DEUTSCHE BUNDESBANK
EUROSYSTEM

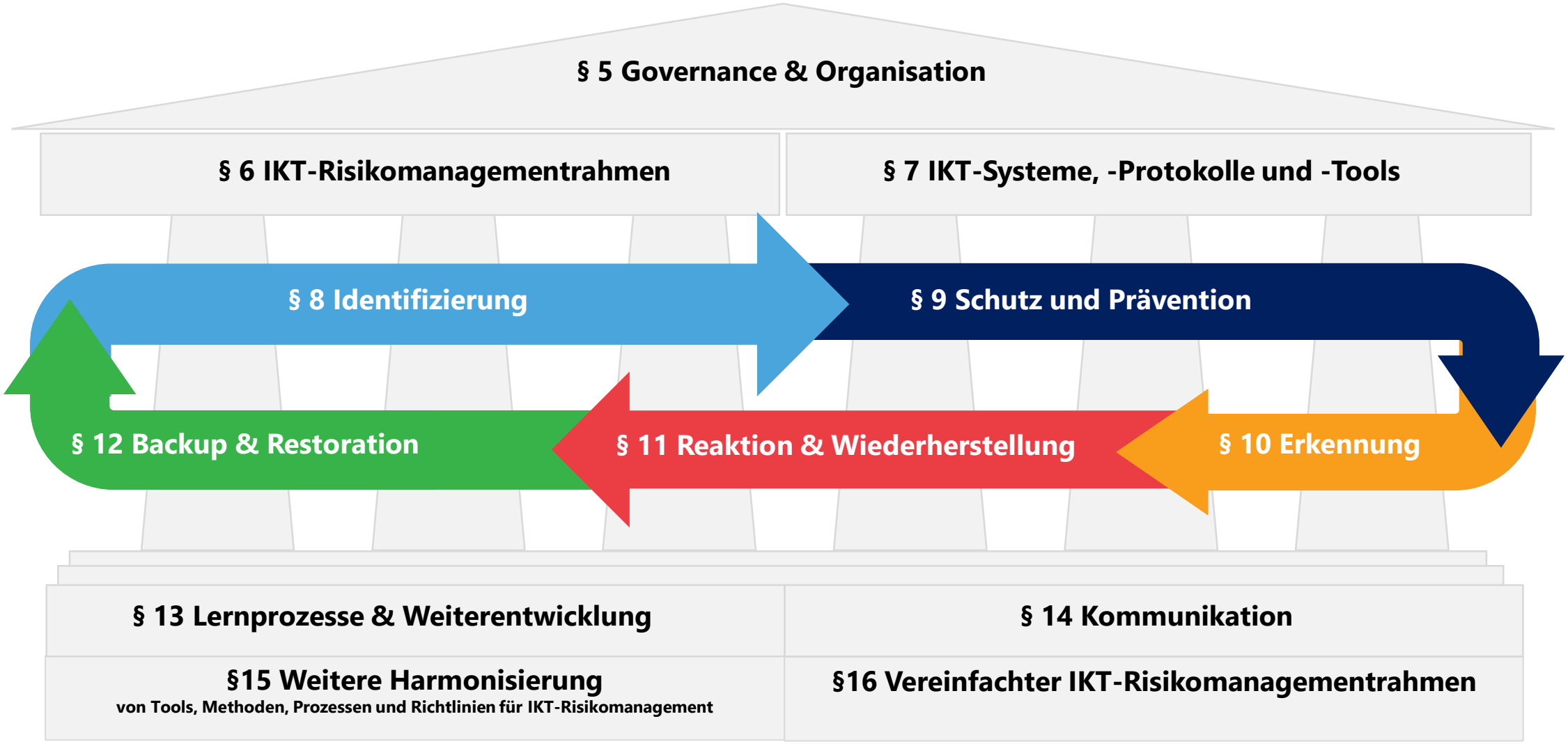
BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Was bedeutet DORA in der Praxis?

Highlights im IKT-Risikomanagementrahmenwerk

Jan Kiefer (BaFin), Dominik Schäfer (Deutsche Bundesbank)

Was ist das IKT-Risikorahmenwerk nach DORA?



Risikokontrollfunktion und Systeme, Protokolle und Tools

IKT-Risikokontrollfunktion

DORA Artikel 6 (4)

Finanzunternehmen (FU) übertragen die **Zuständigkeit für das Management und die Überwachung des IKT-Risikos** an eine Kontrollfunktion und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden.

IKT-Systeme, -Protokolle und -Tools

DORA Artikel 7

Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten FU **stets auf dem neuesten Stand zu haltende** IKT-Systeme, -Protokolle und –Tools die (a) **angemessen**, (b) **zuverlässig**, (c) **mit ausreichenden Kapazitäten ausgestattet** und (d) **technologisch resilient** sind.

Weitere Harmonisierung - der Regulatory Technical Standard

ICT security policies, procedures, protocols and tools

- Provisions on governance ★
- ICT risk management ★
- ICT asset management ★
- Encryption and cryptography ★
- ICT operations security ★
- Network security ★
- ICT project and change management ★

Human resources policy and access control

ICT-related incident and detection and response ★

ICT business continuity management ★

Report on the ICT risk management framework

★ Highlight

Fokus des Rahmenwerks und die DOR-Strategie

- Im **Zentrum der Betrachtung** steht **nicht der Prozess**, sondern die eingesetzten **Technologien** und **Daten** (Information- and ICT-Assets/Data).
- **Sicherheitsziele** werden explizit in **Bezug zu Daten** erwähnt.
- Die **DOR-Strategie** ist **nicht** gleichzusetzen mit der **IT-Strategie.**
- **Keine Aussage zum IT-Notfallmanagement** in der **DOR-Strategie.**

Draft RTS RMF:
Article 1 General elements of ICT security

1. […] Financial entities shall establish the ICT security policies, procedures, protocols and tools laid down in Chapter I **with a view** to ensuring the **security of networks**, enable adequate **safeguards against intrusions** and **data misuse**, preserve the **availability, authenticity, integrity and confidentiality of data**, including cryptographic techniques, and guarantee an **accurate and prompt data transmission** without major disruptions and undue delays. […]

2. […] Financial entities shall ensure that the ICT security policies referred to in paragraph 1: are aligned to the financial entity's information security objectives included in **the digital operational resilience strategy** referred to in Article 6(8) of Regulation (EU) 2022/2554;

Akzentverschiebung und neue Funktion

- **Akzentverschiebung** durch **stärkere Betonung** des **IKT-Risikomanagements** vs. **Informationssicherheit.**
- Einführung einer **IKT-Risikokontrollfunktion**, welche **Elemente des ISB** enthält, aber nicht identisch ist.
- Das **Zusammenspiel** von **Risikomanagement und ISB** ist nicht ausgeführt. Lediglich die **Unabhängigkeit** der Funktion **wird betont**.
- **Das Leitungsorgan** wird **stark** in die Prozesse des RMF **eingebunden.**
- **Betonung der Schulungspflichten**, Notwendigkeit von rollenspezifischen Schulungen, auch **für das Leitungsorgan.**

Draft RTS RMF:
Article 3 ICT Risk Management

[...] The ICT risk management policies and or procedures concerning ICT risk management shall include all of the following:[...] **risk tolerance level** for ICT risk [...]
[...] conduct the **ICT risk assessment** [...]
[...] ICT **risk treatment measures** [...] **changes** that could **affect** its overall **ICT risk profile** [...]

DORA
Artikel 6(4)

[...]FU sorgen für eine **angemessene Trennung** und **Unabhängigkeit** von **IKT-Risikomanagementfunktionen**, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle. [...]

Informations- und IKT-Assets sind zentrale Elemente

- **Informations- und IKT-Assets** sind ein **zentrales Element** der **Risikobewertung in DORA.**
- Die **Identifizierung** und **Klassifizierung** (Schutzbedarf) **von Informations- und IKT-Assets** steht am Anfang der Risikobestimmung. Das Mapping auf die Geschäftsprozesse erfolgt nachgelagert.
- **IKT-Systeme und –Informationen**, die **in Geschäftsfunktionen** verwendet werden, **müssen identifiziert und klassifiziert werden**.
- **Wechselwirkung** der **ICT-Assets untereinander** und Verbindung zu den Geschäftsfunktionen müssen berücksichtigt werden.
- **ICT-Assets** müssen **nach Change neu bewertet** werden.

Draft RTS RMF:
Article 4 ICT Asset Management Policy
[...] policy on management of **ICT assets necessary**, with a **view to preserving** the **availability, authenticity, integrity and confidentiality of data**. [...]

Article 5 ICT Asset Management Procedure
[...] 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** [...] impact [...]business processes and activities of the financial entity.

DORA: Artikel 8(4)
Finanzunternehmen ermitteln **alle Informations- und IKT-Assets** [...] **und erfassen diejenigen, die als kritisch gelten**. [...] sowie die **Verbindungen und** Interdependenzen zwischen den verschiedenen **Informations- und IKT-Assets**. [...]

Neue Anforderungen an Quellcodeanalyse und Changes

- **Quellcode von Dritten und proprietäre Software ist** künftig **auf Verwundbarkeiten und Anomalien zu überprüfen**.
  - Dies betrifft z. B. auch **Software**, welche von **Cloud-Anbietern** bereitgestellt wird.
- **DORA** nennt **keine Wesentlichkeitsgrenze für Änderungen**. Somit müssen **alle Änderungen** den in Artikel 17 beschrieben **Prozess durchlaufen**.
- **Legacy Systeme** müssen **mindestens einmal jährlich** und bei **jeder Änderung** bzgl. des **IKT-Risikos neu untersucht** werden.

Draft RTS RMF:
Article 16 ICT systems acquisition, development, and maintenance
[...] that the **source code and proprietary software** provided by **ICT third-party service providers** or coming from **open-source projects** shall be **analysed and tested**, in accordance with paragraph 3 prior to their deployment in the production environment. [...]

Article 17 ICT change management
[...] ICT **change management procedures**, in respect of **all changes to software, hardware, firmware components, systems or security parameters** [...]

DORA: Artikel 8(7)
FU [...] führen für **alle IKT-Altsysteme** regelmäßig, **mindestens** jedoch **einmal jährlich** und in jedem Fall vor und nach Anschluss von Technologien, Anwendungen oder Systemen eine spezifische Bewertung des IKT-Risikos durch.

Zusammenspiel zwischen Anomalie und Incident

- **FU müssen** eine **Anomalieerkennung implementieren**.
- Die Begrifflichkeiten **Events oder Problems werden in DORA nicht verwendet**.
- Der **Schwellenwert**, der einen durch eine **Anomalie** ausgelösten Alarm **zu einem Incident** werden lässt, **ist durch das FU zu bestimmen**.
  - **DORA nennt** hierfür **Trigger**, welche eine Behandlung im Incident-Management auslösen (**data loss, malicious activity, unavailiblity**…)

Draft RTS RMF:
Article 24 Anomalous activities detection and criteria for ICT-related incidents detection and response

[…] **detect anomalous activities** that can **result in ICT network performance issues and ICT-related incidents** […] financial entities shall **implement detection mechanisms.**

[…] implement **tools generating alerts** for **anomalous activities and behaviour**, **at least for ICT assets and information assets supporting critical or important functions.** This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies **affecting the completeness and the integrity of the data sources or, monitor thelog collection and issue an alert if the log collection failed** […]

Verschlüsselung von Daten auch während der Verarbeitung

- Daten sind entsprechend ihrer **Kritikalität** in allen Zuständen zu **verschlüsseln** (at rest, in transit & in use).
  - Falls Verschlüsselung während der Verarbeitung nicht möglich ist, müssen die Daten in **separierten und besonders Geschützen** Umgebungen verarbeitet werden oder **anderer geeigneter Maßnahmen** getroffen werden.
- Regeln für die Verschlüsselung von internem und externem Netzwerkverkehr sind zu treffen.
- Für **kryptographische Schlüssel** ist ein Lifecycle-Management einzurichten.

Draft RTS RMF:
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 or take other equivalent measures**[…]
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 […]

Zeitnahe Erkennung und Behandlung von Schwachstellen

- FU müssen über die sie betreffenden Schwachstellen bei ihren **Dienstleistern** informiert werden und auch **selbst** ihre Schwachstellen an Kunden und Partner **angemessen kommunizieren**.
- Anforderungen an **automatisierte Schwachstellenscans** und die Behebung von Schwachstellen sind gestiegen, ICT-Assets, die kritische oder wichtige Funktionen unterstützen, müssen **wöchentlich gescannt** werden.
- Bei der Behebung von Schwachstellen sind **Patches prioritär** gegenüber anderen Maßnahmen zu installieren.
- FU müssen die **Priorisierung** nach **Kritikalität** der **Schwachstelle** und des betroffenen **Assets** durchführen.
- **Fremdbezogene Softwarekomponenten** sind ebenfalls regelmäßig auf **Schwachstellen** zu **überprüfen** (Lieferkettenrisiko).

Draft RTS RMF:
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;

Netzwerksicherheit stärken

- **Detaillierung**, welche Arten von Netzwerkverkehr zu **verschlüsseln** sind, bspw. auch lokale Netzwerke.
- Für **Firewallregeln** ist ein **Lebenszyklus** einzurichten, Firewallregeln, die den Netzwerkverkehr von kritischen oder wichtigen Funktionen steuern, sind **halbjährlich** zu **rezertifizieren**, alle anderen jährlich.
- Die gesamte **Netzwerkarchitektur** ist mindestens einmal im Jahr einem **vollständigen Review** zu unterziehen.
- Möglichkeiten zur **temporären Isolation von Subnetzen**, Netzwerkkomponenten und Geräten sind zu schaffen.

Draft RTS RMF:
Article 13 Network security management
(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;

Konkretisierung der Testszenarien im BCM

- DORA legt bereits im Verordnungstext viele Anforderungen an die Reaktion und Wiederherstellung fest. Dazu ist eine IKT-Geschäftsfortführungsleitlinie zu implementieren.
- Der RTS fokussiert sich insbesondere auf das Testen und die **Mindestinhalte der Wiederherstellungspläne**.
- Tests sind auf Basis von **realistischen Szenarien** durchzuführen, dabei sind auch die **Services von IKT-Drittdienstleistern** einzubeziehen.
- Für kritische und wichtige Funktionen ist zu testen, ob der **Switch-Over zu einem Backup-Rechenzentrum funktioniert**.
- Die definierten **Mindesttestszenarien,** die zu Betrachten sind, sind im Vergleich zur MaRisk von **vier auf neun gestiegen**.

Draft RTS RMF:
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

Vielen Dank für Ihre Aufmerksamkeit!