BaFinTech Mit der Deutschen Bundesbank

Digital Operational Resilience Act (DORA) Was kommt auf den deutschen Finanzsektor zu?

Dr. Sibel Kocatepe, BaFin

Dominik Schäfer, Deutsche Bundesbank

BaFinTech Mit der Deutschen Bundesbank

Fragen an das Publikum

Ist ihr Unternehmen von DORA betroffen?

Haben Sie sich an der öffentlichen Konsultationen zu den Technical Standards beteiligt?

Wurden bereits Handlungsfelder bezgl. der DORA Implementierung identifiziert?

In wie weit fühlen Sie sich für DORA gewappnet?

Digital Operational Resilience Act (DORA)

Ziel 

- Die **Verordnung** über die digitale operationale Resilienz im Finanzsektor (DORA) ist die europäische Antwort auf den **digitalen Wandel** im Bereich der Finanzdienstleistungen und auf die **zunehmende Gefahr von Cyberbedrohungen** im Finanzsektor.

Fokus 

- Angemessener Umgang mit der zunehmenden **Abhängigkeit** des Finanzsektors **von Drittanbietern**
- Finanzsystem der Union in die Lage versetzen, die **Betriebsstabilität** im Falle einer schwerwiegenden Störung **aufrechtzuerhalten**

Kern 

- Umfassend **harmonisierter IT-Risikomanagement-rahmen**
- Ausweitung und Vereinheitlichung der **Meldepflichten** von schwerwiegenden IT-Vorfällen
- Schaffung eines Europäischen **Überwachungsrahmens** für **kritische IT-Drittdienstleister**

Schwerpunkte DORA

IKT-Risikomanagement (Art. 5 bis 16)

- **Verantwortung** verbleibt beim Leitungsorgan des Finanzunternehmens
- **IKT-Risikomanagement und –Governance**
- **Technische Anforderungen** (identify, protect, detect, response, recover…)

+2 RTS und 1 GL

IKT-Vorfallmeldewesen (Art. 17 bis 23)

- **IKT-Vorfallmeldewesen-prozesse**
- **Klassifikation** von IKT-bezogenen Vorfällen und Cyberbedrohungen

+1 RTS

- **Berichtswesen von schwerwiegenden IKT-bezogenen Vorfällen** (und freiwillige Meldung erheblicher Cyberbedrohungen)

+ 1 RTS, 1 ITS und Bericht

Tests der digitalen operationalen Resilienz (Art. 24 bis 27)

- **Allgemeine Anforderungen an das Testen der digitalen operationalen Resilienz**
- **Basistests**
  - Schwachstellentests etc.
  - Gesamter Finanzsektor
- **Fortgeschrittene Tests**
  - Threat Led Penetration Tests (TLPT)

➔TIBER-EU als Blaupause

+1 RTS

IKT-Drittparteirisiko-management (Art. 28 bis 44)

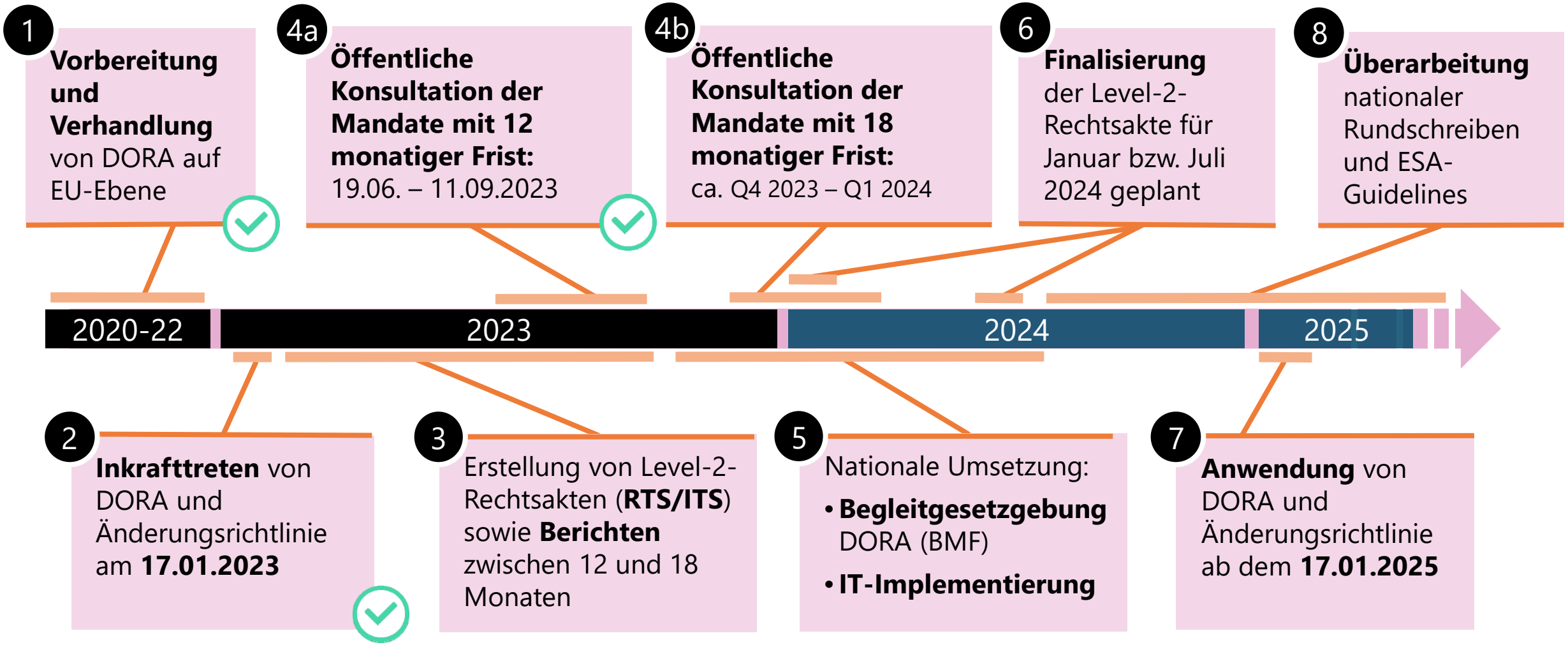
- **Allgemeine Prinzipien** (u.a. Führung eines Informationsregisters über IKT-Drittparteivertrags-beziehungen und Mindestvertragsklauseln)

+ 2 RTS und 1 ITS

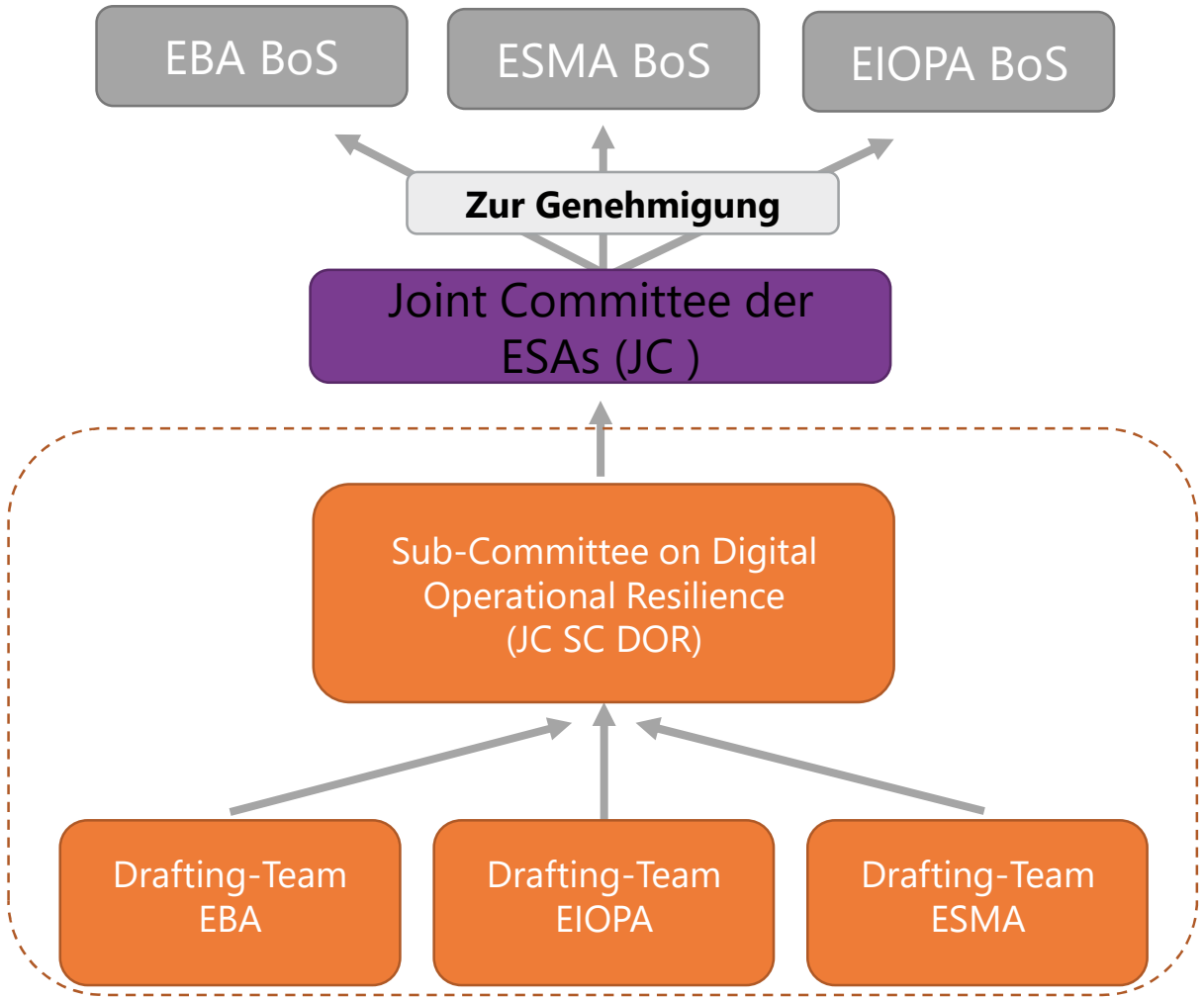
- EU-**Überwachungs-rahmenwerk** für kritische IKT-Drittdienstleister

+ 1 RTS, 1 GL und 2 CfA

Vergangenes, Aktuelles und nächste Schritte



Europäische Umsetzungsarbeiten unter DORA



- **JC SC DOR** wurde als **Unterausschuss** zum JC der ESAs eingerichtet, um die politischen Mandate der ESAs für DORA zu erstellen.
- Die **drei Drafting-Teams** sind jeweils einer ESA zugeordnet und teilen die politischen Mandate zwischen sich auf.
- **BaFin und Bundesbank** sind in den Drafting-Teams vertreten.
- **Konsultationen** der Regulierungsentwürfe ab Juni bzw. ab Q4 2023
- Die finalen Entwürfe müssen der EU-Kommission bis zum **17. Januar 2024** bzw. **17. Juli 2024** vorgelegt werden.

Europäische Umsetzungsarbeiten und Fälligkeiten

- RTS on ICT risk management framework (Art. 15)
- RTS on simplified ICT risk management framework (Art. 16.3)
- RTS to specify the policy on ICT-services (Art. 29.10)
- RTS on criteria for the classification of ICT-related incidents (Art. 18.3)
- ITS to establish the templates for the register of information (Art. 29.9)

Vorlage bei EU-Kommission bis zum 17. Januar 2024

- Öffentliche Konsultation der RTS/ITS erfolgte durch die ESAs bis zum 11. September 2023

Europäische Umsetzungsarbeiten und Fälligkeiten

- RTS to specify threat led penetration testing aspects (Art. 26.11)
- RTS to specify elements when sub-contracting critical or important functions (Art. 30.5)
- RTS on specifying the reporting of major ICT-related incidents (Art. 20.a)
- ITS to establish the reporting details for major ICT-related incidents (Art. 20.b)
- GL on the estimation of aggregated annual costs/losses caused by major ICT incidents (Art. 11.12)
- GL on cooperation between ESAs and CAs regarding the structure of the oversight (Art. 32.7)
- RTS to specify information on oversight conduct (Art. 41.2)
- ESRB recommendations

Vorlage bei EU-Kommission bis zum 17. Juli 2024

BaFinTech Mit der Deutschen Bundesbank

Schwerpunkt: Risikomanagementrahmenwerk

Verantwortung des Managements

- Management Body (bspw. Vorstand bei Banken) trägt die Verantwortung für das IKT-Risikomanagement.
- Member des Management Bodys (bspw. Vorstände bei Banken) müssen sich **aktiv bzgl. IKT-Risiken auf dem laufenden halten** und regelmäßige IKT-spezifische Weiterbildungen erhalten.

DORA Article 5 - Governance and organisation

2. The management body of the financial entity shall define, approve, **oversee and be responsible** for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).

(a) bear the ultimate responsibility for **managing the financial entity's ICT risk**;

(d) bear the overall responsibility for **setting and approving the digital operational resilience strategy**

4. Members of the management body of the financial entity shall **actively keep up to date** with **sufficient knowledge and skills** to understand and assess ICT risk and its impact on the operations of the financial entity, including by following **specific training on a regular basis**, commensurate to the ICT risk being managed.

ICT risk management control function – CISO, ISO, ISB?

- Die Funktion der ICT risk management control function ist durch den Management Body einzurichten.
- Aufgaben ähnlich denen des aus den X-AIT bekannten Informations-sicherheitsbeauftragten (ISB)
- Strenge Trennung von Control Function und First Line (IT)
- Weiterhin **starke aufsichtsrechtliche Erwartung**, den ISB im eigenem Hause vorzuhalten.

DORA Article 6 - 4. ICT risk management control function:

[...] **assign the responsibility for managing and overseeing ICT risk to a control function** and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. [...] ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.

RTS Article 2

1. c) **defining the ICT and information security objectives** and setting the qualitative and quantitative measures of their attainment, key performance indicators and key risk metrics

d) **remaining independent** from the function or functions in charge of the ICT development, management, changes and operations;

e) **monitoring the accuracy of classification** of information assets and ICT assets

Kenne deine Informationen und Systeme

RTS Article 5 ICT asset management procedure

2. […] detail the criteria to perform the criticality assessment of **information assets** and **ICT assets** supporting business functions […]

[…] take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities.

DORA Article 8 Identification

1. […] identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the **information assets and ICT assets supporting** those functions, and their roles and dependencies in relation to ICT risk. […]

- IKT-Systeme und **–Informationen**, die in Geschäftsfunktionen verwendet werden, müssen identifiziert und klassifiziert werden.
- Das betrifft besonders auch Informationen, die nicht in zentralen Systemen gehalten werden (bspw. Office-Dokumente).

Strengere Anforderungen an Verschlüsselungen

- 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.

RTS Article 6 Encryption and cryptographic controls

2. (a) […] rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification […] **If encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment** […]

b. […] encryption of internal network connections and traffic with external parties […]

Article 7 Cryptographic key management

1. […] cryptographic key management policy […] requirements for managing cryptographic keys through their whole lifecycle, including generating, storing, backing up, archiving, retrieving, transmission, retiring, revoking and destroying keys […]

Fokus voll auf Schwachstellen

RTS Article 10 Vulnerability and patch management

2. (b) […] performance of automated vulnerability scanning […] for those supporting critical or important functions it shall be performed **at least on a weekly basis**.

(c) […] ensure that **ICT third-party service providers handle** any **vulnerabilities** related to the ICT services provided to the financial entity and report them to the financial entity. […]

(d) track the **usage of third-party libraries**, including open source, monitoring the version and possible updates;

(e) establish procedures for responsible **disclosure of vulnerabilities to clients** and counterparts as well as to the public, as appropriate;

(f) deploy **patches** to address identified vulnerabilities. If no patches are available for a vulnerability, financial entities shall identify and implement other mitigation measures;

- 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.**

Detaillierte Sicherheitsanforderungen

- Sicherstellen, dass **nur autorisierte** Software und Speichermedien verwendet werden
- Gewährleisten, dass die Sicherheit auch bei Home-Office und BYOD gegeben ist
- Mitarbeiter, welche das Cloud-Interface administrieren, müssen gesondert geschult werden.
- Die Credentials zum Cloud-Interface sind besonders sicher zu schützen.

RTS Article 11 Data and system security

2. (c) […] **only authorised software** is installed in ICT systems and end point devices;

(e) […] ensure the use of **only authorised data storage media** […]

(f) […] secure the use of **portable endpoint devices** and private non-portable endpoint […]

(j) […] measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the ICT security […]

(k) for **cloud computing resources**: […] the requirement that the individual in charge of using the cloud client interface […] have **adequate competences and training** […] implement technical and organisational security measures on the **credentials** used to access the cloud client interface […]

Source Code Testing

- Fachbereiche und Asset Owner müssen u.a. Sicherheitsmaßnahmen genehmigen
- Testumgebungen sollen adäquat die Produktionsumgebung wiedergeben.
- Die Integrität des Quellcodes ist zu schützen.
- Quellcode und proprietäre Software von Dritten ist zu analysieren und zu testen.

RTS Article 16 acquisition, development, and maintenance

1 b. require the identification of functional and non-functional requirements relating to acquisition, development and maintenance of ICT systems, **including ICT security requirements and their approval by the relevant business function and ICT asset owner**

4. Financial entities shall perform **source code review** covering both static and dynamic testing. The testing shall include security testing for **internet-exposed** systems and applications.

8. Financial entities shall implement controls to protect the integrity of the source code of ICT systems that are developed in-house or by an ICT third-party service provider and delivered to the financial entity by an ICT third-parties service provider.

9. The **source code** and **proprietary software** provided by ICT third-party service providers or coming from open-source projects shall be a**nalysed and tested for vulnerabilities and for absence of malicious codes**

Netzwerksicherheit stärken

RTS Article 13 Network security management

1. (b) **mapping and visual presentation of** [...] networks/data flows

(e) [...] encryption of network connections passing over corporate networks, public networks, domestic networks, third party networks and wireless networks [...]

(g) [...] **securing the network traffic** between the internal networks and the internet and other external connections; [...]

(h) [...] definition, implementation, approval, change and review of **firewall rules and connections filters**. [...] perform the review on a regular basis [...] ICT systems supporting critical or important functions, [...] perform this review at least every six months;

(i) [...] reviews of the network architecture and of the network security design once a year [...]

(j) [...] **measures to temporarily isolate**, where necessary, subnetworks and network components and devices;

- Ein visueller Netzwerkplan muss erstellt werden.
- Netzwerkverkehr ist sowohl intern als auch extern zu schützen.
- Firewall-Regeln sind zu **rezertifizieren.**
- Jährlicher Review der Netzwerkarchitektur
- Möglichkeiten zur **temporären Isolation** von Subnetzen, Netzwerkkomponenten und Geräten sind zu schaffen.

Wer ist wer? Eindeutige Regel für Identitäten

- Jede natürliche Person soll eine eindeutige Identität erhalten, diese soll auch bei Reorganisation und nach Beendigung des Verhältnisses beibehalten werden.
- Anforderungen im Zugriffs- und Zutrittsmanagement bleiben weitestgehend gleich.

RTS Article 21 Identity Management

3. (a) A unique identity corresponding to a unique user account shall be assigned to each staff member of the financial entity or staff of the third-party service providers accessing the information assets and ICT assets of the financial entity. **These identities shall be linked to a specific natural person** also in the case of reorganisation or after the contractual relationship has ended without prejudice to the retention requirements set out in EU and national law. Financial entities **shall maintain records containing every identity assignment**.

(b) A **lifecycle management process** for identities and accounts managing the creation, change, recertification, temporary deactivation and termination of user accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process.

Konkretisierung der Testszenarien im BCM

RTS Article 27 ICT response and recovery plans

ICT response and recovery plans shall identify relevant scenarios [...]

2. (a) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities

(b) [...] quality of the provision of a critical or important function deteriorates to an unacceptable level or fails [...]

(c) partial or total failure of premises

(d) substantial failure of ICT assets or of the communication infrastructure

(e) the non-availability of a critical number of staff or key staff members

(f) natural disasters, pandemic situations and physical attacks, including intrusions and terrorist attacks

(g) insider attack

(h) political and social instability [...]

(i) widespread power outage

- Umfassende Vorgaben zum BCM in DORA
- RTS fokussiert sich auf die Mindestinhalte der Recovery Plans und auf das Testen dieser.
- Mindesttestszenarien steigen von **vier** (MaRisk) auf **neun.**

Regelmäßige Überprüfung des IKT-Rahmenwerkes

- Eine formelle Dokumentation des aktuellen Stands des IKT-Risikorahmenwerks ist zu erstellen.
- Diese muss auf Anfrage der Aufsicht aktuell zur Verfügung gestellt werden.

DORA Article 6(5)

[...] ICT risk management framework shall be **documented and reviewed at least once a year** [...] as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes

RTS Chapter V: Report on the ICT Risk Management Framework review

2. (f) description of the major changes and improvements to the ICT risk management framework since the previous review. [...]

(g) summary of the findings of the review and detailed analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period;

(h) description of the measures to address identified weaknesses, deficiencies and gaps, including all of the following:

BaFinTech Mit der Deutschen Bundesbank

Schwerpunkt: Überwachung von kritischen IKT-Drittdienstleistern

Europäische Überwachung von kritischen IKT-Drittdienstleistern

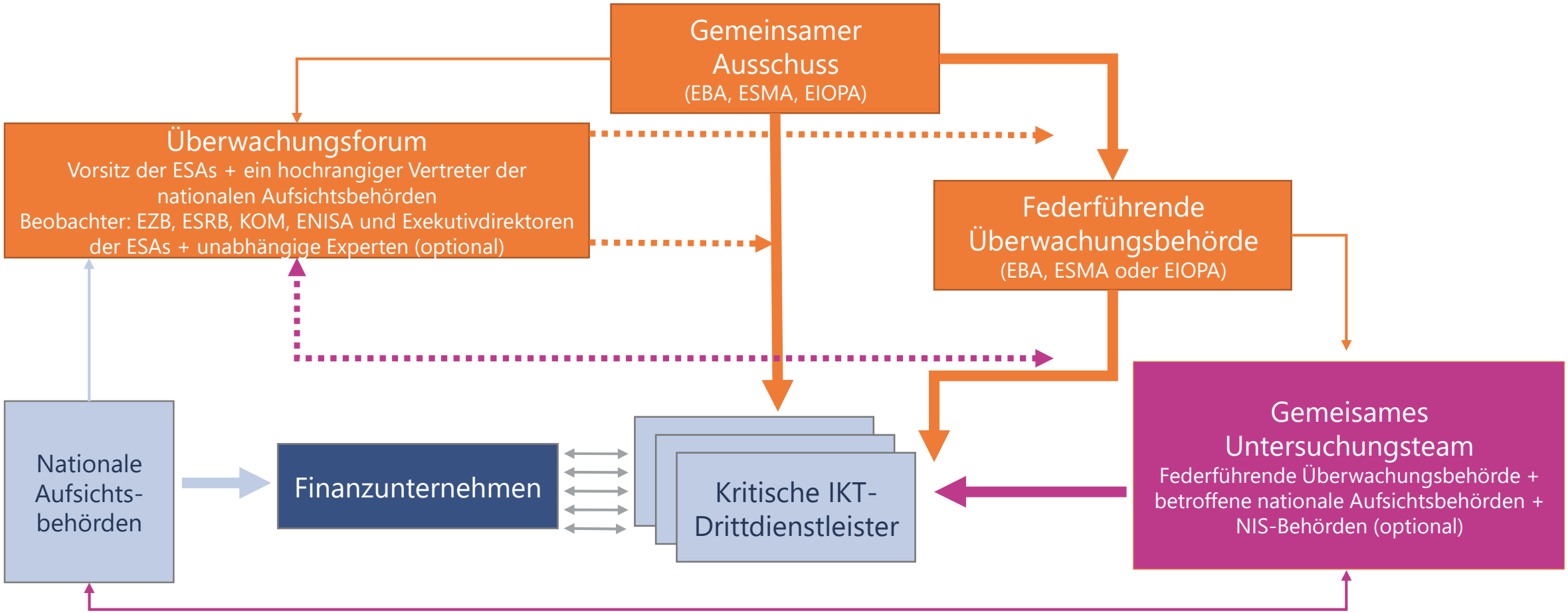
- Neues Element der EU-Finanzregulierung stellt **keine direkte Aufsicht** über kritische IKT-Drittdienstleister dar (vgl. Erwägungsgrund 76).
- **Cloud-Dienstleister** stehen ausdrücklich im Fokus von DORA (vgl. Erwägungsgrund 20):

  „Anbieter von Cloud-Computing-Diensten sind eine Kategorie digitaler Infrastruktur, die unter die Richtlinie (EU) 2022/2555 fällt. Der mit dieser Verordnung geschaffene Überwachungsrahmen der Union (im Folgenden „Überwachungsrahmen") gilt für alle kritischen IKT-Drittdienstleistungen, einschließlich Anbietern von Cloud-Computing-Diensten, die Finanzunternehmen IKT-Dienstleistungen bereitstellen (...)."
- Finanzunternehmen dürfen kritische IKT-Drittdienstleister aus Drittstaaten nur dann nutzen, wenn diese binnen zwölf Monaten nach ihrer Einstufung einen **Sitz in der EU** begründen („no emty shell").
- DORA enthält **keine** Verpflichtung zur **Datenhaltung innerhalb der EU** in DORA (vgl. Erwägungsgrund 82).

Europäische Überwachung von kritischen IKT-Drittdienstleistern

- Genaue **Kriterien für die Einstufung kritischer IKT-Drittdienstleister** werden von der EU-Kommission in einer delegierten Verordnung normiert (Konsultationsfassung: ESAs Discussion Paper on criticality criteria and oversight fees on DORA (europa.eu)).
- DORA enthält bereits erste **Grundkriterien** (vgl. Art. 31 Abs. 2):
  - Systematische Auswirkungen der Zusammenarbeit mit einem IKT-Drittdienstleister auf die Stabilität, Kontinuität oder Qualität der Services des Finanzunternehmens
  - Systemrelevanz der Finanzunternehmen, die den IKT-Drittdienstleister nutzen
  - Abhängigkeit der Finanzindustrie vom IKT-Drittdienstleister und dessen Substituierbarkeit
- **Einstufung** wird ab 2025 im Einzelfall auf Grundlage der **Informationsregister** der Finanzunternehmen und der **Kritikalitätskriterien** der EU-Kommission erfolgen.
- **Rein national** oder **gruppenintern** tätige IKT-Drittdienstleister bleiben von der Überwachung **ausgenommen**.
- IKT-Drittdienstleister können sich auch **auf Antrag überwachen** lassen.

Europäische Überwachung von kritischen IKT-Drittdienstleistern



Europäische Überwachung von kritischen IKT-Drittdienstleistern

- Die aufsichtliche Überwachung auf europäischer Ebene erfolgt u.a. durch folgende **Befugnisse** gegenüber kritischen IKT-Drittdienstleistern (vgl. Art. 35 ff.)
  - Anforderung von **Informationen und Unterlagen**
  - Durchführung von **Prüfungen**
  - Abgabe von **Empfehlungen**, z. B. im Hinblick auf die Anwendung relevanter spezifischer IKT-Sicherheits- und Qualitätsanforderungen und risikobehafteter Weiterverlagerungen
  - Verhängung von **Zwangsgeldern** (bis zu einem Prozent des weltweiten Tagesumsatzes des vergangenen Geschäftsjahrs)
  - ggf. **Veröffentlichung** der verhängten **Zwangsgelder**
  - ggf. **Veröffentlichung** von Informationen über nicht erfolgte oder nicht ausreichende Reaktion auf ausgesprochene **Empfehlungen** (unter Nennung der Identität und Art und Wesen der Nichtkonformität)
- Die Überwachung kritischer IKT-Drittdienstleister durch die Aufsicht **entbindet Finanzunternehmen nicht** von ihrer **Pflicht zur Überwachung** des Dienstleisters.

Europäische Überwachung von kritischen IKT-Drittdienstleistern

- **Folgemaßnahmen der Finanzunternehmen** nach Aussprache einer Empfehlung an den kritischen IKT-Drittdienstleister stehen unter Aufsicht der nationalen Aufsichtsbehörden (vgl. Art. 42).
- Nationale Aufsichtsbehörden prüfen, wie die Finanzunternehmen die in den Empfehlungen festgestellten **Risiken** beim kritischen IKT-Drittdienstleister im Rahmen ihres **Drittparteirisikomanagements** berücksichtigen.
- Bei **nicht oder nicht ausreichender Berücksichtigung der Risiken** durch Finanzunternehmen, teilt die nationale Aufsichtsbehörde 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**.

Praxishinweise zu DORA

- Die Finanzunternehmen sollten sich auf die neuen Anforderungen durch **DORA vorbereiten**:
  - **Lektüre** der Verordnung und der Konsultationsfassungen der RTS/IST/Guidelines, einschließlich der Erwägungsgründe
  - **Gegenüberstellung der Anforderungen** aus DORA mit bestehenden regulatorischen Anforderungen (z. B. MaRisk, BAIT, EBA Guidelines on outsourcing arrangements, BaFin Orientierungshilfe Cloud)
  - **GAP-Analyse** unter Berücksichtigung des eigenen Reifegrads der operationalen Resilienz
  - Beteiligung an den für Q4 2023 geplanten **Konsultationen** der delegierten Rechtsakte
  - **Finalisierung** und **Priorisierung** des individuellen Handlungsbedarfes nach Veröffentlichung der noch ausstehenden delegierten Rechtsakte.
- Die Aufsicht wird in naher Zukunft mit der **Überarbeitung aufsichtlicher Anforderungen** mit Blick auf DORA beginnen.

BaFinTech Mit der Deutschen Bundesbank

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Sibel Kocatepe, BaFin, Sibel.Kocatepe@bafin.de

Dominik Schäfer, Bundesbank, Dominik.Schaefer@bundesbank.de