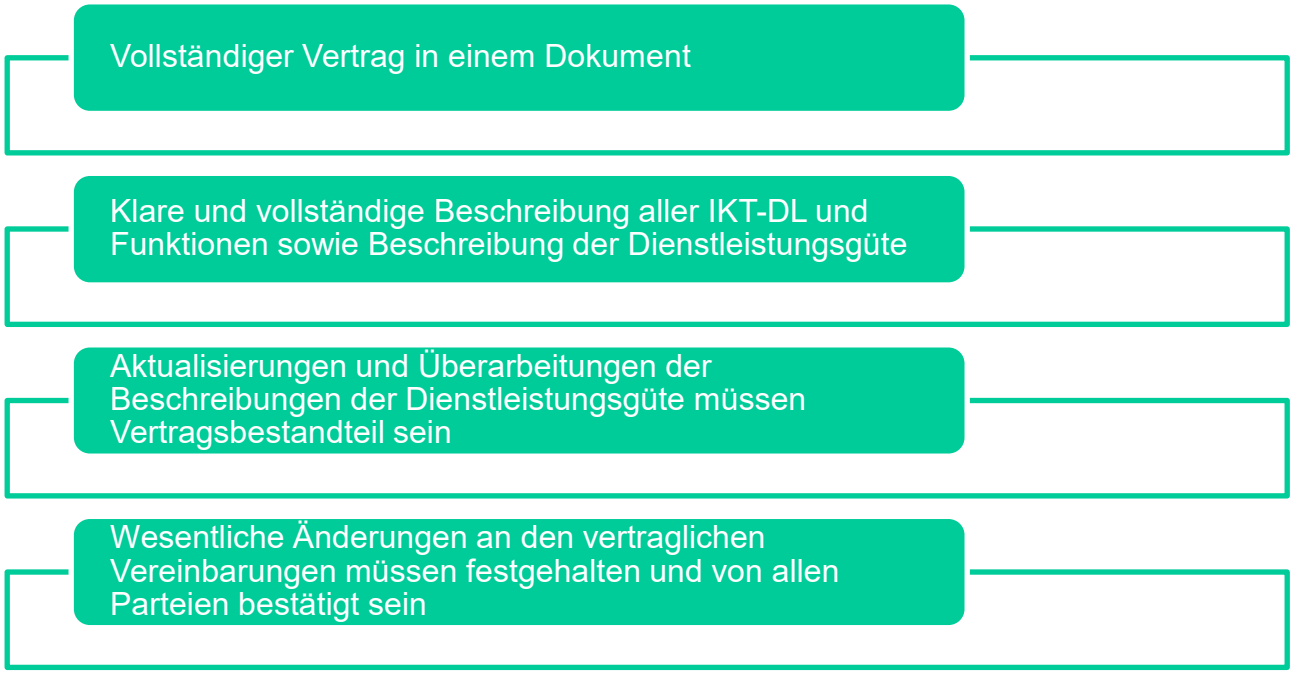
  darstellen würde.



Im Sinne einer RISIKOANALYSE – AT 9 Tz. 2 MaRisk

DORA – Vertragsanforderungen

- **Status Quo**
  - häufig komplexe, unklare und unübersichtliche Verträge, insbesondere bei großen IKT-Drittdienstleistern oder bereits lang laufenden Vertragsbeziehungen
- **Anforderung DORA**

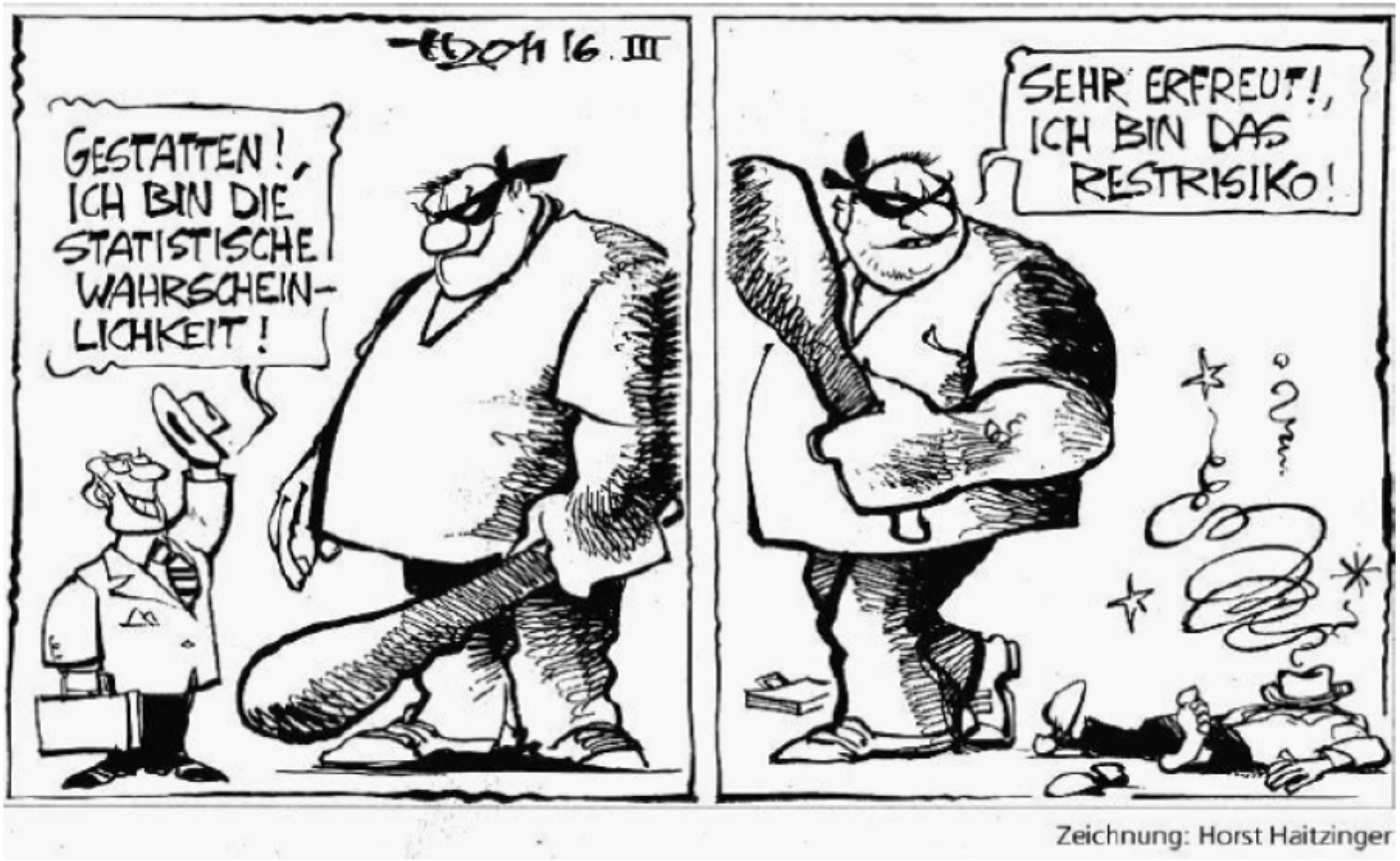


Es sind keine Übergangsfristen für die Anpassung der bestehenden vertraglichen Vereinbarungen vorgesehen.
Die Anpassung der vertraglichen Vereinbarungen soll so schnell wie möglich vorgenommen werden.
Hierzu kann auf einen Implementierungszeitplan zurückgegriffen werden.

DORA – Prüfrechte für Finanzunternehmen

1. Recht zur fortlaufenden Überwachung der Leistung des IKT-Drittdienstleisters (Art. 30 Abs. 3 lit. e DORA)
2. Prüfrechte für das Finanzunternehmen und die Aufsicht, inkl. dem Recht Kopien anzufertigen (Art. 30 Abs. 3 lit. e (i) DORA)
3. Uneingeschränkte Zusammenarbeit bei Vor-Ort-Inspektionen und Audits (Art. 30 Abs. 3 lit. e (iii) DORA)
4. Prüfungs- und Testrechte (Art. 8 Abs. 2, Art. 8 Abs. 3 lit. g und h sowie Art. 3 Abs. 9 lit. c und d RTS-E TPPol)

- **Zulässige Einschränkung der Prüfrechte:**
  - bei Betroffenheit Rechte anderer Kunden, Vereinbarung „alternativer Bestätigungsniveaus“ (Art. 30 Abs. 3 lit. e (ii) DORA)
  - Mitteilungspflicht zur Prüfungsplanung, d.h. Umfang und Häufigkeit (Art. 30 Abs. 3 lit. e (iv) DORA)
  - Wahrnehmung der Prüfungsrechte durch unabhängigen Dritten bei Kleinstunternehmen, keine eigenen Prüfungen (Art. 30 Abs. 3 DORA)



Zeichnung: Horst Haitzinger

AKTUELLE PRÜFUNGSERFAHRUNGEN

Beispielfeststellungen (Institut A - 1)

[Strategie]

- Die strategischen Vorgaben des Instituts zum Auslagerungsmanagement sind weder ausreichend konkret noch überprüfbar. Zudem sind die organisatorischen Vorgaben in Teilen unzureichend.
- Aufgrund der unzureichenden Sollvorgaben sind die Anforderungen gemäß AT 4.2 Tz. 1 MaRisk sowie AT 5 Tz. 1 i. V. m. AT 5 Tz. 3 f MaRisk nicht hinreichend erfüllt.

[Personalausstattung]

- Die Dokumentation der Überwachungshandlungen des zentralen Auslagerungsmanagements sowie seine quantitative Personalausstattung sind nicht angemessen.
- Durch die fehlende angemessene Dokumentation und die unzureichende quantitative Personalausstattung sind die Anforderungen gemäß AT 6 Tzn. 1 und 2 MaRisk sowie AT 7.1 Tz. 1 MaRisk nicht hinreichend erfüllt.

Beispielfeststellungen (Institut A - 2)

[Identifikation]

- Im Bereich Definition und Identifikation von Auslagerungen offenbarten sich die folgenden Schwächen:
  - Die Vertragsdatenbank, welche die Grundlage für die Erkennung von Auslagerungen ist, wird nicht vollständig gepflegt.
  - Es liegt nicht für jeden Dienstleister eine einzelfallbezogene Analyse zur Auslagerungsrelevanz vor.
  - Die vom Institut verwendete Definition zur Abgrenzung der Auslagerungen vom sonstigen (IT) Fremdbezug ist nicht sachgerecht.
  - Infolgedessen wurden mehrere Dienstleister fälschlicherweise nicht als Auslagerungen erkannt.
- Die Anforderungen an die Identifikation von Auslagerungen gemäß AT 9 Tz. 1 MaRisk sind nicht erfüllt.
- Ursächlich für die Mängel sind eine von der aufsichtlichen Sicht abweichende Auslagerungsdefinition sowie die angespannte Personalsituation im zentralen Auslagerungsmanagement. Wegen der nicht erfolgten Einstufung von verschiedenen Dienstleistern als Auslagerung wurden für diese Dienstleister keine Risikoanalysen erstellt und in der Folge auch keine gegebenenfalls notwendigen weiteren Maßnahmen (Mindestvertragsbestandteile, Exit-Pläne angemessene Steuerung etc.) ergriffen.

Beispielfeststellungen (Institut A - 3)

[Risikoanalyse]

- Im Zusammenhang mit der Erstellung von Risikoanalysen und Risikobewertungen durch das Institut offenbarten sich die folgenden Mängel:
  - Die Anrechnung von risikominimierenden Maßnahmen bei der Ermittlung der Wesentlichkeit einer Auslagerung ist nicht sachgerecht.
  - Die Einstufung der Risiken in den durchgeführten Risikoanalysen war in einigen Fällen weder plausibel noch sachgerecht.
  - Nur für 24 von 62 erkannten sonstigen IT-Fremdbezüge wurden Risikobewertungen durchgeführt.
- Die Anforderungen an die Risikoanalysen gemäß AT 9 Tz. 2 MaRisk sowie an die Risikobewertungen gemäß Art. 9.2 BAIT sind nicht erfüllt.
- Ursächlich für die offengelegten Mängel sind eine von der aufsichtlichen Meinung abweichende Berechnungsgrundlage für die Risikomessung bei der Erstellung der Risikoanalysen (sog. Nettobetrachtung) sowie die angespannte Personalsituation im zentralen Auslagerungsmanagement. Durch die Mängel in der Erstellung der Risikoanalysen wurden mehrere wesentliche Dienstleister nicht als solche erkannt, wodurch die für wesentliche Auslagerungen notwendigen Maßnahmen (Mindestvertragsbestandteile, Exit-Pläne, angemessene Steuerung etc.) nicht sichergestellt sind.

Beispielfeststellungen (Institut A - 5)

[Handlungsoptionen und Ausstiegsprozesse für wesentliche Auslagerungen]

- Es gibt keine Vorgaben hinsichtlich der regelmäßigen oder anlassbezogenen Überprüfung von den Plänen für die erwartete oder unerwartete Beendigung von wesentlichen Auslagerungen. Für die wesentlichen Auslagerungen an Unternehmen der eigenen Gruppe wurden keine formalisierten Pläne erstellt. Bei den Plänen für einen Dienstleister gibt es Mängel hinsichtlich der Detailtiefe sowie der Überprüfung der Durchführbarkeit der Ausstiegsprozesse.
- Die Anforderungen an das Vorgehen für den Ausstiegsprozess gemäß AT 9 Tz. 6 MaRisk sind nicht hinreichend erfüllt.

[Weiterverlagerungen]

- Es ist nicht sichergestellt, dass dem Institut alle aufsichtlich relevanten Weiterverlagerungen bekannt sind. Zudem ist die anschließende Einstufung in Teilen nicht sachgerecht und notwendige Risikoanalysen wurden in vier von neun Fällen noch nicht durchgeführt.
- Die Anforderungen an den Umgang mit Weiterverlagerungen gemäß AT 9 Tzn. 8 und 11 MaRisk sind nicht hinreichend erfüllt.

Beispielfeststellungen (Institut A - 6)

[Steuerung und Überwachung]

- Im Zusammenhang mit der Steuerung von wesentlichen Auslagerungen zeigten sich die folgenden Mängel:
  - Es existieren weder zentrale Vorgaben für die Steuerung von wesentlichen Auslagerungen noch wird die Einhaltung der entsprechenden SLAs überprüft.
  - Die vierteljährlichen Risikoberichte des Dienstleisters CBA beinhalten nicht die dem Dienstleister bekannten Risiken.
  - Die Dokumentation der Steuerung und Überwachung des Dienstleisters CBA ist teilweise nicht nachvollziehbar.
  - Das Risiko aus der mangelnden Kooperationswilligkeit des Dienstleisters CBA wird nicht angemessen gesteuert.
  - Es gibt keine Kontrollen auf nicht autorisierte Änderungen der Parametrisierung beim Dienstleister RATING-ABC.
  - Die fachliche Steuerung des Dienstleisters RATING-ABC erfolgt komplett in xxx Sprache. Daher ist die Angemessenheit der Maßnahmen sowohl durch das zentrale Auslagerungsmanagement des Instituts als auch durch die Aufsicht nicht hinreichend überprüfbar.
  - Die vierteljährlichen Risikoberichte des Dienstleisters RATING-ABC sind nicht geeignet, um sich ein transparentes Bild von der Risikolage bei diesem Dienstleister zu verschaffen.
  - Es gibt keine zentralen Vorgaben zu vierteljährlich von den wesentlichen Dienstleistern zur Verfügung zu stellenden Risikoinformationen und das Institut bekommt diese Informationen auch nicht von allen wesentlichen Dienstleistern.
- …

Beispielfeststellungen (Institut A - 6)

[Steuerung und Überwachung] … Fortsetzung

- Aufgrund der unzureichenden Steuerung und Überwachung der wesentlichen Dienstleister sind die Anforderungen gemäß AT 9 Tzn. 9 und 12 i. V. m. AT 4.3.2 Tz. 2 MaRisk sowie AT 7.2 Tz. 3 MaRisk nicht erfüllt.
- Ursächlich für diesen Mangel ist eine zu geringe Sensibilität für die Risiken, welche sich aus der rein dezentralen Steuerung von Auslagerungen ergeben. Eine einheitliche Sicht auf die Steuerung der wesentlichen Dienstleister und eine vollständige Transparenz über die eingegangenen Risiken sind so nicht möglich. Die rein dezentrale Steuerung der wesentlichen Dienstleister und die unvollständige Transparenz eingegangener Risiken machen es für das Institut unmöglich, diese Risiken angemessen zu steuern. Auch in Anbetracht des Umfangs der für das Institut wesentlichen Auslagerungsaktivitäten wird diese Feststellung als xxx eingestuft.

Beispielfeststellungen (Institut B - 1)

[Compliance]

- Die institutsinternen schriftlich fixierten Regelungen und Prozesse im Zusammenhang mit der Identifizierung und Umsetzung wesentlicher rechtlicher Regelungen und Vorgaben sind nicht konkret genug, sodass auch die implementierten Prozesse selbst im Zusammenhang mit der Umsetzung dieser Regelungen und Vorgaben nicht hinreichend ausgestaltet wurden. Die Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben gemäß AT 4.4.2 Tz. 1 MaRisk ergeben können, sind somit nicht vollumfänglich erfasst worden. Systematische Überprüfungen im Hinblick auf die institutsinternen Verfahren/Kontrollen zur Einhaltung rechtlicher Regelungen und Kontrollen werden von der Compliance-Funktion bisher nicht in hinreichendem Umfang durchgeführt. Für den Prozess der Ad-hoc-Berichterstattung wurden bisher keine konkreten Anlass-Dimensionen definiert.

- Die Compliance-Funktion hat gemäß AT 4.4.2 Tz. 1 MaRisk auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinzuwirken, was die angemessene Identifizierung wesentlicher rechtlicher Regelungen und Vorgaben gemäß AT 4.4.2 Tz. 2 MaRisk voraussetzt. Laut AT 4.4.2 Tz. 7 MaRisk ist zudem die Geschäftsleitung auch anlassbezogen zu informieren.

Beispielfeststellungen (Institut C - 1)

[Interne Revision]

- Das Institut hat insbesondere bei wesentlichen Auslagerungen u. a. deren laufende Überwachung sowie Aufgaben der Internen Revision auf die XAY ausgelagert. In diesem Zusammenhang sind mehrere Schwächen zu monieren:
  - Die von der XAY übermittelten (Revisions-)Feststellungen sowie ihre Kategorisierung werden ohne nähere institutsseitige Plausibilisierung unverändert übernommen. Die Interne Revision bildet sich somit nicht ausreichend ein eigenes Urteil.
  - Dem Institut werden nicht durchgängig alle relevanten Revisionsergebnisse der Auslagerungsunternehmen zwecks Plausibilisierung der von der XAY vorgenommenen Auswertung rechtzeitig zur Verfügung gestellt.
  - Es findet hinsichtlich der XAY-betreuten Auslagerungen keine Einwertung der Funktionsfähigkeit der Internen Revision bei den Dienstleistern statt. Somit erfolgt beispielsweise keine Aussage zur Vollständigkeit der geprüften Themen.
  - Zudem findet kein revisionsseitiger Abgleich statt, inwiefern nicht abgestellte Mängel in den Risikoinformationen für die IKS-Überwachung der Dienstleister von der XAY behandelt werden.
- Gemäß BT 2.1 Tz. 3 MaRisk kann die Interne Revision des Instituts im Fall von Auslagerungen auf ein anderes Unternehmen auf eigene Prüfungshandlungen verzichten, sofern die anderweitig durchgeführte Revisionstätigkeit den Anforderungen in AT 4.4.3 und BT 2 MaRisk genügt. Die Interne Revision des auslagernden Instituts hat sich von der Einhaltung dieser Voraussetzungen regelmäßig zu überzeugen. Die für das Institut relevanten Prüfungsergebnisse sind an die Interne Revision des auslagernden Instituts weiterzuleiten. Durch die aufgezeigten Schwächen im Zusammenhang mit den von der XAY-betreuten externen Dienstleister werden die Anforderungen nicht vollumfänglich erfüllt.

Informationssicherheitsmanagement - Zusammenfassung (= Baustellen)

- **Hauptkritikpunkte**
  - Der Informationssicherheitsbeauftragte ist nicht unabhängig.
  - Die Richtlinien/Sicherheitsrichtlinien/Konzepte sind nicht vollständig und/oder stehen im Widerspruch zur Informationssicherheitsleitlinie.
  - Es findet keine Überprüfung der Vorgaben in den Richtlinien und deren konkrete Ausformulierung in den Arbeitsanweisungen und technischen Konzepten der 1st-Line sowie deren Umsetzung in den IT-Systemen statt => Internes Kontrollsystem
  - Es werden keine bzw. nur unzureichenden Überprüfungen der Sicherheitsmaßnahmen durchgeführt.
  - Es finden keine bzw. unzureichende Schulungsmaßnahmen zum Thema Informationssicherheit statt.
  - Der Informationssicherheitsbeauftragte ist nicht bzw. nur unzureichende in den Managementprozess zu den Themen Auslagerung und Notfallmanagement eingebunden.

Informationsrisikomanagement - Zusammenfassung! (= Baustellen)

- Anforderungen an den Sollmaßnahmenkatalog
  - objektiv überprüfbar
    - Soll-Ist-Abgleich muss möglich
    - Sachkundige Dritte müssen sich in angemessener Zeit einlesen können
  - Institutsspezifisch!
  - Verprobung auf den (instituts)relevanten Standard (!)
  - Maßnahme muss umsetzbar sein / Einbindung Fachbereiche
  - Risikoorientierte Umsetzung möglich (Art, Umfang und Turnus)
    aber: Begründung muss nachvollziehbar und plausibel sein
    Stichwort: Expertenschätzung
  - [bei Auslagerung!] Detailausgestaltung muss bekannt sein und mit eigenen Anforderungen verprobt sein … Was macht mein DL?
  - Funktionsfähigkeit und Wirksamkeit der Kontrolle bzw. Schutzmaßnahme muss sichergestellt sein
  - Laufende Überwachung auf Sinnhaftigkeit bzw. Arbitrage
  - Papier ist geduldig! Umsetzung erforderlich

Security Information & Event Management - Zusammenfassung! (= Baustellen)

- **Hauptkritikpunkte**
  - Es ist nicht definiert, wann es sich um ein Sicherheitsrelevantes Ereignis handelt.
  - Es liegt keine vollständige und/oder qualitätsgesicherte Infrastrukturanalyse vor.
  - Es existieren keine Richtlinien, welche Informationen zu sammeln sind (Loggingkonzept).
  - Die Logdateien sind nicht manipulationssicher abgelegt.
  - Es erfolgt keine bzw. unvollständige Auswertung der Loginformationen.
  - Die Bewertung der Risiken (z. B.: noch nicht vorliegenden Auswertungsregeln, noch nicht angebunden Systemen) erfolgt nicht
  - Die Steuerung der Bearbeitung der sicherheitsrelevanten Ereignisse erfolgt nicht durch bzw. unter Beteiligung des Informationssicherheitsbeauftragten.
  - Eine korrelierte Auswertung von einzelnen sicherheitsrelevanten Ereignissen und /oder Incidents und Problems erfolgt nicht.
  - Es gibt keine Regelungen für die forensische Auswertung.

Vielen Dank für IHRE Aufmerksamkeit!

Literaturempfehlung in eigener Sache ;-)

MaRisk-Berichtswesen
ISBN 978-3-95725-134-3 – 502 Seiten

„**MaRisk: Prüfungserkenntnisse aus Praxisfällen**“ –
Herausgeber: Henning Riediger

Inklusiver umfangreicher Fallstudien und Beispielfeststellungen zu Strategie, Informationsrisikomanagement, Informationssicherheitsmanagement, Auslagerungen, Benutzerberechtigung, Individuelle Datenverarbeitung usw.

- ISBN: 978-3-95725-164-0 - 482 Seiten