BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Incident-Meldewesen

Michael Göddecke, Referat GIT 2
Incident Reporting, Überwachung IT-MMDL und Krisenprävention

Geltungsbereich des Kapitels III

- Alle Finanzunternehmen

➔ gilt <u>nicht</u> für IKT-Drittdienstleister *(Buchstabe u)*

> **DORA Art. 2 (2):**
> *Für die Zwecke dieser Verordnung werden die in Absatz 1 Buchstaben a bis t genannten Unternehmen zusammen als „Finanzunternehmen" bezeichnet.*

- Lex specialis zur NIS-2-Richtlinie

➔ Vermeidung von Doppelmeldungen

> **DORA Erwägungsgrund 16:**
> *[…]*
> *Folglich verkörpert diese Verordnung eine Lex specialis zur Richtlinie (EU) 2022/2555.*
> *[…]*

Gegenstand der Berichterstattung

IKT-bezogener Vorfall (DORA Art. 3 Nr. 8)

- Nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse
- Beeinträchtigt die Sicherheit der Netzwerk- und Informationssysteme
- Hat nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf erbrachte Dienstleistungen

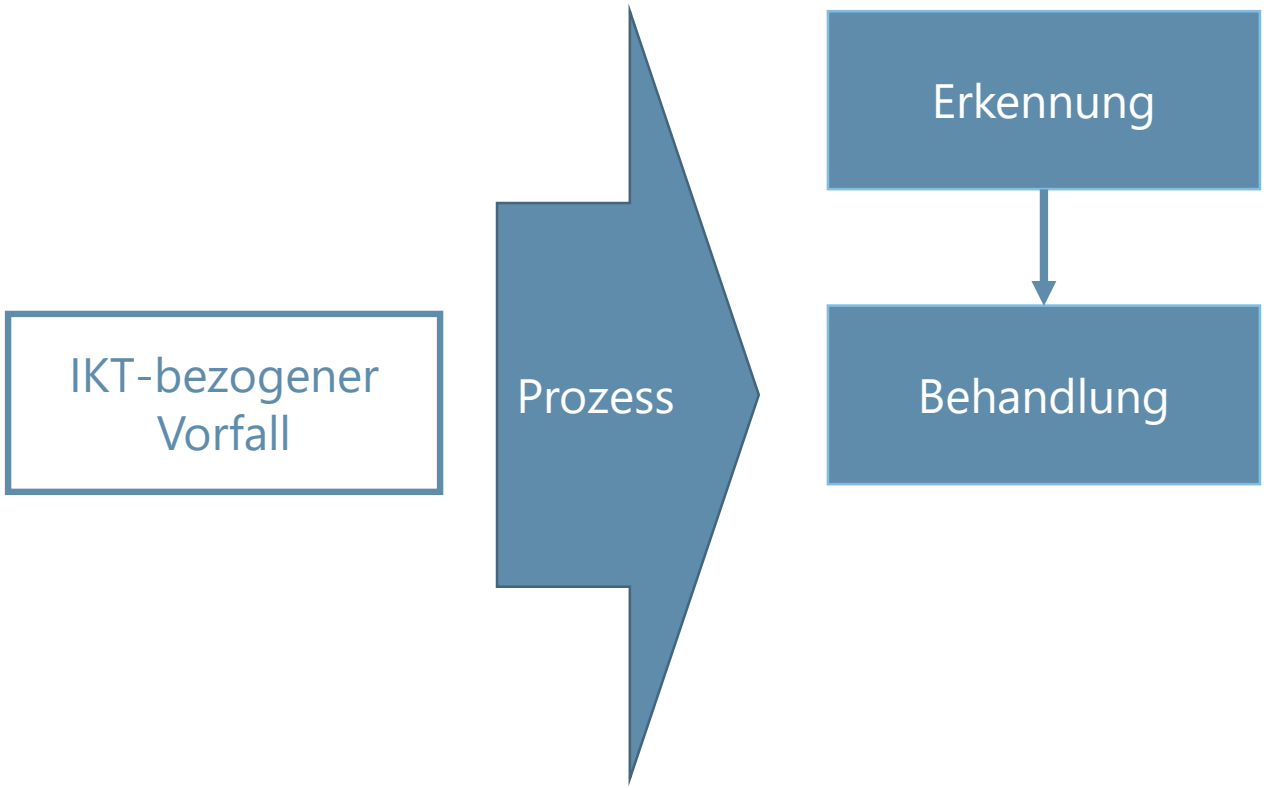
Schwerwiegender IKT-bezogener Vorfall (DORA Art. 3 Nr. 10)

- Umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen

Sicherheit von Netz- und Informationssystemen (NIS-2 Art. 6 Nr. 2):

***Fähigkeit von Netz- und Informationssystemen**, auf einem bestimmten Vertrauensniveau alle **Ereignisse abzuwehren**, **die** die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter **Daten oder** der **Dienste**, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, **beeinträchtigen können**.*

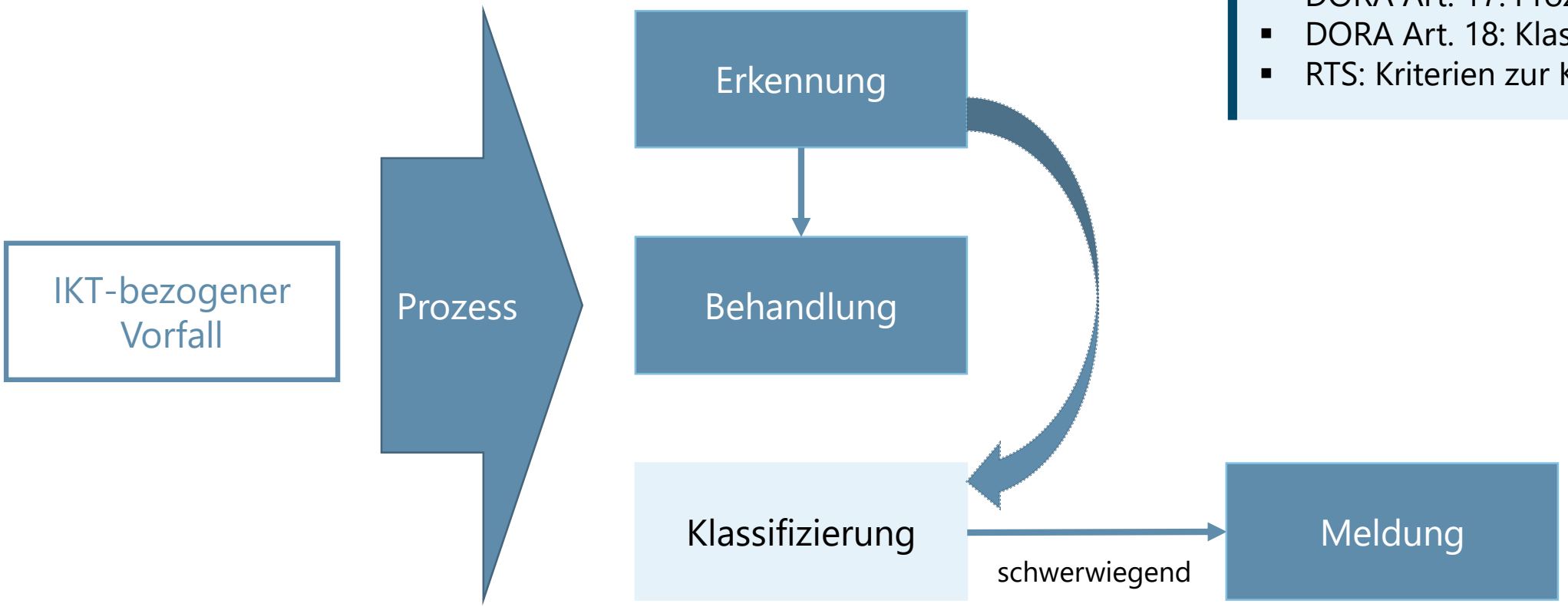
Kapitel III: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle



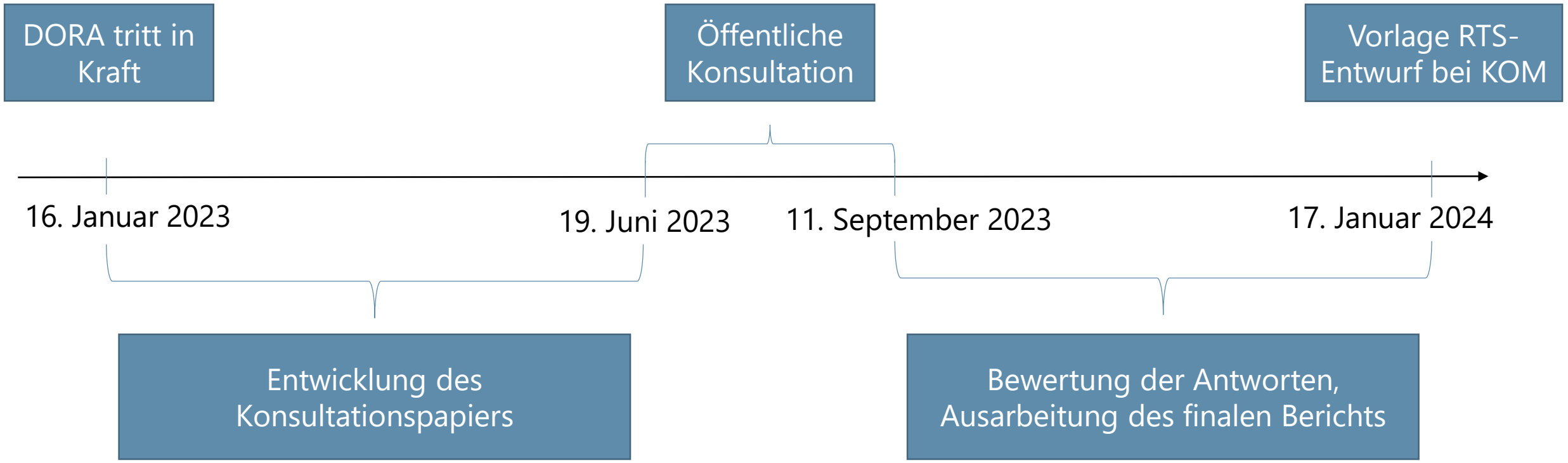
- DORA Art. 17: Prozess

Kapitel III: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

- DORA Art. 17: Prozess
- DORA Art. 18: Klassifizierung
- RTS: Kriterien zur Klassifizierung



Umsetzungszeitplan RTS Klassifizierung (Art. 18 (3) DORA)



Klassifizierungskriterien (I)

Kunden, finanzielle Gegenparteien und Transaktionen

- **Kunden** die den Service nicht nutzen konnten
- **Finanzielle Gegenparteien**
- Betroffene **Transaktionen**
- Als **relevant** identifizierte Kunden oder finanzielle Gegenparteien

Auswirkungen auf die Reputation

- Vorfall **in den Medien präsent**
- **Beschwerden** bezüglich betroffener Services
- Nicht-Einhaltung **aufsichtlicher Anforderungen**
- **Verlust von Kunden oder finanziellen Gegenparteien**

Duration und Dienst-Ausfallzeit

- **Dauer** des Vorfalls
- **Dienstausfallzeit**

Geografische Ausbreitung

- **Auswirkungen in andern Mitgliedsstaaten** z. B. bezüglich:
  - Kunden und finanziellen Gegenparteien
  - Niederlassungen oder Gruppenunternehmen
  - Finanzmarktinfrastrukturen oder Drittparteien

Klassifizierungskriterien (II)

VIVA-Verlust von Daten

- **VIVA-Verlust:**
  - **V**ertraulichkeitsverlust
  - **I**ntegritätsverlust
  - **V**erfügbarkeitsverlust
  - **A**uthentizitätsverlust

Kritikalität der betroffenen Dienste

- IKT-Dienste, die **kritische oder wichtige Funktionen** unterstützen

Wirtschaftliche Auswirkungen

- Nennung mehrerer **Kostenarten**
- **Direkte und indirekte Kosten** und Verluste

Wiederkehrende Vorfälle

- **Für sich alleine genommen nicht schwerwiegend, aber in Summe**

Inhalte RTS und ITS gemäß Art. 20 DORA

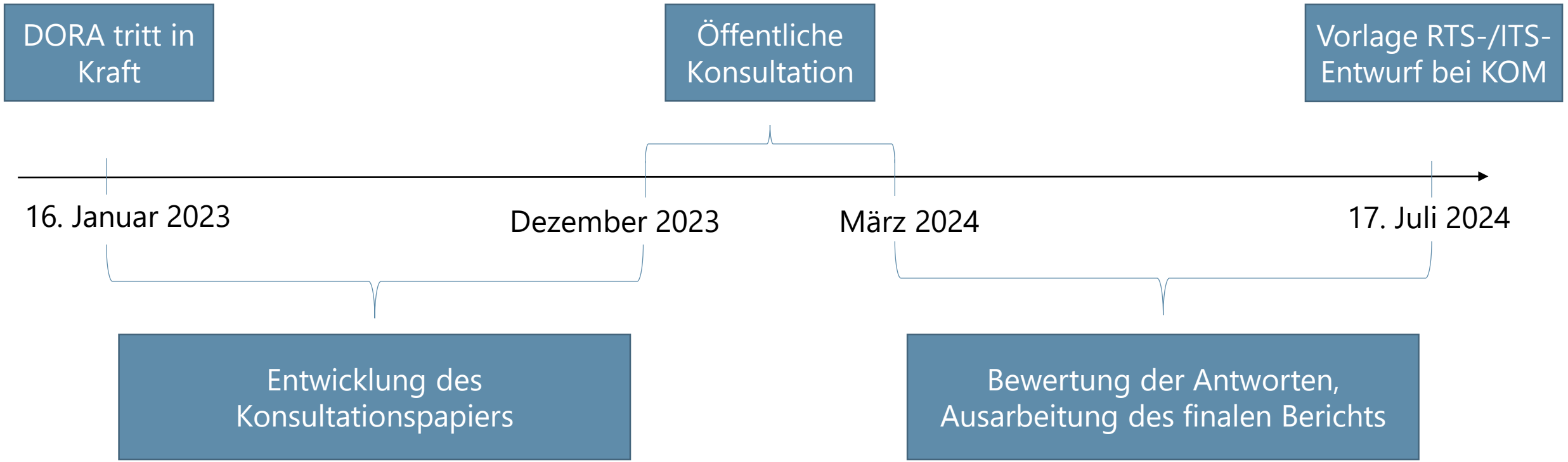
RTS regelt:

- Inhalte der Erst-, Zwischen- und Abschlussmeldungen
- Fristen zur Meldungsabgabe
- Inhalte freiwillige Meldung Cyberbedrohungen

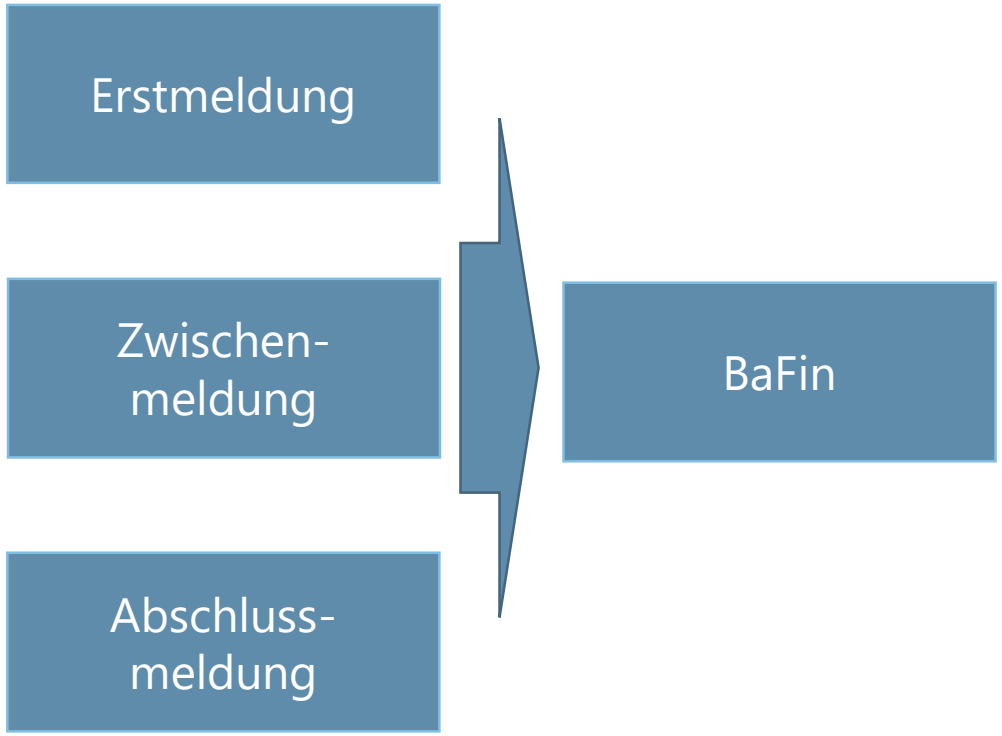
ITS regelt:

- Formulare, Vorlagen und Meldeverfahren

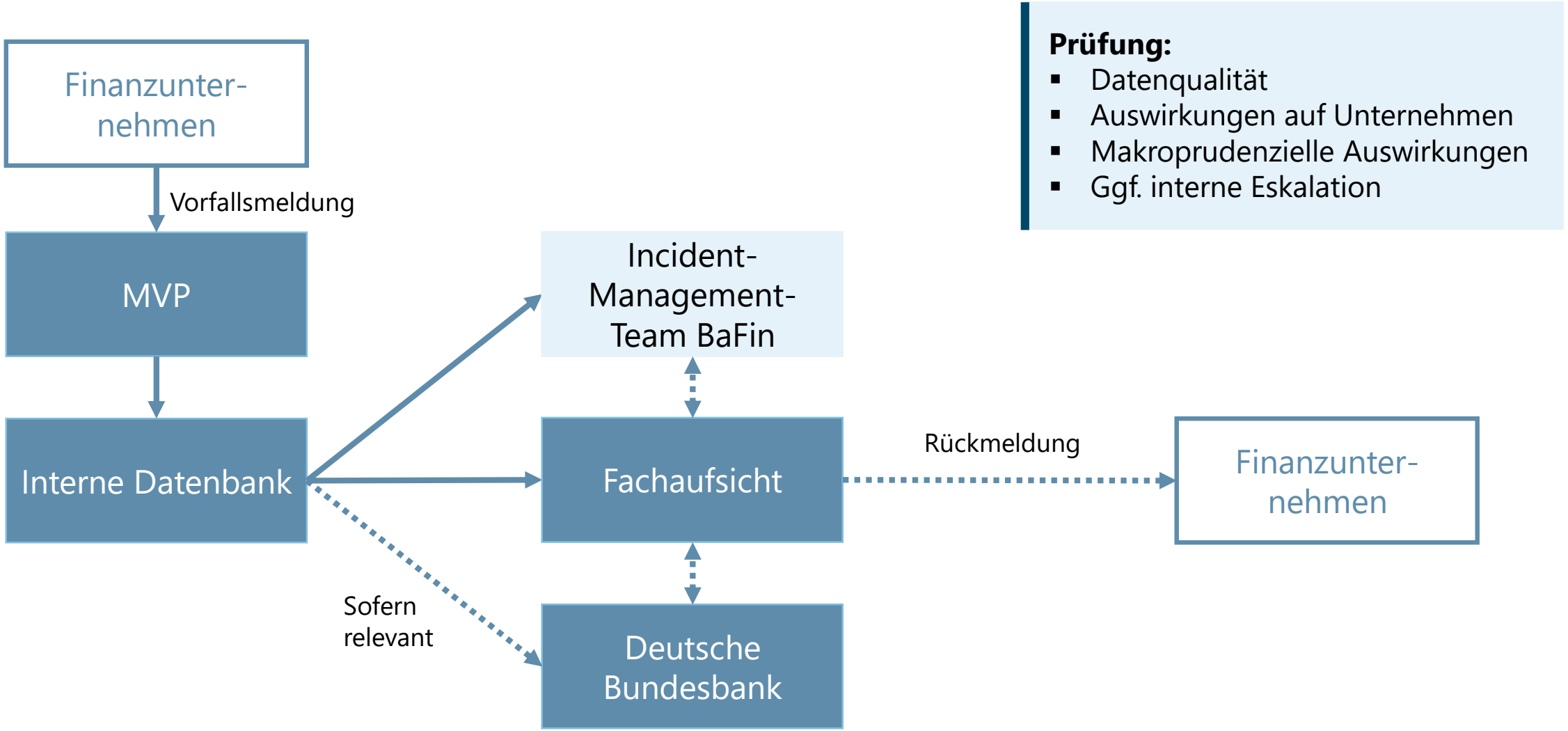
Umsetzungszeitplan RTS-/ITS-Inhalt und Formulare (Art. 20 DORA)



Meldeprozess

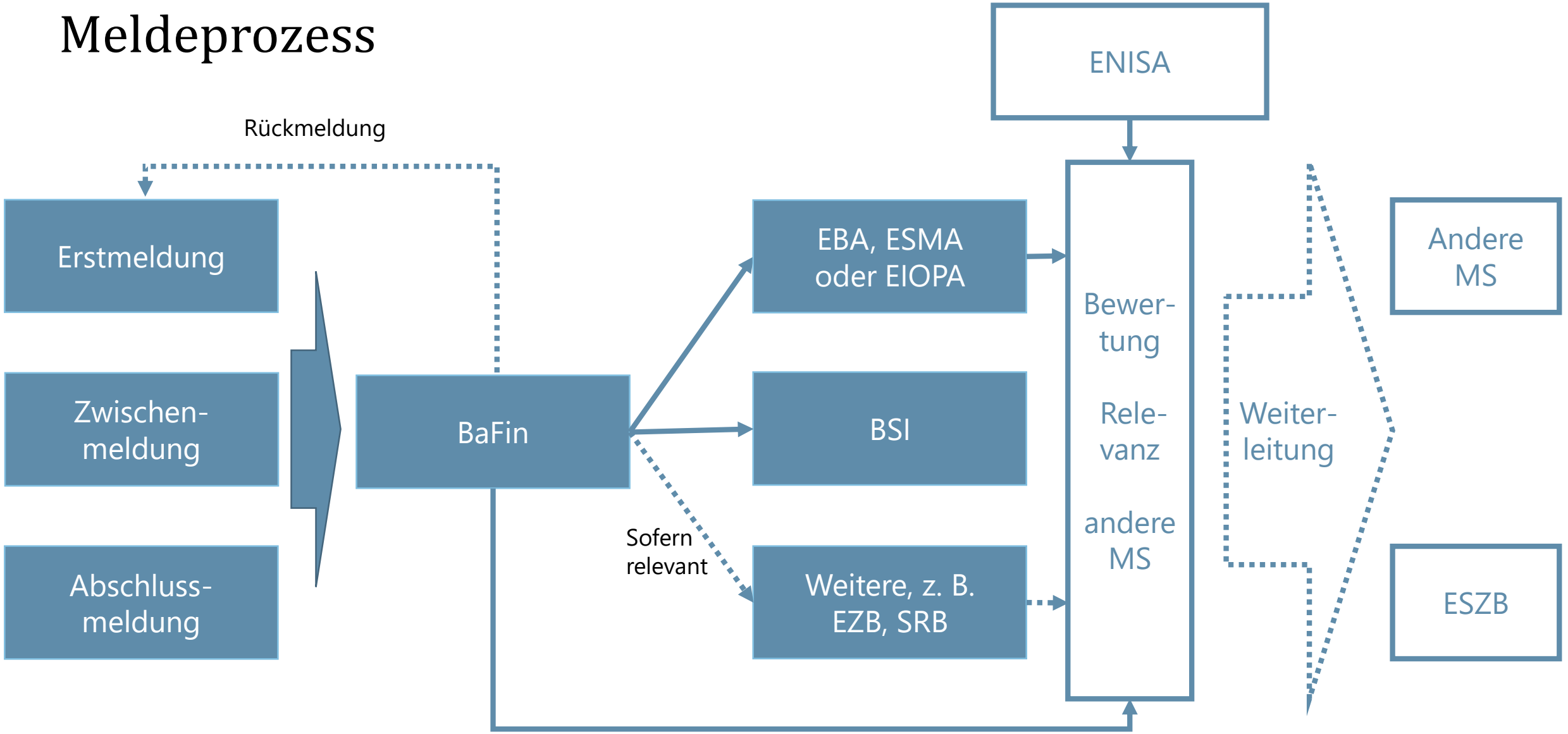


Vorgesehener BaFin Prozess (vereinfacht)



Prüfung:
- Datenqualität
- Auswirkungen auf Unternehmen
- Makroprudenzielle Auswirkungen
- Ggf. interne Eskalation

Meldeprozess



Cyberbedrohungen

Meldung von Cyberbedrohungen:

- Freiwillige Meldung
- Eigenes Meldeformular
- Weitergabe an andere Behörden möglich

DORA Art. 19 (2)
Finanzunternehmen können der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist. Die jeweils zuständige Behörde kann derartige Informationen anderen in Absatz 6 genannten einschlägigen Behörden zur Verfügung stellen. […]

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Vielen Dank für Ihre Aufmerksamkeit!