FORUM Anwendertagung
24.05. – 26.05.2023

FORUM
Gesellschaft für
Informationssicherheit mbH

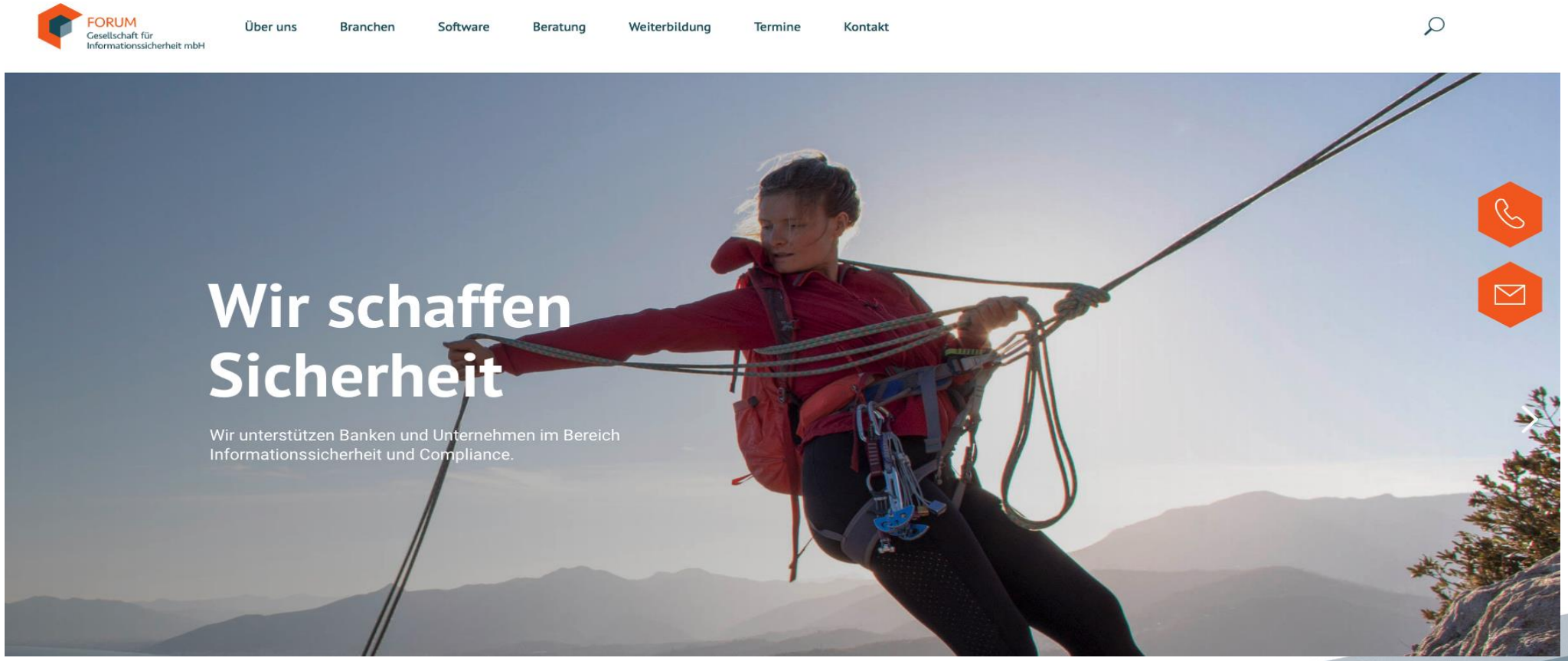
Organisatorisches

- Hybrid-Veranstaltung (vor Ort und virtuell)
- Livestream aus Dresden
- Mehr als 100 Teilnehmer, daher Stummschaltung
- Die Veranstaltung wird nicht aufgezeichnet
- Teilnehmer-Umfragen für Interaktion und Meinungsbildung (mit QR-Code)
- Nutzung des Hotel-Checkouts bereits am Donnerstag

Organisatorisches

- Die Präsentationen stehen im Unterlagenbereich zum Download zur Verfügung
- Feedbackbogen im Nachgang
- Übersendung eines Teilnehmerzertifikats
- Danke an die FORUM-MitarbeiterInnen für die tolle Vorbereitung
- Nächste Anwendertagung: **12.06. – 14.06.2024**

Neue FORUM-Website ab 01.06.2023



Agenda

Mittwoch, 24. Mai 2023

- **14:00 Uhr** **Begrüßung durch die Geschäftsführung**
- **14:15 Uhr** **Inside FORUM – Podiumsdiskussion zur BAIT- und DORA-Umsetzung**

  Referenten: Martin Wiesenmaier, Jörg Weske, Dr. Katharina Petzold
- **15:30 Uhr** **Kaffeepause**
- **16:00 Uhr** **Neues Rollen- und Rechtekonzept in der ForumSuite**

  Referenten: Jörg Weske, Aron Mildemann, Henrik Lehmann
- **17:00 Uhr** **Ende**
- **18:30 Uhr** **Abendprogramm**

Agenda

Donnerstag, 25. Mai 2023

- **09:00 Uhr** **Aktuelle Anforderungen der Bankenaufsicht (Teil 1)**
  Referent: Henning Riediger, Deutsche Bundesbank
- **10:30 Uhr** **Kaffeepause**
- **11:00 Uhr** **Aktuelle Anforderungen der Bankenaufsicht (Teil 2)**
  Referent: Henning Riediger, Deutsche Bundesbank
- **12:00 Uhr** **Mittagspause**
- **13:00 Uhr** **Aufsichtsrecht: Wenn Widerstand zum Risiko wird**
  Referentinnen: Petra Förster, Judith Bollinger (Beratung-auf-Sicht GmbH)

Agenda

Donnerstag, 25. Mai 2023

- **13.30 Uhr** **Compliance-Management aus einem Guss**
  Referenten: Jan Gschwandtner, Florian Rößle, Frank Felsmann (AWADO WPG)
- **14.30 Uhr** **Kaffeepause**
- **15:00 Uhr** **Praxisbericht: Umsetzung Banken-SiMaKat**
  Referenten: Marco Grether, Florian Geißer, Sarah Niederer (BBBank eG)
- **15:45 Uhr** **Praxisbericht: Überwachungshandlungen des ISB**
  Referent: Matthias Weskamp (Bank für Kirche und Caritas eG)
- **16:30 Uhr** **Ende**
- **18:15 Uhr** **Abendprogramm**

Agenda

Freitag, 26. Mai 2023

- **09:00 Uhr** **Notfallmanagement gemäß BSI-Standard 200-4 und BAIT**

  Referenten: Martin Wiesenmaier, Henning Wilhelm

- **10:00 Uhr** **Kaffeepause**

- **10:30 Uhr** **Ausblick und Innovationen**

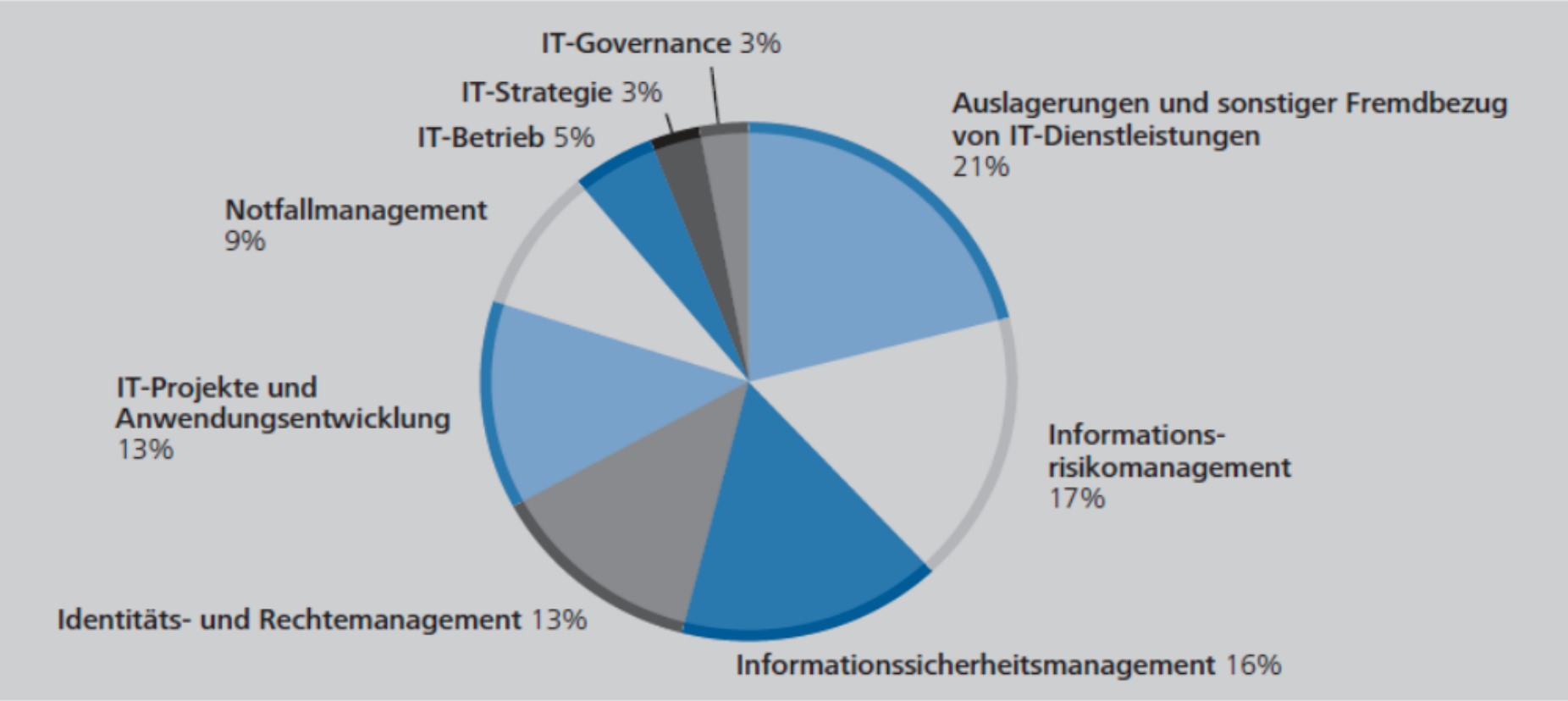
  Referenten: Martin Wiesenmaier, Jörg, Weske

- **12:30 Uhr** **Abschluss der Anwendertagung**

  danach Mittagssnack

Podiumsdiskussion zur Umsetzung der BAIT und DORA

Wesentliche Mängel aus IT-Prüfungen der letzten 10 Jahre



Quelle: Deutsche Bundesbank, Monatsbericht – Juli 2021, S. 64

… die größten Baustellen

Informationsrisikomanagement:

- Erweiterter Informationsverbund (Abhängigkeiten und Schnittstellen)
- Prozesslandkarte mit fachlichen Geschäftsprozessen und IT-Prozessen
- Sollmaßnahmenkatalog / Banken-SiMaKat
- Steuerung und Überwachung von risikoreduzierenden Maßnahmen
- Überprüfung von Schutzbedarfs- und Risikoanalysen durch das IRM

… die größten Baustellen

Informationssicherheitsmanagement:

- Test und Überprüfung von Maßnahmen zum Schutz der Informationssicherheit (BAIT 4.8)

Operative Informationssicherheit:

- Sicherheitsrelevante Ereignisse und Vorfälle (BAIT 5.5)
- Regelmäßige Überprüfung der Sicherheit der IT-Systeme (BAIT 5.6)

… die größten Baustellen

(IT-)Notfallmanagement:

- Risikoanalyse / Business Impact Analyse
- Festlegung der zeitkritischen Geschäftsprozesse und Schutzobjekte
- Ableitung von Notfallszenarien für die zeitkritischen Prozesse
- Erstellung von (IT-)Notfallkonzepten
- Festlegung von Abhängigkeiten und Parametern (u.a. RTO / RPO)
- Jährliche Übungen

… die größten Baustellen

Auslagerungsmanagement:

- Erweiterte Kriterien für die Risikoanalyse
- Erweiterung der vertraglichen Anforderungen
- Kriterienbasierte Überwachung der Auslagerungen (SLA, KPI)
- Wesentliche Weiterverlagerungen
- Auslagerungsbeauftragte(r) / zentrales Auslagerungsmanagement
- Auslagerungsregister mit EBA-Pflichtangaben

Rückblick zur BAIT-Umsetzung

Prozesslandkarte

Diskussionspunkte

- Informationsverbund mit Geschäfts- und Unterstützungsprozessen
- BAIT: Berücksichtigung von „zugehörigen IT-Prozessen“
  - Neue BVR-Prozesslandkarte wird bislang von den Kunden relativ verhalten angenommen und umgesetzt
  - Erweiterung um IT-Prozesse durch BVR vorgesehen
  - Zeitnahe Umsetzung der Erweiterung durch FORUM als Vorschläge in der ForumSuite

Prozesslandkarte

- Geschäftsprozesse haben als Stammdaten in der ForumSuite „universelle Ausstrahlungskraft“ zur Umsetzung regulatorischer Anforderungen:
  - **ForumISM**: Informationsverbund, Schutzbedarfsklassifizierung, Grundlagen für ISB-Überwachung
  - **ForumBCM:** Zeitkritische Prozesse im Notfallmanagement
  - **ForumDSM:** Verarbeitung personenbezogener Daten in Geschäftsprozessen
  - **ForumOSM:** Ausgelagerte Prozesse im Outsourcing-Management
  - **ForumNSR:** Schutzbedarf und Festlegung Sollmaßnahmenkatalog, Banken-SiMaKat, LFI, ISO 2700X

Umsetzung der neuen ISO 2700X

- Anlass für Aktualisierung in 10/2022: Reaktion auf **zunehmende Cyberbedrohungen**
- Bisher: Informationstechnik – Sicherheitsverfahren – ISMS-Anforderungen
- Neu: Informationssicherheit, **Cybersicherheit** und **Datenschutz** –ISMS-Anforderungen
- Aktuell sind 27001 und 27002 in Englisch und als deutsche Entwurfsfassung verfügbar
- Voraussichtlich im Juni wird eine **finale Fassung** beider Dokumente erwartet
- **Mapping-Tabelle** für bestehende Controls in DIN 27002
- Reduzierung der Controls im Anhang A von 114 auf 93

Umsetzung der neuen ISO 2700X

- **Deutliche Reduzierung der Abschnitte von bisher 14 auf künftig 4:**
  - Organisatorische Maßnahmen
  - Personenbezogene Maßnahmen
  - Physische Maßnahmen
  - Technologische Maßnahmen

- **Zahlreiche komplett neue Maßnahmen, wie z.B.:**
  - Informationssicherheit für Cloud-Dienste
  - Verhinderung von Datenlecks
  - Sicheres Coding

Umsetzung der neuen ISO 2700X

„Hashtag-Einstufungen“ für die Maßnahmen der DIN 27002

- Maßnahmenart (z.B. #Präventiv, #Detektiv, #Korrektiv)
- Informationssicherheitseigenschaften (z.B. #Vertraulichkeit, #Integrität, #Verfügbarkeit)
- Konzepte zur Cybersicherheit (z.B. #Identifizieren, #Erkennen, #Reagieren)
- Betriebsfähigkeit (z.B. #System- und Netzwerksicherheit, #Informationsschutz)
- Sicherheitsdomänen (z.B. #Verteidigung, #Resilienz)

Umsetzung der ISO 2700X in ForumNSR

Diskussionspunkte:

- Abbildung in **ForumNSR** als neuen Katalog?
- Auswirkungen auf Banken-SiMaKat?
- Termin für neues Release des Banken-SiMaKat?

Umsetzung Banken-SiMaKat

- Banken-SiMaKat als sehr relevantes Thema bei den FORUM-Kunden
- Zahlreiche Umsetzungsfragen an der FORUM-Hotline, im Ticketsystem und per E-Mail
- Zahlreiche Workshops durch FORUM-Berater
- Video zum Banken-SiMaKat in der FORUM Academy kommt sehr gut bei Kunden an
- Neue Komfortfunktionen in **ForumISM** zur effizienten Bearbeitung

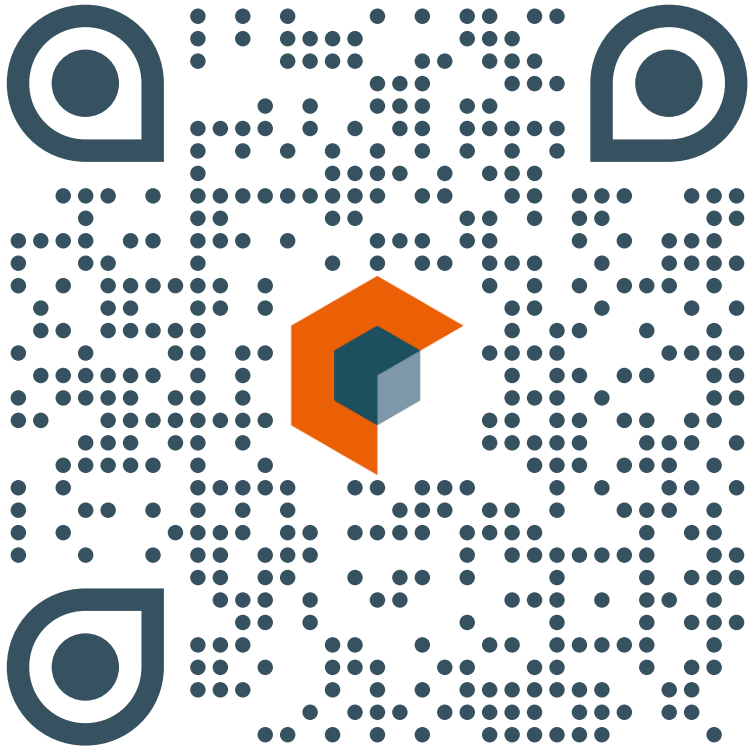
Live-Demo zu Banken-SiMaKat

in **ForumISM**

Sollmaßnahmenkatalog für Dienstleister

- Häufig gewünschtes Thema von Kunden
- Ggf. weiterer Cluster für Dienstleister im Banken-SiMaKat?
- Erfassung von Sollmaßnahmen an Leistungen bereits in der ForumSuite realisiert
- Nächste Ausbaustufe: Excel-Export und Import der vom Dienstleister bearbeiteten Datei
- Nicht umgesetzte Sollmaßnahmen beim Dienstleister führen zu Auslagerungsrisiken
- Umgang mit organisationsrelevanten Maßnahmen aus dem Banken-SiMaKat?

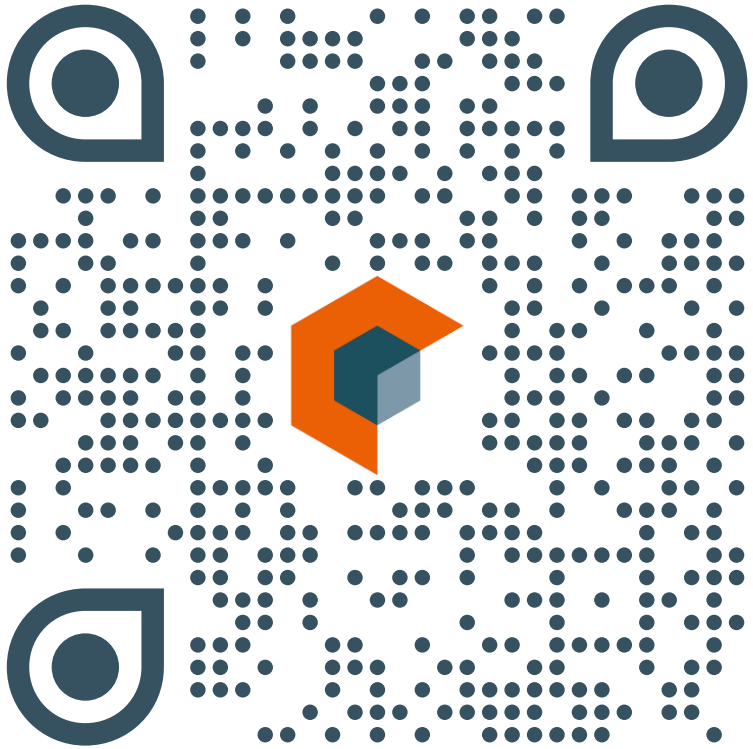
Teilnehmer-Umfrage
www.forum-is.de/umfragen



Welchen **IT-Standard** setzt Ihre Bank als Grundlage für das Informationsrisikomanagement ein?

1. ISO 2700X
2. BSI-Grundschutz-Kompendium

Teilnehmer-Umfrage
www.forum-is.de/umfragen



Welchen **Sollmaßnahmenkatalog** setzt Ihre Bank ein?

1. Bankindividueller Sicherheitsmaßnahmenkatalog (Banken-SiMaKat)
2. BSI-Grundschutz-Kompendium
3. Individueller Sollmaßnahmenkatalog

Umsetzung DORA in der ForumSuite

Ausgangssituation

- DORA: EU-Verordnung zur digitalen operationalen Resilienz im Finanzsektor
- Zielsetzung: Finanzsektor in der EU **widerstandsfähiger und sicherer** gestalten („Stärkung der digitalen operationellen Resilienz“)
- Verordnung wurde am 17.01.2023 im EU-Amtsblatt veröffentlicht
- Umsetzungsfrist: 24 Monate
- Erstellung zahlreicher **technischer Regulierungsstandards** über delegierte Rechtsakte durch ESA

  zum 17.01.2024 bzw. 17.07.2024 vorgesehen
- DORA gilt verbindlich ab dem **17.01.2025**

Schwerpunkte der DORA

- DORA enthält **gezielte Vorschriften** zu:
  - IKT-Risikomanagement
  - Meldung von Vorfällen
  - Tests der operationalen Resilienz
  - Überwachung kritischer IKT-Drittdienstleister (inkl. Informationsregister)

- Zahlreiche Anforderungen der DORA sind bereits in den BAIT enthalten, werden aber weiter verschärft oder ergänzt (z.B. Sicherheitsvorfälle)

Umsetzungsplanung FORUM Suite

Generelle Vorgehensweise

- Abwarten, bis die **technische Regulierungsstandards** vorliegen
- Abwarten, bis die BaFin die DORA-Anforderungen in die **BAIT** eingearbeitet hat
- Abwarten, bis der BVR bzw. der Verfahrenslieferant die DORA-Anforderungen in den **Leitfaden IT-Regulatorik** (LFI) eingearbeitet hat und **Arbeitshilfen** zur Verfügung stehen
- AWT: frühzeitige Diskussion ausgewählter Themen zur DORA-Umsetzung

Umsetzungsplanung ForumISM

IKT-Risikomanagement

- Vererbung der IKT-Kritikalität über Geschäftsprozesse
- Dokumentation der IKT-Relevanz am Schutzobjekt („IKT-Asset“)
- Idee: Übergreifende Risiken + Übergreifende Maßnahmen
- Bewertung von (Cyber-)Bedrohungen und Schwachstellen
- Neue auswertbare Risikoarten (z.B. für Cyberbedrohungen und IKT-Schwachstellen)

Umsetzungsplanung ForumISM

Meldung IKT-bezogener Vorfälle

- Einrichtung eines Prozesses für die Erkennung, Behandlung und Meldung IKT-bezogener Vorfälle
- Dokumentation und Bewertung für IKT-bezogene Vorfälle
- Klassifizierung der Vorfälle nach ihren Auswirkungen („schwerwiegend“)
- Definition von Wesentlichkeitsschwellen für Melderelevanz
- Meldung wesentlicher IKT-bezogener Vorfälle an die Behörden (inkl. schwerwiegender PSD 2-Vorfälle)

Umsetzungsplanung ForumISM

Meldung IKT-bezogener Vorfälle

- Umsetzungsideen:
  - Erweiterung der bisherigen Sicherheitsvorfälle
  - Zwischenstufe über Anzeigenverordnung
  - Aufnahme des Kriterienkatalogs
  - Ergebnisdokumentation
  - Nachbetrachtung („lessions learned“)
  - Erfassung von Nachsorgemaßnahmen
  - Herleitung Schweregrad

Umsetzungsplanung ForumISM

Tests der operationalen Resilienz

- Planung, Dokumentation und Reporting von eigenen Tests und der IKT-Dienstleister
- Orientierung an Notfallübungen in **ForumBCM**
- Mind. jährliche Sicherheitstests für Anwendungen und Systeme, die **kritische oder wichtige Funktionen** unterstützen
- Etablierte Wesentlichkeitskriterien noch ausreichend (z.B. Zeitkritikalität)?
- Flexible Relevanzen für Definition der Wesentlichkeit („DORA-Relevanz“)
- Auswertbarkeit der DORA-relevanten Prozesse und Schutzobjekte
- Ziel: risikoorientiertes Testprogramm mit abgestuften Intervallen und wirksamen Testformen (z.B. Penetrationstests, Cyberattacken)

Überwachung kritischer IKT-Dienstleister

- Dienstleister und Leistungen in **ForumOSM**
  - Kennzeichnung als kritische oder wichtige Funktion (ggf. über verknüpfte Geschäftsprozesse)
  - Dokumentation der IKT-Relevanz
  - Risikoanalyse nach vorgegebenen IKT-Kriterien (geht über MaRisk hinaus)
  - Steuerung und Überwachung
  - Kritische IKT-Dienstleister müssen die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit einhalten

- Informationsregister
  - Pflichtangaben für alle IKT-Dienstleistungen
  - Klassifizierung von kritischen oder wichtigen IKT-Dienstleistungen
  - Zusatzangaben gehen über EBA-Auslagerungsregister hinaus

Umsetzungsplanung FORUM Suite

Strategie der FORUM

- Frühzeitige Auseinandersetzung mit den neuen und verschärften Anforderungen
- Berücksichtigung der technischen Regulierungsstandards und Vorarbeiten aus dem Verbund
- Erstellung eines **fachlichen und technischen Umsetzungskonzepts** in der FORUM Suite
- **Frühzeitige Abstimmung** der Entwicklungsschritte mit ausgewählten Kunden und Partnern

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

FORUM
Gesellschaft für Informationssicherheit mbH

DRESDEN
Obergraben 17a
01097 Dresden

Tel: (0351) 30 70 74 0
Fax: (0351) 30 70 74 99

E-Mail: forum@forum-is.de
Web: www.forum-is.de