Welcome to the 26th Investmentforum

Breakout Session
Update Investmentrecht

pwc

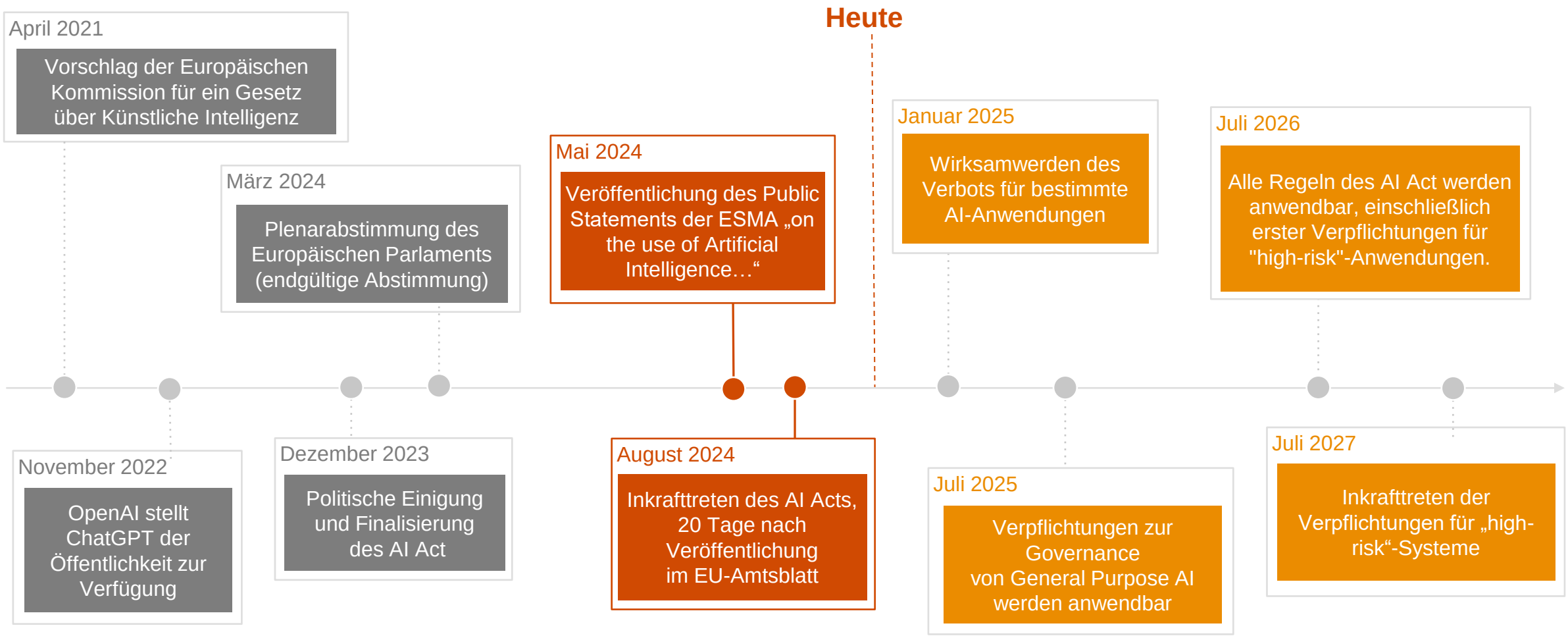
Frankfurt

26th September 2024

1

Regulatorische Anforderungen an Künstliche Intelligenz

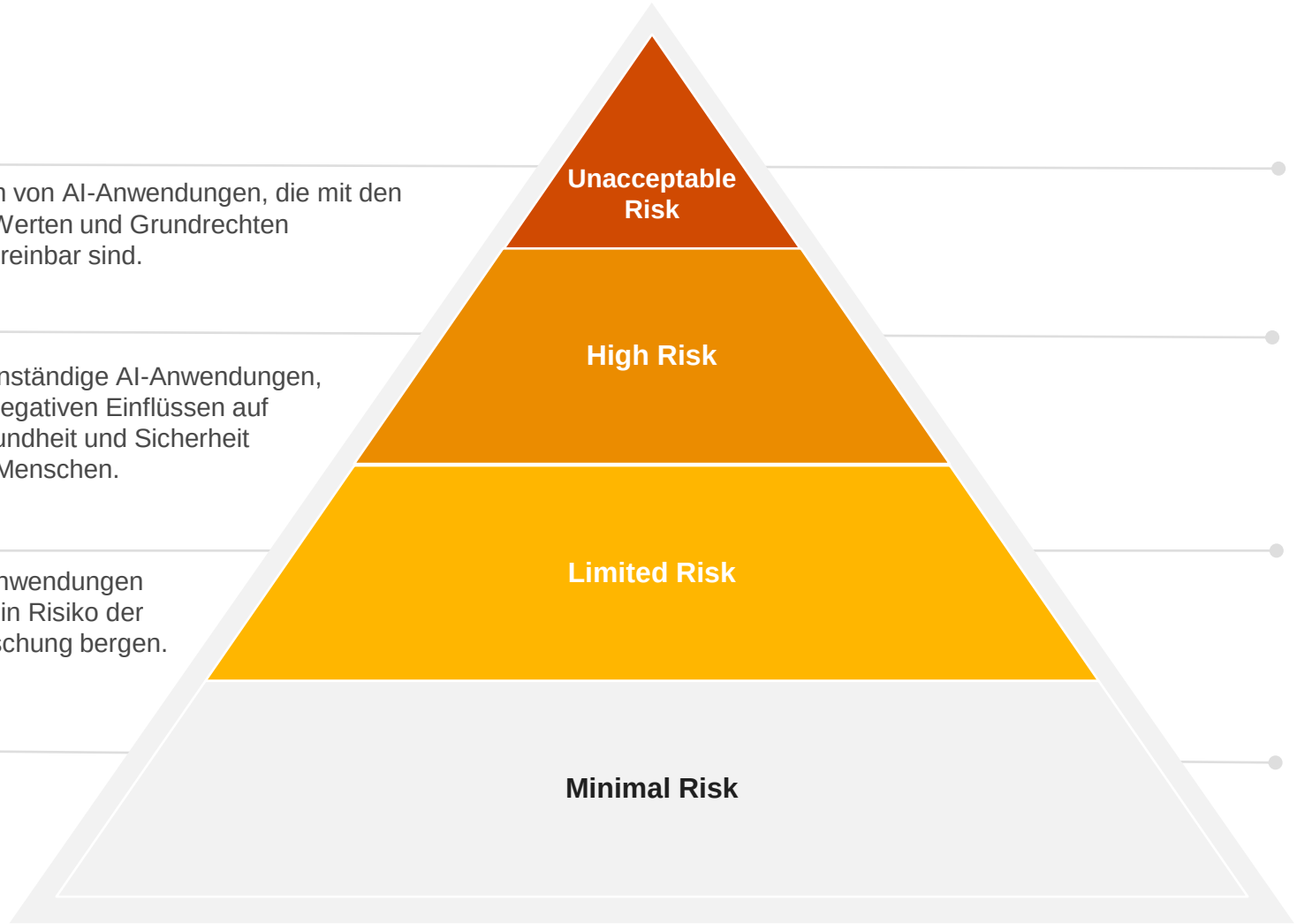
Der Artificial Intelligence Act ist im August 2024 als weltweit erste Regulierung von Künstlicher Intelligenz in Kraft getreten



Der AI Act kategorisiert AI-Anwendungen in vier Gruppen

Verbotene Anwendungen

Arten von AI-Anwendungen, die mit den EU-Werten und Grundrechten unvereinbar sind.



Beispiele:
- Social Scoring
- Verhaltensmanipulation

Konformitäts-bewertung

Eigenständige AI-Anwendungen, mit negativen Einflüssen auf Gesundheit und Sicherheit von Menschen.

Beispiele:
- Analyse von Bewerbungen und Bewertung von Kandidat:innen
- Kreditwürdigkeitsprüfungen

Transparenz-anforderungen

AI-Anwendungen die ein Risiko der Täuschung bergen.

Beispiele:
- Chatbots
- ChatGPT

Keine Auflagen/ Selbstregulierung

Beispiele:
- Spamfilter
- AI-Videospiele

Die Anforderungen an KI-Systeme unterscheiden sich nach ihrem Risikogehalt

Limited-Risk-AI-Systeme

- **Nutzer** müssen vor der ersten Nutzung in klarer und eindeutiger Weise darüber **informiert** werden, dass sie mit einem AI-System interagieren
- Anbieter und Betreiber von AI-Systemen, die synthetische Audio-, Bild, Video- oder Textinhalte erzeugen, müssen sicherstellen, dass die **Ausgaben** als **künstlich erzeugt** oder **manipuliert** erkennbar sind
- Die **Kennzeichnungspflicht besteht nicht**, wenn von einem AI-System erzeugte Texte einer **redaktionellen Kontrolle** unterzogen wurden und eine natürliche oder juristische Person die redaktionelle **Verantwortung** für die Veröffentlichung der Inhalte trägt

Hochrisiko-AI-Systeme

- **Anbieter:**

  Konformitätsbewertung/ Risikomanagementsystem/ Verfahren für Trainings-, Validierungs- und Testdaten/ Technische Dokumentation/ Protokollierungs-, Transparenz- und Informationspflichten/ ggfs. Grundrechtsfolgenabschätzung
- **Betreiber:**
  - Gewährleistung der **menschlichen Aufsicht**
  - Überwachung der Eingabedaten
  - Einbeziehung in Anforderungen an interne Unternehmensführung
  - Etablierung von **Qualitätsmanagementsystemen** anhand der Betriebsanleitung
  - Eskalationsverfahren
  - Einbeziehung der Arbeitnehmer(-vertretung)

KI-Kompetenz

Die Anforderungen der ESMA zur Nutzung von AI-Anwendungen gehen über die Vorgaben des AI Acts hinaus

Einsatzmöglichkeiten

- **Kundenservice und Support:**
  Einsatz von Chatbots oder Virtual Assistents beispielsweise im First-Level-Support (Beantwortung von Kundenfragen, Account Informationen).
- **Anlageberatung/ Portfolioverwaltung:** Automatisierte Analyse von Kundendaten (z.B. Risikoappetit), Entwicklung/ Überprüfung von kunden-spezifischen Investment-Strategien; Investitionsmöglichkeiten
- **Compliance:** Zusammenfassung und Analyse von neuen regulatorischen Anforderungen, Überprüfung der Regelkonformität der sfO, Vorbereitung der Compliance-Berichterstattung
- **Risikomanagement:** Evaluierung von Risiken im Verbindung mit bestimmten Investment-Optionen (Produkte, Strategien), Monitoring des Risk-Exposure von Kundenportfolios
- **Betrugserkennung:** Monitoring von Transaktionsdaten und Kommunikationsanalyse
- **Effizienz:** Automatisierung von Aufgaben (z.B. Generierung von Reports), Vorbereitung von Marketing-/ Kundenkommunikation, Werbung, Social Media Post

Anforderungen

- **Verantwortung der Geschäftsleitung** (Strategie, Risiko, Governance & Compliance)
- **Best Interest**
- Implementierung von Maßnahmen zur **Kontrolle** der (**auch unabgestimmten**) Nutzung von AI-Anwendungen
- **Transparenz** hinsichtlich des Einsatzes von AI-Anwendungen
- **Verständnis** der Technologie/ **Training**
- **Controlling**: Überwachung von Performance und Auswirkungen
- **Entwicklung eines AI-spezifischen Risikomanagement-Rahmens**
  - Entstehen von **übermäßigem Vertrauen/ Abhängigkeiten**
  - Robustheit und **Verlässlichkeit** des Outputs (insbes. „Halluzinationen“ und Algorithmic biases)
  - **Fehlende Transparenz und Nachvollziehbarkeit** (AI = Blackbox)
  - **Datensicherheit**
- Besondere Anforderungen bei Einsatz im **Anlageentscheidungsprozess** (insbes. bzgl. Datenqualität sowie Implementierung von ex-ante- und **ex-post-Kontrollen)**

In fünf Schritten zur erfolgreichen und sicheren KI-Integration

- Bestimmung von **Zielen und Use Cases** für den Einsatz von KI-Systemen; ggfs. Priorisierung
- Definition eines **Wertesystems** für integritätsbewusstes Handeln und **Regelkonformität** im Kontext künstlicher Intelligenz in Übereinstimmung mit Geschäfts- und Risikostrategie

- **Risikoanalyse** der geplanten KI-Systeme der jeweiligen Use Cases zur **Identifizierung und Bewertung von Risiken**.
- Einordnung und **Risikokategorisierung** der KI-Systeme in den Kontext des AI-Acts und der ESMA Anforderungen zur Ableitung der einzuhaltenden Vorgaben

- Unternehmensweite **Kommunikation** zur **Sensibilisierung** der Mitarbeitenden und zur Steigerungen des Bewusstseins.
- Sicherstellung, der jeweils **notwendigen** rechtlichen und technischen **Kenntnisse**

- **Lifecycle-Management**
- **Entwicklung von Richtlinien** und Arbeitsanweisungen zum Umgang mit KI, ggfs. Erstellung eines Code of Conduct
- Festlegen von Verantwortlichkeiten und Gestaltung von **Kontrollprozessen (1st-/2nd-Line)**
- Definition von **bereichsübergreifenden** Entscheidungs- und **Eskalationskanälen**

- Entwicklung und Umsetzung von **Präventionsmaßnahmen** für identifizierte Risiken
- Orientierung an **Best Practices** und Standards
- **Monitoring** von rechtlichen Entwicklungen auf europäischer und nationaler Ebene

“How can our organization define and manage the roles and responsibilities across the AI lifecycle?”

Chief Executive Officer:
„How do we use AI to create a competitive advantage?”

Chief Compliance Officer:
“I want to set up separate governance structures for AI in order to have clear and controllable rules for AI.”

“Are AI specific controls implemented for the development and go life of our AI solutions?”

Chief Information (Security) Officer:
„How do we manage data privacy and security risks in the operation of our AI models?”

69% of companies fear new IT security risks from AI.

Risk Manager:
“What changes are needed in our current AI governance to ensure compliance and mitigate risks?”

“How can our organization manage and steer AI compliance initiatives in complex organizational structures?”

“How do we ensure maintaining the accuracy of an AI algorithm’s output over time?”

Chief Data and AI Officer:
“I want to have certainty of action and clear guidelines for the development and procurement of AI solutions.”

46% of companies are concerned about the lack of AI explainability.

Chief Operating Officer:
“How do we leverage AI to optimize operational efficiency and streamline business processes?”

Internal Audit Leader:
„What AI governance structures exist within our organization?”

Chief Executive Officer:
“I want to keep reputation and security risks away from the company and still develop innovative AI solutions.”

Chief Compliance Officer:
“How do we ensure AI compliance with regulations?”

“How do we ensure high quality data is used to train our AI models?”

Chief Risk Officer:
“How prepared is our organization to meet the requirements of the AI Act?”

2

DORA

Digital Operational Resilience Act (DORA)

IKT-Risikomanagement
Taktische, organisatorische und technische Fähigkeiten im Bereich der Cybersicherheit

IKT-bezogene Vorfälle
Erkennung, Meldung und Behandlung von IKT-bezogenen Vorfällen

Testen der digitalen operationalen Resilienz
Regelmäßige Tests von Ausfallsicherheitsmaßnahmen und kritischen Systemen

Management des IKT-Drittparteienrisikos
Fortgeschrittene Überwachung und Verwaltung von Drittparteirisiken

Informationsaustausch
Austausch von Bedrohungsdaten, Best Practice

HEUTE

<4 Monate bis zur Umsetzungsfrist verbleiben

Jan 2023

Inkrafttreten

DORA trat am 16. Jan. 2023 in Kraft

Jun 2023

Öffentliche Konsultation

Erste öffentliche Konsultation zu 5 RTS / ITS

Dez 2023

Öffentliche Konsultation

Zweite öffentliche Konsultation zu 5 RTS / ITS

Juli 2024

Veröffentlichung aller RTS / ITS

Am 26.07.2024 wurden die finalen Drafts veröffentlicht

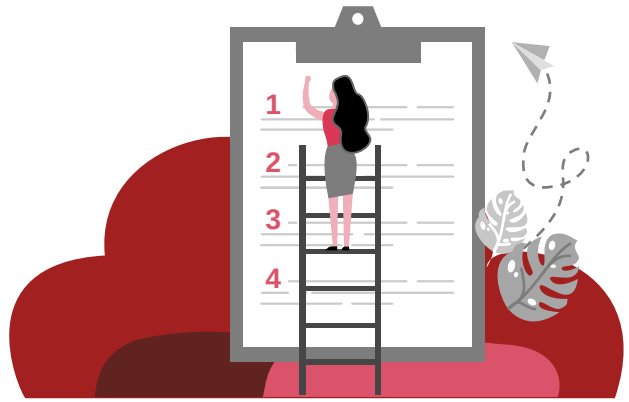
Jan 2025*

Durchsetzung & Prüfpflicht

**Der Referentenentwurf des Finanzmarktdigitalisierungsgesetzes (FinmadiG) sieht eine Prüfpflicht von DORA für den Jahresabschlussprüfer vor*

DORA – Deadline 17.1.2025

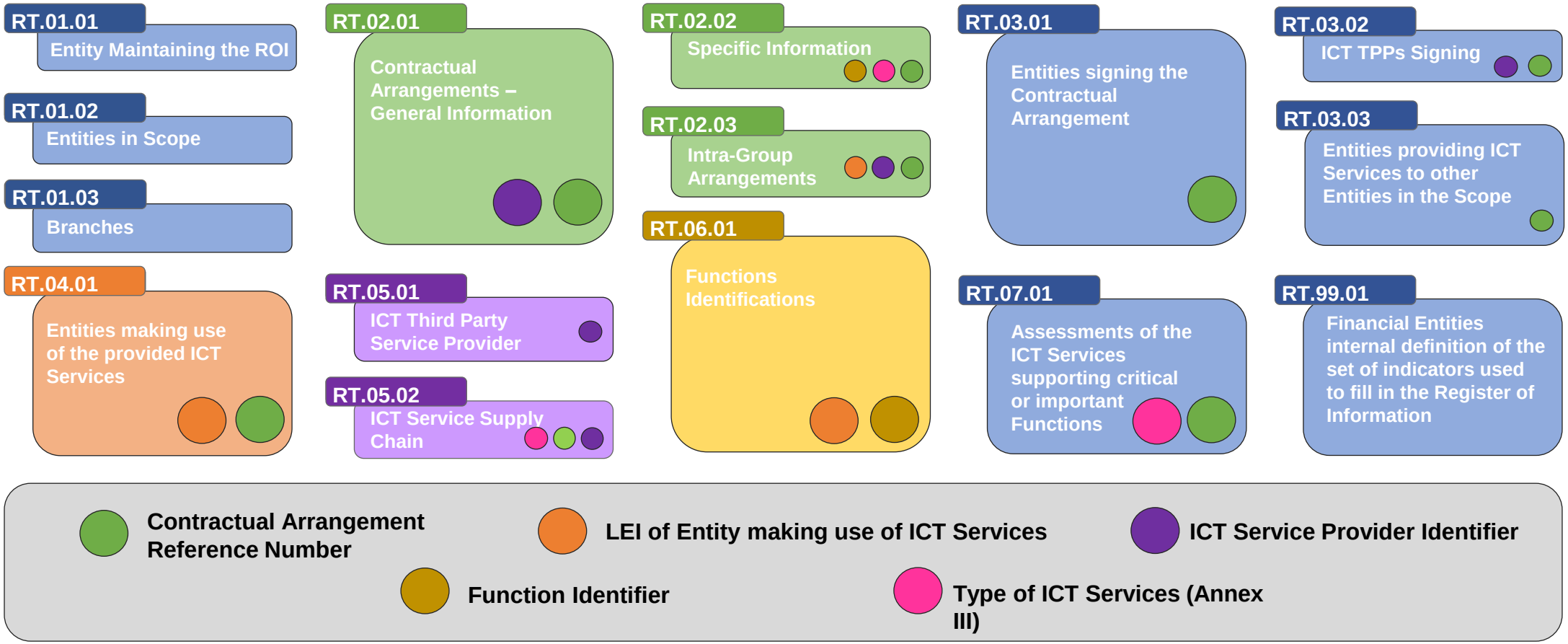
- Übersicht über aktuellen DORA-Status & DORA-Compliance
- Realistische Zeitplanung & Zieldatum zur vollständigen DORA-Compliance inklusive IKT-Dienstleister & Tools
- Definition der kritischen und wichtigen Funktionen
- Klassifizierung im Informationsverbund, Identifizierung von Anwendungen und IKT-Dienstleistern, die kritische und wichtige Funktionen unterstützen
- Wesentliche Fertigstellung der schriftliche fixierten Ordnung inklusive einer DOR-Strategie
- Vollständiges Informationsregister
- Funktionierende Identifikation- & Meldeprozesse für IKT-Vorfälle



DORA Informationsregister

Das Informationsregister muss zum 17.1.2025 fertig sein und der BaFin zur Verfügung gestellt werden

96 **Datenfelder** sind für das **Informationsregister** gemäß der DORA-Verordnung erforderlich



Meldung von schwerwiegenden IKT-Vorfällen

“

RTS and ITS on major incident reportings

Finanzinstitute sind verpflichtet

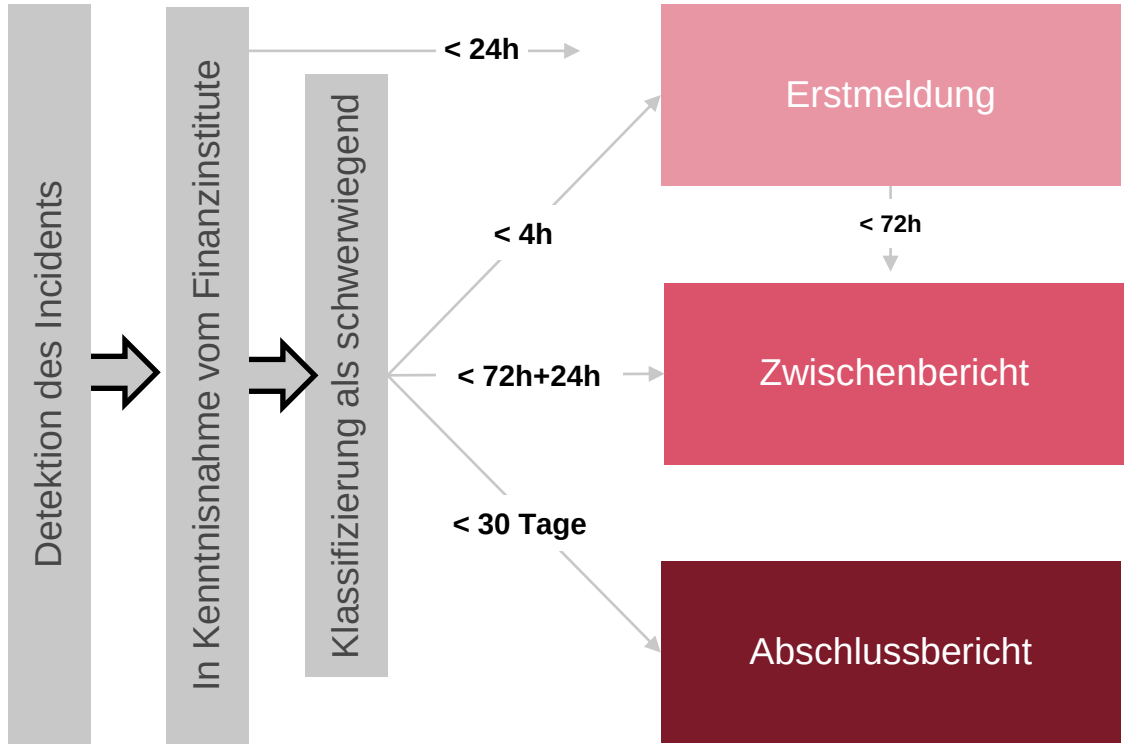
eine erste Meldung über den Vorfall einzureichen, und zwar 4 Stunden, nachdem der Vorfall als schwerwiegend eingestuft wurde, spätestens jedoch 24 Stunden nach dem Zeitpunkt, an dem das Finanzinstitut von dem Vorfall Kenntnis erlangt hat;

Zwischenbericht spätestens innerhalb von 72 Stunden nach Übermittlung der ersten Meldung vorzulegen, auch wenn sich der Status oder die Behandlung des Vorfalls gemäß Artikel 19 Absatz 4 Buchstabe b der Verordnung (EU) 2022/2554 nicht geändert haben. Die Finanzunternehmen legen in jedem Fall unverzüglich einen aktualisierten Zwischenbericht vor, wenn die regulären Tätigkeiten wieder aufgenommen wurden.

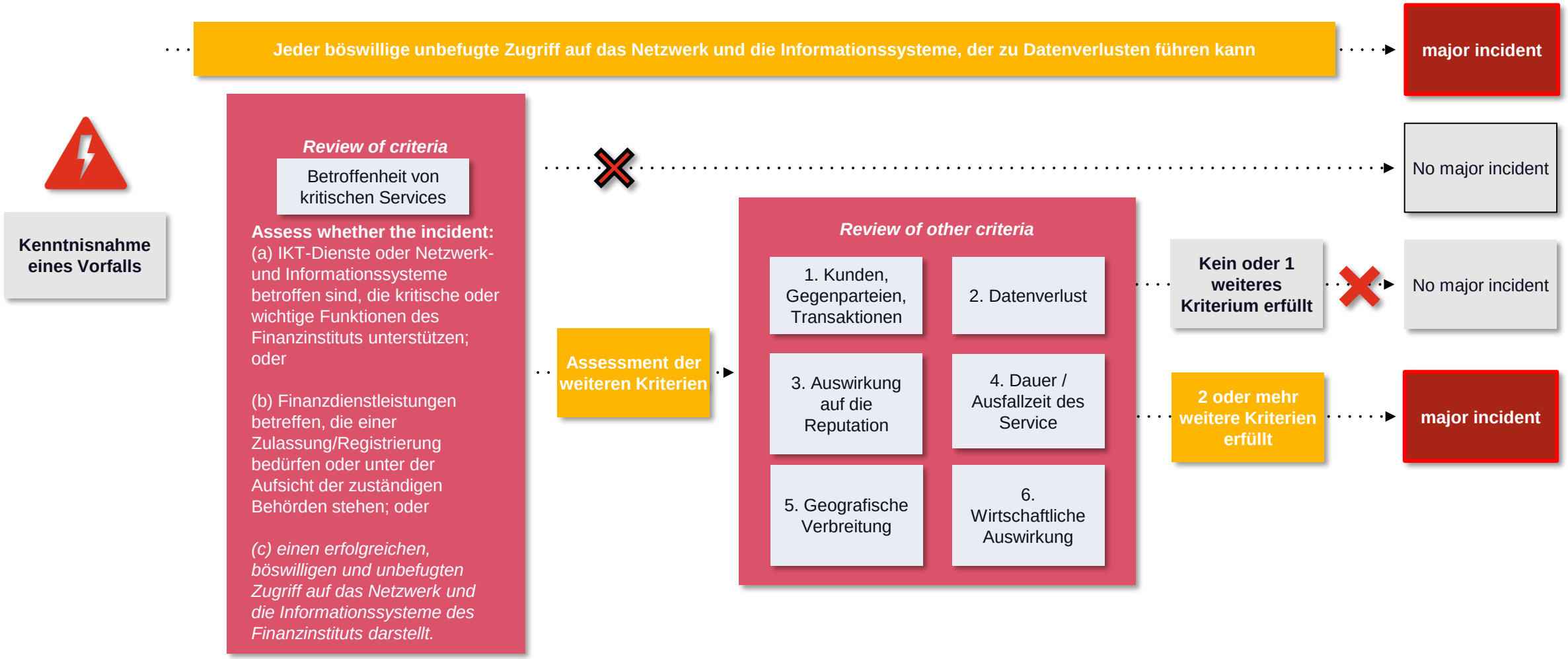
Einen Abschlussbericht vorzulegen, mindestens 30 Tage, nachdem der Vorfall als schwerwiegend eingestuft wurde, der Informationen zur Ursache des Vorfalls und zu den Maßnahmen enthält, die ergriffen wurden, um ihn zu beheben und ein erneutes Auftreten zu verhindern;

Vorfälle auf Einzelbasis zu melden; (gruppeninterne) Drittanbieter können einen Bericht auf nationaler Ebene für die beaufsichtigten Finanzunternehmen vorlegen, wenn relevante Einzelinformationen für jedes Finanzunternehmen bereitgestellt werden

”



Meldung von schwerwiegenden IKT-Vorfällen



Ihre Ansprechpartner:

RA Judith Schmalzl
Partner
Risk & Regulation
Asset & Wealth Management

Düsseldorf
+49 170 4533038
judith.caroline.schmalzl@pwc.com

Felix Guski
Senior Associate, CISA
Risk & Regulation
Asset & Wealth Management

Frankfurt a. M.
+49 160 5917547
felix.f.guski@pwc.com

pwc.de