Digital Operational Resilience Act

Konkretisierung durch technische Durchführungs- und Implementierungsstandards: Ein Ausblick

Patrick Schmidt, Dr. Christian Schwartz

07/08.Nov.2023

ISACA
Germany Chapter

Digital Operational Resilience Act (DORA) stellt neue Anforderungen an Finanzinstitute und IT-Dienstleister

Im Januar 2023 trat DORA, eine neue Verordnung des Europäischen Parlaments und des Rates, zur Steigerung der operationellen Resilienz im Finanzwesen in Kraft.

Die in DORA gestellten Anforderungen werden durch technische Durchführungs- und Implementierungsstandards bis 2024 weiter konkretisiert.

ISACA Germany Chapter

Der DORA betrifft eine größere Menge an Branchen als bisherige Finanzregulatorik zum IKT-Risikomanagement.

- Kreditinstitute
- Zahlungsinstitute
- Kontoinformations-dienstleister
- E-Geld Institute
- Wertpapierfirmen
- Anbieter von Krypto-Dienstleistungen
- Zentralverwahrer
- Zentrale Gegenparteien
- Handelsplätze
- Transaktions-register
- Verwalter alternativer Investmentfonds
- Verwaltungs-gesellschaften
- Datenbereit-stellungsdienste
- Versicherungen und Rückversicherungen
- Versicherungs-vermittler[1]
- Einrichtungen der betriebl. Altersvorsorge
- Ratingagenturen
- Administratoren kritischer Referenzwerte
- Schwarmfinanzierungs-dienstleister
- Verbriefungsregister

+

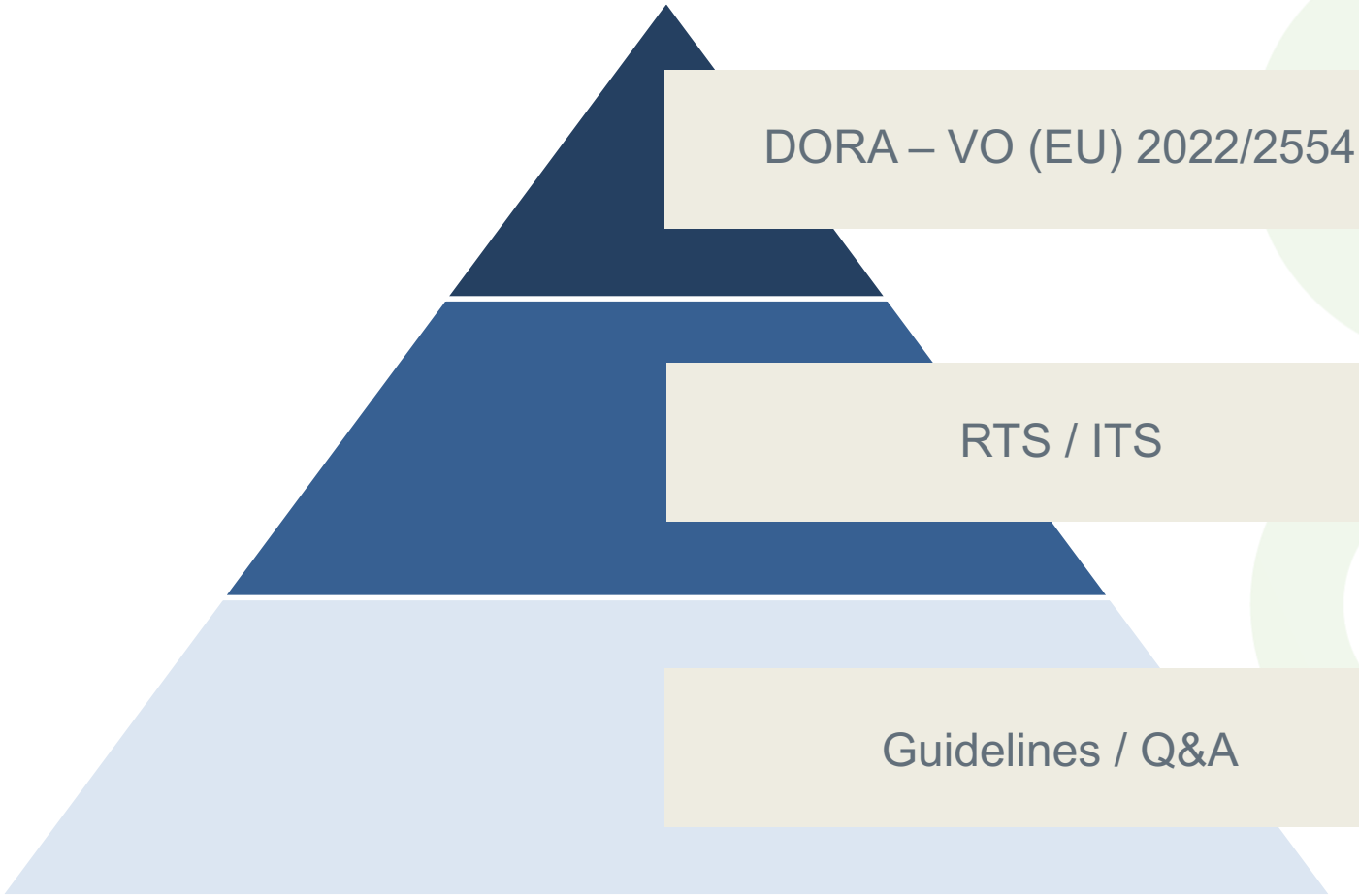
Kritische IKT-Drittdienstleister nach der Definition der ESA

[1]. Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit

ISACA Germany Chapter


Projekt zur DORA Implementierung
RTS / ITS

Die Konkretisierung der DORA erfolgt auf verschiedenen Ebenen und durch verschiedene Institutionen



Level 1
Rat/Europäisches Parlament

Level 2
Europäische Kommission

Level 3
ESAs / Nationale Aufsichtsbehörden

ISACA Germany Chapter

Technische Durchführungs- und Implementierungsstandards werden durch europäische Aufsichtsbehörden verfasst.

Technische Durchführungs- (Regulatory Technical Standards, RTS) und Implementierungsstandards (Implementing Technical Standards, ITS) präzisieren einen Rechtsakt bzw. stellen eine einheitliche Anwendung sicher.

Erstellung
Europäische Aufsichtsbehörden erstellen Entwurf nach Delegation in Rechtsakt.

Konsultation
Aufsichtsbehörden konsultieren Entwürfe und nehmen Feedback an.

Weitergabe
Aufsichtsbehörden geben die Entwürfe an Kommission weiter.

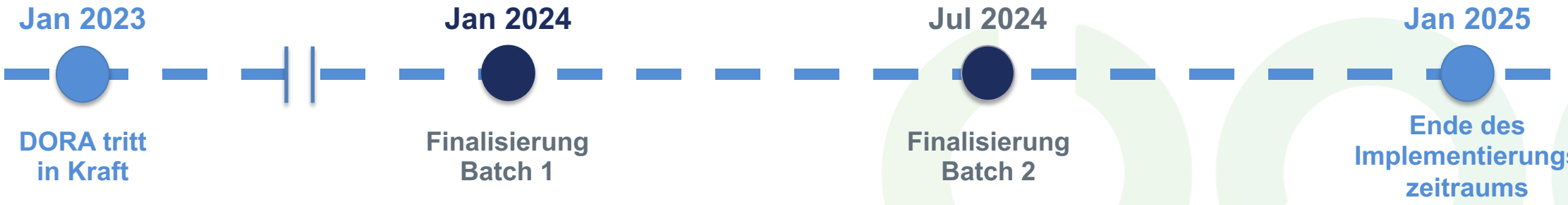
Prüfung
Die europäische Kommission prüft die Inhalte und nimmt diese an[1].

In Kraft treten
Parlament und Rat nehmen ITS/RTS explizit oder implizit an[1].

[1]. Falls der Entwurf nicht angenommen wird, wird das Dokument zurückgegeben und muss in einer Frist überarbeitet werden.

ISACA Germany Chapter

ITS und RTS des DORA werden in zwei großen Paketen am 17. Januar und 17. Juli 2024 an die Kommission übergeben.



Level 1

- Anforderungen an die Governance
- Anforderungen an IKT-RisikoMgmt
- Meldung IKT-bezogener Vorfälle
- Prüfung der digitalen Betriebsstabilität
- Risiko durch IKT-Drittanbieter
- Informations-austausch

Level 2

- RTS –IKT-RiskoMgmt Framework
- GL – Schätzung der Kosten und Verluste durch Vorfälle
- RTS – IKT Vorfall Klassifizierung
- RTS – Meldung von schwerwiegenden Vorfällen
- ITS – Meldedetails von schwerwiegenden Vorfällen
- RTS – Tests der digitalen Betriebsstabilität
- RTS – Drittanbieter-Risiko Policy
- ITS – Template des Informationsregisters
- RTS – Klassifizierung von Auslagerungs-DL
- RTS – Überwachungs-rahmenwerk für kritische DL

ISACA Germany Chapter

Batch I: Die erste Runde RTS & ITS

Jan 2023 — DORA tritt in Kraft

Jan 2024 — Finalisierung Batch 1

Jul 2024 — Finalisierung Batch 2

Jan 2025 — Ende des Implementierungszeitraums

Level	Anforderungen an die Governance	Anforderungen an IKT-RisikoMgmt	Meldung IKT-bezogener Vorfälle	Prüfung der digitalen Betriebsstabilität	Risiko durch IKT-Drittanbieter	Informations-austausch
Level 1						
Level 2		**RTS –IKT-RiskoMgmt Framework** GL – Schätzung der Kosten und Verluste durch Vorfälle	**RTS – IKT Vorfall Klassifizierung** RTS – Meldung von schwerwiegenden Vorfällen ITS – Meldedetails von schwerwiegenden Vorfällen	RTS – Tests der digitalen Betriebsstabilität	**RTS – Drittanbieter-Risiko Policy** **ITS – Template des Informationsregisters** RTS – Klassifizierung von Auslagerungs-DL RTS – Überwachungs-rahmenwerk für kritische DL	

ISACA Germany Chapter

RTS zur Harmonisierung der IKT-Risikomanagementinstrumente, -methoden, Prozesse und Policies

Was macht DORA neu?

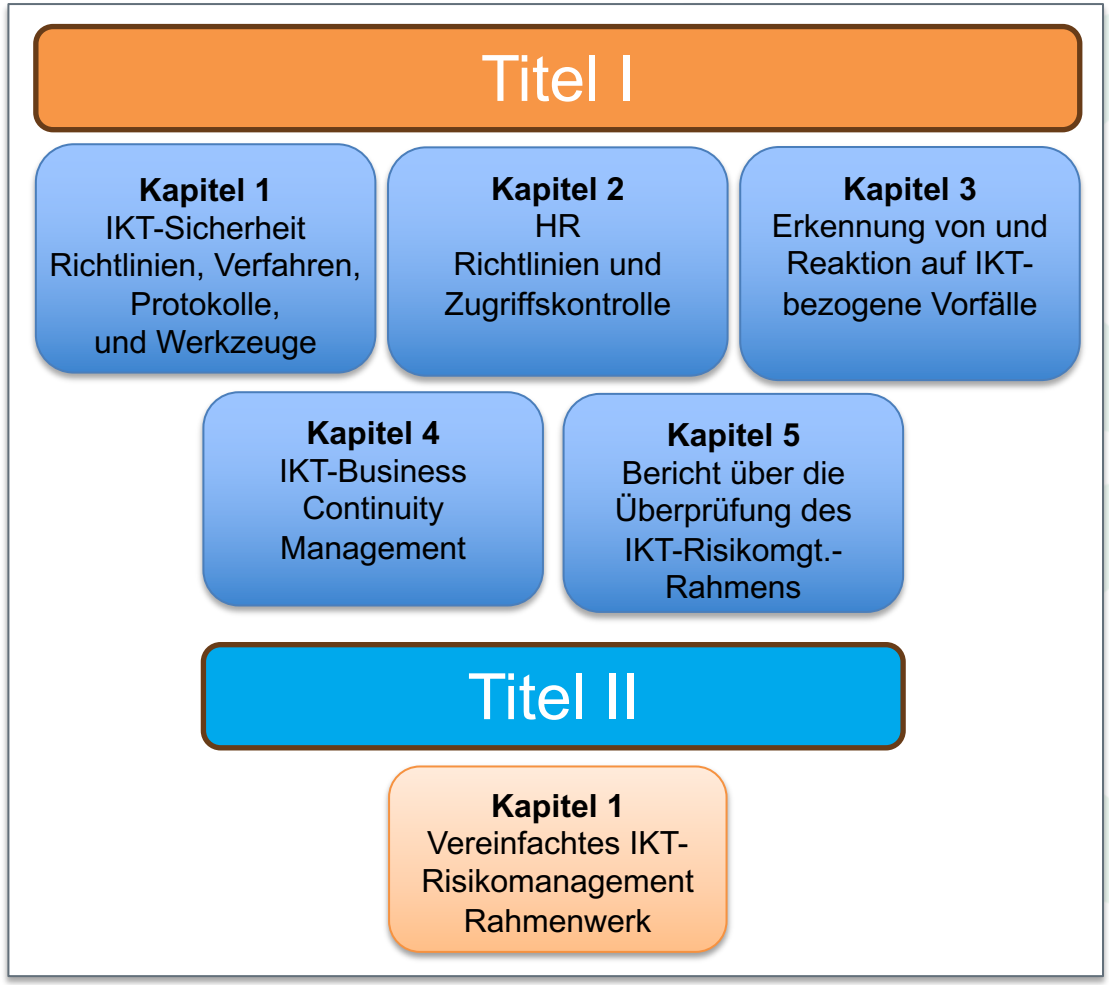
- Stärkere Rolle der Leitung in der Steuerung des IKT-Risikos (lauf. Weiterbildung)
- Unternehmen müssen einen gut dokumentierten und wirksamen Rahmen für das IKT-Risikomanagement schaffen und aufrechterhalten
- DORA fokussiert speziell auf eine schnelle Erkennung und Reaktion von Störungen und entsprechende Kommunikationsrichtlinien

Was konkretisiert der RTS? (Was war durch den Text der DORA nicht direkt klar)

- Elemente die in den Sicherheitsrichtlinien und Policies enthalten sein müssen
- Vorgaben, welche Aspekte im Rahmen der internen Kontrolle zu prüfen sind
- Konkrete Maßnahmen die mindestens umzusetzen sind
- Inhaltliche Anforderungen an die Berichterstattung über den Review des IKT-Risikomanagement-Frameworks

Was sind Aufwandstreiber?

- Detailliertere Anforderungen an Richtlinien, Werkzeuge, Maßnahmen
- Erstellung eines visuellen Netzwerkplans
- Zusätzliche Szenarien, die in den BCM-Plänen berücksichtigt werden müssen



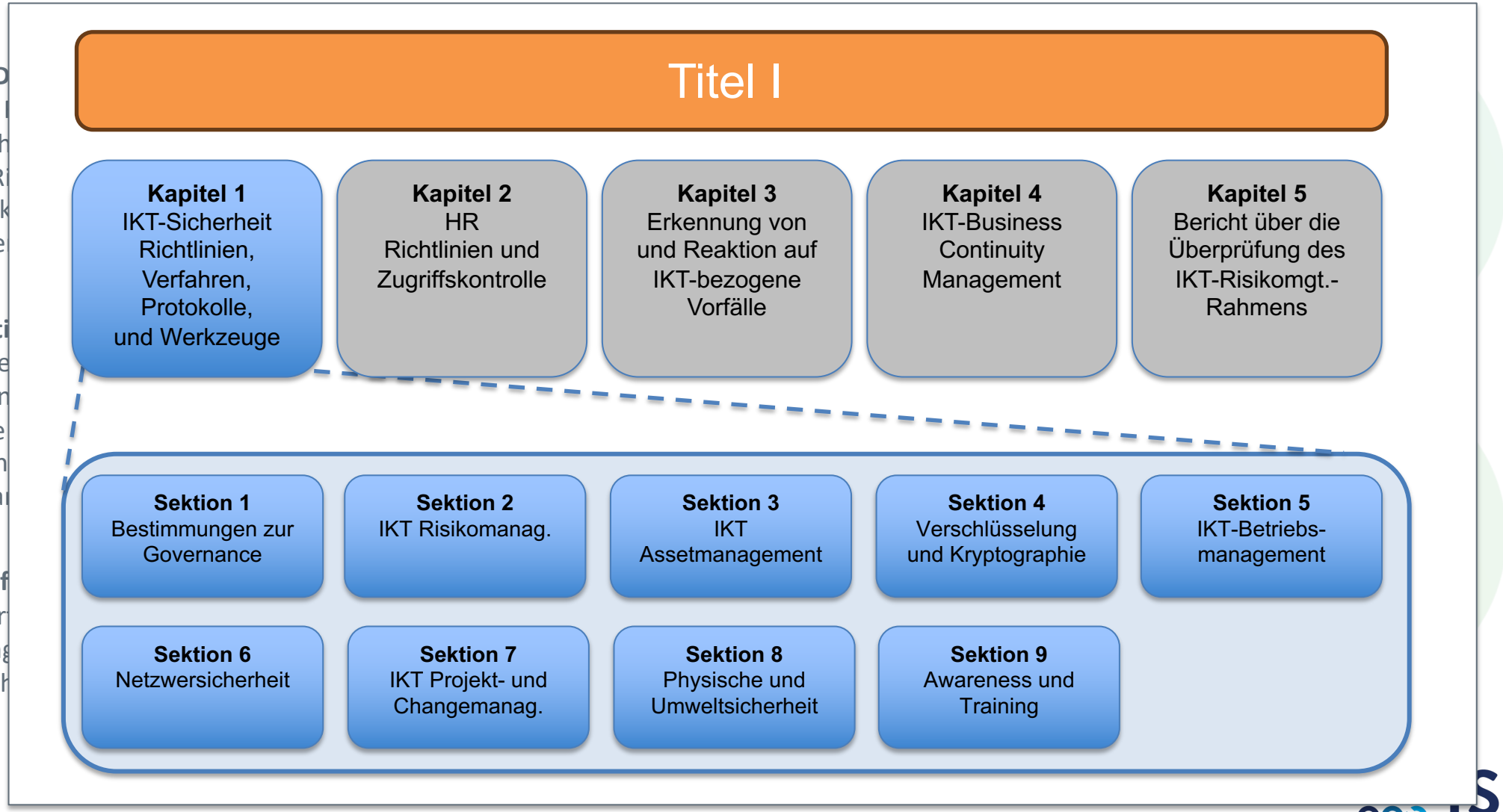
ISACA Germany Chapter

RTS zur Harmonisierung der IKT-Risikomanagementinstrumente, -methoden, Prozesse und Policies

Was macht D
- Stärkere
- Unterneh
  das IKT-Ri
- DORA fok
  Störunge

Was konkreti
- Elemente
- Vorgaben
- Konkrete
- Inhaltlich
  Risikoma

Was sind Auf
- Detaillier
- Erstellung
- Zusätzlich



ISACA Germany Chapter

RTS zur Harmonisierung der IKT-Risikomanagementinstrumente, -methoden, Prozesse und Policies

Was macht DORA neu?

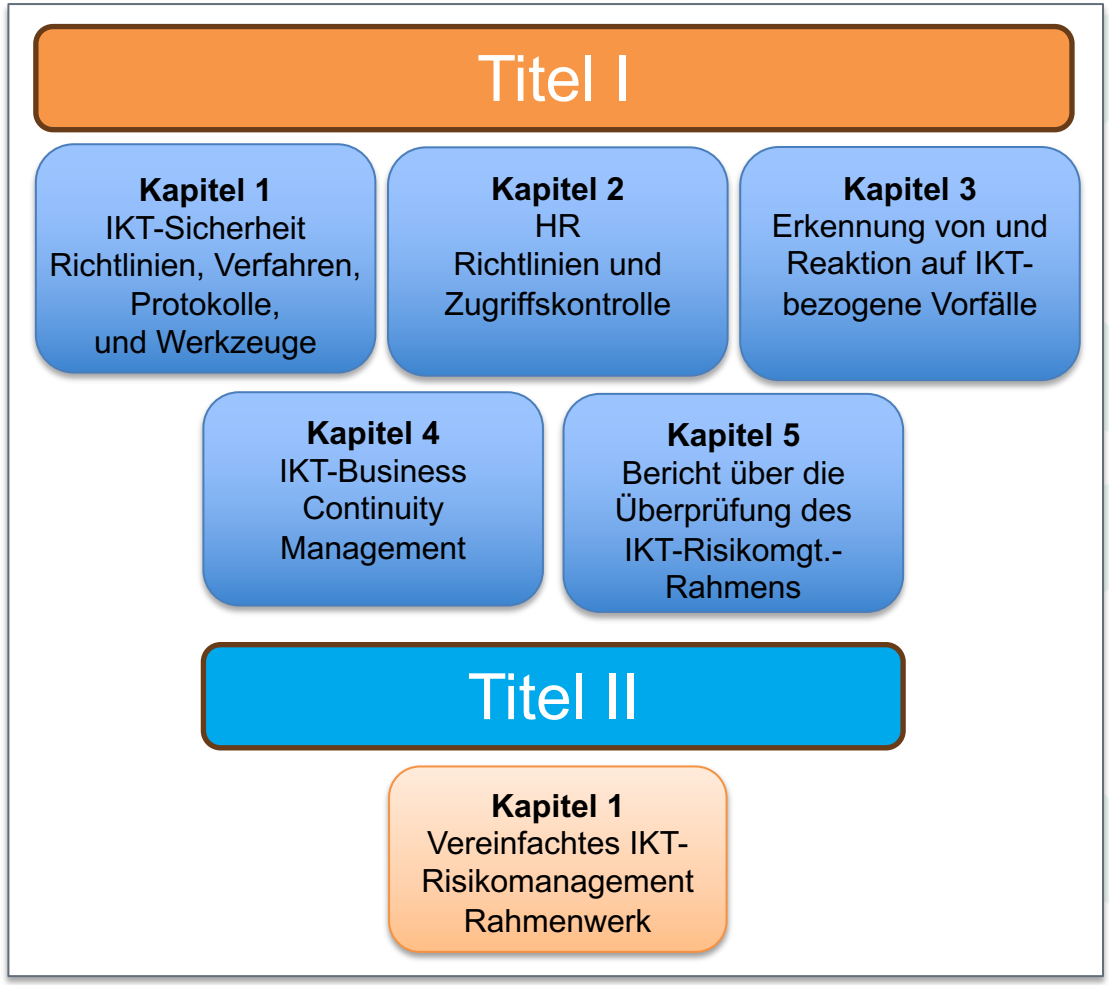
- Stärkere Rolle der Leitung in der Steuerung des IKT-Risikos (lauf. Weiterbildung)
- Unternehmen müssen einen gut dokumentierten und wirksamen Rahmen für das IKT-Risikomanagement schaffen und aufrechterhalten
- DORA fokussiert speziell auf eine schnelle Erkennung und Reaktion von Störungen und entsprechende Kommunikationsrichtlinien

Was konkretisiert der RTS? (Was war durch den Text der DORA nicht direkt klar)

- Elemente die in den Sicherheitsrichtlinien und Policies enthalten sein müssen
- Vorgaben, welche Aspekte im Rahmen der internen Kontrolle zu prüfen sind
- Konkrete Maßnahmen die mindestens umzusetzen sind
- Inhaltliche Anforderungen an die Berichterstattung über den Review des IKT-Risikomanagement-Frameworks

Was sind Aufwandstreiber?

- Detailliertere Anforderungen an Richtlinien, Werkzeuge, Maßnahmen
- Erstellung eines visuellen Netzwerkplans
- Zusätzliche Szenarien, die in den BCM-Plänen berücksichtigt werden müssen



ISACA Germany Chapter

RTS zur Klassifizierung von IKT-bezogenen Vorfällen, Wesentlichkeitsschwellen für schwerwiegende Sicherheitsvorfälle und erhebliche Cyberbedrohungen

Was macht DORA neu?

- DORA legt Kriterien für die Einstufung von Vorfällen als schwerwiegend fest
- DORA verlangt von Instituten, Cyberbedrohungen anhand bestimmter Kriterien zu klassifizieren

Was konkretisiert der RTS? (Was war durch den Text der DORA nicht direkt klar)

- Klassifizierungskriterien für IKT-bezogene Vorfälle
- Wesentlichkeitsschwellen für die Bestimmung schwerwiegender Vorfälle
- Kriterien und Wesentlichkeitsschwellen zur Bestimmung signifikanter Cyberbedrohungen
- Kriterien für die zuständigen Behörden zur Bewertung der Relevanz von Sicherheitsvorfällen für andere Mitgliedstaaten

Was sind Aufwandstreiber?

- Implementierung eines Prozesses zum Sammeln, Analysieren und Auswerten von Informationen im Falle eines potenziellen Ereignisses
- Berechnung, um festzustellen, ob relative und/oder absolute Schwellenwerte erreicht werden (z. B. % der betroffenen Kunden, direkte und indirekte Kosten in € usw.)
- Dokumentation, die zeigt, wie die Bewertung erreicht wurde

	DORA RTS	ISO/IEC 2700X	XAIT / XaRisk
Erfordert die Klassifizierung von Vorfällen	✓	✓	✓
Nennt Kriterien	✓	✗	✗
Spezifiziert Kriterien	✓	✗	✗
Erfordert Prozess für Bedrohungen	✓	✓	✓
Nennt Kriterien	✓	✗	✗
Spezifiziert Kriterien	✓	✗	✗

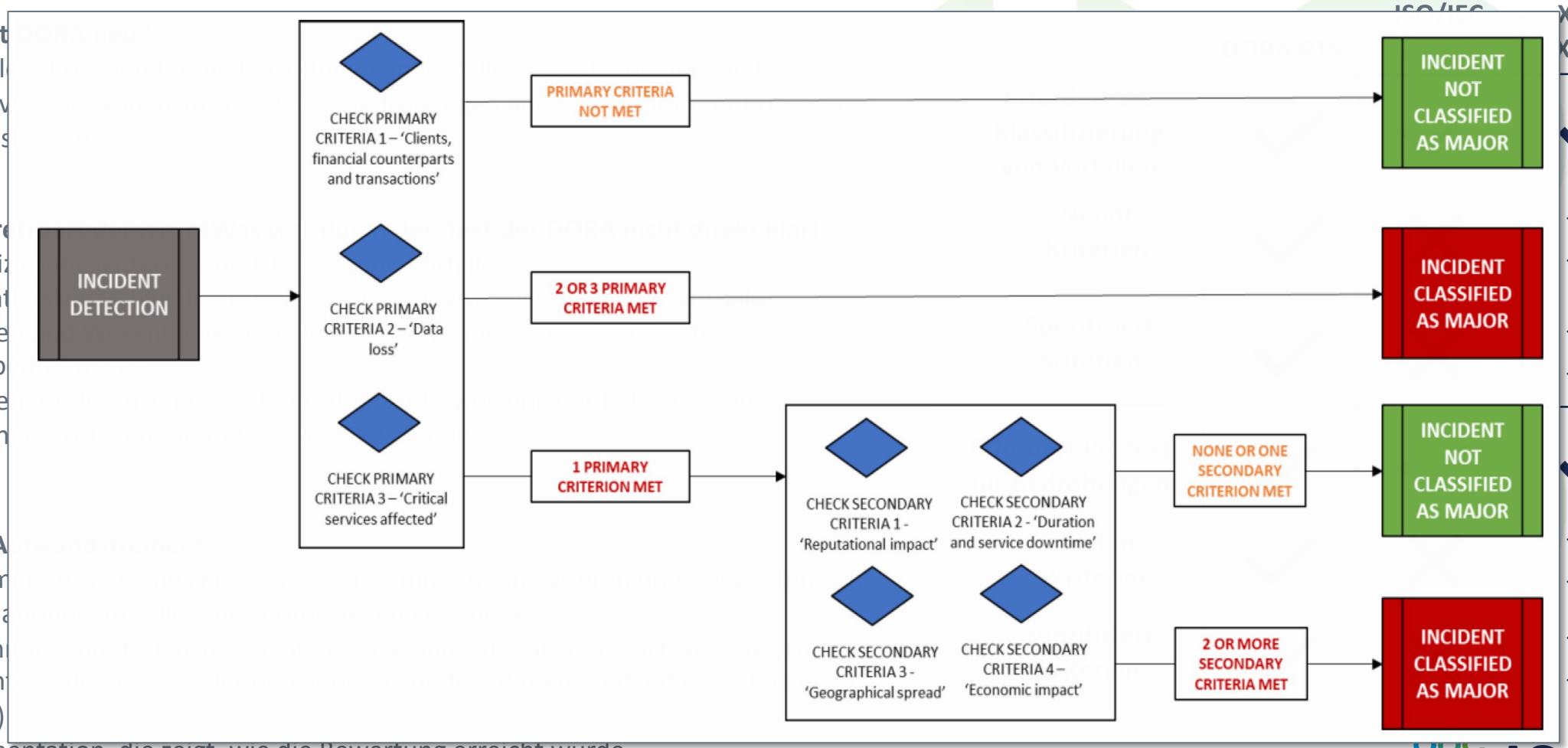
ISACA Germany Chapter

RTS zur Klassifizierung von IKT-bezogenen Vorfällen, Wesentlichkeitsschwellen für schwerwiegende Sicherheitsvorfälle und erhebliche Cyberbedrohungen

Was macht
- DORA l
- DORA v
  zu klass

Was konkr
- Klassifiz
- Wesent
- Kriterie
  Cyberb
- Kriterie
  Sicherh

Was sind A
- Implem
  Informa
- Berech
  erreich
  € usw.)
- Dokumentation, die zeigt, wie die Bewertung erreicht wurde



Quelle: ESMA, [RTS on criteria for the classification of ICT-related incidents;]

RTS zur Klassifizierung von IKT-bezogenen Vorfällen, Wesentlichkeitsschwellen für schwerwiegende Sicherheitsvorfälle und erhebliche Cyberbedrohungen

Was macht DORA neu?

- DORA legt Kriterien für die Einstufung von Vorfällen als schwerwiegend fest
- DORA verlangt von Instituten, Cyberbedrohungen anhand bestimmter Kriterien zu klassifizieren

Was konkretisiert der RTS? (Was war durch den Text der DORA nicht direkt klar)

- Klassifizierungskriterien für IKT-bezogene Vorfälle
- Wesentlichkeitsschwellen für die Bestimmung schwerwiegender Vorfälle
- Kriterien und Wesentlichkeitsschwellen zur Bestimmung signifikanter Cyberbedrohungen
- Kriterien für die zuständigen Behörden zur Bewertung der Relevanz von Sicherheitsvorfällen für andere Mitgliedstaaten

Was sind Aufwandstreiber?

- Implementierung eines Prozesses zum Sammeln, Analysieren und Auswerten von Informationen im Falle eines potenziellen Ereignisses
- Berechnung, um festzustellen, ob relative und/oder absolute Schwellenwerte erreicht werden (z. B. % der betroffenen Kunden, direkte und indirekte Kosten in € usw.)
- Dokumentation, die zeigt, wie die Bewertung erreicht wurde

	DORA RTS	ISO/IEC 2700X	XAIT / XaRisk
Erfordert die Klassifizierung von Vorfällen	✓	✓	✓
Nennt Kriterien	✓	✗	✗
Spezifiziert Kriterien	✓	✗	✗
Erfordert Prozess für Bedrohungen	✓	✓	✓
Nennt Kriterien	✓	✗	✗
Spezifiziert Kriterien	✓	✗	✗

ISACA Germany Chapter

RTS für die die Leitlinie für die Nutzung von IKT-Dienst-leistungen für kritische und wichtige Funktionen […]

Was ist durch die DORA neu?

- Konkrete Anforderungen an die „Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden“
- Mindestvertragsinhalte zum Bezug von IKT-Dienstleistungen für kritische und wichtige Funktionen

Was konkretisiert der RTS? (Was war durch den Text der DORA nicht direkt klar)

- Mindestanforderungen an den Lebenszyklus von IKT-Dienstleistungen für kritische und wichtige Funktionen
- Mindestanforderungen an die Ex-Ante Risikobewertung
- Mindestanforderungen an Due-Diligence Prüfungen bei der Dienstleisterauswahl
- Anforderungen an die Überwachung der vertraglichen Vereinbarungen
- Ergänzungen der Mindestvertragsinhalte im Bezug auf die Prüfung des IKT-Drittdienstleisters

Was sind Aufwandstreiber?

- Anpassung und Neuverhandlung von Verträgen
- Umsetzung der Due-Dilligence bei der Dienstleisterauswahl
- Überwachung der IKT-Dienstleister in Bezug auf die Einhaltung der Sicherheits-Schutzziele sowie der Richtlinien und Standards des Finanzinstituts

Komponenten der Ex-Ante Risikobewertung

Rechtsrisiken

Operationelle Risiken

Risiken bzgl. vertrauliche oder personenbezogene Daten

Ortsbezogene Risiken

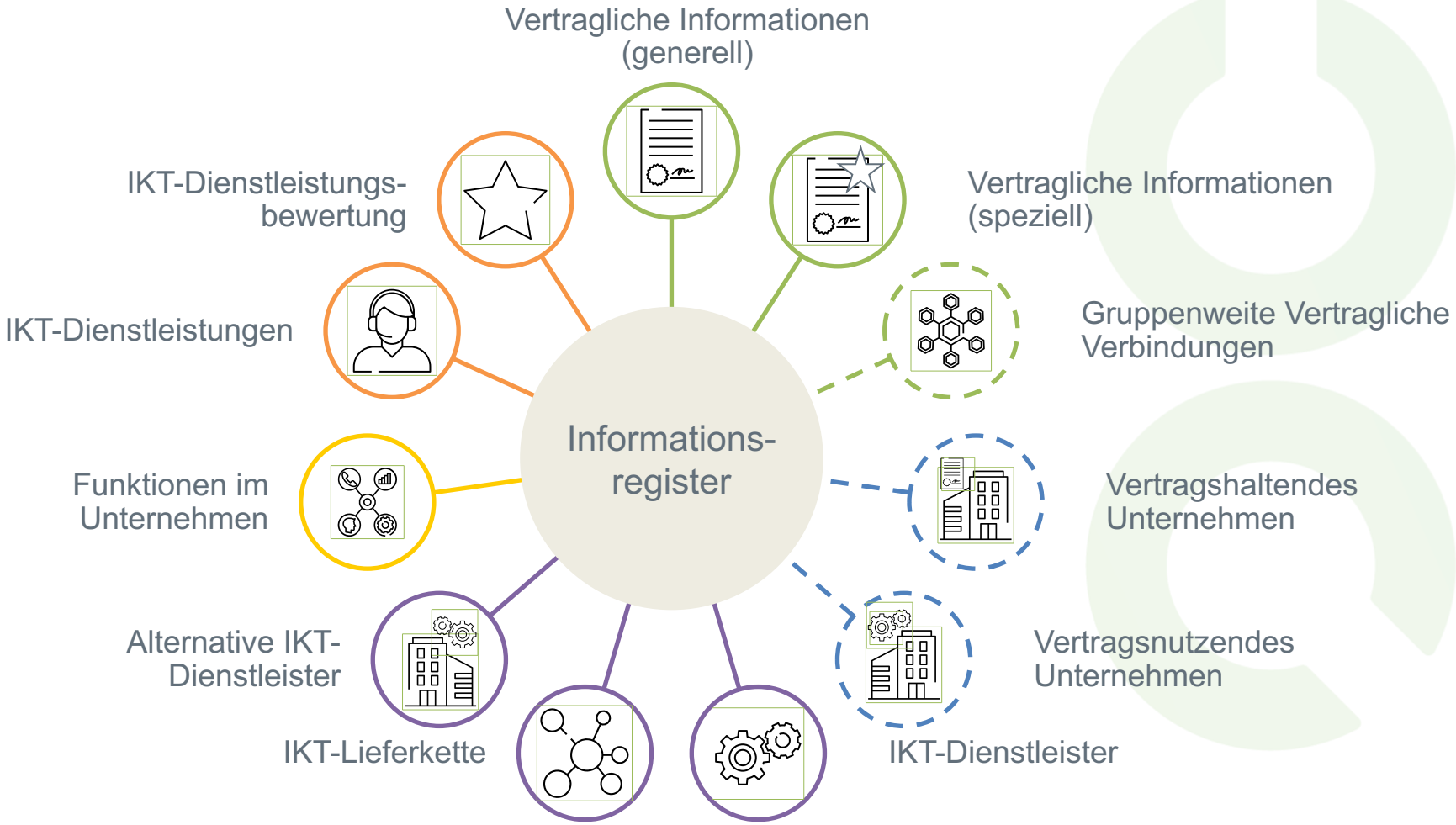
Verfügbarkeitsrisiken

IKT-Risiken

IKT-Konzentrationsrisiken

ISACA Germany Chapter

ITS um die Standardvorlage für das Informations-register zu definieren



Das Register

- muss von Funktion im Unternehmen geführt werden;
- ist aktuell zu halten;
- muss der Aufsicht zur Verfügung gestellt werden;
- muss Unternehmen über ihre LEI identifizieren.

Unternehmensbezogen | Dienstleisterbezogen | Funktionsbezogen | Dienstleistungsbezogen | Vertragsbezogen | Nur im konsolidierten Fall

ISACA Germany Chapter

ITS um die Standardvorlage für das Informations-register zu definieren

Auszug aus der Vorlage für das Informationsregister für Vertragsbeziehungen (spezifisch)

TEMPLATE RT.02.02: Contractual Arrangements – Specific information

RT.02.02.0010	RT.02.02.0020	RT.02.02.0030	RT.02.02.0040	RT.02.02.0050	RT.02.02.0060	RT.02.02.0070	RT.02.02.0080	RT.02.02.0090	RT.02.02.0100
Contractual arrangement reference number	Function identifier	ICT services identifier	Start date of the contractual arrangement	Date of next renewal of the contractual arrangement	End date of the contractual arrangement	Reason of the termination or ending of the contractual arrangement	Notice period for the financial entity	Notice period for the ICT third-party service provider	Country of the governing law of the contractual arrangement
Alphanumerical	Alphanumerical	Alphanumerical	Date	Date	Date	Closed set of options	Integer	Integer	Country

RT.02.02.0110	RT.02.02.0121	RT.02.02.0122	RT.02.02.0123	RT.02.02.0130	RT.02.02.0140	RT.02.02.0150
Country of provision of the ICT services	Storage of data	Location of the data at rest (storage)	Location of management of the data (processing)	Sensitiveness of the data stored by the ICT third-party service provider	Are customers data stored or processed by the ICT third-party service provider?	Level of reliance on the ICT service supporting the critical or important function
Country	[Yes/No]	Country	Country	Closed set of options	[Yes/No]	Closed set of options

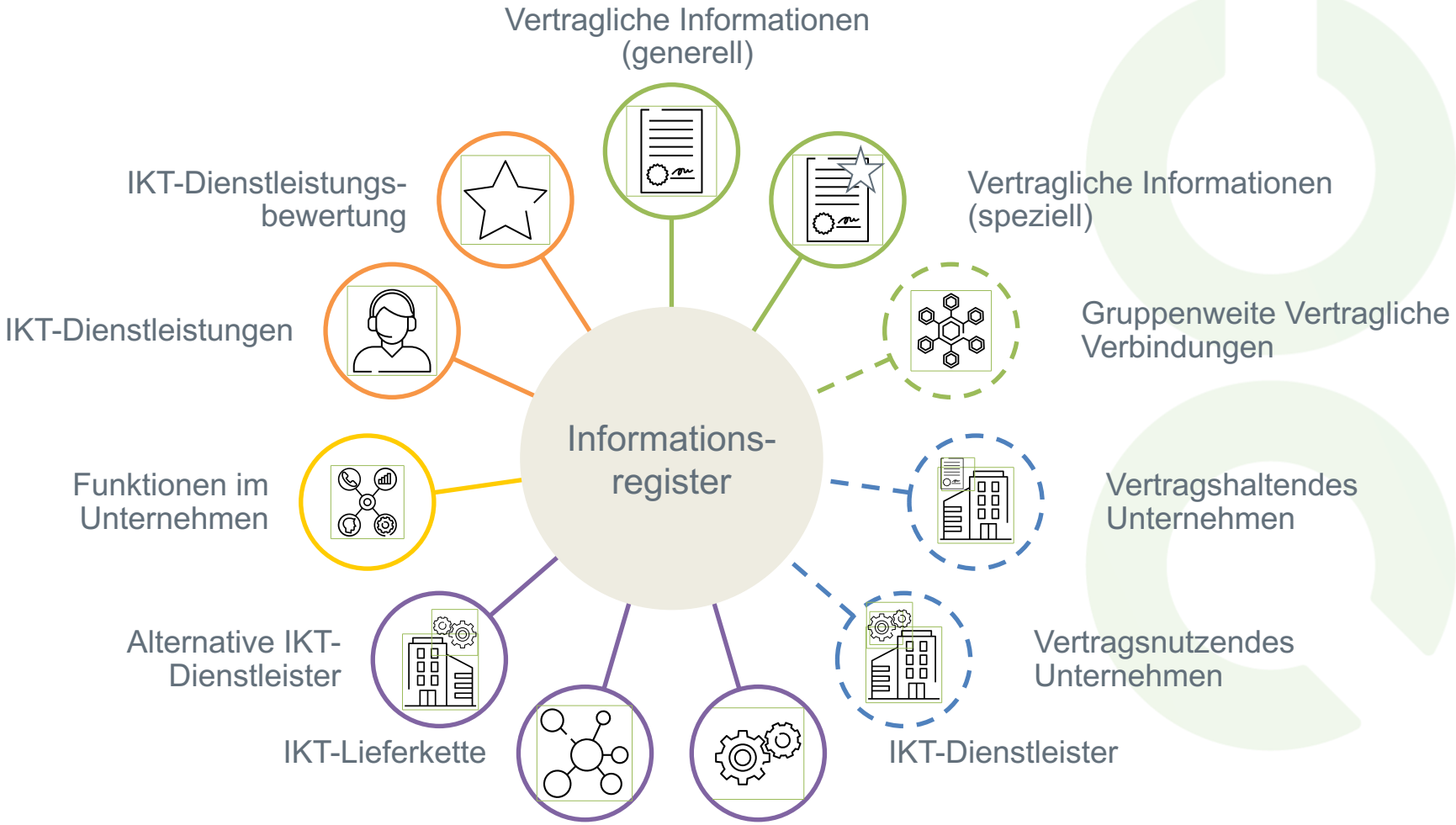
IKT-Lieferkette

IKT-Dienstleister

Unternehmensbezogen | Dienstleisterbezogen | Funktionsbezogen | Dienstleistungsbezogen | Vertragsbezogen | Nur im konsolidierten Fall

ISACA Germany Chapter

ITS um die Standardvorlage für das Informations-register zu definieren



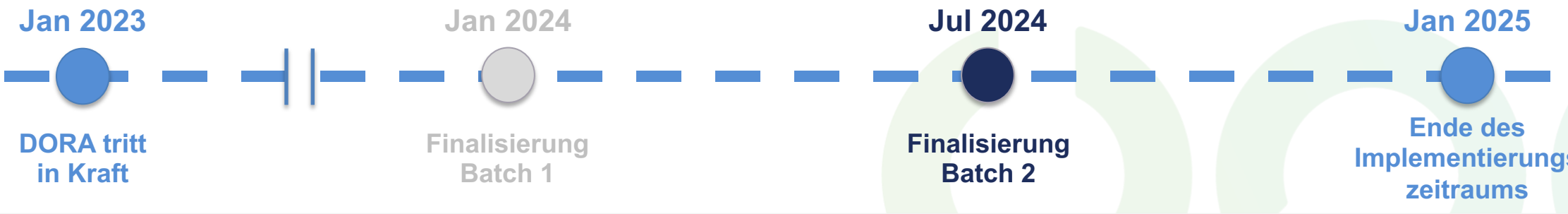
Das Register

- muss von Funktion im Unternehmen geführt werden;
- ist aktuell zu halten;
- muss der Aufsicht zur Verfügung gestellt werden;
- muss Unternehmen über ihre LEI identifizieren.

Unternehmensbezogen | Dienstleisterbezogen | Funktionsbezogen | Dienstleistungsbezogen | Vertragsbezogen | Nur im konsolidierten Fall

ISACA Germany Chapter

Batch II: Die nächste Runde RTS & ITS

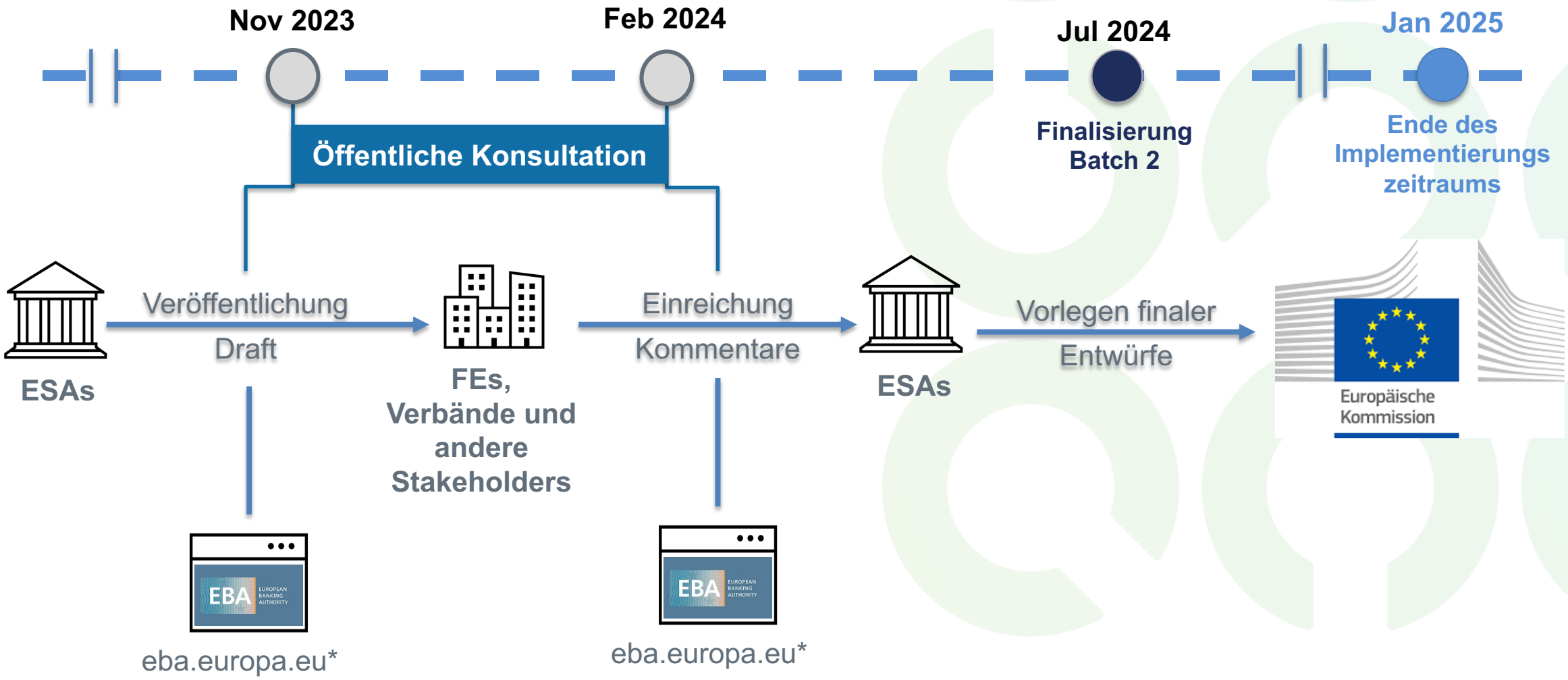


	Anforderungen an die Governance	Anforderungen an IKT-RisikoMgmt	Meldung IKT-bezogener Vorfälle	Prüfung der digitalen Betriebsstabilität	Risiko durch IKT-Drittanbieter	Informations-austausch
Level 1						
Level 2		○ RTS –IKT-RiskoMgmt Framework ● **GL – Schätzung der Kosten und Verluste durch Vorfälle**	○ RTS – IKT Vorfall Klassifizierung ● **RTS – Meldung von schwerwiegenden Vorfällen** ● **ITS – Meldedetails von schwerwiegenden Vorfällen**	● **RTS – Tests der digitalen Betriebsstabilität**	○ RTS – Drittanbieter-Risiko Policy ○ ITS – Template des Informationsregisters ● **RTS – Klassifizierung von Auslagerungs-DL** ● **RTS – Überwachungs-rahmenwerk für kritische DL**	*

*GL- Kooperation zwischen ESAs und CAs

ISACA Germany Chapter

Die öffentliche Konsultation steht vor der Tür



*Alternativ esma.europa.eu oder eiopa.europa.eu

ISACA Germany Chapter

Die öffentlic

Nov

Jan 2025

Ende des Implementierungszeitraums

Veröffentlich

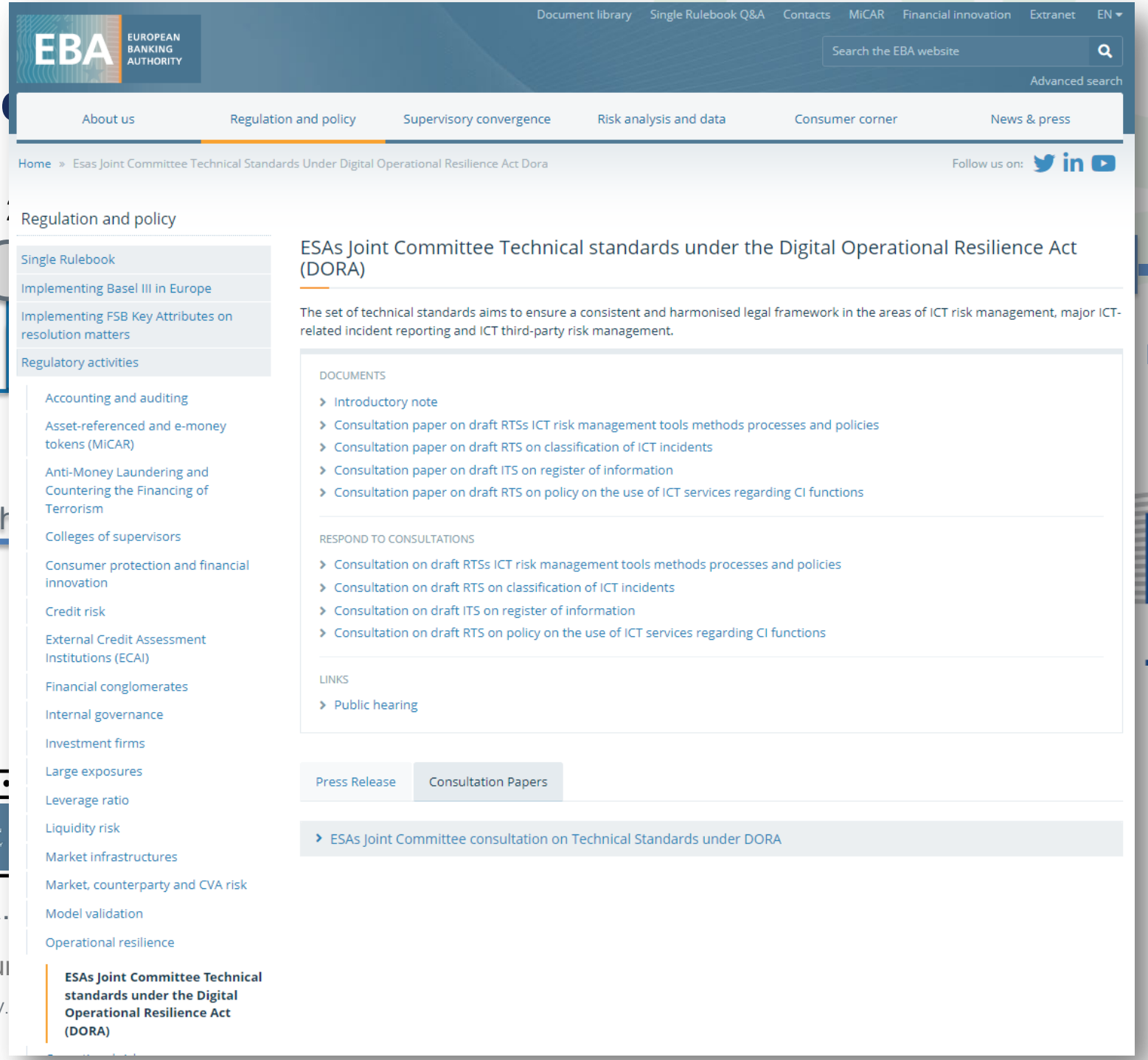
Draft

ESAs

eba.europa.

*Alternativ esma.eu

Europäische Kommission



ISACA Germany Chapter

Die öffentl

Nov

ESAs

Veröffentli

Draf

eba.europ

*Alternativ esma.e

EB

5. D
stan

laying
the reg

THE EUR

Having re

Having re
of 14 Dec
Regulatio
and (EU)

Whereas:

(1) Ar
IC
co
co
Se

(2) In
de
te
co

(3) Th
of
fra
in
Re
20
at
fra

(4) Fi
in

Co

On
ten
cor
thi
202

EBA ESMA JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Overview of questions for consultation

1. Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?

2. Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?

3. When implementing the Register of Information for the first time:

   - What would be the concrete necessary tasks and processes for the financial entities?
   - Are there any significant operational issues to consider?

   Please elaborate.

4. Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?

5. Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?

6. Do you see significant operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at entity level?

7. Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?

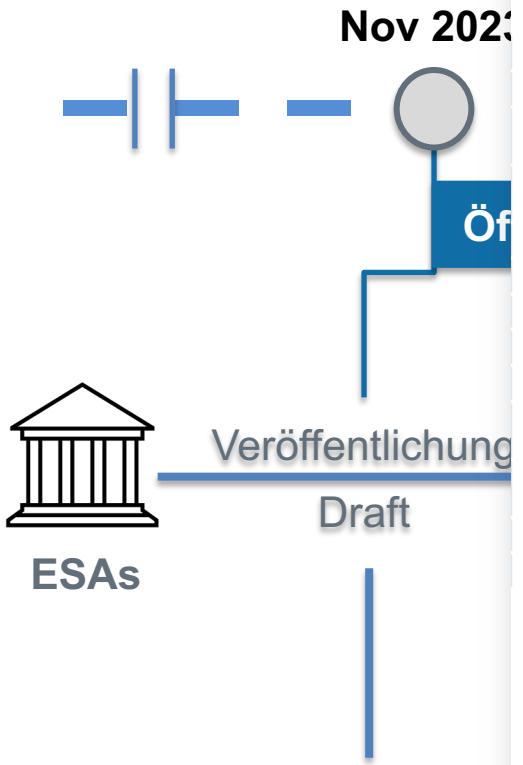
Jan 2025

Ende des
plementierungs
zeitraums

ropäische
mmission

ISACA
Germany Chapter

Die öffentlich



Liquidity risk
Market infrastructures
Market, counterparty and
Model validation
Operational resilience
ESAs Joint Committe standards under the Operational Resilien (DORA)
Operational risk
Own funds
Passporting and supervis branches
Payment services and ele money
Recovery, resolution and
Supervisory benchmarkir
Remuneration
Securitisation and Covere
Supervisory reporting
Supervisory Review and E Process (SREP) and Pillar
Third country equivalenc international cooperatior
Transparency and Pillar 3
Other topics

EIO

JC 2023 36

Deadline:

Joint
Cons

Draft
the te
in rela
use of
servic
2022/

Backgr

The Digital
EIOPA and
ensure a c
related inc

The first ba

- RT fra
- RT
- RT
- ITS

German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Consultation on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Berit Schimm
Telephone: +49 30 2021- 2111
E-mail: b.schimm@bvr.de

Berlin, 2023-09-08

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry.

25

s
rungs
ns

SACA
many Chapter

Now its your turn!

ISACA Germany Chapter

ISACA Fachgruppe IT-Compliance im Finanz- und Versicherungswesen

Die Fachgruppe vernetzt gezielt ISACA-Mitglieder und Anwender aus dem Finanz- und Versicherungswesen und bietet ihnen ein Forum für den Erfahrungsaustausch im Hinblick auf die Umsetzung dieser Anforderungen.

Hierzu beschäftigt sie sich insbesondere mit

- Bewertung bzw. Kommentierung neuer und überarbeiteter Regularien
- Erarbeitung von Arbeitshilfen zur Umsetzung der Vorgaben
- Diskussion und Erfahrungsaustausch zu Umsetzungen der Vorgaben, Best-Practices und Entwicklung der Regulatorik

Kontakt

E-Mail: fg-it-compliance-fvw@isaca.de

Web: https://www.isaca.de/ueber-uns/fachgruppen-2/fachgruppe-it-compliance-im-finanz-und-versicherungswesen.html

ISACA Germany Chapter

Ihre Speaker

Patrick Schmidt, CISA
E-Mail: patrick.schmidt@deutsche-boerse.com
LinkedIn: linkedin.com/in/patrick-schmidt-00a23311a

Dr. Christian Schwartz, CISM, CRISC, GSTRT
E-Mail: christian.schwartz@usd.de
LinkedIn: https://www.linkedin.com/in/schwartzc

ISACA Germany Chapter