



Bundesanstalt für
Finanzdienstleistungsaufsicht

Aktuelles rund um die IT-Regulierung im Finanzsektor

TeleTrust
IT-Sicherheitsrechtstag 2022

Aktuelle regulatorische Entwicklungen mit Bezug zu Informations- und Cybersicherheit

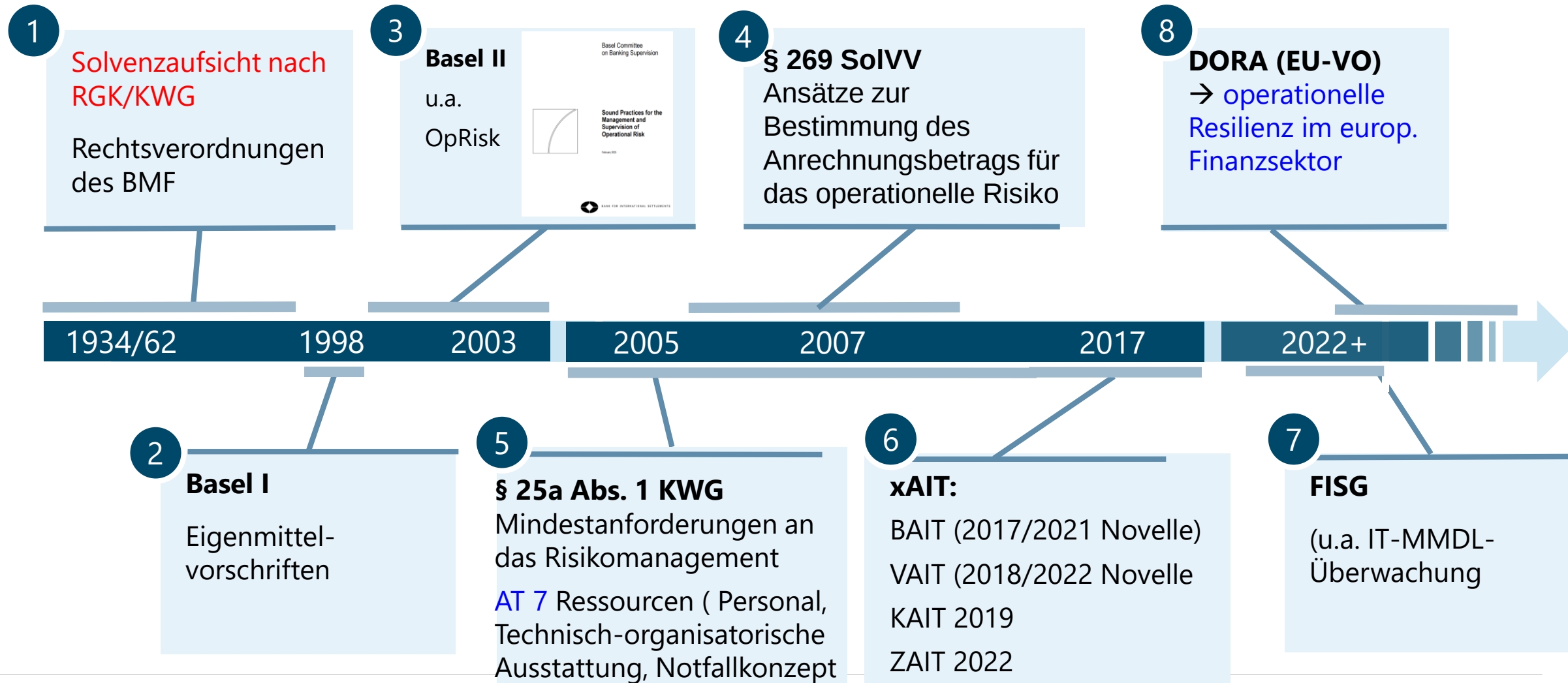
Dr. Jens Gampe,
Referat GIT 2

Incident Reporting, Überwachung IT-MMDL und Krisenprävention

Inhalt

1. Ausgangslage – wo kommen wir her
2. IT-/Cybersicherheit
3. DORA
4. FISG
5. BAIT
6. Zusammenfassung

1. Ausgangslage – wo kommen wir her?



1. Ausgangslage - Definitionen

Art. 4 Abs. 1 Nr. 52 CRR (VO 575/2013):

Operationelles Risiko ist demnach das

„**Risiko von Verlusten**, die durch die

- Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen oder
- durch externe Ereignisse verursacht werden,
- einschließlich Rechtsrisiken“.

→ Reputationsrisiko ist entfallen

Begriffsbestimmungen Nr. 10 (EBA/GL 2019/04)

IKT- und Sicherheitsrisiko

Verlustrisiko aufgrund einer

- Verletzung der Vertraulichkeit,
- Verlust der Integrität von Systemen und Daten,
- einer unzureichenden oder fehlenden Verfügbarkeit von Systemen und Daten,
- einer mangelnden Fähigkeit, die Informationstechnologie (IT) in einem angemessenen Zeit- und Kostenrahmen zu ändern, wenn sich die Umgebungs- oder Geschäftsanforderungen ändern (d. h. Agilität).
- Dies umfasst **Sicherheitsrisiken**, die aus unzulänglichen oder fehlgeschlagenen internen Prozessen oder externen Ereignissen resultieren, einschließlich Cyber-Attacken oder unzureichender physischer Sicherheit.

1. Ausgangslage

Cyberisiken sind mittlerweile das **größte operationelle Risiko** für die Geldhäuser!

„Dieses Risiko ist sehr präsent, und **es wächst stark**. Ich bin persönlich nicht sicher, ob wir alle miteinander - staatlicher Sektor, Privatsektor - gut genug **vorbereitet** sind **auf einen wirklich schwerwiegenden Sicherheitsvorfall**“

„Je digitaler die Finanzwelt wird, **desto mehr gewinnt das Thema IT-Sicherheit an Bedeutung**. ... Wir werden die **IT-Verantwortlichen** der Banken daher künftig **noch stärker in die Pflicht** nehmen ...“

Euro Finance Week 2021
BaFin-Präsident Mark Branson

IT-Info-Tag 2021
Exekutivdirektor (BA) Raimund Röseler

1. Ausgangslage

Es gibt zwei Arten von Unternehmen

- solche, die gehackt wurden, und solche, **die es noch werden**

FBI-Direktor Robert Mueller (2012)

- die, die gehackt worden sind und die, **die es noch nicht wissen**

Kaspersky Lab (2017)

2. IT-/Cybersicherheit – sektorweite Schwachstellen

Häufig beobachtbare Schwachstellen – eine [europäische Sicht](#):

- unzureichende „**Cyber-Hygiene**“ im IT-Umfeld
- unzureichende Überwachung von **dritten Dienstleistern** bzw. der Lieferkette
- unzureichendes **Testen** von Prozessen, Technologien, aber auch Personen
- unzureichende **Investitionen** in die Fähigkeiten, Cyber-Angriffe zu entdecken und Bedrohungen zu identifizieren → ggf. SOC oder CDC notwendig
- unzureichende **strategische Planung** und strategische Steuerung im Bereich Cyber
- **Technologisches Problem**: häufig Nutzung von „End-of-Life“ – Systemen
- Technikzentrierter Fokus; Faktor Mensch wird vernachlässigt

2. IT-/Cybersicherheit – mögliche Maßnahmen

Prämisse: Die Geschäftsleitung ist **unmittelbar** verantwortlich für IT-/Cybersicherheit

- **Klare Anforderungen/Regeln** (Compliance und Governance) und **Überwachung der Einhaltung** derselben
- **Sensibilisierung** der Beschäftigten bzgl. IT-/Cyberrisiken / **Informationssicherheit**
- Informationssicherheitsschulungen und **(IT-) Notfallübungen**
- **IT-Notfalltests** (intern) bzw. Penetrationstests (extern) einzelner Komponenten der IT-Landschaft
- **TIBER-DE** (Threat Intelligence-based Ethical Red Teaming) richtet sich in erster Linie an kritische Unternehmen des Finanzsektors, um deren Cyberwiderstandsfähigkeit zu stärken und IT-basierte Dominoeffekte im Finanzsektor zu verringern

2. IT-/Cybersicherheit – weiterführende Informationen



Inhalt u.a.:

- Digital hilflos? Ein kurzer Überblick über die IT-Sicherheit in Deutschland
- Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten
- Cyber-Resilienz mittels TIBER-DE – Ein zukünftiges Rahmenwerk für ethische Hackerangriffe auf Finanzunternehmen in Deutschland
- Aufsicht über Kritische Infrastrukturen im Finanzwesen – ein Überblick über den Status

3. Digital Operational Resilience Act (DORA)

Wesentliche Elemente

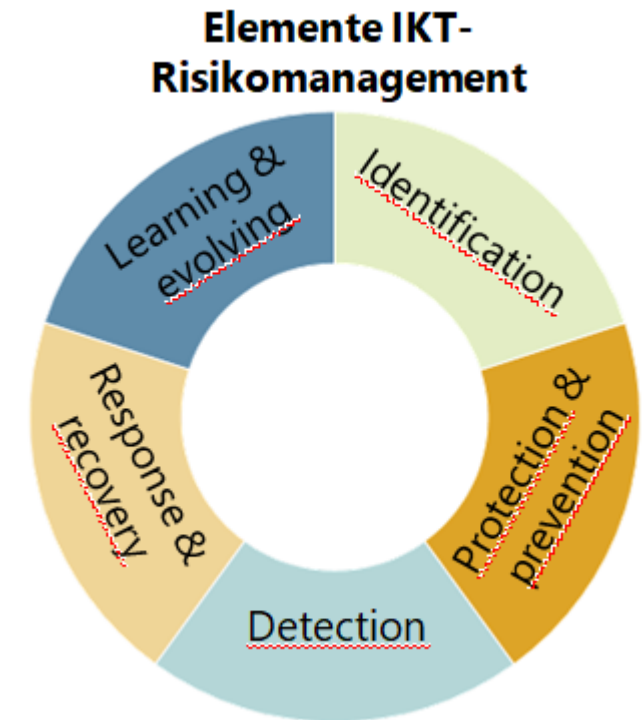
- **Harmonisierung** des **IKT-Risikomanagements** (IKT-Governance und IKT-Risikomanagement-Rahmenwerk)
-> Orientierung am NIST Framework for Improving Critical Infrastructure Cybersecurity
- Vereinheitlichung und Ausweitung der **Meldepflichten** von schwerwiegenden **IKT-Vorfällen** auf den gesamten Finanzsektor
-> Nationale Aufsichtsbehörde als alleinige Empfängerin, Informationsweitergabe an ESAs, EZB und BSI
- **Europäisches Oversight Framework für kritische IKT-Drittdienstleister** (ESA's verantwortlich)

Weitgefasster Anwendungsbereich:

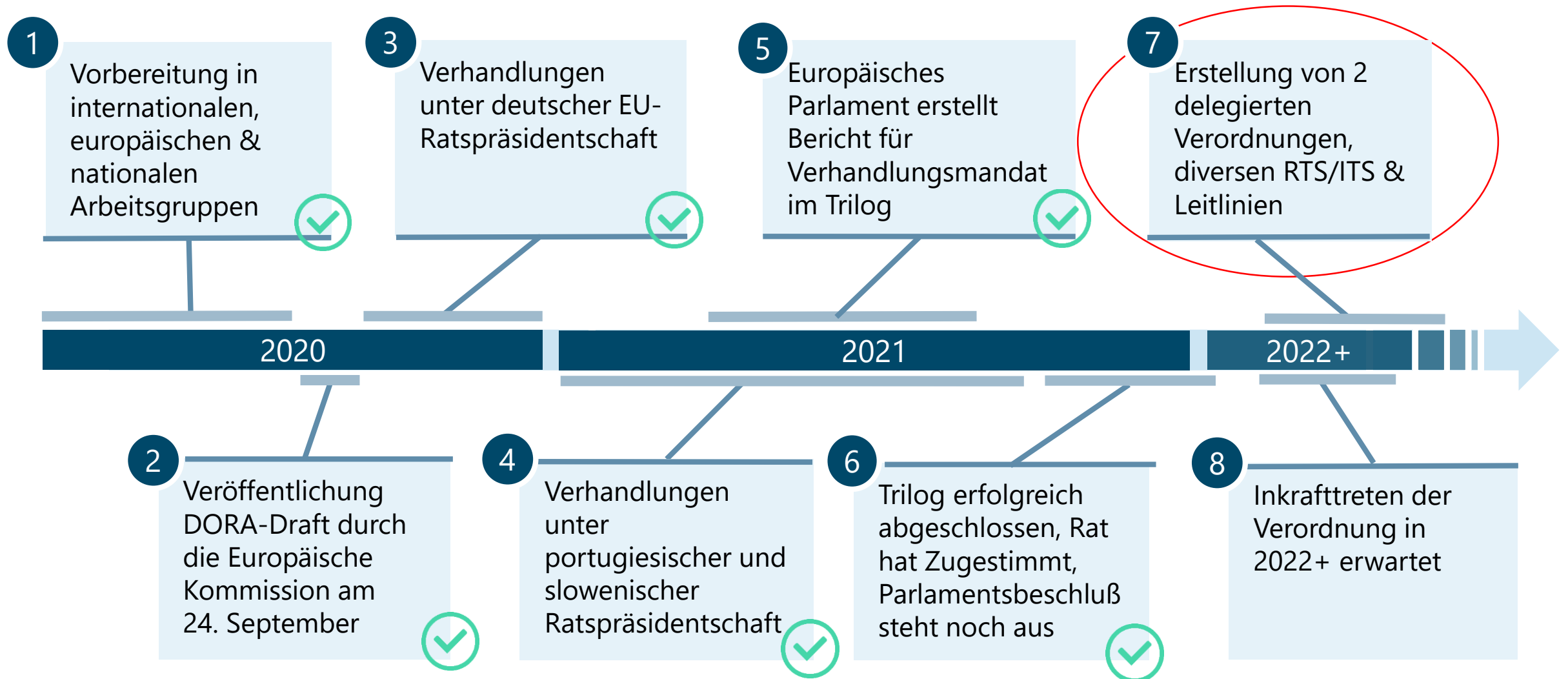
- Kreditinstitute
- Zahlungsdienstleister
- Erst- und Rückversicherungsunternehmen & EbAV
- Wertpapierfirmen
- E-Geld-Institute
- „Kryptoverwahrer“
- Central Securities Depositories (CSD)
- Zentrale Gegenparteien
- Handelsplätze
- ...

3. Digital Operational Resilience Act (DORA)

- Harmonisierte und einheitliche **Prinzipien**
 - **IKT-Governance & Organisation**
 - **Gesamtverantwortung der Geschäftsleitung** als allumfassendes Prinzip
 - **IKT-Risikomanagement-Rahmenwerk**
 - **Orientierung** am **NIST Framework** for Improving Critical Infrastructure Cybersecurity
 - **Vorgehensweise:** Standardneutrale und **risikoorientierte Umsetzung**
 - **Ziel:** Aufrechterhaltung & Wiederherstellung der Funktionsfähigkeit des Finanzunternehmens
- ➔ DORA macht vsl. eine **Anpassung der einschlägigen Leitlinien der ESAs** notwendig



Aktuelles und nächste Schritte



4. Zielsetzung des FISG (Gesetz zur Stärkung der Finanzmarktintegrität)

Zielsetzung des Gesetzgebers: Stärkung des **Vertrauens** in den deutschen Finanzmarkt

- Stärkung der Corporate Governance
Einführung einer gesetzlichen Pflicht zur Errichtung eines **angemessenen und wirksamen** internen Kontrollsystems (IKS) sowie eines entsprechenden Risikomanagementsystems (RMS) für börsennotierte Aktiengesellschaften
- **verpflichtende** Errichtung eines Prüfungsausschusses für Unternehmen von öffentlichem Interesse
- **Stärkung** der Unabhängigkeit des Abschlussprüfers,
- eine **Verschärfung** der Haftung des Abschlussprüfers
- eine **wesentliche Ausweitung der Prüfungsbefugnisse der BaFin**

4. Zielsetzung des FISG

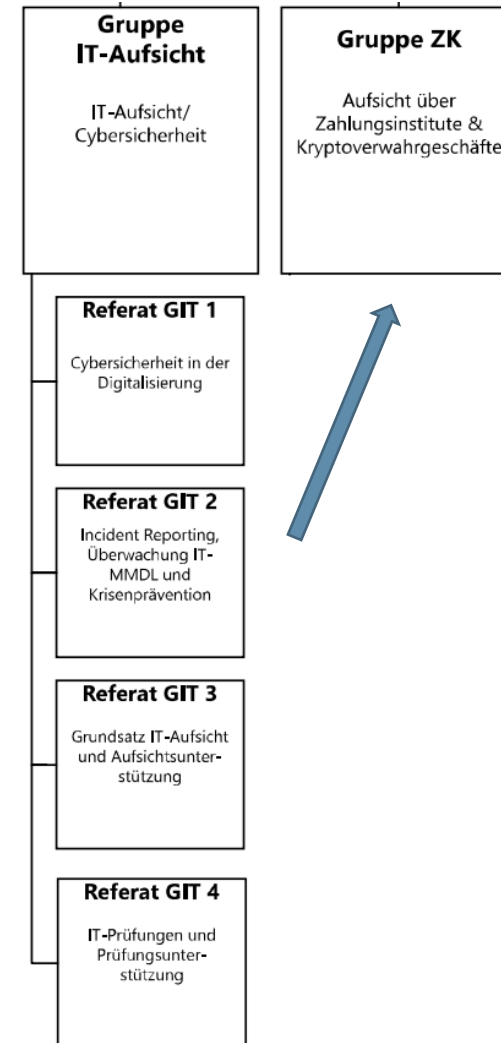
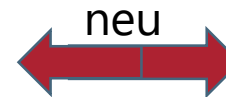
Ab 2022 wird die Aufsicht **direkt** auf Unternehmen zugreifen, auf die Banken **wesentliche** Aktivitäten und Prozesse auslagern, **insbesondere IT-MMDL**.

- erweiterter **Anordnungsbefugnisse**:
 - die BaFin kann künftig **unmittelbar** auf das Auslagerungsunternehmen zugreifen, wenn sie einen Missstand vermeiden oder beheben will
 - Auch Bußgelder kann die BaFin dann direkt gegenüber dem jeweiligen Unternehmen verhängen
 - Für den Fall, dass Institute Auslagerungsunternehmen in Drittstaaten außerhalb des Europäischen Währungsraums beauftragen, müssen sie mit diesen vertraglich einen **inländischen Zustellungsbevollmächtigten** vereinbaren
- **Auslagerungsregister, Auslagerungsbeauftragter** und (Wieder)Einführung der **Anzeigepflicht für wesentliche Auslagerungen**, was der Aufsicht einen flächendeckenden Überblick über Auslagerungen und die damit einhergehenden (Konzentrations-)Risiken verschafft → via BaFin-Meldeplattform

4. Zielsetzung des FISG

Neue Aufbauorganisation in der BaFin
zur IT-Mehrmandantendienstleister - Überwachung

- SSM
- Bundesbank
- Verbände der Finanzwirtschaft
- BSI
- Cyber AZ
- UP Kritis

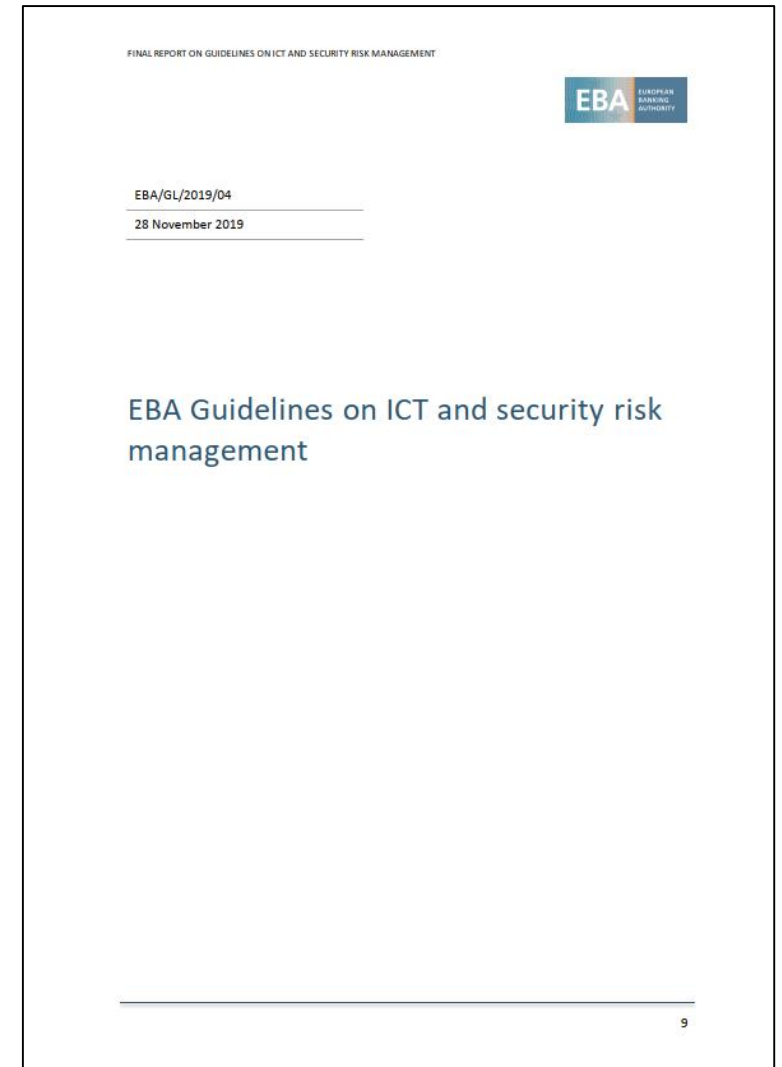


5. Zielsetzung der BAIT (Bankaufsichtliche Anforderungen an die IT)

- Die **Erwartungshaltung der Aufsicht** an die Institute wird durch die BAIT **transparent**.
- BAIT stellen einen **flexiblen und praxisnahen Rahmen** insbesondere für das
 - Management der IT-Ressourcen sowie
 - das Informationsrisikomanagement und
 - das Informationssicherheitsmanagement dar.
- BAIT tragen dazu bei, das **unternehmensweite IT-Risikobewusstsein** im Institut und gegenüber den Auslagerungsunternehmen zu **erhöhen**.
- Mit der **aktuellen Novelle 2021** sind sämtliche Anforderungen der ICT-Guidelines (EBA/GL/2019/04) in den BAIT berücksichtigt.

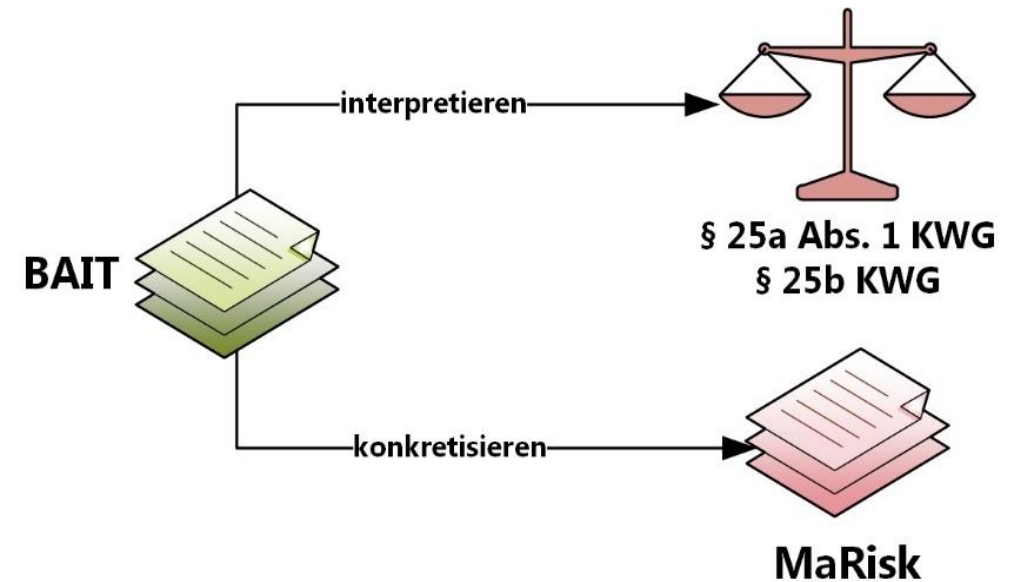
Hintergrund der BAIT-Novellierung 2020

- EBA veröffentlichte im November 2019 die „Leitlinien zum IKT- und Sicherheitsrisikomanagement“ (ICT-Guidelines: EBA/GL/2019/04).
 - **Einheitlicher** Ansatz für Kreditinstitute und Zahlungsdienstleister im gesamten Binnenmarkt
 - Neu:
 - Anforderungen an operative IT-Sicherheit
 - Anforderungen an Notfallmanagement
 - Anforderungen an das Management der Beziehungen zwischen den ZDL und den Zahlungsdienstnutzern
- Erfahrungen von IT-Prüferinnen und IT-Prüfern einbezogen



Grundprinzipien der BAIT

- **Interpretieren** als Verwaltungsinnenrecht den § 25a Abs. 1 KWG
- **Konkretisierung** der MaRisk in bestimmten Bereichen → MaRisk-Anforderungen bleiben unberührt
- Gängige Standards sind zu beachten und **wirksam umzusetzen**
- Modularer Aufbau und daher flexibel erweiterbar

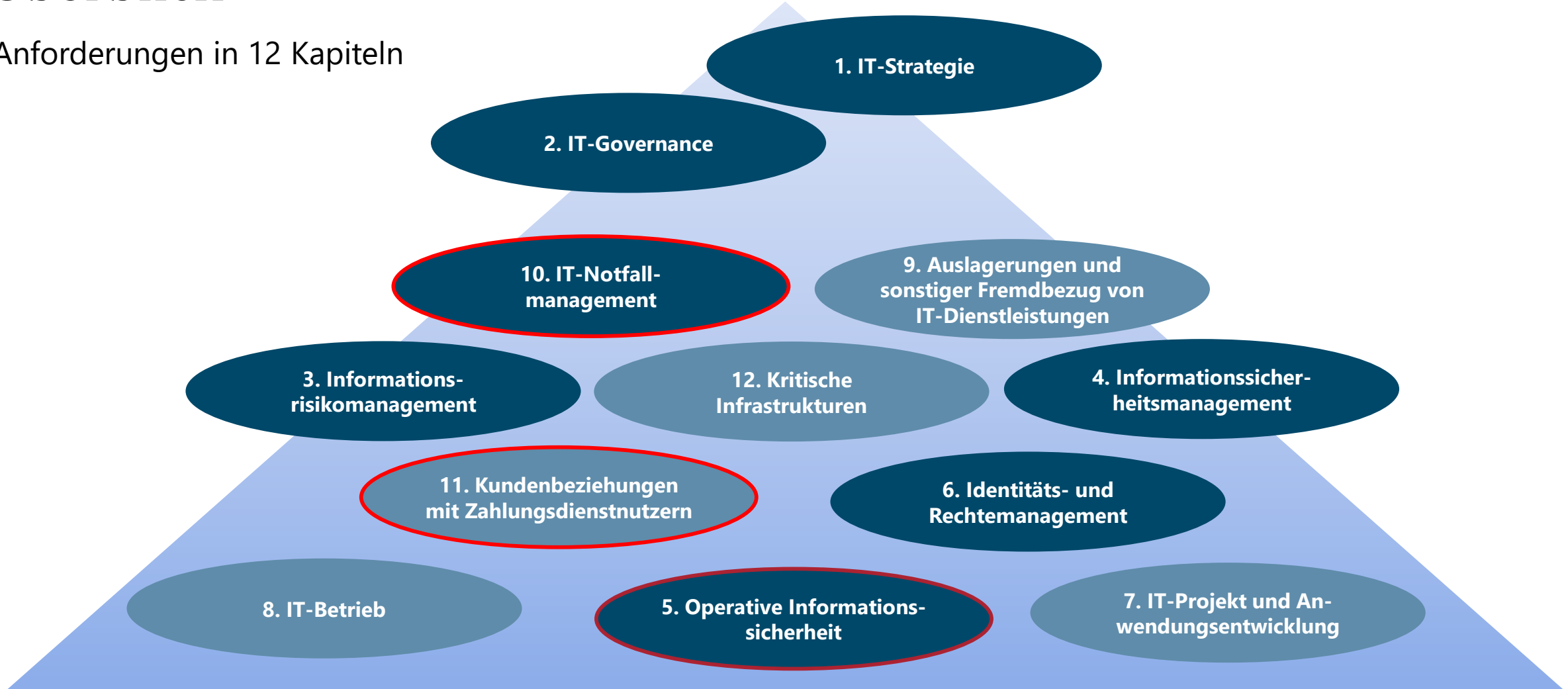


Grundprinzipien der BAIT

- Proportionalitätsprinzip: die BAIT ist zu verstehen und auf eine Weise zu erfüllen, die der **Art**, dem **Umfang** und der **Komplexität** der mit der Tätigkeit im Institut **einhergehenden Risiken** gerecht wird.
- Prinzipienorientierung: betrifft das „**wie**“ der Umsetzung der aufsichtlichen Anforderungen und räumt insoweit Spielräume für eine **individuelle Umsetzung** ein
- Technologieneutralität: **Aufsichtsrecht soll** gegenüber technologischen Entwicklungen und Geschäftsmodellen **neutral sein**, diese also weder aktiv fördern noch behindern

Überblick

Anforderungen in 12 Kapiteln



Kapitel 4. Informationssicherheitsmanagement

→ Informationssicherheitsbeauftragter

- **Wahrnehmung aller Belange der Informationssicherheit**
- Steuert und koordiniert den Informationssicherheitsprozess
- Initiiert und koordiniert die Maßnahmen-Realisierung
- Macht Ziele und Maßnahmen transparent
- Überprüft und überwacht regelmäßig deren Einhaltung
- Erstellung/Fortschreibung Informationssicherheitsrichtlinien
- **Untersucht/berichtet über Informationssicherheitsvorfälle**
- Überwachung und Hinwirkung auf Einhaltung der Informationssicherheit bei Projekten und Beschaffung

Rahmenbedingungen:

- Organisatorisch/prozessual unabhängig
- Getrennt von Bereichen für Betrieb/ Weiterentwicklung der IT-Systeme
- Keine Aufgaben der Internen Revision
- **Verpflichtung der Beschäftigten/der IT-Dienstleister: Unterrichtung des ISB über IT-sicherheitsrelevanten Sachverhalte**
- Grundsätzlich im eigenen Haus, bei Ausnahmen (gemäß Erläuterung Tz. 20)
 - Ein Gemeinsamer ISB muss die Aufgaben der Funktion in allen betreffenden Instituten gewährleisten
 - In jedem Institut ist eine zuständige Ansprechperson für den ISB zu benennen

Kapitel 5. Operative Informationssicherheit (neu)

- Tz. 5.2: Dem **Stand der Technik** **entsprechende** Informationssicherheitsmaßnahmen und Prozesse
 - Schwachstellenmanagement (1.4.6. ICT-GL)
 - Sichere Konfiguration der IT-Systeme und Netzwerkkomponenten (1.4.4.)
 - Netzwerksegmentierung (1.4.4.)
 - Kryptographie bei Speicherung und Übertragung von Daten (1.4.4.)
 - Perimeterschutz (1.4.3.)
- Tz. 5.3 bis 5.5.: Überwachung der Informationssicherheit (1.4.5.)
- Tz. 5.6: Kontrollen der Wirksamkeit der Informationssicherheit (1.4.6.)

Kapitel 5. Operative Informationssicherheit

Anknüpfungspunkte im Kapitel 4 (Strahlwirkung)

- Neu in Tz. 4.7

Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit **zeitnah zu analysieren** und **angemessene Nachsorgemaßnahmen** zu **veranlassen**.

- Neu in Tz. 4.8

Das Institut hat eine **Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit einzuführen** und diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen.

Kapitel 10. IT-Notfallmanagement (**neu**)

§ 25a Abs. 1 KWG

Nr. 5: die Festlegung eines angemessenen Notfallmanagements,
insbesondere für IT-Systeme

- Ziele und Rahmenbedingungen des IT-Notfallmanagements bauen auf dem allg. Notfallmanagement auf (siehe AT 7.3 MaRisk) → Szenarien
- IT-Notfallpläne *sind* für **alle** IT-Systeme mit **zeitkritischen** Aktivitäten / Prozessen *zu erstellen*
- IT-Notfalltests (auf Basis eines IT-Testkonzeptes)
überprüfen **jährlich** die Wirksamkeit bei zeitkritischen Aktivitäten / Prozessen
- Nachweis zu erbringen für hinreichend langen IT-Notbetrieb
→ auch aus anderem Rechenzentrum

Kapitel 11. Management der Beziehungen mit Zahlungsdienstnutzern (neu)

- Das Institut hat die Zahlungsdienstnutzer in Bezug auf alle Fragen, Unterstützungsanfragen, Benachrichtigungen über Unregelmäßigkeiten oder alle sicherheitsrelevanten Fragen hinsichtlich der Zahlungsdienste zu unterstützen
- Die den Zahlungsdienstnutzern angebotene Unterstützung und Beratung sind aktuell zu halten und an neue Risikolagen anzupassen
- Risikominderungsmaßnahmen zur Beherrschung der operationellen und sicherheitsrelevanten Risiken beinhalten auch Maßnahmen, mit denen die Zahlungsdienstnutzer für die Reduzierung, insbesondere von Betrugsrisiken, direkt adressiert werden.
 - Möglichkeit, einzelne der angebotenen Zahlungsfunktionalitäten zu deaktivieren
 - Möglichkeit, vereinbarte Betragsobergrenzen durch Zahlungsdienstnutzer anzupassen

6. Zusammenfassung

- Normgeber (EU und national) entwickeln Rechtsrahmen stetig weiter (Orientierung an der Bedrohungslage)
- **IT-/Cybersicherheit** ist stets **unmittelbare Chefsache** (im Institut und beim IT-Dienstleister)
- Bei Fragen rund um DORA, FISG-Umsetzung sowie zu den xAIT stehen BaFin und Bundesbank jederzeit zum konstruktivem Austausch zur Verfügung

... zum Schluß

Zentrales Ziel aller vorgestellten Regelungen

Schaffung einer **ganzheitlichen operationellen Resilienz**

- im Hinblick auf die **Geschäftstätigkeit der Institute und ihrer Drittdienstleister sowie**
- die **jederzeitige Sicherstellung der Versorgungssicherheit der Endkunden mit Finanzdienstleistungen**

Vielen Dank für Ihre Aufmerksamkeit!

Für Ihre Fragen steht zur Verfügung

Dr. Jens Gampe

Telefon: 0228 4108-2332

E-Mail: jens.gampe@bafin.de