Umsetzung DORA in der ForumSuite

FORUM
Gesellschaft für
Informationssicherheit mbH

Agenda

- Rückblick zur Anwendertagung 2023
- DORA-Umsetzung in 3 Phasen
- Feature-Set für Starterpaket
- Feature-Set für Phase 2
- Feature-Set für Phase 3

Rückblick zur Anwendertagung 2023

Strategie der FORUM zur DORA-Umsetzung

Folie aus 2023

- Die **ForumSuite** deckt bereits heute die Anforderungen der BAIT vollständig ab, sodass hinsichtlich der DORA ein Umsetzungsstand von 70-80 % je Themengebiet erreicht wird
- Das Notfallmanagement in **ForumBCM** sowie die Umsetzung von IT-Standards in **ForumNSR** sind bereits „DORA ready“
- Frühzeitige Auseinandersetzung mit den neuen DORA-Anforderungen
- Berücksichtigung der technischen Regulierungs- und Implementierungsstandards
- Abwarten, bis der BVR bzw. der Verfahrenslieferant die DORA-Anforderungen in den **Leitfaden IT-Regulatorik** (LFI) eingearbeitet hat und **Arbeitshilfen** zur Verfügung stehen
- Erstellung eines **fachlichen und technischen Umsetzungskonzepts** in der FORUM Suite
- **Frühzeitige Abstimmung** der Entwicklungsschritte mit ausgewählten Kunden

Umsetzungsplanung in ForumISM

Folie aus 2023

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 in ForumISM

Folie aus 2023

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 in ForumISM

Folie aus 2023

Meldung IKT-bezogener Vorfälle

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

Umsetzungsplanung in ForumISM

Folie aus 2023

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
- Ziel: risikoorientiertes Testprogramm mit abgestuften Intervallen und wirksamen Testformen (z.B. Penetrationstests, Cyberattacken)

Umsetzungsplanung in ForumOSM

Folie aus 2023

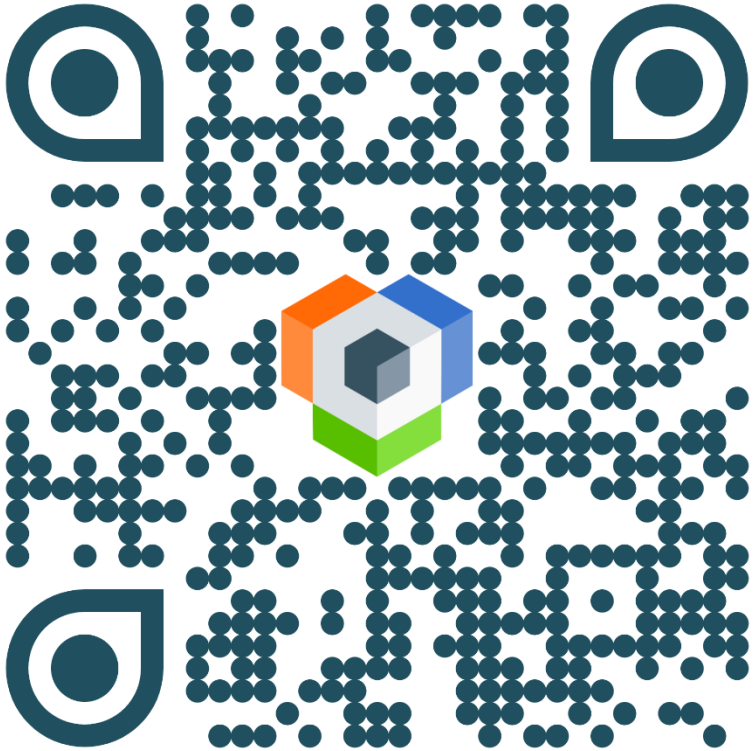
Dienstleister und Leistungen

- 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

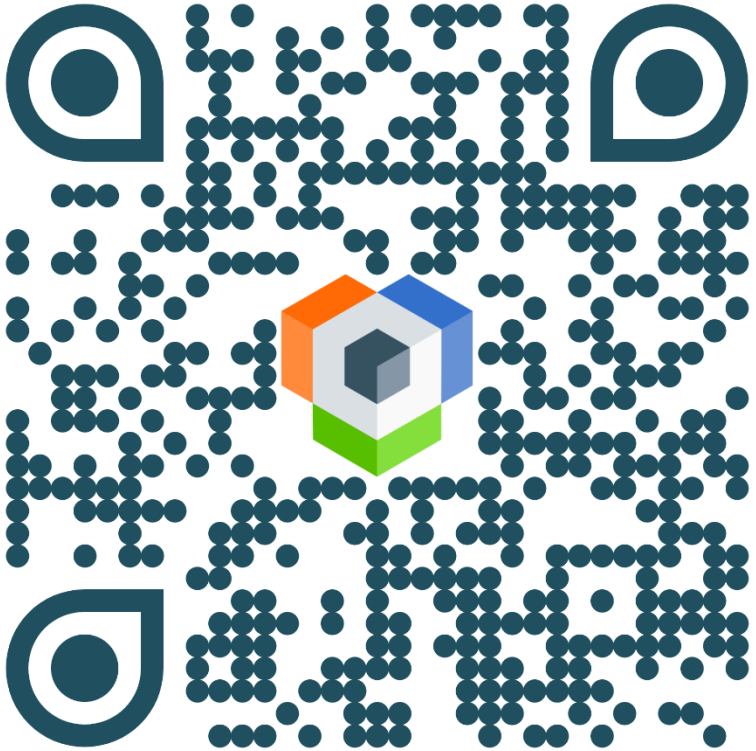
Teilnehmer-Umfrage
www.forum-is.de/umfragen



Wie stufen Sie den aktuellen Umsetzungsstand der DORA-Anforderungen in Ihrem Unternehmen ein?

1. kleiner 50%
2. kleiner 75%
3. größer 75%

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



Wie schätzen Sie den Umsetzungsaufwand hinsichtlich der DORA-Umsetzung in Ihrem Unternehmen ein?

1. gering (kleiner 50 Personentage)
2. mittel (kleiner 200 Personentage)
3. hoch (größer 200 Personentage)

DORA-Umsetzung in 3 Phasen

DORA-Umsetzung in 3 Phasen

Ziele des Projekts:

- Zeitgerechte Releasepakete mit DORA-spezifischen Feldern, Funktionen und Methoden
- Berücksichtigung sämtlicher aufsichtlichen und verbundspezifischen Regelwerke und Konzepte
- Praxisgerechte und revisionssichere Umsetzung in der ForumSuite

Realisierung in der ForumSuite in 3 Phasen:

- Phase 1 im Sommer 2024: „Starterpaket“
- Phase 2 im Herbst 2024: „erweiterter Funktionsumfang“
- Phase 3 im Winter 2024: „ergänzende Funktionen“

Feature-Set für Starterpaket

Feature-Set für Starterpaket

Assetmanagement und Klassifizierung

- Klassifizierung von kritischen oder wichtigen Funktionen in der Prozesslandkarte
- Abhängigkeitsgrad: Vererbung von Eigenschaften auf IKT-Assets und Leistungen
  - Kritische oder wichtige Funktion, Zeitkritikalität, Schutzbedarf
  - Bisherige Unterscheidung „benötigt“ und „unterstützend“ entfällt bzw. wird migriert
- Zusätzliche Felder für IKT-Assets und Leistungen
  - Z.B. IKT-Altsystem, Technologie, Externer Zugriff

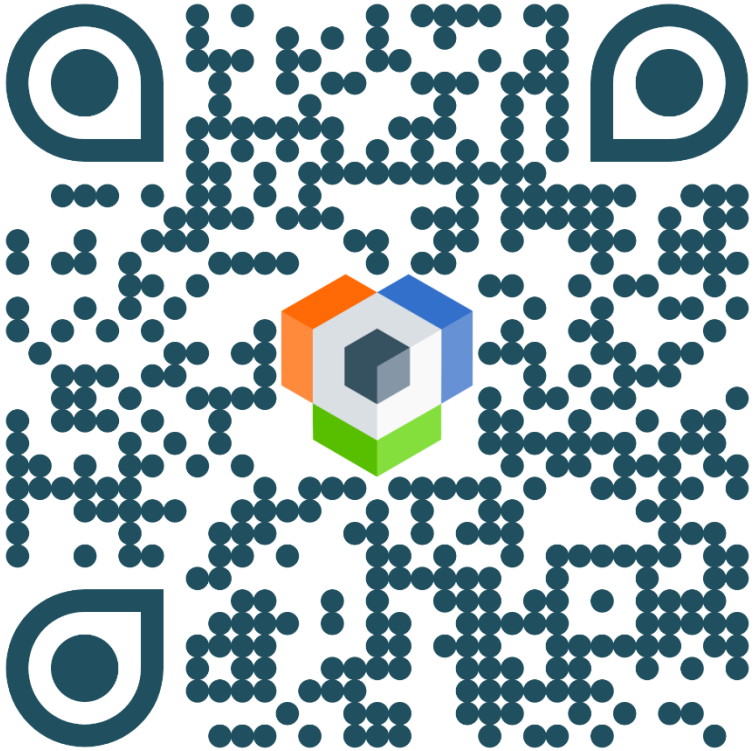
Feature-Set für Starterpaket

Assetmanagement und Klassifizierung

- DORA-konforme Umbenennungen
  - Menüstruktur
  - Neugliederung im Bereich „Assetmanagement“
  - Neue Begrifflichkeiten (z.B. IKT-Assets, Informationsklassen)

→ Live-Demo in ForumISM

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



Wird die Zeitkritikalität neben der Einstufung als kritische oder wichtige Funktion gemäß DORA weiterhin benötigt?

1. ja
2. nein

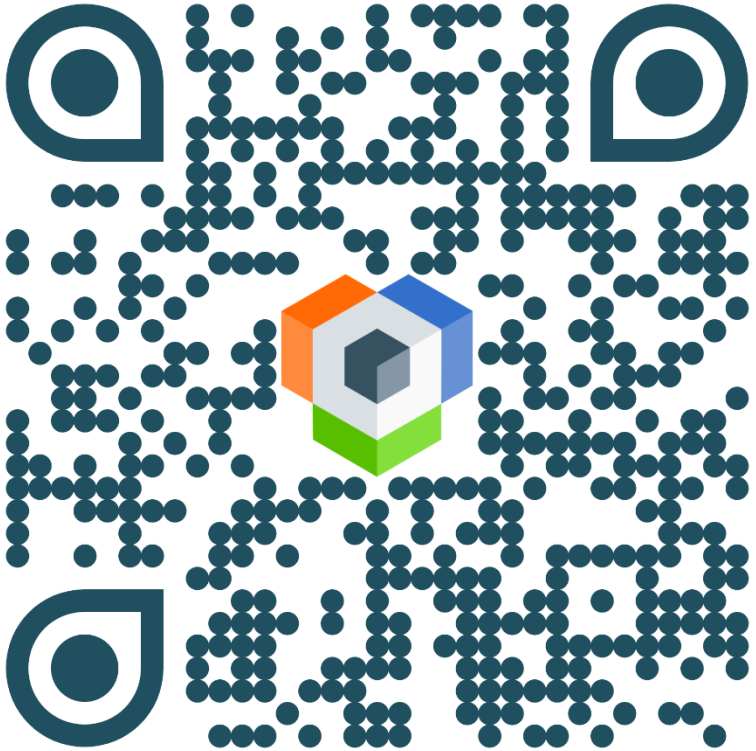
Feature-Set für Starterpaket

Schutzbedarfsklassifizierung

- Kombinierter Ansatz über Einstellungen parametrisierbar:
  - A-Wert (Verfügbarkeit) wird am Geschäftsprozess ermittelt
  - CIN-Werte (Vertraulichkeit, Integrität, Authentizität) werden an Informationsklassen ermittelt
- Vererbung an IKT-Assets und IKT-Dienstleistungen
- Rückbau des AACIN-Schemas mit Service- und Datenverfügbarkeit

→ Live-Demo in ForumISM

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



Setzt Ihr Unternehmen das AACIN-Schema für die Schutzbedarfsklassifizierung ein?

1. ja
2. nein

Feature-Set für Starterpaket

Sollmaßnahmenkatalog

- Unterstützung Soll-/Soll- sowie Soll-/Ist-Abgleich
- Abbildung des Banken-Sollmaßnahmenkatalogs (BaSo)
- Verweise auf ISO-Norm 2700X
- Zusätzliche Felder gegenüber BASI
- Hashtags gemäß ISO-Norm 2700X
  - z.B. #Resilienz, #Schutz, #Präventiv

→ Live-Demo in ForumNSR

Feature-Set für Starterpaket

IKT-Dienstleistungen

- Darstellung von IKT-Dienstleistungen in **ForumISM**
  - Für Anwender von **ForumOSM** bisher schon möglich
  - Für Anwender ohne **ForumOSM** als weitere IKT-Asset-Kategorie

- Klassifizierung von IKT-Dienstleistungen
  - Klassifizierung nach MaRisk
  - Neu: Klassifizierung nach DORA
  - Mapping der 19 IKT-Dienstleistungsarten gemäß DORA auf den zutreffenden BaSo-Cluster

Feature-Set für Starterpaket

IKT-Dienstleistungen

- Checkliste zur Vertragsprüfung gemäß DORA

- Zwei Reifegrade an Sollmaßnahmen:
  - vertraglich geregelt (Soll-/Soll-Abgleich)
  - operativ umgesetzt (Soll-/Ist-Abgleich)

→ Live-Demo in ForumOSM

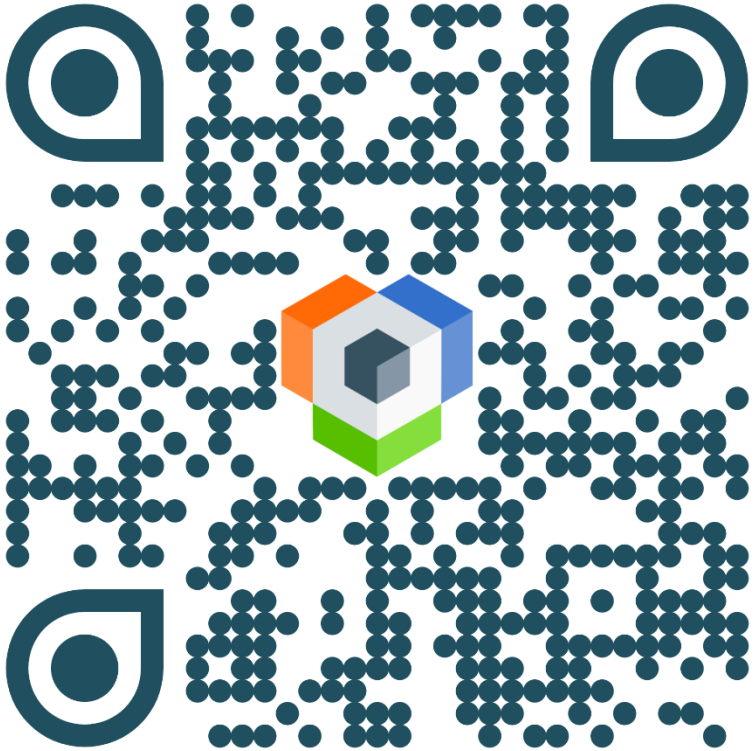
Feature-Set für Phase 2

Feature-Set für Phase 2

Assetmanagement

- Neue Verknüpfungs-/Vererbungslogik für Informationsklassen
- Ermittlung der Wesentlichkeit von Geschäftsprozessen aus der BIA
- Deaktivierung des Schutzniveaus in den Einstellungen

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



Wird die Schutzniveauklassifizierung künftig noch benötigt?

1. ja
2. nein

Feature-Set für Phase 2

IKT-Risikomanagement

- Überprüfung des Risikomanagements mit erweiterten Kriterien
  - z.B. zeitliche Entwicklung der IKT-Risiken
- Erweiterung der Bedrohungen
  - Neuer Bedrohungskatalog auf Basis BSI
  - Bedrohungsarten: mit und ohne Vorsatz
  - Zusätzliche Felder zur Ermittlung von Bedrohungsfaktoren

Feature-Set für Phase 2

IKT-Risikomanagement

- Erweiterung der Schwachstellen und Bedrohungsanalyse bis hin zur automatisierten Risikoermittlung
- Erweiterung der Risikoträger (z.B. Audits, Berichte, Vorfälle)

Feature-Set für Phase 2

ForumBCM ist bereits weitgehend DORA-konform
→überschaubarer Anpassungsbedarf

Notfallmanagement in ForumBCM

- Überarbeitung der Risk-Impact-Analyse
- Erweiterung der Notfallszenarien (z.B. Cyberangriff)
- Erweiterung der Gefährdungen
- Geringfügige Anpassungen an Notfallplänen und Übungen
- Erweiterung der Ereignisdokumentation

→ Live-Demo in ForumBCM

Feature-Set für Phase 2

IKT-Dienstleistungen

- Bereitstellung ergänzender Felder für das Informationsregister **ForumOSM**
- Verwendung der vorhandenen EBA-Felder soweit möglich
- Weitere Anpassungen in **ForumOSM**
  - Due Diligence
  - Erweiterung der Risikoanalysen gemäß DORA
  - Abgrenzung MaRisk/DORA Klassifizierung

Feature-Set für Phase 2

Erweiterung der Komfortfunktionen

- Workflow-Engine 2.0
  - Impulssteuerung
  - Vererbungen erst nach Freigabe
  - Wiedervorlagen als Workflow
- Teilautomatisierte Berichte
  - z.B. zeitraumbezogene Entwicklung der Risiken

Feature-Set für Phase 3

Feature-Set für Phase 3

Cyberbedrohungen

- Dokumentation und Behandlung von Cyberbedrohungen
- Ausgestaltung in Anlehnung an „sicherheitsrelevante Ereignisse“
- Erstellung von IKT-Vorfällen aus Cyberbedrohungen

IKT-Dienstleistungen

- Import von Sollmaßnahmen
- Exportmöglichkeit für das Informationsregister

Feature-Set für Phase 3

Test der operationalen Resilienz

- Testarten gemäß DORA
- Testplanung
- Testdurchführung
- Testdokumentation
- Ableitung Handlungsbedarf

Feature-Set für Phase 3

Management von Informationssicherheitsvorfällen

- Checkliste zur Ermittlung des Schweregrads
- Ergänzung weiterer Felder zur Klassifizierung von IKT-bezogenen Vorfällen
- Zusätzliche Felder für die Meldung von schwerwiegenden Sicherheitsvorfällen
- Zusätzliche Felder für die Information von Kunden bei schwerwiegenden Sicherheitsvorfällen
- Nachbetrachtung von Sicherheitsvorfällen
- Neue Auswertung: Kosten-/Verlustübersicht für Vorfälle

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