DORA zielgerichtet umsetzen

13. Juni 2024

ZAM eG

Agenda

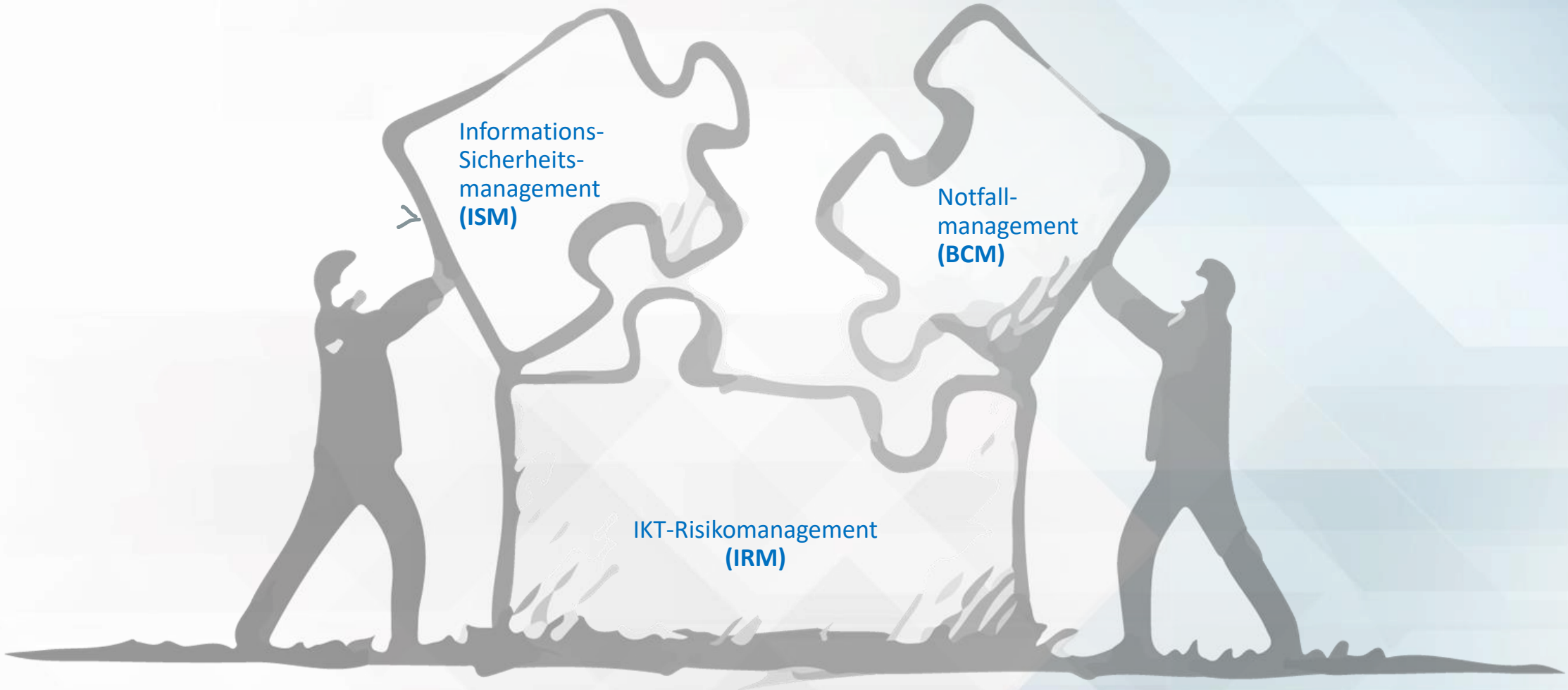
Termin

13.06.2024

Tagesordnung

1. **Entwicklung des Verfahrens**
2. **Handlungspakete aus DORA**
    1. Identifizierung
    2. Anpassung der Sicherheitsmaßnahmen
    3. Vorgehen und Umsetzung des Testprogramms
    4. IKT-Notfallmanagement
    5. Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen
3. **Fragen**

Entwicklung des Verfahrens

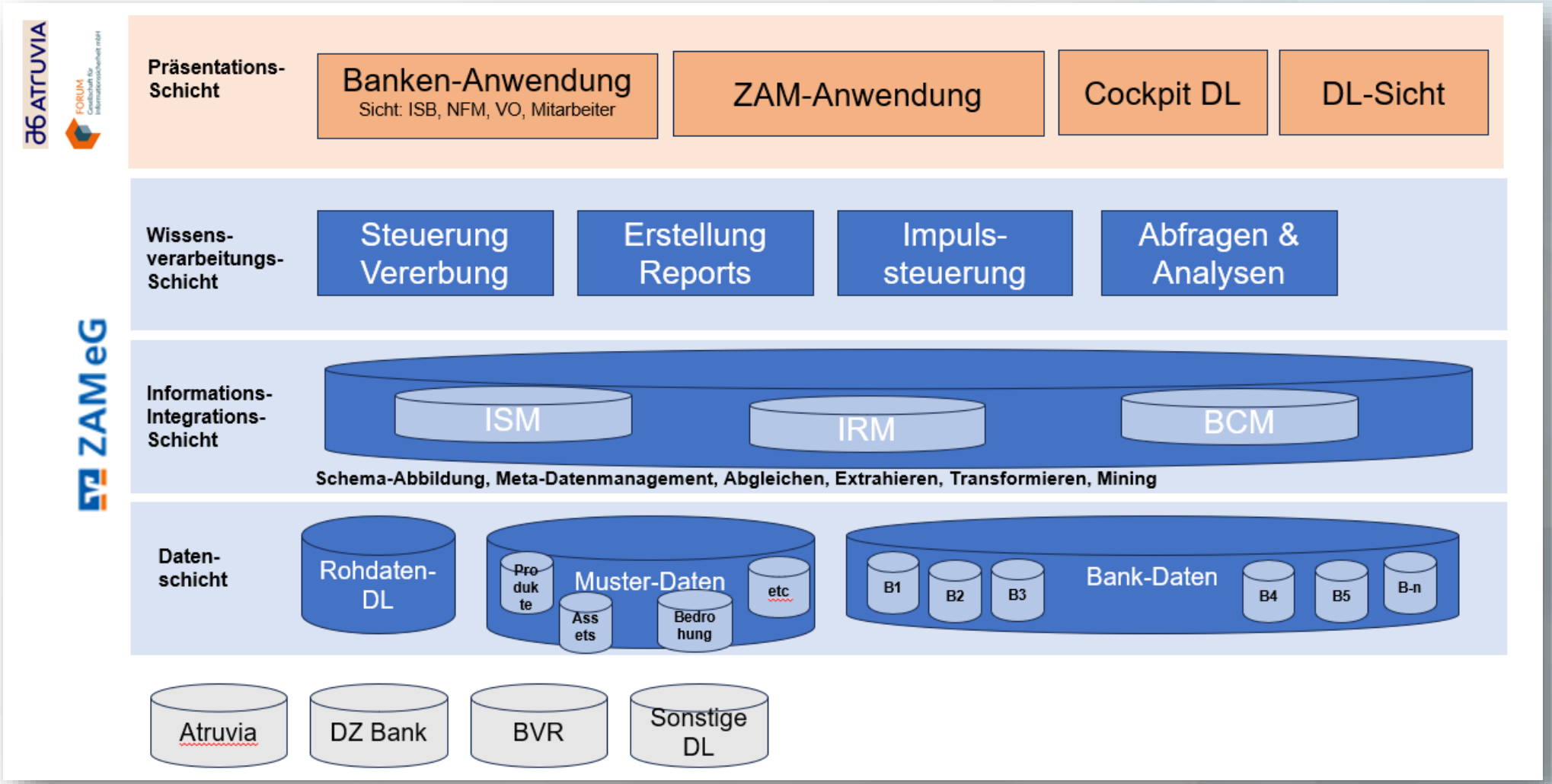


- Praxisnahe Umsetzung der Anforderungen an den zum Verfahren zugehörigen Themenfeldern

Entwicklung des Verfahrens

- Zentraler Verfahrenslieferant für die Genossenschaftliche FinanzGruppe Volksbanken Raiffeisenbanken (GFG)
- Zukunftsweisende, verbundeinheitliche und aufsichtskonforme Lösung
- Mit den Regionalverbänden, dem BVR und diversen Pilotbanken unterschiedlicher Bankgrößen und Regionen validiertes Verfahren
- Strukturierte Prozesse, automatisierte Bereitstellung vieler Musterinformationen
- Umsetzung der DORA-Anforderungen
- Bereitstellung der integrierten Software-Lösung im Systemumfeld der Atruvia
- Effiziente und effektive Umsetzung der Themenfelder durch maximale Muster-Vorbefüllung und bankindividueller Zuordnung

Entwicklung des Verfahrens



- Erstellung und Betrieb Software und Datenpool
- Anforderungs-management für Software (einschl. fachl. Vorgaben)
- Prüfung und Veredelung Daten der Dienstleister
- Maximale Vorbefüllung von Vorschlägen für die Bank

Bereitstellung des Verfahrens

Übersicht Ausbaustufen *)

Starterpaket Sommer 2024

In der ersten Stufe stellt die ZAM eG ihren Kunden den Banken-Sollmaßnahmenkatalog (BaSo), die Geschäftsprozesse inkl. Vorschläge für die jeweilige Business Impact Analyse (BIA), den Bedrohungskatalog, Informationsklassen, Schutzbedarfsklassifizierungen, grundsätzliche Dokumente wie bspw. Leitfäden, Richtlinien sowie diverse Muster und Vorschläge zur Verfügung.

Das Starterpaket mit bereits vielen DORA-relevanten Feldern wird von der Atruvia AG bereitgestellt. Die Versorgung mit Vorschlagswerten erfolgt durch die ZAM mittels einer allgemeinen Datenbank, die von der Atruvia AG automatisiert importiert wird. Erste Banken können bereits die neue Software-Suite nutzen.

DORA-Paket Herbst 2024

Die ZAM eG erfasst zentral die IKT-Assets der von ihr gesteuerten Dienstleister, führt mit diesen Dienstleistern die Soll-/Ist-Abgleiche für die zugehörigen IKT-Assets durch. Des Weiteren werden Risiken der Dienstleister als Risikovorschläge von der ZAM eG erfasst, Musterberichtsbausteine erstellt und weitere Dokumente wie bspw. Benutzerleitfäden bereitgestellt.

Alle Banken bekommen die neue Software-Suite über eine SaaS-Plattform der Atruvia AG, in der das Verfahren abgebildet sein wird. Dabei sind alle DORA-Erweiterungen im Verfahren enthalten. Die Atruvia AG bereitet die Anbindung an den Data Integration Hub (DIH) vor.

*) Grundvoraussetzung / verpflichtend zur Nutzung des Verfahrens ist der vorherige Abschluss der erforderlichen Verträge mit der ZAM eG und der Atruvia AG.

Übersicht Ausbaustufen *)

Ausbaupaket Winter 2024 / 2025

Abschließend wird in der letzten Stufe das Onboarding aller Beteiligten zum Verfahrenstool durchgeführt. Die von der ZAM eG gesteuerten Dienstleister werden gem. Sollmaßnahmen und Berichten gesteuert, deren Notfallübungen geprüft und bewertet sowie Audits durchgeführt. Das Verfahren wird gemäß bestehenden und zukünftigen regulatorischen Vorgaben stetig weiterentwickelt.

Alle Anforderungen an das Verfahren werden fristgerecht zum DORA-Start durch Atruvia AG bereitgestellt.

Finales Paket 2025

Letzte technische Features für eine effiziente und effektive Unterstützung werden durch die Atruvia AG bereitgestellt.

*) Grundvoraussetzung / verpflichtend zur Nutzung des Verfahrens ist der vorherige Abschluss der erforderlichen Verträge mit der ZAM eG und der Atruvia AG.

Leistungsangebot der ZAM eG

- Allgemein -

- Zukunftsweisende, verbundeinheitliche und aufsichtskonforme Lösung
  - Prozesse sowie Fachkonzepte zu den Verfahren ISM, IRM und BCM
  - Muster und Templates für verfahrensrelevante Dokumente (z.B. Berichtswesen)
  - Vorbefüllung gängiger IKT-Assets der Genossenschaftlichen FinanzGruppe (GFG)
  - Verwendung einheitlicher Geschäftsprozesse aus der Prozesslandkarte der Genossenschaftsbanken (BVR) mit Verknüpfung zu Informationsklassen und gängigen IKT-Assets
  - Abbildung und Überwachung von Risiken der GFG aus z. B. Schwachstellen bzw. Abweichungen zum Sollmaßnahmenkatalog
  - Vorschläge für verfahrensrelevante Workflows (z.B. Schutzbedarfsklassifizierung, Soll-Soll/Soll-Ist-Abgleich, IRM & BCM)
- Anforderungsmanagement
  - Identifizierung der Anforderungen aus regulatorischem Umfeld
  - Erhebung der fachlichen Abhängigkeiten innerhalb der GFG
  - Analyse mit Spezifikation und Priorisierung der Anforderungen
  - Validierung und Verifikation der Anforderungen
  - Fachliche Vorgaben an den Softwareentwickler und an den Softwarebetreiber
  - Kontrolle, Freigabe und Abnahme der einzelnen Weiterentwicklungen
  - Sicherstellung der konsistenten und aktuellen Dokumentation

Leistungsangebot der ZAM eG

- Methodische und fachliche Umsetzung -

- Banken-Sollmaßnahmenkatalog als zentrales Instrument zur Steuerung
  - Formulierung aller notwendigen Sollmaßnahmen aus den IT-regulatorischen Anforderungen
  - Automatisierte Erstellung von übergreifenden Sicherheitsrichtlinien
  - Integration eines bankindividuellen Soll-/Soll-Abgleichs der IT-regulatorischen Anforderungen mit der eigenen schriftlich fixierten Ordnung
  - Definition der bankeigenen Anforderungen an einen sicheren Einsatz der IKT-Assets
  - Verwendung als Grundlage und Bestandteil einer Vertragsanlage gegenüber Dienstleister zum Schutz der bankeigenen Informationen
  - Strukturierte Ableitung von IKT-Risiken aus den Soll-/Soll- und Soll-/Ist-Abgleichen nicht umgesetzter Maßnahmen

- IKT-Risikomanagement als zentrales Instrument zur Bewertung und Überwachung von:
  - nicht umgesetzten Maßnahmen innerhalb der schriftlich fixierten Ordnung (Soll-/Soll-Abgleich)
  - nicht umgesetzten Maßnahmen an den jeweiligen IKT-Assets (Soll-/Ist-Abgleich)
  - nicht umgesetzten Maßnahmen im Rahmen von Dienstleistungsverhältnissen
  - Schwachstellen, Sicherheitsvorfällen und Cyberbedrohungen
  - Feststellungen im Rahmen von Audit-, Test- und Prüfungshandlungen bezüglich der Informationssicherheit

- Notfallmanagement
  - Abbildung der Business Impact Analyse (BIA) für alle Geschäftsprozesse auf Basis der Ebene 3 der Prozesslandkarte der Genossenschaftsbanken
  - Entwicklung und Abbildung von Notfallszenarien für vorklassifizierte zeitkritische Geschäftsprozesse und IKT-Assets
  - Integration von Notfallplänen und Notfallübungen für vorentwickelte Notfallszenarien
  - Überwachung von Dienstleistungsverhältnissen bzgl. der vorentwickelten Notfallszenarien

Leistungsangebot der ZAM eG

- Vorschlagswesen -

- Bereitstellung von Vorschlägen
  - Für Informations-Assets
    - Informationsklassen inklusive Schutzbedarfsklassifizierung für die Schutzziele Vertraulichkeit, Integrität und Authentizität sowie deren Eigenschaften (steuerungsrelevant, rechnungslegungsrelevant und personenbezogen)
    - Geschäftsprozesse auf Basis der Ebene 3 der Prozesslandkarte für Genossenschaftsbanken des BVR mit bereits verknüpften Informationsklassen und IKT-Assets der durch die ZAM eG gesteuerten Dienstleister
    - Vererbung des Schutzbedarfs aus den verknüpften Informationsklassen sowie Vorbewertung für das Schutzziel Verfügbarkeit
  - Für IKT-Assets
    - Anwendungen der von der ZAM eG gesteuerten Dienstleister inkl. Schutzbedarfe, Soll-/Ist-Abgleiche und IKT-Risiken
    - IT-Systeme der von der ZAM eG gesteuerten Dienstleister inkl. Soll-/Ist-Abgleich
    - Gängige Infrastrukturobjekte
    - IKT-Dienstleistungen inkl. Schutzbedarfe, Soll-/Soll- und Soll-/Ist-Abgleich, IKT-Risiken sowie Notfallübungen
  - Für die Überprüfung der Informationssicherheit
    - Informationssicherheits-Audits und Kontrollen in Form von Kennzahlen
    - Test- und Prüfungsaktivitäten bei IKT-Assets (technische Audits)
  - Für Notfallmanagement
    - Business Impact Analyse (BIA)
    - Notfallszenarien
    - Notfallpläne
  - Für Berichte
    - Templates zum Informationssicherheits-, IKT-Risiko- und Notfallmanagement

Vergleich - aktuell vs. zukünftig

Mehrwerte

„Ready for DORA“

- Unterstütze Erfassung und Klassifizierung des Informationsverbundes durch umfassende Musterdatenbank
- Systematische Erkennung von Bedrohungen und Schwachstellen sowie Ableitung der IKT-Risiken
- Identifizierung und Priorisierung von Schwachstellen mit Hilfe vordefinierter Risiko- und Kontrollkataloge
- Erkennung von Abweichungen und Optimierungsmöglichkeiten im Rahmen eines Management-Reviews
- Schnelle und nachvollziehbare Reaktion auf festgestellte Non-Konformitäten in der IT-Regulatorik
- Verwendung des integrierten Audit-Moduls, um vollumfängliche Compliance zu gewährleisten
- Nutzung des integrierten Testmanagement-Moduls, um DORA-Compliance zu gewährleisten
- Verwendung von vordefinierten Berichten sowie Risiko- und Kontrollkatalogen
- Zeiteinsparungen durch automatisierte ISMS-Prozesse und Vermeidung vieler manueller Tätigkeiten

Vorteile mit Einsatz des Verfahrens*

Vorteile

- Regulatorische Sicherheit bei der Umsetzung
- Zentrale Bereitstellung von Mustern aller notwendigen Informations- und IKT-Assets der überwachten Dienstleister der ZAM
- Umfassende, in der GFG abgestimmte Sollmaßnahmen in Form des Banken-Sollmaßnahmenkatalogs (BaSo)
- Bereitstellung aller Muster von Soll- / Soll- und Soll- / Ist-Abgleiche inkl. der vorbewerteten IKT-Risiken der überwachten Dienstleister
- Automatisierte Bereitstellung von übergreifenden Sicherheitsrichtlinien auf Basis des BaSo
- Vorschläge für Risikobewertung automatisiert auf Basis bankeigener OpRisk-Parameter
- Zentrale Abstimmung des Notfallmanagements mit überwachten Dienstleistern
- Umfangreiche Vorschläge für ISM- und BCM-Kontrollen, die teilweise automatisiert im Verfahren stattfinden
- Reine Erfassungsaufwände, Abstimmungen mit vielen Dienstleistern und zentrale Kontrollen werden durch die ZAM ausgeführt und entfallen im Institut

Jährlicher Aufwand:
Kosten für das Verfahren

Ca. 2,0 MAK Kosten-ersparnis im Jahr

Ersparnis

15 % Reduktion in der 2nd line (ISB, IRM,..)

20 % Reduktion in der 1st line (Fachbereichen, IT)

40 % Reduktion aus Mehraufwand durch DORA

Jährliche Ersparnis:
ca. 0,5 MAK in der 2nd line
ca. 1,5 MAK in der 1st line

* Darstellung für eine mittelgroße Bank, die bereits gut aufgestellt ist in den Themen ISM, IRM und BCM

Agenda

Termin

13.06.2024

Tagesordnung

1. **Entwicklung des Verfahrens**
2. **Handlungspakete aus DORA**
    1. Identifizierung
    2. Anpassung der Sicherheitsmaßnahmen
    3. Vorgehen und Umsetzung des Testprogramms
    4. IKT-Notfallmanagement
    5. Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen
3. **Fragen**

Handlungspaket: Identifizierung

Referenzen DORA
Art. 8.1, 8.4-7

Referenzen RTS
RTS on ICT risk mgmt tools, methods, processes and policies Art. 4, 5

Wesentliche Anpassungen unter DORA
Informationsverbund der Bank wird durch Anforderungen an die Identifizierung und Klassifizierung ersetzt bzw. ergänzt

- Identifizierung und Klassifizierung von Informations- und IKT-Assets, Abhängigkeiten von IKT-Diensten
- erweiterte Anforderungen an IKT-Assetmanagement / Inventare
- Assets / IKT-Dienste, die kritische oder wichtige Funktionen unterstützen

Handlungsbedarf
Umsetzung der Einwertung von Funktion als "kritische oder wichtige Funktionen" oder sonstige Funktionen sowie etwaiger notwendiger Anpassungen am Informationsverbund.

Handlungspaket: Identifizierung

Unterstützung ZAM eG
Die ZAM eG wird kritische und wichtige Funktionen sowie kritische IKT-Assets im Verfahren darstellen. Alt-Systeme (EOL) und Systeme mit externen Netzwerkzugang sind ebenfalls im Verfahren abbildbar.

Das Verfahren bietet u. a.
Vorschläge für **Informationsklassen**, **Geschäftsprozesse** (aus der Prozesslandkarte der Genossenschaftsbanken - Ebene 3) und **IKT-Assets** sowie **IKT-Dienstleistungen** der von der ZAM eG gesteuerten Partner inkl. deren **Abhängigkeiten** mit **Schutzbedarfseinwertung** an. Daraus ermittelte **Gaps** werden **als Risiko** im Verfahren automatisiert zur Weiterverarbeitung aufbereitet.

Das Verfahren erzeugt Wiedervorlagen, um mindestens einmal jährlich zu prüfen, ob diese Klassifizierungen und jegliche einschlägige Dokumentation angemessen und aktuell ist.

Handlungspaket: Identifizierung -„Kritische oder wichtige Funktion“

Verbunddefinition der „Kritische oder wichtige Funktion“

DORA Kap. 3.22

„kritische oder wichtige Funktion“ eine **Funktion,**

deren Ausfall

- die **finanzielle Leistungsfähigkeit** eines Finanzunternehmens
- oder die **Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen** erheblich beeinträchtigen würde

oder

deren unterbrochene, fehlerhafte oder unterbliebene Leistung

- **die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen** eines Finanzunternehmens
- **oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht** erheblich beeinträchtigen würde;

Funktion = Bezeichnet Dienstleistung, Prozess oder Tätigkeit der Bank
Anknüpfungspunkt: welche Bankdienstleistungen/ Finanzservices erbringt die Bank, welche Prozesse (einschl. Management-/ Steuerungsprozesse) sind dafür notwendig?

Ergebnis der Schadensanalyse	Kriterien
Geschäftskritischer finanzieller Schaden	Wirtschaftliche Bedeutung
Aufgabenerfüllung ist kaum oder gar nicht mehr zu tätigen	Aufgabenerfüllung
Wahrnehmung in der breiten Öffentlichkeit, Ansehen kann erheblich und nachhaltig beschädigt werden	Reputation
Gravierende Konsequenzen bei Verstößen in Bezug auf das Finanzdienstleistungsrecht	Regulatorische Bedeutung

Handlungspaket: Identifizierung -„Kritische oder wichtige Funktion“

einmal Wert 4 = Kritische & wichtige Funktion

	Geschäftspolitische Bedeutung	Personal / Ressourcen	exogen bedingte Notwendigkeit	
	Wirtschaftliche Bedeutung	**Aufgabenerfüllung**	**Regulatorische Bedeutung**	**Reputation**
1	Der Prozess hat eine geringe Bedeutung hinsichtlich der Erreichung gesamtunternehmensbezogener, finanzieller Ziele.	Der Prozess beinhaltet wenige Schnittstellen zu anderen Prozessen (= geringe Abhängigkeit), benötigt wenige Ressourcen und/oder ist für die unternehmerische Aufgabenerfüllung (= Geschäftszweck) von geringer unmittelbarer Bedeutung.	Es existieren geringe regulatorische Anforderungen an den Geschäftsprozess; der Geschäftsprozess unterstützt unmittelbar lediglich in geringem Umfang die Einhaltung regulatorischer Anforderungen.	Der Prozess hat in seiner Ausführung lediglich geringe unmittelbare Auswirkung auf die Reputation des Unternehmens.
niedrig	Der finanzielle Schaden ist bei einem Ausfall nicht relevant [bis TEUR xx (individueller Wert der Bank, z.B. Bagatellgrenze)].	Die Aufgabenerfüllung ist auch bei einem Ausfall nicht beeinträchtigt.	Bei einer unterbrochenen, fehlerhaften oder fehlgeschlagenen Ausführung können Verstöße gegen regulatorische Anforderungen vorliegen, führen aber nicht zu Konsequenzen.	Auch bei einem Ausfall ist eine Wahrnehmung in der Öffentlichkeit nicht gegeben.
2	Der Prozess hat eine bedeutsame Bedeutung hinsichtlich der Erreichung gesamtunternehmensbezogener, finanzieller Ziele.	Der Prozess beinhaltet diverse Schnittstellen zu anderen Prozessen (= mittlere Abhängigkeiten), benötigt moderate Ressourcen und/oder ist für die unternehmerische Aufgabenerfüllung (=Geschäftszweck) von mittlerer unmittelbarer Bedeutung.	Es existieren moderate vertragliche und/oder rechtliche Anforderungen an den Geschäftsprozess; der Geschäftsprozess unterstützt unmittelbar lediglich in moderatem Umfang die Einhaltung regulatorischer Anforderungen.	Der Prozess hat in seiner Ausführung lediglich moderate unmittelbare Auswirkungen auf die Reputation des Unternehmens.
mittel	Der finanzielle Schaden ist bei einem Ausfall überschaubar [TEUR xx bis TEUR xx (individuelle Werte der Bank, z.B. bedeutender Schaden gemäß BTR 4 Tz. 3 MaRisk)].	Ein längerer Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Es ist mit Arbeitsrückständen zu rechnen.	Ein Nichterfüllen regulatorische Anforderungen und selbstauferlegter Verpflichtungen kann bei einer unterbrochenen, fehlerhaften oder fehlgeschlagenen Ausführung vorliegen, führt aber nur zu geringen Konsequenzen.	Bei einem Ausfall wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen.
3	Der Prozess hat eine hohe Bedeutung hinsichtlich der Erreichung gesamtunternehmensbezogener finanzieller Ziele.	Der Prozess beinhaltet viele Schnittstellen zu anderen Prozessen (=hohe Abhängigkeiten) benötigt viele Ressourcen und/oder ist für die unternehmerische Aufgabenerfüllung (= Geschäftszweck) von hoher, unmittelbarer Bedeutung.	Es existieren hohe regulatorische Anforderungen an den Geschäftsprozess; der Geschäftsprozess unterstützt unmittelbar in großem Umfang die Einhaltung regulatorischer Anforderungen.	Der Prozess hat in seiner Ausführung hohe Auswirkungen auf die Reputation des Unternehmens.
hoch	Der finanzielle Schaden ist bei einem Ausfall und nachhaltig spürbar [TEUR xx bis TEUR xx (individuelle Werte der Bank, z.B. bedeutender Schaden gemäß BTR 4 Tz. 3 MaRisk)].	Bei einem Ausfall ist der Geschäftsbetrieb massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.	Ein Nichterfüllen regulatorische Anforderungen und selbstauferlegter Verpflichtungen bei einer unterbrochenen, fehlerhaften oder fehlgeschlagenen Ausführung führt zu spürbaren Konsequenzen.	Eine nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist bei einem Ausfall intern und extern zu erwarten.
4	Der Prozess hat eine sehr hohe Bedeutung hinsichtlich der Erreichung gesamtunternehmensbezogener, finanzieller Ziele.	Der Prozess beinhaltet sehr viele Schnittstellen zu anderen Prozessen (=sehr hohe Abhängigkeiten), benötigt sehr viele Ressourcen und/oder ist für die unternehmerische Aufgabenerfüllung (= Geschäftszweck) von sehr hoher unmittelbarer Bedeutung.	Es existieren sehr hohe regulatorische Anforderungen an den Geschäftsprozess; der Geschäftsprozess unterstützt unmittelbar in immensem Umfang die Einhaltung regulatorischer Anforderungen.	Der Prozess hat in seiner Ausführung sehr hohe Auswirkungen auf die Reputation des Unternehmens.
sehr hoch	Der finanzielle Schaden ist bei einem Ausfall erheblich bzw. geschäftskritisch [größer TEUR xx (individueller Wert der Bank, z.B. existenzbedrohender Schaden)].	Ein längerer Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden.	Ein Nichterfüllen regulatorische Anforderungen und selbstauferlegter Verpflichtungen durch eine unterbrochene, fehlerhafte oder fehlgeschlagene Ausführung führt zu gravierenden Konsequenzen.	Bei einem Ausfall ist eine erhebliche bzw. fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, zu erwarten.

Definitionen	
Wesentlichkeit	**Kritische oder wichtige Funktion (DORA)**

A-Prozess	**B-Prozess**	**C-Prozess**
einmal Wert 4 in einer Kategorie oder der Durchschnitt größer/gleich als 3,0	Durchschnittswert kleiner 3,0 und größer/gleich 2,5	Durchschnittswert kleiner 2,5
wesentlich		nicht wesentlich

ZAM eG

Handlungspaket: Identifizierung -„Kritische oder wichtige Funktion“

Bsp. für die Bestimmung von kritischen/wichtigen IKT-Assets und Dienstleistungen

* **Grad der Abhängigkeit**
(nach JC 2023 85 - Final report on draft ITS on Register of Information de – RT.02.02.180)

1. **Nicht signifikant**

2. **Geringe Abhängigkeit**: Im Falle einer Unterbrechung der Dienste werden die unterstützten Funktionen nicht wesentlich beeinträchtigt (keine Unterbrechung, kein größerer Schaden) oder die Unterbrechung kann schnell und mit minimalen Auswirkungen auf die unterstützte(n) Funktion(en) behoben werden.

3. **Erhebliche Abhängigkeit**: Im Falle einer Unterbrechung der Dienste würden die unterstützten Funktionen erheblich beeinträchtigt, wenn die Unterbrechung länger als ein paar Minuten/ein paar Stunden dauert, und die Unterbrechung kann zu Schäden führen, die aber noch überschaubar sind.

4. **Vollständige Abhängigkeit**: Im Falle einer Unterbrechung der Dienste würden die unterstützten Funktionen sofort und für einen langen Zeitraum stark unterbrochen/beschädigt.

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Referenzen DORA
Art. 9., 12.1, 12.2, 12.4

Referenzen RTS
RTS on ICT risk mgmt tools, methods, processes and policies: alle Artikel

Wesentliche Anpassungen unter DORA
Maßnahmen zum Schutz von Assets, Prävention vor Bedrohungen. Viele Themen, die bisher nur in den Erläuterungen der BAIT erwähnt wurden, werden im technischen Regulierungsstandard über die Anforderungen der BAIT hinaus detailliert. U. a. in Bezug auf:

- Verschlüsselung von Daten und kryptografische Steuerung
- Daten-, System- und Netzwerksicherheit (u. a. automatisierte Isolation)
- IKT-Betrieb
- IKT-Änderungsmanagement
- Identitäts- und Zugriffsmanagement, Protokollierung
- IKT-Projektmanagement, Anschaffung, Entwicklung von IKT-Systemen
- Schwachstellen- und Patch-Management (u. a. automatisierte Scans)
- Umgehende / umfassende Detektion von anomalen Aktivitäten/ Verhalten

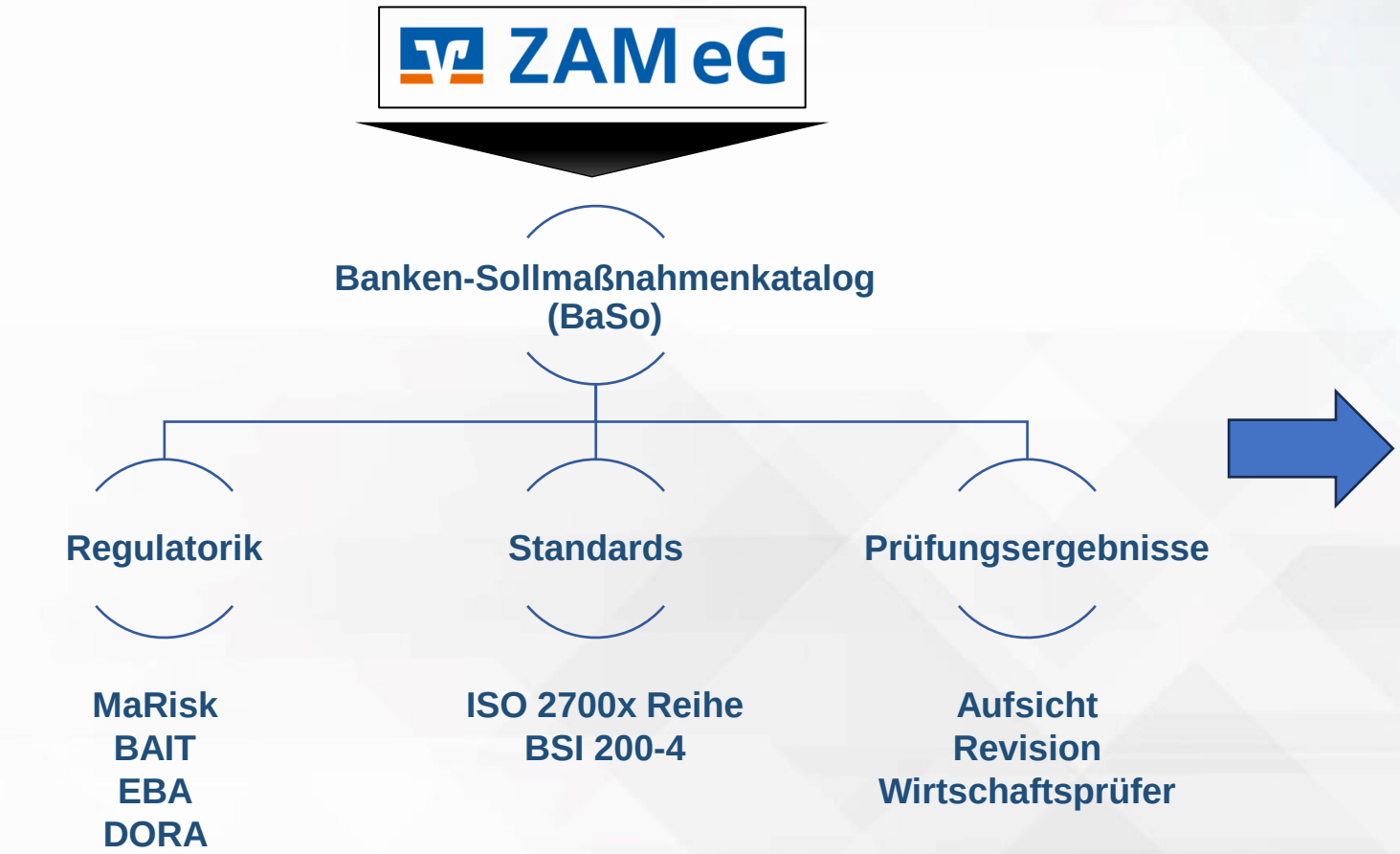
Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Handlungsbedarf
Banken sollten auf Basis der DORA-Anforderungen die Sollmaßnahmenkataloge und Konzepte bezüglich Sicherheitsmaßnahmen aktualisieren, mit den Dienstleistern vereinbaren und für die bankindividuelle IT die Umsetzung selbst sicherstellen.

Unterstützung ZAM eG
Die ZAM eG berücksichtigt die Anforderungen aus DORA im **Banken-Sollmaßnahmenkatalog** des Verfahrens **(BaSo)**. Entsprechend dem IKT-Asset-Cluster und dem Schutzbedarf sind die Anforderungen in den Prozessen Soll-/Soll- und Soll-/Ist-Abgleich mit eigenen IKT-Assets bzw. mit den IKT-Dienstleistern abzugleichen. Die regelmäßig geforderten Rezertifizierungen der umgesetzten Maßnahmen finden ebenfalls im Verfahren statt.

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Banken-Sollmaßnahmenkatalog (BaSo)



- Automatisierte Erstellung von Sicherheitsrichtlinien zum BaSo
- Vorschläge zu Soll-/Soll- und Soll-/Ist-Abgleichen für IKT-Assets und IKT-Dienstleistungen
- Vordefinierte Bedrohungen für mögliche GAPs und daraus abgeleitete Risiken

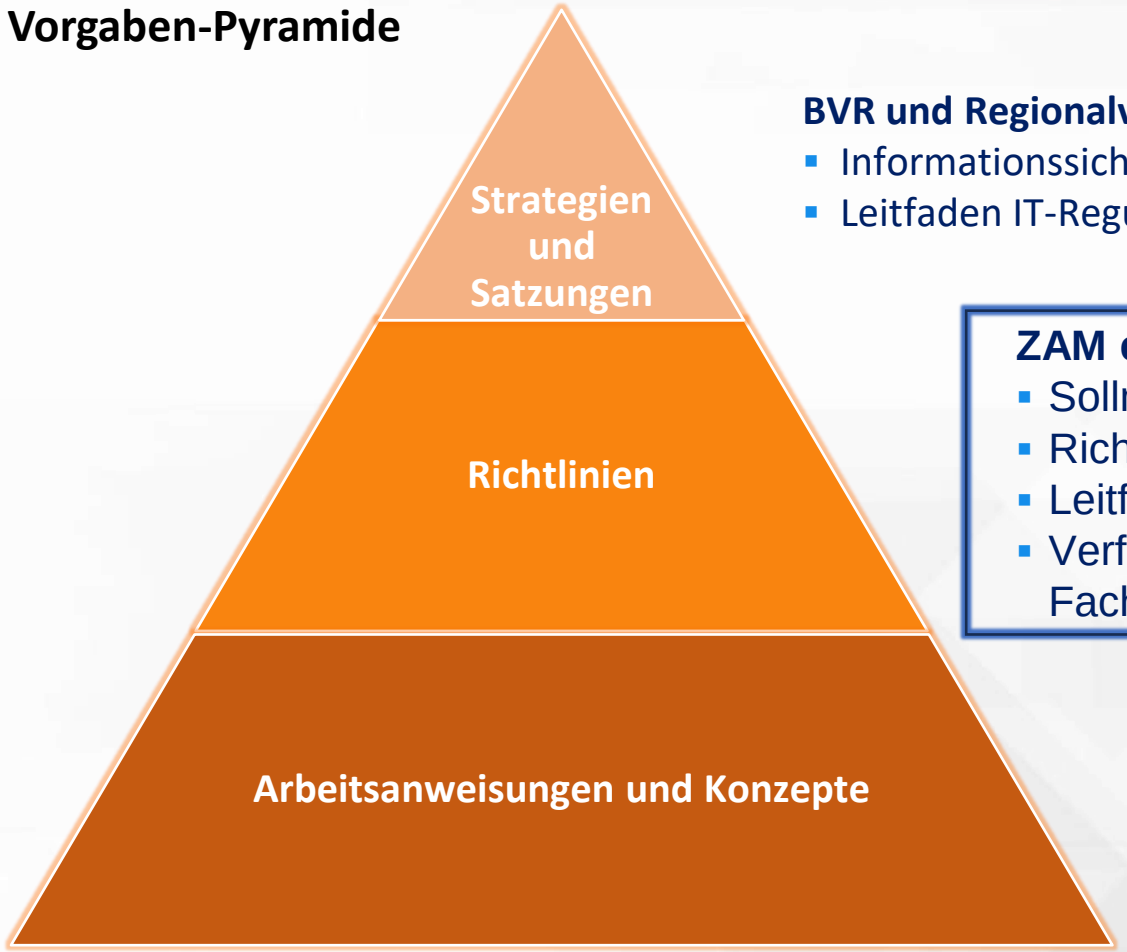
Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Auszug aus dem Banken-Sollmaßnahmenkatalog (BaSo)

Nummerierung und Referenz auf Norm				Richtlinien-Zuordnung			Sollmaßnahmen-Beschreibung	Referenz IT-Governance und regulatorische Anforderung		Schutzbedarfsausprägung							
BASO-ID	Norm-ID	Normbezeichnung	Sollmaßnahmen-Bezeichnung	Richtlinien-ID	Richtlinienname	Richtlinien-Kategorie	Sollmaßnahme	MaRisk + BAIT	DORA	Vertraulichkeit (Confidentiality)	Integrität (Integrity)	Authentizität (Non Repudation)	Verfügbarkeit (Availability)	Servicespezifisch	Organisation	Gebäude, Räume, Schränke	Wechseldatenträger
BASO-00.A.5.1-1	ISO 27002:2022 A.5.1	Informationssicherheitsrichtlinien	Informationssicherheitsrichtlinien - Allgemeine Vorgaben	SR.001	Informationssicherheitsorganisation und Informationssicherheitsmanagement	Informationssicherheitsleitlinie- und themenspezifsche Sicherheitsrichtlinien	Für die Organisation ist ein IKT-Risikomanagementrahmen zu definieren sowie zugehörige Strategien, eine Informationssicherheitsleitlinie, themenspezifische Sicherheitsrichtlinien und Verfahren sowie IKT-Protokolle und -Tools zu beschreiben, festzulegen und von der Geschäftsführung genehmigen zu lassen. Die Informationssicherheitsleitlinie selbst legt dabei einen Ansatz zur Bewältigung der Informationssicherheitsziele (insbesondere - Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen) fest und ist bei Anpassungen immer erneut durch die Geschäftsführung zu genehmigen. Die im Rahmen der Informationssicherheitspolitik festzulegende Informationssicherheitsleitlinie, themenspezifischen Sicherheitsrichtlinien (kurz: Sicherheitsrichtlinien), Verfahren sowie IKT-Protokolle und -Tools sind innerhalb des Anweisungswesens der Organisation zu veröffentlichen und anschließend von allen Mitarbeitern zur Kenntnis zu nehmen. Über Anpassungen diesbezüglich ist die Geschäftsführung in Kenntnis zu setzen, wobei Änderungen bezüglich der Informationssicherheitspolitik durch diese zu genehmigen sind. Weiterhin ist innerhalb des IKT-Risikomanagementrahmens eine Strategie für die digitale operationelle Resilienz zu erstellen sowie diese mindestens einmal jährlich sowie anlassbezogen (z.B. Auftreten schwerwiegender IKT-bezogene Vorfälle oder aufsichtsrechtlichen Feststellungen, die sich aus einschlägigen Tests der digitalen operationellen Resilienz oder Auditverfahren ergeben) durch das Informationssicherheitsmanagement (ISM) der Organisation zu überprüfen und bei Bedarf entsprechend anzupassen. Den zuständigen Behörden ist auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens	MaRisk AT 4.3.1, MaRisk AT 4.3.2, MaRisk AT 5Tz. 1, MaRisk AT 5Tz. 2, MaRisk AT 5 Tz. 3, MaRisk AT 7.2Tz. 2 BAIT Tz. 2.1, BAIT Tz. 2.2, BAIT Tz. 4.2	DORA Art. 6 Tz. 2, DORA Art. 6 Tz. 5 DORA Art. 6 Tz. 8 DORA Art. 9, DORA Art. 15	1-4	1-4	1-4	1-4	nein	x		
BASO-00.A.5.1-2	ISO 27002:2022 A.5.1	Informationssicherheitsrichtlinien	Informationssicherheitsrichtlinien - Informationssicherheitsorganisation	SR.001	Informationssicherheitsorganisation und Informationssicherheitsmanagement	Allgemeines zur Informationssicherheitsorganisation	Im Rahmen der Informationssicherheitsorganisation sind die folgenden Rahmenbedingungen umzusetzen: - Das Informationssicherheitsmanagement (ISM) muss die Instanz innerhalb der Organisation sein, dass für alle Belange der Informationssicherheit zuständig ist; - Es sind aus der Informationssicherheitsleitlinie themenspezifische Sicherheitsrichtlinien abzuleiten, welche die jeweils relevanten Anforderungen beschreiben. Diese Sicherheitsrichtlinien sind allen relevanten Parteien mitzuteilen; - In der Informationssicherheitsleitlinie, den themenspezifischen Sicherheitsrichtlinien und den Verfahren sowie IKT-Protokolle und -Tools sind die wesentlichen Zuständigkeiten (IKT-gestützten Unterstützungsfunktionen, Rollen	MaRisk AT 4.3.1, MaRisk AT 4.3.2, MaRisk AT 5Tz. 1, MaRisk AT 5Tz. 2, MaRisk AT 5 Tz. 3, MaRisk AT 7.2Tz. 2 BAIT Tz. 2.1, BAIT Tz. 2.2, BAIT Tz. 4.2, BAIT Tz. 5.2	DORA Art. 5 Tz 4 DORA Art. 6 Tz 4 DORA Art. 8	1-4	1-4	1-4	1-4	nein	x		

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Vorgaben-Pyramide



BVR und Regionalverbände liefern:

- Informationssicherheits-, IRM und BCM-Strategien/ -leitlinien
- Leitfaden IT-Regulatorik

ZAM eG liefert:

- Sollmaßnahmenkatalog
- Richtlinien zum Sollmaßnahmenkatalog
- Leitfaden zum Sollmaßnahmenkatalog
- Verfahrensrelevante Methodik und Dokumentation (Prozesse, Fachkonzepte, etc.)

Regionalverbände bzw. Bank selbst liefert:

- (Muster-)Arbeitsanweisungen auf Grundlage vorgegebener Richtlinien
- Benutzerhilfen zur Konkretisierung von Arbeitsanweisungen

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Vorgaben zum Sollmaßnahmenkatalog

Sicherheitsrichtlinien zum Banken-Sollmaßnahmenkatalog

ZAM eG

SR.001 Informationssicherheitsorganisation und Informationssicherheitsmanagement

Zielsetzung Sicherheitsrichtlinie

Ziel dieser Sicherheitsrichtlinie ist es, die Inhalte der Informationssicherheitsleit- und Richtlinien, notwendige Rollen und Verantwortlichkeiten sowie zugehörige Abläufe für das Informationssicherheitsmanagement zu beschreiben und zu definieren. Bei dieser Sicherheitsrichtlinie handelt es sich um eine thematische Bündelung und Zuordnung von Sollmaßnahmen im Kontext zum Thema der Sicherheitsrichtlinie selbst. In Ergänzung dieser Zuordnung sind die relevanten Sollmaßnahmen übersichtlich in zugehörige Sollmaßnahmenkategorien zugeteilt.Der Inhalt und die Pflege dieser Sicherheitsrichtlinie und zugehörige Sollmaßnahmen liegen im Verantwortungsbereich des Informationssicherheitsbeauftragten und sein Team. Die Verantwortung zur Umsetzung bzw. Implementierung der hier beschriebenen Sollmaßnahmen, z.B. in Form von Regelungen (Anweisungen oder Richtlinien) gegenüber den Mitarbeitern oder der Erstellung zugehöriger Konzepte liegt in den jeweils umsetzungsverantwortlichen Organisationseinheiten innerhalb der Organisation.Ergänzende Erläuterungen zu den Inhalten und Angaben dieser Sicherheitsrichtlinie können dem Glossar entnommen werden.

Referenzen

ISO 27002:2022 A.5.1 Informationssicherheitsrichtlinien
ISO 27002:2022 A.5.2 Informationssicherheitsrollen und –verantwortlichkeiten
ISO 27002:2022 A.5.3 Aufgabentrennung
ISO 27002:2022 A.5.4 Verantwortlichkeiten der Leitung
ISO 27002:2022 A.5.5 Kontakt mit Behörden
ISO 27002:2022 A.5.6 Kontakt mit speziellen Interessensgruppen
ISO 27002:2022 A.5.7 Bedrohungsintelligenz

Umsetzungsverantwortlicher

ISB / Geschäftsführung

Informationssicherheitsleitlinie- und themenspezifsche Sicherheitsrichtlinien

BASO-00.A.5.1-1 **Schutzbedarfsklassen: A1-4 C1-4 I1-4 N1**

Informationssicherheitsrichtlinien - Allgemeine Vorgaben

Für die Organisation ist ein IKT-Risikomanagementrahmen zu definieren sowie zugehörige Strategien, eine Informationssicherheitsleitlinie, themenspezifische Sicherheitsrichtlinien und Verfahren sowie IKT-Protokolle und -Tools zu beschreiben, festzulegen und von der Geschäftsführung genehmigen zu lassen. Die Informationssicherheitsleitlinie selbst legt dabei einen Ansatz zur Bewältigung der Informationssicherheitsziele (insbesondere - Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen) fest und ist bei Anpassungen immer erneut durch die Geschäftsführung zu genehmigen. Die im Rahmen der Informationssicherheitspolitik festzulegende Informationssicherheitsleitlinie, themenspezifischen Sicherheitsrichtlinien (kurz: Sicherheitsrichtlinien), Verfahren sowie IKT-Protokolle und -Tools sind innerhalb des Anweisungswesens der Organisation zu veröffentlichen und anschließend von allen Mitarbeitern zur Kenntnis zu nehmen. Über Anpassungen diesbezüglich ist die Geschäftsführung in Kenntnis zu setzen, wobei Änderungen bezüglich der Informationssicherheitspolitik durch diese zu genehmigen sind.

Weiterhin ist innerhalb des IKT-Risikomanagementrahmens eine Strategie für die digitale operationelle Resilienz zu erstellen sowie diese mindestens einmal jährlich sowie anlassbezogen (z.B. Auftreten schwerwiegender IKT-bezogene Vorfälle oder aufsichtsrechtlichen Feststellungen, die sich aus einschlägigen Tests der digitalen operationellen Resilienz oder Auditverfahren ergeben) durch das Informationssicherheitsmanagement (ISM) der Organisation zu überprüfen und bei Bedarf entsprechend anzupassen. Den zuständigen Behörden ist auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorzulegen.

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Banken-Sollmaßnahmenkatalog als zentrales Instrument zur Steuerung

- Formulierung aller notwendigen Sollmaßnahmen aus den IT-regulatorischen Anforderungen
- Automatisierte Erstellung von übergreifenden Sicherheitsrichtlinien
- Integration eines bankindividuellen Soll-/Soll-Abgleichs der IT-regulatorischen Anforderungen mit der eigenen schriftlich fixierten Ordnung
- Definition der bankeigenen Anforderungen an einen sicheren Einsatz der IKT-Assets
- Verwendung als Grundlage und Bestandteil einer Vertragsanlage gegenüber Dienstleister zum Schutz der bankeigenen Informationen
- Strukturierte Ableitung von IKT-Risiken aus den Soll-/Soll- und Soll-/Ist-Abgleichen nicht umgesetzter Maßnahmen

Handlungspaket: Anpassung der Sicherheitsmaßnahmen

Soll-Soll- & Soll-/Ist-Abgleich an Dienstleister

BASO-ID	Sollmaßnahmen-Bezeichnung	Sollmaßnahme	Realisierungsgrad Vertrag	Realisierungsgrad operativ	Umsetzung	Abweichung / Bemerkung
BASO-A.5.1-1	Informationssicherheitsrichtlinien - Allgemeine Vorgaben	Für die Organisation ist ein IKT-Risikomanagementrahmen zu definieren sowie zugehörige Strategien, eine Informationssicherheitsleitlinie, themenspezifische Sicherheitsrichtlinien und Verfahren sowie IKT-Protokolle und -Tools zu beschreiben, festzulegen und von der Geschäftsführung genehmigen zu lassen. Die Informationssicherheitsleitlinie selbst legt dabei einen Ansatz zur Bewältigung der Informationssicherheitsziele (insbesondere - Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen) fest und ist bei Anpassungen immer erneut durch die Geschäftsführung zu genehmigen. Die im Rahmen der Informationssicherheitspolitik festzulegende Informationssicherheitsleitlinie, themenspezifischen Sicherheitsrichtlinien (kurz: Sicherheitsrichtlinien), Verfahren sowie IKT-Protokolle und -Tools sind innerhalb des Anweisungswesens der Organisation zu veröffentlichen und anschließend von allen Mitarbeitern zur Kenntnis zu nehmen. Über Anpassungen diesbezüglich ist die Geschäftsführung in Kenntnis zu setzen, wobei Änderungen bezüglich der Informationssicherheitspolitik durch diese zu genehmigen sind.	erfüllt	erfüllt	Für das Unternhemen sind ein IKT-Risikomanagementrahmen definiert sowie zugehörige Strategien, eine Informationssicherheitsleitlinie, themenspezifische Sicherheitsrichtlinien beschrieben.	
BASO-A.5.1-2	Informationssicherheitsrichtlinien - Informationssicherheitsorganisation	DORA fordert, dass die Organisation über einen internen Governance- und Kontrollrahmen verfügen, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen. Im Rahmen der Informationssicherheitsorganisation sind die folgenden Rahmenbedingungen umzusetzen:	nicht erfüllt	nicht erfüllt	Das Managment der IKT-Risiken befindet sich zur Zeit im Aufbau und kann daher nicht vertraglich zugesichert werden.	
BASO-A.5.1-3	Informationssicherheitsrichtlinien - Informationssicherheitsmanagement-Prozess	Im Rahmen Informationssicherheitsorganisation ist ein Informationssicherheitsmanagement-Prozess gemäß den folgenden Kriterien umzusetzen: - Es sind die Abläufe des Informationssicherheitsmanagements der Organisation zu beschreiben; - Der Prozess muss in Verantwortung des Informationssicherheitsbeauftragten (ISB) nach den Vorgaben bzw. Konventionen	erfüllt	nicht erfüllt	Der Informationssicherheitsmanagement-Prozessist dokumentiert und und in Richtlinien beschrieben.	Die Vorgaben und Regelungen zur Informationssicherheit der Organisation unterliegen keinem kontinuierlichen
BASO-A.5.2-1	Informationssicherheitsrollen und –verantwortlichkeiten - Geschäftsführung	DORA weist den Mitgliedern des Leitungsorgans die letztendliche Verantwortung für das Management der IKT-Risiken und für alle zu treffenden Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen als Aufgabe zu. Im Rahmen der Informationssicherheitsorganisation sind durch die Geschäftsführung der Organisation die folgenden Verantwortlichkeiten und Aufgaben bzw. Tätigkeiten wahrzunehmen und umzusetzen:	erfüllt	erfüllt	Der Vorstand trägt gem. Risiko- und IT-Strategie die Verantwortung für das Management der IKT-Risiken und für alle zu treffenden Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen als	
SMK-IS-A.08.01.04-01	Informationssicherheitsrollen und –verantwortlichkeiten - Informationssicherheitsbeauftragter (ISB)	Im Rahmen der Informationssicherheitsorganisation sind durch den Informationssicherheitsbeauftragten (ISB) der Organisation die folgenden Verantwortlichkeiten und Aufgaben bzw. Tätigkeiten wahrzunehmen und umzusetzen: - Der ISB muss wie folgt organisatorisch eingegliedert sein und die nachfolgende fachlich/persönliche Eignung aufweisen: 1) Das ISMS der Organisation muss durch die Rolle des ISB koordiniert und umgesetzt werden. Dies umfasst die Wahrnehmung aller Belange des Informationssicherheitsmanagements (ISM) und des IKT-Risikomanagements innerhalb der Organisation und gegenüber externen Auftragnehmern bzw. Dienstleistern. Er muss sicherstellen, dass die in der Informationssicherheitsleitlinie	erfüllt	erfüllt	Der physische Besitz von Assets durch Mitarbeiter ist für die Erbringung der Servicedienstleistungen nicht relevant. Alle Betriebskomponenten befinden nicht im physischen Besitz eines Mitarbeiters.	

Handlungspaket: Vorgehen und Umsetzung des Testprogramms

Referenzen DORA
Art. 24-27

Referenzen RTS
RTS on ICT risk mgmt tools, methods, processes and policies: Artikel 10 RTS TLPT

Wesentliche Anpassungen unter DORA
Nennung einer Reihe von Testarten über die in den BAIT hinaus genannten z. B.

- Netzwerksicherheitsbewertungen
- Überprüfungen der physischen Sicherheit
- Lückenanalysen, Fragebögen
- Scans von Softwarelösungen
- Open-Source-Analysen, Quellcodeprüfungen, soweit durchführbar
- Szenariobasierte-, Kompatibilitäts-, Leistungs-, End-to-End-Tests
- Penetrationstests
- Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen - sogenannte Thread Lead Penetration Tests (TLPT) für signifikante und cyberreif eingestufte Institute

Handlungspaket: Vorgehen und Umsetzung des Testprogramms

Handlungsbedarf
Das Programm zur Durchführung von Tests u. a. durch Einholung von Angeboten externer Dienstleister ist zu erweitern.

Das Test- und Überprüfungsprogramm beinhaltet angemessene Tests, wie etwa

- Schwachstellenscans
- Open-Source-Analysen
- Netzwerksicherheitsbewertungen
- Gap-Analysen
- Überprüfungen der physischen Sicherheit
- Fragebögen und Scans von Softwarelösungen
- Quellcodeprüfungen
- Szenariobasierte Tests
- Kompatibilitätstests
- Leistungstests
- End-to-End-Tests und
- Penetrationstests

Thread Lead Penetration Tests (TLPT)
Von der Finanzaufsicht können Banken aufgrund der Auswirkungen ihrer Dienstleistungen auf den Finanzsektor, auf die Finanzstabilität sowie aufgrund ihres spezifischen IKT-Risikoprofils und IKT-Reifegrads aufgefordert werden, erweiterte bedrohungsorientierte Penetrationstests vorzunehmen – sogenannte Thread Lead Penetration Tests (TLPT). Nach derzeitiger Aussage der Aufsicht steht die durchschnittliche Genossenschaftsbank nicht im Fokus für solche Tests. (Benennung der Institute durch die Aufsicht ab 2025).

Handlungspaket: Vorgehen und Umsetzung des Testprogramms

Unterstützung ZAM eG

Die ZAM eG stellt im Verfahren eine Dokumentationsmöglichkeit der Tests gem. den Anforderungen aus den Art. 24 – 27 zur Verfügung und überführt evtl. auftretende Schachstellen daraus in das Risikomanagement.

Im Testmanagement können Testrahmenbedingungen und Erwartungen an die Tests vorher definiert werden.

Handlungspaket: IKT-Notfallmanagement

Referenzen DORA
Art. 5.2, 11, 12, 14

Referenzen RTS
RTS on ICT risk mgmt tools, methods, processes and policies: Artikel 25-27

Wesentliche Anpassungen unter DORA

- Erstellung einer IKT-Geschäftsfortführungsleitlinie
- IKT-Reaktions- und Wiederherstellungspläne berücksichtigen mindestens neun relevante Szenarien
- Tests sind auf der Basis von realistischen Szenarien durchzuführen
- Etablierung einer Krisenmanagementfunktion

Handlungsbedarf
Eine (IKT-)Geschäftsfortführungsleitlinie ist zu verabschieden und es sollten Reaktions- und Wiederherstellungspläne aktualisiert, erweitert und operationalisiert und dabei zusätzliche Notfallszenarien berücksichtigt werden.

Handlungspaket: IKT-Notfallmanagement

Szenarien schwerer Geschäftsunterbrechungen wurden erweitert (in MaRisk AT 7.3: vier Szenarien)
Es werden Szenarien entwickelt, die auf aktuellen Informationen über Bedrohungen und auf Lehren aus früheren Ereignissen von Unternehmensstörungen beruhen. Die Szenarien umfassen alle folgenden Punkte:

- teilweiser oder vollständiger Ausfall von Räumlichkeiten, einschließlich Büro- und Geschäftsräumen und Rechenzentren;
- die Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern oder Schlüsselbediensteten;
- Cyberangriffe und Umstellungen zwischen der primären IKT-Infrastruktur und den redundanten Kapazitäten, Backups und redundanten Einrichtungen;
- Szenarien, in denen sich die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau verschlechtert oder fehlschlägt, wobei die potenziellen Auswirkungen der Insolvenz oder anderer Ausfälle eines relevanten IKT-Drittanbieters gebührend berücksichtigt werden;
- erhebliches Versagen der IKT-Anlagen oder der Kommunikationsinfrastruktur;
- Naturkatastrophen, Pandemien und physische Angriffe, einschließlich Eindringlinge und Terroranschläge;
- Insiderangriff;
- politische und soziale Instabilität, gegebenenfalls auch in der Gerichtsbarkeit, aus der der IKT-Drittanbieter seine Dienste erbringt, und den Ort, an dem die Daten gespeichert und verarbeitet werden;
- weit verbreiteter Stromausfall.

Handlungspaket: IKT-Notfallmanagement

Entwicklung von IKT-Reaktions- und Wiederherstellungsplänen
IKT-Reaktions- und Wiederherstellungspläne werden unter Berücksichtigung der Ergebnisse der BIA entwickelt und müssen:

- die Bedingungen angeben, die ihre Aktivierung veranlassen, und etwaige Ausnahmen;
- beschreiben, welche Maßnahmen ergriffen werden müssen, um die Verfügbarkeit, Integrität, Kontinuität und Wiederherstellung mindestens der kritischen IKT-Systeme und -Dienste der Finanzunternehmen sicherzustellen;
- so konzipiert sein, dass sie die Wiederherstellungsziele der Geschäfte von Finanzunternehmen erreichen;
- dokumentiert sein, klare Rollen und Verantwortlichkeiten festlegen und dem an der Ausführung des Plans beteiligten Personal zur Verfügung gestellt werden und im Notfall leicht zugänglich sein und;
- sowohl kurzfristige als auch langfristige Handlungsoptionen, einschließlich Teilsysteme und Wiederherstellung, vorsehen;
- Festlegung der Ziele des Plans und der Bedingungen für die Feststellung der erfolgreichen Durchführung des Plans;
- anlassbezogen angepasst werden (Anlässe; Erkenntnisse aus IKT-bezogenen Vorfällen, Ergebnisse der Überprüfungen, neu identifizierten Risiken und Bedrohungen, bei geänderten Wiederherstellungszielen und -prioritäten, Feststellungen aus Prüfungen oder aufsichtlichen Überprüfungen)

Handlungspaket: IKT-Notfallmanagement

Unterstützung ZAM eG

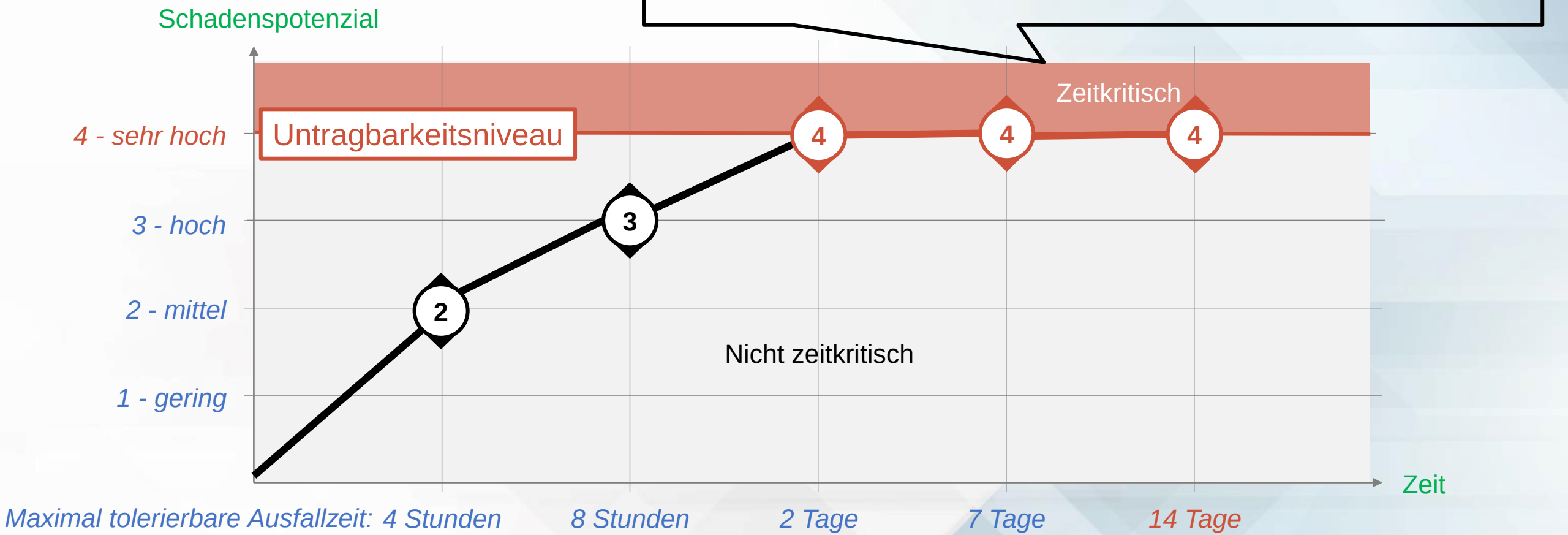
Die ZAM eG stellt mit ihrem Verfahren einen strukturierten Rahmen zur Erfassung der Notfallszenarien, des jeweiligen Business Impacts auf alle erfassten Prozesse sowie den jeweils damit verknüpften IKT-Assets. Daraus abgeleitet können die Risiken für potenzielle Auswirkungen schwerwiegender Betriebsstörungen und Ausfälle anhand quantitativer und qualitativer Kriterien für die Bank ermittelt sowie Notfallpläne (in Form von Geschäftsfortführungsplänen, IKT-Reaktions- und Wiederherstellungsplänen) beschrieben werden. Die notwendigen Tests können mit Ergebnis strukturiert nachgewiesen und mit den Sollvorgaben verglichen werden. Zudem werden Tätigkeiten vor und während Störungen dokumentiert.

Die Berichterstattung und Meldung der Risken an das Leitungsorgan sowie eine Exportfunktion für OpRisk werden ebenfalls im Verfahren sichergestellt.

Handlungspaket: IKT-Notfallmanagement

Wenn der Geschäftsprozess […] ausfällt, mit welchem Schadens-potenzial ist im Zeithorizont […] zu rechnen, hinsichtlich

- *Beeinträchtigung der Aufgabenerfüllung, (->Aufgabenerfüllung)*
- *Verstoß gegen Gesetze, Vorschriften und Verträge, (-> regul. Bedeutung)*
- *negative Innen- und Außenwirkung (Imageschaden), (->Reputation)*
- *finanzielle Auswirkungen sowie (-> wirtsch. Bedeutung)*



Handlungspaket: Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen

Referenzen DORA
Art. 11.10, 17-19

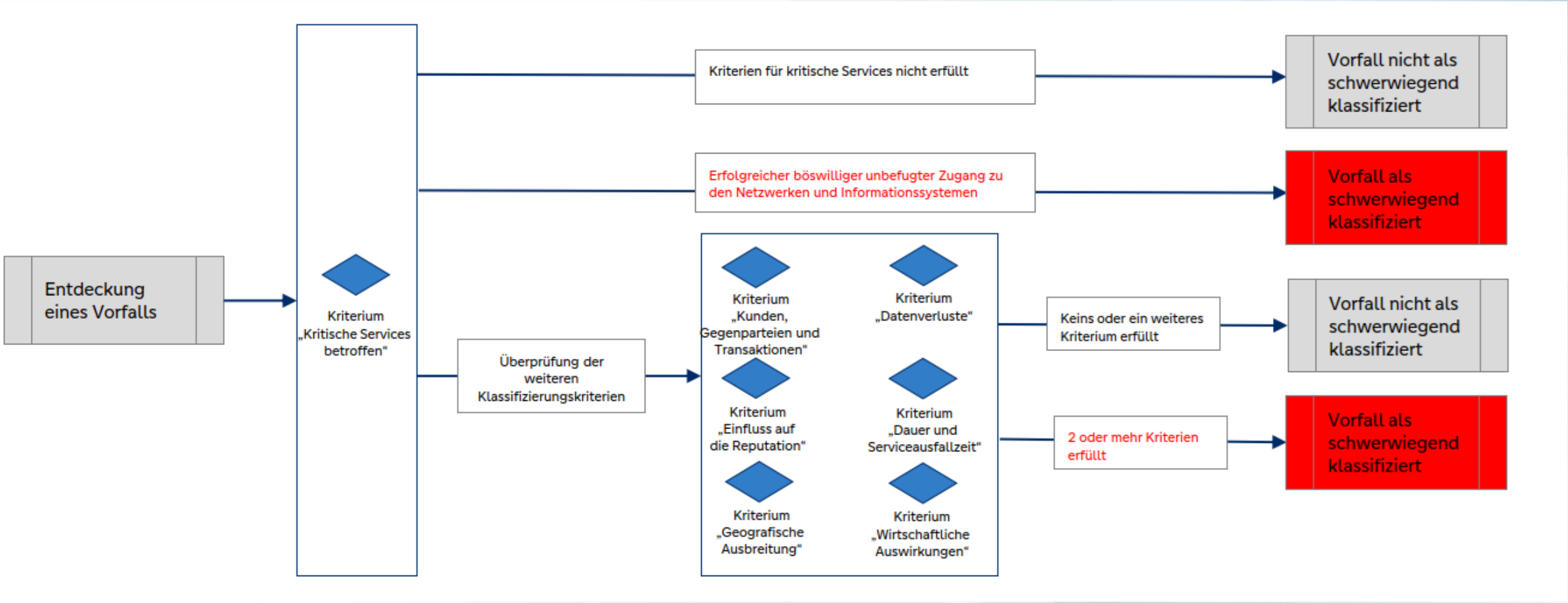
Referenzen RTS
RTS on incident response, RTS / ITS on major incident reporting
GL on costs and losses

Wesentliche Anpassungen unter DORA

- Klassifizierung aller IKT-bezogenen Vorfälle nach vorgegebenen Klassifizierungskriterien
- Meldung schwerwiegender IKT-bezogener Vorfälle an die BaFin (Ausweiterung der PSD2-Meldungen)
- Meldung der geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden

Handlungsbedarf
Anleitungen hinsichtlich der Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblichen Cyberbedrohungen sind zu berücksichtigen.

Handlungspaket: Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen



Quelle: DORA RTS Entwurf zur Incident Klassifizierung der ESAs vom 17.1.2024

Handlungspaket: Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen

Initiale Meldung	4 Stunden nach Klassifizierung, nicht später als 24 Stunden nach Entdeckung des Vorfalls	• Datum / Zeit der Entdeckung und Klassifizierung, zutreffende Klassifizierungskriterien • Beschreibung des Vorfalls • Information, wie der Vorfall entdeckt wurde und wenn bekannt, zur Ursache, ob er zu einer Folge von Vorfällen gehört, zur Aktivierung von Notfallplänen etc. • Falls bekannt: weitere EU-Staaten, andere Finanzinstitute und Dienstleister, die potenziell betroffen sind • Angaben zur Aktivierung des Business-Continuity-Plans
Zwischen-meldung	72 Stunden nach Klassifizierung oder nach Herstellung der normalen Aktivitäten.	• Datum/Zeit zum Beginn des Vorfalls, zur Wiederherstellung normaler Aktivitäten • Detailinformation zu den Klassifizierungskriterien • Art des Vorfalls • Information zu betroffenen Funktionsbereichen, Geschäftsprozessen sowie Infrastrukturkomponenten • Kommunikation mit Kunden und finanziellen Gegenparteien • Information, ob an andere Behörden gemeldet wurde • Aktivitäten, die zur Erholung vom Vorfall durchgeführt wurden oder geplant sind • Falls bekannt: Information zu ausgenutzten Schwachstellen, Indicators of compromise
Abschluss-meldung	spätestens 1 Monat nach Klassifizierung (oder nach finaler Lösung, wenn dies später erfolgt)	• Datum/Zeit der Lösung/Beseitigung der Ursache, Info zur zugrundeliegenden Ursache • Bei Bedarf Reklassifizierung • Maßnahmen/ Aktivitäten zur Lösung des Vorfalls sowie präventive Maßnahmen, um ähnliche Vorfälle zukünftig zu vermeiden • Information, ob gesetzlichen Anforderungen oder vertragliche Vereinbarungen nicht erfüllt werden konnten • für Abwicklungsbehörden relevante Informationen • Direkte und indirekte Kosten/Verluste/finanzielle Rückflüsse, die sich aus dem Vorfall ergeben (13 Felder!) -> zusätzlich jährliche Meldung von Kosten und Verlusten

Handlungspaket: Klassifizierung und Meldung IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen

Unterstützung ZAM eG

Die ZAM eG stellt im Verfahren einen Prozess für die Erfassung und Behandlung IKT-bezogener Vorfälle bereit. Dieser sieht die Ermittlung, Kategorisierung, Klassifizierung, Nachverfolgung, Protokollierung und Prüfungen IKT-bezogener Vorfälle gem. Art. 13.2 und Art 17.3 DORA vor.

Zeitverlauf, Häufigkeit, Art, Ausmaß und Entwicklung IKT-bezogener Vorfälle können analysiert werden.

Das Verfahren unterstützt die Meldung aus Sicherheitsvorfällen und Cyberbedrohungen an Behörden und Kunden. Die jeweilige Meldung hat jedoch individuell außerhalb des Verfahrens durch die Bank zu erfolgen.

Haben Sie Fragen?

Wir beantworten sie gerne.

Andreas Kötter
ZAM eG
mailto: Andreas.Koetter@ZAM-EG.de
Telefon: 069 5095-4400

ZAM eG

Vielen Dank

Für Ihre Aufmerksamkeit

ZAM eG