VR-Bank Musterstadt eG
DORA GAP-Analyse

- Anwenderhinweise
- Institutsstammdaten
- Anwendbarkeitskriterien
- GAP-Analyse Übersicht
- Reifegrad
- Kapitel 2 (IKT-Risikomanagement)
- Kapitel 3 (Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle)
- Kapitel 4 (Test der digitalen operationalen Resilienz einschließlich Threat-Led Penetration Testing (TLPT))
- Kapitel 5 (IKT Drittparteien-Risikomanagement)
- Kapitel 6 (Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen)

Ziel und Zweck

Dieses GAP-Analyse Tool hilft, aktuelle Richtlinien, Prozesse und Verfahren mit den Anforderungen des Digital Operational Resilience Act (DORA) abzugleichen. Anhand von Ja/Nein-Fragen kann festgestellt werden, wo Prozesse und Verfahren ausreichen, und welche konkreten Maßnahmen zu ergreifen sind, um Lücken zu schließen. In den gelb hinterlegten Tabellenblättern sind Eingaben erforderlich. **Das Tool erhebt keinen Anspruch auf Vollständigkeit und wurde auf Grundlage der aktuellen Gesetzgebung nach gesundem Menschenverstand entwickelt. Die Nutzung erfolgt auf eigenes Risiko, der Hersteller übernimmt keine Haftung hinsichtlich Prüfungsfeststellungen aufgrund der eingesetzten GAP-Analyse.**

Bei der Beantwortung der Fragen sollte der Grundsatz der Verhältnismäßigkeit berücksichtigt werden, der in der Verordnung definiert ist. Darin heißt es, dass die Vorschriften in angemessener Weise entsprechend ihrer „Größe und ihrem Gesamtrisikoprofil" sowie „die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte" Rechnung zu tragen ist. **Zu beachten ist jedoch, dass letztlich die zuständige Behörde entscheidet, was „verhältnismäßig" ist.**

Institutsstammdaten (Einwertung der Verhältnismäßigkeit)

Hier werden grundlegende Stammdaten des Instituts hinterlegt, für die die GAP-Analyse erstellt wird. Die Einwertung der Verhältnismäßigkeit wird hier ebenfalls dokumentiert. Die Parametrisierung ist ein Vorschlag und kann eigenverantwortlich angepasst werden.

Anwendbarkeitskriterien

Obwohl DORA für eine Vielzahl von Finanzunternehmen gilt, sind die Anforderungen nicht für alle identisch. Für bestimmte Organisationen gelten Ausnahmen oder vereinfachte Anforderungen. **Dieses GAP-Analyse Tool ist speziell für genossenschaftliche Kreditinstitute, die nicht als bedeutend gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 eingestuft sind, konzipiert und anwendbar.**

GAP-Analyse Übersicht

Hier wird eine Übersicht der Antworten nach Kapitel und Artikel als Zahlenwerk ausgegeben. In dieser Übersicht kann leicht ermittelt werden, wo noch Antworten fehlen bzw. wie das prozentuale Verhältnis der Beantwortungsstandes ist.

Reifegrad

Dieser Abschnitt bietet eine visuelle Zusammenfassung des Reifegrades der DORA Umsetzung, basierend auf den Antworten der GAP-Analyse.
In der Gesamtübersicht erhält man eine Momentaufnahme der Antworten und sieht den Reifegrad der Konformität für jedes Kapitel als Prozentsatz an.
Die Detailansicht bietet eine Aufschlüsselung des DORA Status, zunächst in Kapitel unterteilt und dann in Artikel unterteilt. Es zeigt, wo Anforderungen erfüllt sind, wo es Lücken gibt und ob Anforderungen nicht anwendbar sind.

Kapitel 2–6

Hier sind die GAP-Analyse Fragen zu jedem Kapitel von DORA zu beantworten. (Im Kapitel 1 werden die Allgemeinen Bestimmung der Verordnung darlegt und sind keine Anforderungen enthalten.)

Jede Frage ist mit einer Internen Referenznummer versehen und kann über das Dropdown-Menü beantwortet werden. **Ebenfalls wurde eine DORA Referenz implementiert, in der die entsprechende Anforderung geregelt ist.** Alle Fragen, die aufgrund Ihrer Anwendbarkeitskriterien nicht zutreffen, werden automatisch auf „N/A" gesetzt, während weitere Fragen je nach Struktur und Betrieb des Instituts möglicherweise nicht zutreffen und diese auch auf „N/A" gesetzt werden können.

Darüber hinaus gelten die Kapitel 5 und 6 nur unter bestimmten Umständen. Der Geltungsbereich wird durch die Frage auf oberster Ebene festgelegt.

Institutsstammdaten DORA GAP-Analyse

Name des Instituts:	**VR-Bank Musterstadt eG**
Bilanzsumme in Mio. €	**1200**
Verantwortlicher Vorstand	**Herr Volker Vorstand**
Verantwortlicher GAP-Analyse	**Herr Gottfried Gaplinski**

Verhältnismäßigkeit	**Punkte**
Größe/Risiko (200 Punkte)	
Größe (Bilanzsumme)	**20**
Gesamtrisikoprofil	**50**
Dienstleistungen (100 Punkte)	
Art, Umfang, Komplexität	**40**
Tätigkeiten – IT-Prozesse (100 Punkte)	
Art, Umfang, Komplexität	**40**
Geschäfte (100 Punkte)	
Art, Umfang, Komplexität	**40**
Gesamtpunktzahl:	**190**
Maximalpunktzahl:	**500**
% Verhältnismäßigkeitsindex:	**38**

DORA Einwertung der Organisation	Auswahl
Als **nicht** bedeutend eingestuftes genossenschaftliches Kreditinstitut	Ja

Kapitel 2	
Ja	112
Nein	45
Keine Antwort	0

Kapitel 3	
Ja	18
Nein	8
Keine Antwort	0

Kapitel 4	
Ja	5
Nein	4
Keine Antwort	0

Kapitel 5	
Ja	47
Nein	27
Befreit	0
Keine Antwort	0

Kapitel 6	
Ja	4
Nein	3
Befreit	0
Keine Antwort	0

C-M-SOLUTIONS
Vom Praktiker für Praktiker

Reifegrad				
	Ja	Nein	Befreit	Keine Antwort
Kapitel 2	71 %	29 %	-	0 %
Kapitel 3	69 %	31 %	-	0 %
Kapitel 4	56 %	44 %	-	0 %
Kapitel 5	64 %	36 %	0 %	0 %
Kapitel 6	57 %	43 %	0 %	0 %

C-M-SOLUTIONS
Vom Praktiker für Praktiker

Kapitel 2											
	Art. 5	Art. 6	Art. 7	Art. 8	Art. 9	Art. 10	Art. 11	Art. 12	Art. 13	Art. 14	Art. 16
Ja	11	17	2	12	19	4	10	16	18	3	0
Nein		9	2	5	4	2	10	0	8	1	0
N/A	0	4	0	0	0	1	1	5	0	0	16
Keine Antwort	0	0	0	0	0	0	0	0	0	0	0

Kapitel 3			
	Art. 17	Art. 18	Art. 19
Ja	7	6	5
Nein	3	1	4
N/A	0	0	2
Keine Antwort	0	0	0

Kapitel 4				
	Art. 24	Art. 25	Art. 26	Art. 27
Ja	5	0	0	0
Nein	3	1	0	0
N/A	2	2	16	9
Keine Antwort	0	0	0	0

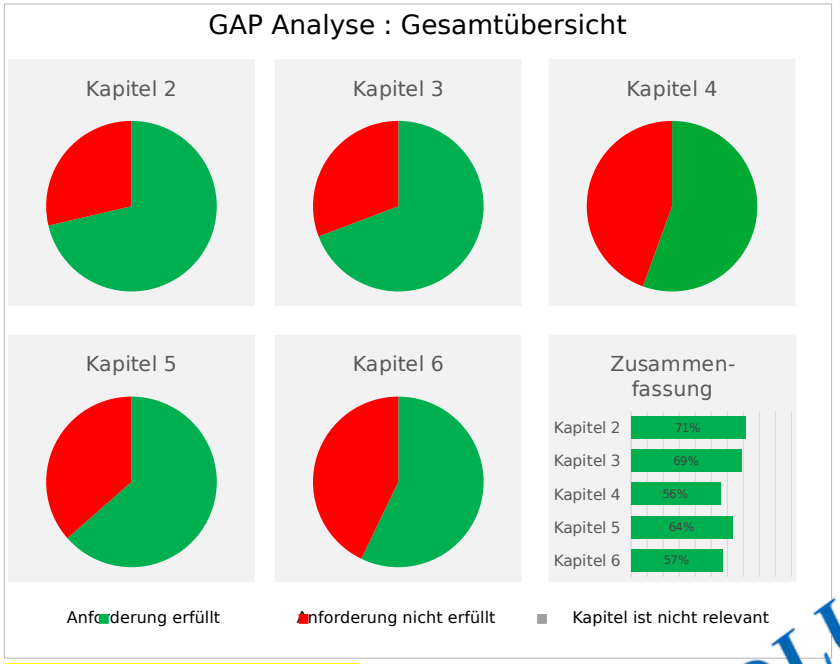
Kapitel 5			
	Art. 28	Art. 29	Art. 30
Ja	22	6	19
Nein	15	1	11
N/A	0	1	0
Keine Antwort	0	0	0

Kapitel 6	
	Art. 45
Ja	4
Nein	3
N/A	0
Keine Antwort	0

DORA GAP-Analyse **VR-Bank Musterstadt eG**

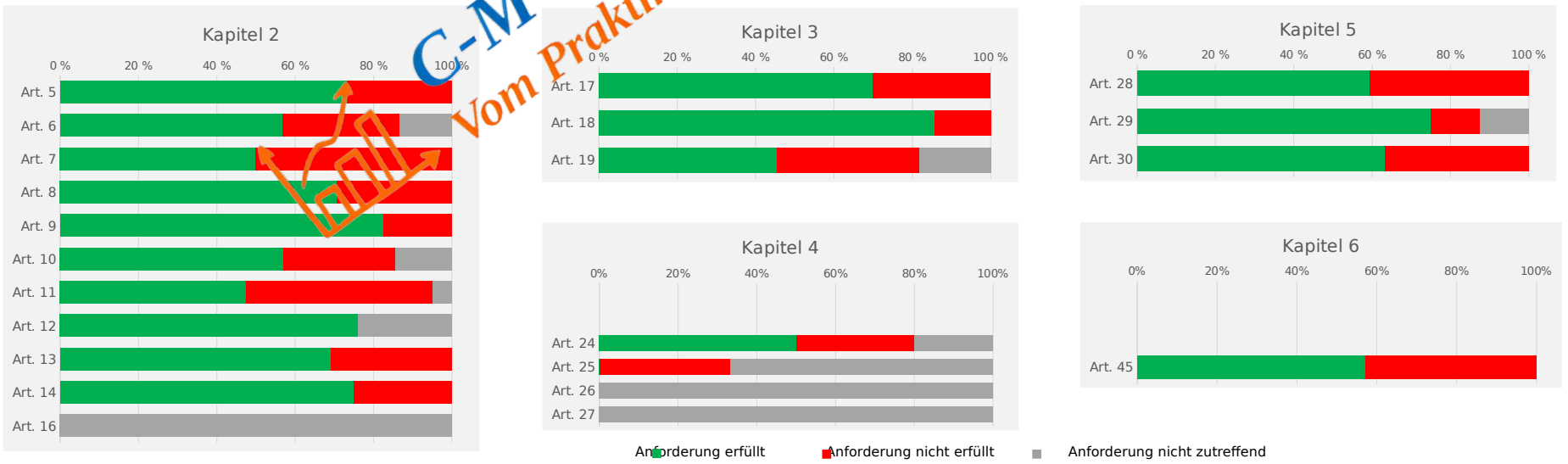
C-M-SOLUTIONS
Vom Praktiker für Praktiker

GAP Analyse : Gesamtübersicht



Lizenziert für: **VR-Bank Musterstadt eG**

GAP Analyse : Detailansicht



Artikel	Handlungsfeld	Interne Referenz	GAP-Analyse Frage	Antwort	Bemerkung/Dokumentation	DORA Referenz
Artikel 5	Governance und Organisation	1.1	Verfügen Sie über einen internen Governance- und Kontrollrahmen zur Steuerung von IKT-Risiken?	Ja		5.1
		1.2	Definiert, genehmigt, überwacht und verantwortet der Vorstand die Umsetzung des IKT-Risikomanagementrahmens?	Ja		5.2
		2.1	Verfügen Sie über Richtlinien zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten?	Ja		5.2 b
		2.3	Hat der Vorstand klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance Regelungen festgelegt und im gesamten Unternehmen kommuniziert?	Ja		5.2 c
		3.1	Hat der Vorstand eine Strategie zur digitalen betrieblichen Resilienz und eine angemessene Toleranzschwelle für das IKT-Risiko festgelegt und genehmigt?	Ja		5.2 d
		4.1	Hat der Vorstand die IKT-Geschäftskontinuitätsrichtlinie sowie die IKT-Reaktions- und Wiederherstellungspläne genehmigt und überwacht und überprüft er diese regelmäßig?	Ja		5.2 e
		5.1	Hat der Vorstand interne IKT-Revisionspläne genehmigt und überprüft er die IKT-Revision und die daran vorgenommen wesentlichen Änderungen regelmäßig?	Ja		5.2 f
		6.1	Hat der Vorstand das Budget für das Risikomanagement zugewiesen und überprüft es regelmäßig, um sicherzustellen, dass Sie über angemessene Ressourcen aller Art , einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz, verfügen?	Ja		5.2 g
		7.1	Hat der Vorstand eine Richtlinie zur Nutzung von IKT-Drittanbietern genehmigt und überprüft sie diese regelmäßig?	Ja		5.2 h
		8.1	Verfügen Sie über Meldekanäle auf Unternehmensebene, um Sie über IKT-Dienstleistungsvereinbarungen Dritter auf dem Laufenden zu halten?	Nein		5.2 i
		8.2	Stellen diese Meldekanäle Informationen zu allen relevanten geplanten wesentlichen Änderungen in Bezug auf IKT-Drittdienstleistern bereit?	Nein		5.2 i II
		8.3	Liefern diese Meldekanäle Informationen darüber, wie sich diese Veränderungen potenziell auf kritische oder wichtige Geschäftsfunktionen auswirken werden?	Nein		5.2 i III
		8.4	Wenn ja, umfassen diese Informationen Zusammenfassungen der Risikoanalyse für diese Änderungen und andere IKT-bezogene Vorfälle?	Nein		5.2 i III
		9.1	Haben Sie eine Funktion eingerichtet oder jemanden im Vorstand benannt, der Ihre IKT-Dienstleistungsvereinbarungen für Dritte überwacht und damit verbundene Risikoposition und die einschlägige Dokumentation verantwortet?	Ja		5.3
		10.1	Halten die Mitglieder des Vorstands ausreichend Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand, nehmen u. a. an Schulungen teil, um die Auswirkungen der IKT-Risiken auf die Geschäftstätigkeit zu verstehen und bewerten zu können.	Ja		5.4

Artikel 6	IKT-Risikomanagementrahmen	1.1	Verfügen Sie über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Teil Ihres gesamten Risikomanagementsystems?	Ja		6.1
		1.2	Enthält dieser Rahmen die Strategien, Richtlinien, Verfahren, IKT-Protokolle und Tools, die erforderlich sind, um alle IKT Assets ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen zu schützen?	Nein		6.2
		1.3	Setzen Sie geeignete Strategien, Richtlinien, Verfahren, Protokolle und Instrumente zur Minimierung von IKT-Risiken ein?	Ja		6.3
		2.1	Verfügen Sie über ein Verfahren, um der zuständigen Behörde auf Anfrage Informationen zum IKT-Risiko und Ihrem IKT-Risikomanagementrahmen zur Verfügung zu stellen?	Nein		6.3
		3.1	Haben Sie die Verantwortung für das Management und die Überwachung von IKT-Risiken einer Kontrollfunktion übertragen?	Nein		6.4
		4.1	Gibt es eine angemessene Trennung und Unabhängigkeit der IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen?	Ja		6.4
		5.1	Verfügen Sie über dokumentierte Anweisungen zur Überprüfung des IKT-Risikomanagementrahmens mindestens einmal im Jahr?	Ja		6.5
		6.1	Verfügen Sie über dokumentierte Anweisungen zur regelmäßigen Überprüfung des IKT-Risikomanagementrahmens?	N/A	nur relevant für Kleinstunternehmen	6.5
		7.1	Verfügen Sie über dokumentierte Anweisungen zur Überprüfung des IKT-Risikomanagementrahmens nach schwerwiegenden IKT-bezogenen Vorfällen?	Ja		6.5
		8.1	Verfügen Sie über dokumentierte Anweisungen zur Überprüfung des IKT-Risikomanagementrahmens, wenn dies aufgrund von Aufsichtsanweisungen, einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren als notwendig erachtet wird?	Ja		6.5
		9.1	Unterliegt der IKT-Risikomanagementrahmen einem formellen kontinuierlichen Verbesserungsprozess?	Ja		6.5
		10.1	Verfügen Sie über ein Verfahren zur Übermittlung von Audit-Berichten zu Ihrem IKT-Risikomanagementrahmen an die zuständige Behörde auf Anfrage?	Nein		6.5
		11.1	Führen Sie regelmäßige interne Audits Ihres IKT-Risikomanagementrahmens im Einklang mit Ihrem Revisionplan durch?	Ja		6.6
		11.2	Werden diese Audits von Revisoren mit ausreichendem Wissend und ausreichender Fähigkeiten und Fachkenntnissen im Bereich IKT-Risiken sowie angemessener Unabhängigkeit durchgeführt?	Ja		6.6
		11.4	Verfügen Sie über ein formelles Follow-up-Verfahren einschließlich Regeln für die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision?	Nein		6.7
		12.1	Verfügen Sie über eine Strategie zur digitalen operationalen Resilienz, die darlegt, wie der Risikomanagementrahmen umgesetzt werden soll?	Ja		6.8
		12.2	Erklärt diese Strategie, wie das IKT-Risikomanagementsystem Ihre Geschäftsziele unterstützt?	Ja		6.8 a
		12.3	Stellt diese Strategie Ihre IKT-Risikotoleranzschwelle im Einklang mit der Ihrer Risikobereitschaft fest?	Ja		6.8 b
		12.4	Wird in der Strategie die Auswirkungstoleranz mit Blick auf IKT-Störungen untersucht?	Nein		6.8.b
		12.4	Enthält diese Strategie klare Ziele für die Informationssicherheit, einschließlich wesentlicher wichtiger Leistungsindikatoren und wesentlicher wichtiger Risikokennzahlen?	Ja		6.8 c
		12.5	Erläutert diese Strategie die IKT-Referenzarchitektur und alle Änderungen, die erforderlich sind, um spezifische Geschäftsziele zu erreichen?	Nein		6.8 d
		12.6	Enthält diese Strategie Mechanismen, die eingesetzt werden um IKT-bezogene Vorfälle zu erkennen und sich vor Schaden zu schützen und daraus entstehende Folgen zu verhindern	Ja		6.8 e
		12.7	Enthält diese Strategie Nachweise über Ihre derzeitige digitale betriebliche Widerstandsfähigkeit, wobei die Anzahl der gemeldeten größeren IKT-bezogenen Vorfälle und die Wirksamkeit Ihrer Präventivmaßnahmen aufgeführt sind?	Ja		6.8 f
		12.8	Beinhaltet diese Strategie Pläne für Tests der digitalen operativen Belastbarkeit?	Ja		6.8 g
		12.9	Enthält diese Strategie eine Kommunikationsstrategie für IKT-bezogenen Vorfällen?	Nein		6.8 h
		13.1	Haben Sie gegebenenfalls eine ganzheitliche Strategie zur Nutzung mehrerer IKT-Drittanbietern auf Gruppen- oder Unternehmensebene definiert?	N/A	N/A = Nein	6.9
		13.2	Wenn ja, zeigt diese Strategie wichtige Beziehungen zwischen externen IKT-Dienstleistern?	N/A		6.9
		13.3	Wenn ja, erklärt diese Strategie die Gründe für den Beschaffungsmix Ihrer externen IKT-Dienstleister?	N/A		6.9
		14.1	Haben Sie gegebenenfalls die Aufgaben zur Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen ausgelagert?	Ja		6.10
		14.2	Wenn ja, haben Sie sichergestellt, dass Sie weiterhin die volle Verantwortung für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen übernehmen?	Nein		6.10

Artikel 7	**IKT-Systeme, Protokolle und Tools**	1.1	Sind Ihre IKT-Systeme, Protokolle und Tools geeignet, um den Umfang von Vorgängen und die Ausübung Ihrer Geschäftstätigkeit zu unterstützen?	Ja		**7. a**
		2.1	Sind diese IKT-Systeme, Protokolle und Tools zuverlässig?	Nein		**7 b**
		3.1	Sind Ihre IKT-Systeme, -Protokolle und -Werkzeuge mit ausreichenden Kapazitäten ausgestattet, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien zu bewältigen.	Ja		**7.c**
		4.1	Sind diese IKT-Systeme, Protokolle und Tools technologisch belastbar und in der Lage, bei angespannten Marktbedingungen oder anderen widrigen Umständen, erforderlichen Bedarf an Informationsverarbeitung angemessen zu erfüllen?	Nein		**7.d**
Artikel 8	**Identifizierung**	1.1	Haben Sie IKT-gestützte Geschäftsfunktionen, Rollen und Verantwortlichkeiten, Informationswerte und die IKT-Werte, die diese Funktionen unterstützen, identifiziert, klassifiziert und angemessen dokumentiert?	Ja		**8.1**
		1.2	Beinhaltet dies auch ihre Rollen und Abhängigkeiten in Bezug auf die IKT-Risiken?	Ja		**8.1**
		1.3	Überprüfen Sie diese Klassifizierung und alle anderen relevanten Unterlagen mindestens einmal jährlich?	Ja		**8.1**
		2.1	Ermitteln Sie kontinuierlich alle Quellen von IKT-Risiken?	Ja		**8.2**
		3.1	Bewerten Sie kontinuierlich Cyberbedrohungen und IKT-Schwachstellen, die für Ihre IKT-gestützten Geschäftsfunktionen, Informationsressourcen und IKT-Ressourcen relevant sind, insbesondere das Risiko gegenüber und von andren Finanzunternehmen?	Nein		**8.2**
		4.1	Überprüfen Sie mindestens jährlich die betreffenden Risikoszenarien?	Ja		**8.2**
		5.1	Führen Sie Risikobewertungen nach wesentlichen Änderungen an Ihrer Netzwerk- und Informationssysteminfrastruktur durch?	Ja		**8.3**
		6.1	Führen Sie Risikobewertungen durch, wenn sich Änderungen an Prozessen oder Verfahren ergeben, die sich auf IKT-gestützte Geschäftsfunktionen, Informations- oder IKT-Assets auswirken?	Nein		**8.3**
		7.1	Haben Sie alle Informationsressourcen und IKT-Ressourcen identifiziert, einschließlich derer an externen Standorten, Netzwerkressourcen und Hardware?	Nein		**8.4**
		8.1	Haben Sie alle Informations- und IKT-Assets ermittelt und die Kritikalität zugeordnet?	Ja		**8.4**
		9.1	Haben Sie die Konfiguration dieser Assets sowie die Verbindungen und gegenseitige Abhängigkeiten zwischen den verschiedenen Informations- und IKT-Assets abgebildet?	Ja		**8.4**
		10.1	Haben Sie alle Prozesse identifiziert und dokumentiert, die von externen IKT-Dienstleistern abhängig sind?	Ja		**8.5**
		11.1	Haben Sie die Abhängigkeiten/Vernetzungen zwischen IKT-Drittanbieterdiensten identifiziert, die kritische oder wichtige Funktionen unterstützen?	Ja		**8.5**
		12.1	Führen Sie Verzeichnisse der IKT-gestützten Geschäftsfunktionen, der Informationswerte und der IKT-Werte?	Ja		**8.6**
		12.2	Aktualisieren Sie diese Bestände regelmäßig und immer dann, wenn sich Änderungen an Ihrer Informationssysteminfrastruktur oder Ihren Prozessen und Verfahren im Zusammenhang mit IKT-gestützten Geschäftsfunktionen, Informationsressourcen oder IKT-Assets ergeben?	Ja		**8.6**
		13.1	Führen Sie mindestens einmal im Jahr eine spezifische IKT-Risikobewertung aller IKT-Altsysteme durch?	Nein		**8.7**
		13.2	Führen Sie eine solche Bewertung in jedem Fall vor und nach der Anbindung von Technologien, Anwendungen oder Systemen durch?	Nein		**8.7**

Artikel 9	**Schutz und Prävention**	1.1	Überwachen und kontrollieren Sie kontinuierlich die Sicherheit und Funktionsfähigkeit von IKT-Systemen und -Tools?	Ja		**9.1**
		2.1	Verfügen Sie über geeignete IKT-Sicherheitstools, Richtlinien und Verfahren, die Auswirkungen von IKT-Risiken auf IKT-Systeme zu minimieren?	Ja		**9.1**
		3.1	Verfügen Sie über IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und Tools, die die Widerstandsfähigkeit, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen gewährleisten?	Ja		**9.2**
		4.1	Verfügen Sie über IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -tools, um hohe Standards in Bezug auf Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten, unabhängig davon ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden?	Nein		**9.2**
		5.1	Haben Sie IKT-Lösungen und -Prozesse eingesetzt, um Daten während der Übertragung zu sichern?	Ja		**9.3 a**
		6.1	Haben Sie IKT-Lösungen und -Prozesse eingesetzt, um das Risiko von Datenkorruption oder -verlust, unbefugtem Zugriff und technischen Mängeln, die die Geschäftstätigkeit beeinträchtigen können, zu minimieren?	Ja		**9.3b**
		7.1	Haben Sie IKT-Lösungen und -Prozesse eingesetzt, um das Risiko eines unbefugten Zugriffs zu minimieren?	Ja		**9.3 b**
		8.1	Haben Sie IKT-Lösungen und -Prozesse eingesetzt, um das Risiko technischer Mängel zu minimieren, die die Geschäftstätigkeit behindern könnten?	Ja		**9.3 b**
		9.1	Haben Sie IKT-Lösungen und -Prozesse eingesetzt, die dem Mangel, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorbeugen?	Ja		**9.3 c**
		9.2	Haben Sie IKT-Lösungen und -Prozesse zum Schutz der Daten vor Datenmanagement-Risiken einschließlich schlechter Verwaltung, verarbeitungsbedingter Risiken und menschlichem Versagen eingesetzt?	Ja		**9.3 d**
		10.1	Verfügen Sie über eine Informationssicherheitsrichtlinie, die Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets, gegebenenfalls einschließlich derjenigen ihrer Kunden, festgelegt sind	Ja		**9.4 a**
		11.1	Haben Sie beim Aufbau einer soliden Netzwerk- und Infrastrukturarchitektur einen risikobasierten Ansatz gewählt?	Ja		**9.4 b**
		11.2	Verwendet diese Struktur angemessene Techniken, Methoden und Protokolle?	Nein	Wozu auch die Umsetzung automatisierter Mechanismen zur Isolierung betroffener Informationsassets im Falle eines Cyberangriffs gehören kann?	**9.4 b**
		12.1	Verfügen Sie über Zugriffskontrollrichtlinien, die den physischen oder logischen Zugriff auf Informations- und IKT-Assets, ausschließlich auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist, regeln?	Ja		**9.4 c**
		13.1	Haben Sie Konzepte und Protokolle implementiert, die auf einschlägigen Normen und speziellen Kontrollsystemen basieren und für starke Authentifizierungsmechanismen sorgen?	Ja		**9.4 d**
		14.1	Verfügen Sie über Verschlüsselungsrichtlinien und -protokolle, die auf der Datenklassifizierung und den Ergebnissen Ihrer IKT-Risikobewertung basieren?	Ja		**9.4 d**
		15.1	Verfügen Sie über Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement?	Ja		**9.4 e**
		15.2	Erfassen diese Richtlinien, Verfahren und Kontrollen Änderungen an Software, Hardware, Firmware-Komponenten, Systemen und Sicherheitsparametern, die auf einem Risikobewertungsansatz basieren?	Nein		**9.4 e**
		15.3	Werden alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft?	Ja		**9.4 e**
		16.1	Verfügen Sie über angemessene und umfassende dokumentierte Richtlinien für Patches und Updates?	Ja		**9.4 f**
		17.1	Haben Sie Ihre Infrastruktur für die Netzanbindung und Netzwerkverbindung so konzipiert, dass sie sofort getrennt oder segmentiert werden kann?	Nein		**9.**
		18.1	Ist der IKT-Änderungsmanagementprozess Vorstand genehmigt?	Ja		**9.**
		19.1	Gibt es spezifische Protokolle für den IKT-Änderungsmanagementprozess?	Ja		**9.**

Artikel 10	**Erkennung**	1.1	Verfügen Sie über Mechanismen, um anomale Aktivitäten, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogenen Vorfällen, umgehend zu erkennen und potentielle einzelne wesentliche Schwachstellen zu ermitteln	Ja		**10.1**
		1.2	Werden diese Erkennungsmechanismen regelmäßig getestet?	Nein		**10.1**
		1.3	Verfügen diese Erkennungsmechanismen über mehrere Kontrollebenen?	Ja		**10.2**
		1.4	Verfügen diese Erkennungsmechanismen über definierte Alarmschwellen?	Ja		**10.2**
		1.5	Verfügen diese Erkennungsmechanismen über definierte Kriterien, um IKT-bezogene Vorfällen auszulösen und einzuleiten, einschließlich automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind?	Nein		**10.2**
		2.1	Verfügen Sie über ausreichende Ressourcen und Kapazitäten, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen?	Ja		**10.3**
		3.1	Verfügen Sie über ein System, um Handelsauskünfte auf Vollständigkeit zu prüfen, Lücken und offensichtliche Fehler zu erkennen und eine erneute Übermittlung dieser Auskünfte anzufordern?	N/A	nur relevant für Datenbereitstellungsdienste	**10.4**
Artikel 11	**Reaktion und Wiederherstellung**	1.1	Verfügen Sie über eine IKT-Geschäftsfortführungsrichtlinie, die als eigenständige spezielle Leitlinie, verabschiedet wurde?	Nein		**11.1**
		1.2	Gewährleistet diese Richtlinie die Fortführung Ihrer kritischen oder wichtigen Funktionen?	Nein		**11.2 a**
		1.3	Stellt diese Richtlinie sicher, dass Sie schnell, angemessen und wirksam auf alle IKT-bezogenen Vorfälle reagieren und diesen so entgegenwirken, dass Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Wiederherstellungsmaßnahmen Priorität einräumt?	Nein		**11.2 b**
		1.4	Beschreibt diese Richtlinie Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfällen um weitere Schäden zu vermeiden, sowie maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Artikel 12 zu aktivieren.	Nein		**11.2 c**
		1.5	Enthält diese Richtlinie einen Ansatz zur vorläufigen Einschätzung von Auswirkungen, Schäden und Verlusten?	Nein		**11.2 d**
		1.6	Sind in dieser Richtlinie Kommunikations- und Krisenmanagementmaßnahmen festgelegt, die sicherstellen, dass aktualisierte Informationen an alle relevanten internen Mitarbeiter, externen Interessenträgern übermittelt werden und die Meldung an die zuständigen Behörden sichergestellt?	Nein		**11.2 e**
		2.1	Haben Sie IKT-Reaktions- und Wiederherstellungspläne implementiert?	Ja		**11.3**
		2.2	Unterliegen diese IKT-Reaktions- und Wiederherstellungspläne unabhängigen internen Revision ?	Ja		**11.3**
		3.1	Haben Sie IKT-Geschäftskontinuitätspläne für kritische und wichtige Funktionen implementiert, die ausgelagert oder durch vertraglicher Vereinbarungen an IKT-Drittdienstleister vergeben werden?	Ja		**11.4**
		3.2	Pflegen und testen Sie diese IKT-Geschäftskontinuitätspläne regelmäßig?	Nein		**11.4**
		4.1	Führen Sie eine Business Impact Analysis (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen durch?	Ja		**11.5**
		4.2	Bewertet die BIA die potenziellen Auswirkungen schwerwiegender Betriebsstörungen anhand quantitativer und qualitativer Kriterien wobei ggf. interne und externer Daten sowie Szenarioanalysen herangezogen werden?	Ja		**11.5**
		4.3	Berücksichtigt die BIA die Kritikalität identifizierter und erfasster Unternehmensfunktionen, Unterstützungsprozesse, Abhängigkeiten von Dritten und Informationsassets sowie Interdependenzen?	Ja		**11.5**
		4.4	Ist die Redundanz aller kritischen Komponenten in der BIA gewährleistet?	Ja		**11.5**
		5.1	Testen Sie die IKT-Geschäftsfortführungspläne der IKT-Systeme, sowie im Falle jeglicher wesentlicher Änderungen an IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, die IKT-Reaktions- und Wiederherstellungspläne mindestens jährlich?	Nein		**11.6 a**
		6.1	Verfügen Sie über einen Krisenkommunikationsplan, in dem klare Prozesse für die interne und externe Krisenkommunikation festgelegt sind?	Nein		**11.6 b**
		6.2	Testen Sie diese Pläne regelmäßig?	Nein		**11.6 b**
		7.1	Decken Ihre IKT-Geschäftsfortführungspläne und IKT-Reaktions- und Wiederherstellungspläne Szenarien für Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme ab?	Ja		**11.6**
		8.1	Können Ihre Dokumentationen über Tätigkeiten vor und während Störungen, wenn ihre IKT-Geschäftsfortführungspläne oder ihre IKT-Reaktions- -und Wiederherstellungspläne aktiviert wurden, jederzeit eingesehen werden.	Ja		**11.8**
		9.1	Können Sie den zuständigen Behörden auf Anfrage die Ergebnisse von IKT-Geschäftskontinuitätstests oder ähnlichen Übungen vorlegen?	N/A	nur relevant für Zentralverwahrer	**11.9**
		10.1	Können Sie den zuständigen Behörden auf Anfrage eine Schätzung der aggregierten jährlichen Kosten und Verluste vorlegen, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden?	Ja		**11.10**

Artikel 12	**Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung**	1.1	Verfügen Sie über Richtlinien und Verfahren zur Sicherung von Systemen und Daten?	Ja		**12.1**
		1.2	Definieren diese Richtlinien und Verfahren auf Grundlage der Kritikalität der Informationen oder des Vertraulichkeitsgrads der Daten den Umfang und die Häufigkeit von Sicherungen?	Ja		**12.1 a**
		2.1	Verfügen Sie über Verfahren und Methoden zur Wiederherstellung von Daten und Systemen?	Ja		**12.1 b**
		3.1	Verfügen Sie über Backup-Systeme, die gemäß diesen Richtlinien, Verfahren und Methoden aktiviert werden können?	Ja		**12.2**
		3.2	Haben Sie sichergestellt, dass die Aktivierung Ihrer Backup-Systeme die Sicherheit des Netzwerks und der Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten nicht gefährdet?	Ja		**12.2**
		3.3	Testen Sie regelmäßig die Verfahren für Backups und Wiederherstellung?	Ja		**12.2**
		3.4	Sind die IKT-Systeme, die Sie für Backups verwenden, physisch und logisch vom Quellsystem getrennt?	Ja		**12.3**
		3.5	Sind diese IKT-Systeme vor unbefugtem Zugriff oder IKT-Manipulation geschützt?	Ja		**12.3**
		3.6	Ermöglichen diese IKT-Systeme die zeitnahe Wiederherstellung von Diensten und nutzen bei Bedarf Daten- und Systemsicherungen?	Ja		**12.3**
		4.1	Ermöglichen Ihnen Ihre Wiederherstellungspläne die Wiederherstellung aller Transaktionen zum Zeitpunkt der Störung, sodass Sie die Abwicklung zum vorgesehenen Zeitpunkt abschließen können.	Ja		**12.3**
		5.1	Verfügen Sie über ausreichende zusätzliche angemessene Ressourcen, und verfügen über die entsprechenden Backup- und Wiedergewinnungseinrichtungen, um sicherzustellen, dass Dienste jederzeit angeboten und aufrechterhalten werden können?	Ja		**12.3**
		6.1	Verfügen Sie über redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind.	Ja		**12.4**
		6.2	Haben Sie anhand Ihres Risikoprofils die Notwendigkeit der Aufrechterhaltung redundanter IKT-Kapazitäten beurteilt?	N/A	nur relevant für Kleinstunternehmen	**12.4**
		7.1	Verfügen Sie über mindestens einen sekundären Verarbeitungsstandort mit den Notwendigen Ressourcen, Fähigkeiten, Funktionen und Personalvereinbarungen, um die Geschäftsanforderungen zu erfüllen?	N/A	nur relevant für Zentralverwahrer	**12.5**
		7.2	Befinden sich sekundäre Verarbeitungsstandorte an einem anderen Standort als der primäre?	N/A	nur relevant für Zentralverwahrer	**12.5**
		7.3	Können sekundäre Verarbeitungsstandorte kritische oder wichtige Funktionen genauso wie der primäre Standort bereitstellen oder ein erforderliches Serviceniveau aufrechterhalten, um sicherzustellen, dass kritische Vorgänge innerhalb der Wiederherstellungsziele bleiben?	N/A	nur relevant für Zentralverwahrer	**12.5**
		7.4	Ist die sekundäre Verarbeitungsanlage für das Personal sofort zugänglich, falls die primäre Verarbeitungsanlage nicht verfügbar ist?	N/A	nur relevant für Zentralverwahrer	**12.5**
		8.1	Berücksichtigen Sie beim Festlegen der Wiederherstellungszeit- und Wiederherstellungspunkt jeder Funktion, ob sie kritisch oder wichtig ist und welche potenziellen Gesamtauswirkungen sie auf die Markteffizienz hat?	Ja		**12.6**
		9.1	Berücksichtigen die Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion, ob es sich um kritische oder wichtige Funktionen handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz?	Ja	Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbart Dienstleistungsgüte in Extremszenarien erreicht wird.	**12.6**
		10.1	Haben Sie Pläne zur Überprüfung der größtmöglichen Datenintegrität nach einem IKT-bezogenen Vorfall implementiert, und stellen Sie sicher das alle Daten systemübergreifend redundant sind?	Ja		**12.7**
		10.2	Umfassen diese Pläne die Datenrekonstruktion durch externe Interessenträger?	Ja		**12.7**

Artikel 13	**Lernprozesse und Weiterentwicklung**	1.1	Verfügen Sie über die Kapazitäten und das Personal, um Informationen über Schwachstellen, Cyber-Bedrohungen und IKT-bezogenen Vorfällen zu sammeln und deren wahrscheinliche Auswirkungen auf Ihre digitale operationale Resilienz zu analysieren?	Ja		**13.1**
		2.1	Haben Sie Prozesse implementiert, die nach Störungen ihrer Haupttätigkeit infolge schwerwiegender IKT-bezogener Vorfälle eine nachträgliche Prüfung anstoßen.	Ja		**13.2**
		2.2	Analysieren diese Prüfungen die Ursachen von Störungen und identifizieren Sie Verbesserungen, die Sie am IKT-Betrieb oder in der IKT-Geschäftsfortführungsleitlinie implementieren ?	Nein		**13.2**
		2.3	Verfügen Sie über ein Verfahren, um den zuständigen Behörden die Änderungen mitzuteilen, die Sie nach der Überprüfung von IKT-bezogenen Vorfällen vorgenommen haben?	Ja		**13.2**
		2.4	Ermitteln diese Überprüfungen, ob die festgelegten Verfahren eingehalten wurden und ob die von Ihnen ergriffenen Maßnahmen wirksam waren?	Nein		**13.2**
		2.5	Analysieren diese Überprüfungen die Geschwindigkeit, mit der Sie auf Sicherheitswarnungen reagiert und die Auswirkungen und den Schweregrad von IKT-Vorfällen ermittelt haben?	Ja		**13.2 a**
		2.6	Untersuchen diese Überprüfungen die Qualität und Geschwindigkeit Ihrer forensischen Analyse, sofern dies als angemessen erachtet wird?	Ja		**13.2 b**
		2.7	Analysieren diese Überprüfungen die Wirksamkeit der Eskalation von Vorfällen innerhalb Ihres Instituts?	Ja		**13.2 c**
		2.8	Analysieren diese Überprüfungen die Wirksamkeit Ihrer internen und externen Kommunikation?	Nein		**13.2 d**
		3.1	Berücksichtigen Ihre Risikobewertungen Erkenntnisse aus digitalen operationalen Resilienz?	Ja		**13.3**
		4.1	Berücksichtigen Sie Erkenntnisse aus durchgeführten Tests der digitalen operationalen Resilienz und aus realen IKT-bezogenen Vorfällen, kontinuierlich in Ihrem IKT-Risikobewertungsprozess und daraus abgeleitet in Ihrem IKT-Risikomanagementrahmen?	Ja		**13.3**
		5.1	Berücksichtigen Ihre Risikobewertungen Erkenntnisse aus der Aktivierung Ihrer IKT-Geschäftsfortführungsplans und der IKT-Reaktions- und Wiederherstellungspläne?	Nein		**13.3**
		6.1	Berücksichtigen Ihre Risikobewertungen die Kenntnisse, die Sie durch den Austausch von Informationen mit Kollegen gewonnen haben?	Ja		**13.3**
		7.1	Berücksichtigen Ihre Risikobewertungen Erkenntnisse aus aufsichtsrechtlichen Überprüfungen?	Ja		**13.3**
		8.1	Nutzen Sie diese Erkenntnisse, um angemessene Überprüfungen der relevanten Komponenten Ihres IKT-Risikomanagementrahmens durchzuführen?	Ja		**13.3**
		9.1	Überwachen Sie die Wirksamkeit Ihrer Strategie zur digitalen operationalen Resilienz?	Ja		**13.4**
		10.1	Bilden Sie die Entwicklung des IKT-Risikos im Laufe der Zeit ab?	Nein		**13.4**
		11.1	Analysieren Sie Ausmaß, Häufigkeit und Art von IKT-Vorfällen, die sich auf kritische oder wichtige Funktionen auswirken?	Ja		**13.4**
		12.1	Berichten leitende IKT-Mitarbeiter mindestens einmal im Jahr dem Vorstand über die Feststellungen?	Nein		**13.5**
		12.2	Geben leitende IKT-Mitarbeiter im Rahmen dieses Prozesses Empfehlungen für die digitale operationale Resilienz und Geschäftsfortführung ab?	Nein		**13.5**
		13.1	Umfassen Ihre Mitarbeiterschulungsprogramme obligatorische Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz?	Ja		**13.6**
		13.2	Sind diese Programme auf alle Mitarbeiter anwendbar, einschließlich des Vorstands?	Ja		**13.6**
		13.3	Bieten diese Programme ein Maß an Komplexität, das dem Aufgabenbereich und Verantwortlichkeiten der Benutzer angemessen ist?	Ja		**13.6**
		14.1	Beziehen Sie ggf. IKT-Drittanbieter in relevante Schulungsprogramme ein?	Nein	N/A wenn keine IKT-Drittanbieter eingesetzt werden (sehr unwahrscheinlich)	**13.6**
		15.1	Überwachen Sie fortlaufend einschlägige technologische Entwicklungen, um mögliche Auswirkungen des Einsatzes solcher neuer Technologien auf die Anforderungen an die IKT-Sicherheit und die digitale operationale Resilienz zu verstehen.	Ja		**13.7**
		16.1	Halten Sie sich über die neuesten IKT-Risikomanagementprozesse auf dem Laufenden?	Ja		**13.7**
Artikel 14	**Kommunikation**	1.1	Verfügen Sie über Krisenkommunikationspläne, die es Ihnen ermöglichen, schwerwiegende IKT-bezogene Vorfälle und Schwachstellen verantwortungsbewusst gegenüber Kunden, Partnern und der Öffentlichkeit offenzulegen?	Ja		**14.1**
		2.1	Verfügen Sie über Kommunikationsstrategien für interne Mitarbeiter und für externe Interessenträger?	Ja		**14.2**
		3.1	Unterscheiden diese Kommunikationsleitlinien zwischen Mitarbeitern, die am IKT-Risikomanagement beteiligt sind, und denen, die über Ihre Prozesse und Verfahren informiert werden müssen?	Nein	Erst 1.1 und 1.2 aufgrund der Logik beantworten	**14.2**
		4.1	Haben Sie eine Person oder ein Team beauftragt, die Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle gegenüber der Öffentlichkeit und der Medien wahrnimmt?	Ja		**14.3**
		1.1	Verfügen Sie über ein Rahmenwerk für das IKT-Risikomanagement, das Maßnahmen zum Management von IKT-Risiken enthält?	N/A	Artikel 16 ist nur relevant für die in der Verordnung 16.1 genannten Institute	**16**
		1.2	Testen Sie diese Maßnahmen regelmäßig?	N/A		**16**

Artikel 16	**Vereinfachter IKT-Risikomanagementrahmen**	2.1	Überwachen Sie kontinuierlich die Sicherheit und Funktion aller IKT-Systeme?	N/A		**16**
		2.2	Testen Sie regelmäßig die Überwachungsprozesse?	N/A		**16**
		3.1	Nutzen Sie IKT-Systeme, -Protokolle und -Tools, um die Auswirkungen von IKT-Risiken zu minimieren?	N/A		**16**
		3.2	Testen Sie diese Systeme, Protokolle und Tools regelmäßig?	N/A		**16**
		4.1	Identifizieren, erkennen und reagieren Sie umgehend auf IKT-Risikoquellen und Schwachstellen in Ihrem Netzwerk und Ihren Informationssystemen?	N/A		**16**
		5.1	Haben Sie gegebenenfalls wesentliche Abhängigkeiten von IKT-Drittanbietern identifiziert?	N/A		**16**
		6.1	Verfügen Sie über Geschäftskontinuitätspläne sowie Reaktions- und Wiederherstellungsmaßnahmen, einschließlich Sicherungs- und Wiederherstellungsmaßnahmen?	N/A		**16**
		6.2	Testen Sie diese Pläne und Maßnahmen regelmäßig?	N/A		**16**
		6.3	Führen Sie auf der Grundlage der Ergebnisse dieser Tests relevante Änderungen an Ihrem Risikobewertungsprozess durch?	N/A		**16**
		6.4	Implementieren Sie relevante Änderungen an Ihrem Risikobewertungsprozess auf der Grundlage einer Post-Incident-Analyse?	N/A		**16**
		8.1	Müssen Ihre Mitarbeiter an Programmen zur Sensibilisierung für IKT-Sicherheit und an Schulungen zur digitalen betrieblichen Belastbarkeit teilnehmen?	N/A		**16**
		9.1	Überprüfen Sie Ihr IKT-Risikomanagementsystem regelmäßig und nach größeren IKT-bezogenen Vorfällen?	N/A		**16**
		9.2	Wird das Framework kontinuierlich verbessert?	N/A		**16**
		10.1	Verfügen Sie über ein Verfahren zur Übermittlung von Berichten zu Ihrem IKT-Risikomanagementrahmen an die zuständige Behörde, wenn diese dazu aufgefordert wird?	N/A		**16**

Artikel	Handlungsfeld	Referenz	GAP-Analyse Frage	Antwort	Bemerkung/Dokumentation	DORA Referenz
Artikel 17	Prozess für die Behandlung IKT-bezogener Vorfälle	1.1	Haben Sie einen Prozess für die Behandlung IKT-bezogener Vorfälle eingerichtet, um IKT-bezogene Vorfälle zu erkennen, zu behandeln verwalten und zu melden?	Ja		17.1
		2.1	Erfassen Sie alle alle IKT-bezogenen Vorfälle und erhebliche Cyber-Bedrohungen?	Nein		17.2
		3.1	Verfügen Sie über Verfahren und Prozesse, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten?	Ja		17.2
		3.2	Verfügen Sie über Verfahren und Prozesse, die die Ursachen von Vorfällen ermittelt, dokumentiert, um das Auftreten solcher Vorfälle zu verhindern?	Nein		17.2
		3.3	Beinhaltet dieser Prozess Frühwarnindikatoren?	Ja		17.3 a
		3.4	Umfasst dieser Prozess Verfahren zur Identifizierung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung von IKT-bezogenen Vorfällen entsprechend ihrer Priorität, ihrem Schweregrad und der Kritikalität der betroffenen Dienste?	Ja		17.3b
		3.5	Umfasst dieser Prozess zugewiesene Funktionen und Zuständigkeiten, die nach bestimmten IKT-bezogenen Vorfallarten und -szenarien aktiviert werden?	Ja		17.3 c
		3.6	Umfasst dieser Prozess Pläne für die interne und externe Kommunikation, einschließlich der Benachrichtigung der Kunden, interner Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzinstitute, die als Gegenparteien fungieren (je nach Sachlage)?	Nein		17.3d
		3.7	Stellt dieser Prozess sicher, dass schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene werden und der zuständige Vorstand in der Lage ist, dass die Auswirkungen und Gegenmaßnahmen und zusätzlichen Kontrollen erläutert werden, informiert wird?	Ja		17.3 e
		3.8	Legt dieser Prozess Verfahren zur Reaktion auf IKT-bezogene Vorfälle fest, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste rechtzeitig verfügbar und sicher sind?	Ja		17.3 f
Artikel 18	Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen	1.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen Sie ihre Auswirkungen auf der Grundlage der Anzahl und/oder Relevanz der Kunden oder Gegenparteien im Finanzbereich, die von dem IKT-bezogenen Vorfall betroffen sind, des Werts oder der Anzahl der davon betroffenen Transaktionen und ob potenziell ein Reputationsschäden verursacht wurde?	Ja		18.a
		2.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen Sie deren Auswirkungen anhand der Dauer des Vorfalls, einschließlich der Ausfallzeit des Dienstes ?	Nein		18.b
		3.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen Sie deren Auswirkungen anhand der geografischen Ausbreitung des Vorfalls, insbesondere wenn mehr als zwei Mitgliedsstaaten betroffen sind?	Ja		18. c
		4.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen deren Auswirkungen anhand des Verlusts der Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten?	Ja		18. d
		5.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen Sie die Kritikalität der betroffenen Dienste einschließlich der Transaktionen und Geschäfte des Kreditinstituts?	Ja		18. e
		6.1	Klassifizieren Sie IKT-bezogene Vorfälle und bestimmen Sie deren Auswirkungen anhand ihrer wirtschaftlichen Auswirkungen, insbesondere direkte und indirekte Kosten und Verluste des IKT-bezogenen Vorfalls auf absoluter und relativer Basis?	Ja		18.f
		7.1	Klassifizieren Sie Cyberbedrohungen als erheblich ein, basierend auf der Grundlage der Kritikalität der risikobehafteten Dienste, einschließlich der Transaktionen und Geschäfte des Kreditinstituts, der Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich und der geografischen Ausbreitung der Risikogebiete?	Ja		18.2
Artikel 19	Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	1.1	Verfügen Sie über ein Verfahren zur Meldung schwerwiegender IKT-bezogener Vorfälle an die zuständige Behörde?	Nein		19.1
		2.1	Verfügen Sie über ein Verfahren zur Meldung schwerwiegender IKT-bezogener Vorfälle an die zuständige nationale Behörde?	N/A	i. d. R. nicht relevant für genossenschaftliche Kreditinstitute	19.1
		3.1	Verfügen Sie über ein Verfahren zur Erstellung eines ersten Meldeberichts und dessen Übermittlung an die zuständige Behörde?	Ja		19.1
		3.2	Enthalten diese ersten Meldeberichte alle Informationen, die die zuständige Behörde benötigt, um die Bedeutung des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten?	Ja		19.1
		4.1	Planen Sie, der zuständigen Behörde erhebliche Cyberbedrohungen zu melden, wenn Sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist?	Nein	explizit „auf freiwilliger Basis“	19.2
		4.3	Verfügen Sie über Prozesse ihre Kunden unverzüglich über einen schwerwiegenden IKT-bezogenen Vorfall und die Maßnahme, die ergriffen wurden um nachteilige Auswirkungen eines solchen Vorfalls zu mindern. zu unterrichten?	Nein		19.3
		5.1	Haben Sie sichergestellt, dass eine erste Meldung an die jeweils zuständige Behörde innerhalb der entsprechenden Frist nach Artikel 20 Absatz 1 Buchstabe a Ziffer ii übermittelt werden kann?	Nein		19.4 a
		6.1	Haben Sie sichergestellt, dass eine Zwischenmeldung gesendet wird, sobald sich der Status des ursprünglichen Vorfalls erheblich geändert hat oder sich die Handhabung des schwerwiegenden IKT-bezogenen Vorfalls auf der Grundlage neuer verfügbarer Informationen geändert hat?	Ja		19.4 b
		7.1	Haben Sie sichergestellt, dass bei jeder relevanten Statusaktualisierung oder auf Verlangen der zuständigen Behörde aktualisierte Meldungen übermittelt werden können?	Ja		19.4 b
		8.1	Haben Sie sichergestellt, dass ein Abschlussmeldung verschickt wird, wenn die Ursachenanalyse abgeschlossen ist und sich die tatsächlichen Auswirkungen beziffern lassen und Schätzungen ersetzen?	Ja		19.4 c
		9.1	Wenn Sie Ihre Meldepflichten an einen externen Dienstleister auslagern, können Sie dann die volle Verantwortung für die Erfüllung der Meldepflichten bei Vorfällen nachweisen?	N/A	N/A wenn Meldepflichten nicht ausgelagert wurden	19.5

Artikel	Handlungsfeld	Referenz	GAP-Analyse Frage	Antwort	Bemerkung/Dokumentation	DORA Referenz
Artikel 24	Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz	1.1	Haben Sie ein Programm für das Testen der digitalen operationalen Resilienz als integralen Bestandteil des IKT-Risikomanagementrahmens implementiert?	Ja		24.1
		1.2	Überprüfen Sie dieses Testprogramm regelmäßig?	Nein		24.1
		1.3	Umfasst das Programm zur Prüfung der digitalen operationalen Resilienz eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools?	Nein		24.2
		1.4	Verfolgt Ihr digitales Testprogramm zur digitalen operationalen Resilienz einen risikobasierten Ansatz?	Ja		24.3
		1.5	Werden Tests von unabhängigen Parteien durchgeführt, sei es intern oder extern?	Ja		24.4
		2.1	Stellen Sie bei der Durchführung von Tests durch einen internen Tester ausreichende Ressourcen zur Verfügung?	N/A	N/A wenn Tests nicht intern durchgeführt werden	24.4
		3.1	Wenn Tests von einem internen Tester durchgeführt werden, stellen Sie sicher, dass Interessenkonflikte während der gesamten Konzeptions- und Durchführungsphase vermieden werden?	N/A		24.4
		4.1	Verfügen Sie über Verfahren und Richtlinien zur Priorisierung, Klassifizierung und Behebung aller bei diesen Tests aufgedeckten Probleme?	Ja		24.5
		5.1	Verfügen Sie über interne Validierungsmethoden, um festzustellen, ob alle identifizierten Schwächen, Mängel und Lücken vollständig angegangen werden?	Ja		24.5
		6.1	Führen Sie mindestens einmal jährlich Tests für alle IKT-Systeme und -Anwendungen durch, die kritische oder wichtige Funktionen unterstützen?	Nein		24.6
Artikel 25	Testen von IKT-Tools und Systemen	1.1	Unterstützt das Programm zur Prüfung der digitalen Betriebsstabilität geeignete Tests, wie z. B. Schwachstellenbewertungen und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfung, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests?	Nein		25.1
		2.1	Führen Sie Schwachstellenbewertungen durch, bevor Sie Anwendungen, Infrastrukturkomponenten und IKT-Dienste bereitstellen oder wieder einsetzen, die kritische oder wichtige Funktionen unterstützen?	N/A	nur relevant für Zentralverwahrer und Gegenparteien	25.2
		3.1	Testen Sie Ihre IKT-Systeme mit einer Kombination aus risikobasiertem Ansatz und strategischer Planung? Sie sollten die verfügbaren Ressourcen, die für die IKT-Tests vorgesehene Zeit sowie die Dringlichkeit der Bewertung, die Art des Risikos und die Kritikalität der Informationsressourcen und der bereitgestellten Dienste berücksichtigen?	N/A	nur relevant für Kleinstunternehemen	25.3
Artikel 26	Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT	1.1	Gehören Sie zu den systemrelevanten Instituten und führen mindestens alle drei Jahre bewegungsbasierte Penetrationstests durch?	N/A	Artikel 26 ist nur relevant für TLPT verpflichtete Institute	26
		1.2	Deckt jeder bedrohungsgesteuerte Penetrationstest kritische oder wichtige Funktionen ab?	N/A		26
		1.3	Wird jeder bedrohungsgesteuerte Penetrationstest auf Live-Produktionssystemen durchgeführt, die solche Funktionen unterstützen?	N/A		26
		2.1	Haben Sie alle relevanten zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien identifiziert, die kritische oder wichtige Funktionen und IKT-Dienste unterstützen, einschließlich derjenigen, die ausgelagert oder an Dritte vergeben wurden?	N/A		26
		3.1	Haben Sie beurteilt, welche kritischen oder wichtigen Funktionen von Ihren bedrohungsgesteuerten Penetrationstests abgedeckt werden müssen?	N/A		26
		3.2	Bestimmt das Ergebnis dieser Bewertung den genauen Umfang Ihrer bedrohungsgesteuerten Penetrationstests?	N/A		26
		4.1	Ist der Umfang Ihrer bedrohungsgesteuerten Penetrationstests von den zuständigen Behörden validiert?	N/A		26
		5.1	Wenn IKT-Drittanbieter in den Umfang der Tests einbezogen sind, haben Sie die erforderlichen Maßnahmen und Sicherheitsvorkehrungen getroffen, um sicherzustellen, dass sie teilnehmen?	N/A		26
		6.1	Wenn gepoolte Tests verwendet werden, decken sie den relevanten Bereich von IKT-Diensten ab, die kritische oder wichtige Funktionen unterstützen und die an den jeweiligen IKT-Drittanbieter vergeben wurden?	N/A		26
		6.2	Haben Sie beim Einsatz gepoolter Tests die Anzahl der teilnehmenden Dritten sowie die Komplexität und Art der von ihnen bereitgestellten Dienste berücksichtigt?	N/A		26
		7.	Arbeiten Sie mit relevanten Dritten, einschließlich IKT-Dienstleistern, zusammen, um Risikomanagementkontrollen anzuwenden, die die Risiken bedrohungsgesteuerter Penetrationstests mindern?	N/A		26
		8.1	Geben Sie der zuständigen Behörde eine Zusammenfassung der relevanten Ergebnisse bedrohungsgesteuerter Penetrationstests, die Sanierungspläne und den Nachweis, dass die Tests gemäß den Anforderungen durchgeführt wurden?	N/A		26
		9.1	Stellen Sie diese Informationen zusammen mit der Bescheinigung der Behörde der jeweils zuständigen Behörde zur Verfügung?	N/A		26
		10.1	Haben Sie interne oder externe Tester mit der Durchführung bedrohungsbasierter Penetrationstests beauftragt?	N/A		26
		10.2	Haben Sie externe Tester mit der Durchführung bedrohungsbasierter Penetrationstests beauftragt?	N/A		26
		11.1	Wenn Sie interne Tester einsetzen, beauftragen Sie dann alle drei Tests auch externe Tester?	N/A		26

Artikel 27	**Anforderungen an Tester bezüglich der Durchführung von TLPT**	1.1	Sind Ihre Penetrationstester von höchster Eignung und Reputation?	N/A	Artikel 27 ist nur relevant TLPT verpflichtete Institute	**27**
		1.2	Verfügen Ihre Penetrationstester über technische und organisatorische Fähigkeiten und weisen sie spezifische Fachkenntnisse in den Bereichen Threat Intelligence, Penetrationstests und Red-Team-Tests auf?	N/A		**27**
		1.3	Sind Ihre Penetrationstester entweder von einer geeigneten Akkreditierungsstelle zertifiziert oder halten sie sich an formelle Verhaltenskodizes oder ethische Rahmenbedingungen?	N/A		**27**
		1.4	Bieten Ihre Penetrationstester einen unabhängigen Bestätigungs- oder Prüfbericht, der die Risiken abdeckt, denen Ihr Unternehmen bei der Durchführung von Tests ausgesetzt ist?	N/A		**27**
		1.5	Sind Ihre Penetrationstester vollständig durch die entsprechende Berufshaftpflichtversicherung abgesichert?	N/A		**27**
		2.1	Haben Sie sichergestellt, dass der Einsatz interner Tester von der zuständigen Behörde genehmigt ist?	N/A		**27**
		2.2	Hat die zuständige Behörde beim Einsatz interner Tester überprüft, dass Sie über ausreichende Ressourcen verfügen und dass in der Entwurfs- und Ausführungsphase dieser Tests keine Interessenkonflikte bestehen?	N/A		**27**
		2.3	Haben Sie beim Einsatz interner Tester sichergestellt, dass der Threat-Intelligence-Anbieter eine externe Partei ist?	N/A		**27**
		3.1	Erfordern Ihre Verträge mit externen Testern, dass diese die Risiken verwalten, die mit den Ergebnissen bedrohungsgesteuerter Penetrationstests verbunden sind? Dies sollte die Zusicherung beinhalten, dass die im Rahmen dieser Tests verarbeiteten Daten keine Risiken für Ihr Unternehmen darstellen?	N/A		**27**

Artikel	Handlungsfeld	Referenz	GAP-Analyse Frage	Antwort	Bemerkung/Dokumentation	DORA Referenz
		0	**Lagern Sie IKT-Dienstleistungen an Dritte aus?**	**Ja**		
Artikel 28	**Allgemeine Prinzipien**	1.1	Verwalten Sie das IKT-Drittparteienrisiko als integralen Bestandteil des IKT-Risikos innerhalb Ihres IKT-Risikomanagementrahmens?	Ja		**28.1**
		2.1	Übernehmen Sie die volle Verantwortung für die Einhaltung und Erfüllung aller Verpflichtungen gemäß DORA Verordnung und anderen gesetzlichen Vorschriften?	Ja		**28.1 a**
		3.1	Berücksichtigen Sie beim Management des IKT-Drittparteienrisikos die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogenen Abhängigkeiten?	Ja	Ausdrücklicher Hinweis auf den Grundsatz der Verhältnismäßigkeit	**28.1 b i**
		4.1	Berücksichtigen Sie beim Management des IKT-Drittparteienrisikos, die sich aus vertraglichen Vereinbarungen über den Einsatz von IKT-Drittanbietern ergeben?	Ja		**28.1 b ii**
		5.1	Berücksichtigen Sie beim Management des IKT-Drittparteienrisikos die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen Auswirkungen dieser Risiken auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätgikeiten auf Einzel- und Gruppenebenen berücksichtigt?	Nein		**28.1 b ii**
		6.1	Verfügen Sie über eine IKT-Drittparteinrisiko Strategie und überprüfen diese regelmäßig diese ggf. unter Berücksichtigung Ihrer ganzheitlichen Strategie (Artikel 6 Absatz 9)?	Nein		**28.2**
		6.2	Enthält Ihre IKT-Drittparteienrisiko Strategie, eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereit gestellt werden?	Nein		**28.2**
		6.3	Gilt die Richtlinie auf individueller Basis?	Nein		**28.2**
		6.4	Gilt diese Richtlinie gegebenenfalls auf teilkonsolidierter und konsolidierter Basis?	Nein		**28.2**
		7.1	Überprüft Ihr Vorstand regelmäßig die Bewertung des Gesamtrisikoprofils und des Umfangs und der Komplexität der Unternehmensdienstleistungen die im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ermittelt werden?	Ja		**28.2**
		8.1	Führen und aktualisieren Sie auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleistern bereitgestellten IKT-Dienstleistungen bezieht?	Ja		**28.3**
		9.1	Sind Ihre Verträge mit Drittparteien angemessen dokumentiert, wobei zwischen Vereinbarungen, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken, und solche, die dies nicht tun, unterschieden wird?	Ja		**28.3**
		10.1	Berichten Sie den zuständigen Behörden mindestens einmal jährlich über die Anzahl der neuen IKT-Dienstleistungsvereinbarungen, den Kategorien der IKT-Drittdienstleister, der Art der vertraglichen Vereinbarungen sowie die bereitgestellten IKT-Dienstleistungen und -Funktionen?	Ja		**28.3**
		11.1	Können Sie der zuständigen Behörde auf Anfrage das Informationsregister mit allen relevanten Informationen zur Verfügung stellen?	Nein		**28.3**
		12.1	Können Sie die zuständige Behörde zeitnah über geplante vertragliche Vereinbarungen zur Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen informieren, sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist?	Ja		**28.3**
		13.1	Wenn Sie einen Vertrag über die Nutzung von IKT-Diensten abschließen, beurteilen Sie, ob die vertragliche Vereinbarung auf die Nutzung von IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion bezieht?	Nein		**28.4 a**
		14.1	Prüfen Sie beim Abschluss eines Vertrages über die Nutzung von IKT-Dienstleistungen, ob die aufsichtsrechtlichen Voraussetzungen für die Auftragsvergabe erfüllt sind?	Nein		**28.4 b**
		15.1	Analysieren und bewerten Sie beim Abschluss eines Vertrages über die Nutzung von IKT-Dienstleistungen alle relevanten Risiken im Zusammenhang mit der Vereinbarung, einschließlich der Möglichkeit, dass diese Vereinbarung dazu beitragen kann, das IKT-Konzentrationsrisiko (Artikel 29) zu erhöhen?	Ja		**28.4 c**
		16.1	Führen Sie beim Abschluss eines Vertrages über die Nutzung von IKT-Dienstleistungen eines potenziellen IKT-Drittdienstleisters eine Due-Diligence-Prüfung durch und stellen Sie sicher, dass der IKT-Drittdienstleister geeignet ist?	Ja		**28.4 d**
		17.1	Erkennen und bewerten Sie beim Abschluss eines Vertrages über die Nutzung von IKT-Drittdienstleistungen potenzielle Interessenkonflikte?	Ja		**28.4 e**
		18.1	Haben Sie sichergestellt, dass IKT-Drittdienstleister die angemessenen Standards für Informationssicherheit einhalten?	Ja		**28.5**
		19.1	Berücksichtigen Sie, wenn Ihre Verträge kritische oder wichtige Funktionen betreffen, ob der IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für Informationssicherheitsstandards anwendet?	Nein	N/A wenn Verträge keine kritischen oder wichtigen Funktionen betreffen	**28.5**
		20.1	Bestimmen Sie auf Grundlage des risikobasierten Ansatz in Bezug auf die Ausübung der Zugangs-, Inspektions- und Auditrechte vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche des IKT-Drittdienstleisters?	Nein		**28.6**
		21.1	Wenn die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen werden, technisch komplex ist, haben Sie überprüft, ob die internen oder externen Revisoren über entsprechende Fähigkeiten und Kenntnisse verfügen?	Ja		**28.6**
		22.1	Können Sie IKT-Dienstleistungsverträge kündigen, wenn der IKT-Drittdienstleister einen erheblichen Verstoß gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen begeht?	Ja		**28.7 a**
		23.1	Können Sie IKT-Dienstleistungsverträge kündigen, wenn Ihre Überwachungsaktivitäten des IKT-Drittparteienrisikos aufdecken, dass die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken könnten?	Nein		**28.7 b**
		24.1	Können Sie IKT-Dienstleistungsverträge kündigen, wenn Sie nachweislich Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement insbesondere bei der Art und Weise in der die Verfügbarkeit Authentizität, Sicherheit und Vertraulichkeit von Daten aufdecken?	Ja		**28.7 c**
		25.1	Können Sie IKT-Dienstleistungsverträge kündigen, wenn die Vereinbarung dazu führt, dass Sie nicht mehr effektiv von der zuständigen Behörde beaufsichtigt werden können?	Nein		**28.7 d**
		26.1	Verfügen Sie über Ausstiegsstrategien für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen?	Nein		**28.8**

		26.2	Berücksichtigen diese Ausstiegsstrategien Risiken, die von IKT-Drittdienstleistern entstehen können, darunter insbesondere ein möglicher Fehler des IKT-Drittdienstleisters, eine Verschlechterung der Qualität der IKT-Dienstleistung, jeder Unterbrechung der Geschäftstätigkeit, oder jedes erhebliche Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der jeweiligen IKT-Dienstleistung?	Nein		**28.8**
		27.1	Können Sie vertragliche Vereinbarungen mit IKT-Drittdienstleistern beenden, ohne den Geschäftsbetrieb zu beeinträchtigen?	Ja		**28.8 a**
		28.1	Verfügen Sie über umfassende und dokumentierte Pläne zur Beendigung vertraglicher Vereinbarungen mit externen IKT-Dienstleistern?	Ja		**28.8**
		28.2	Ermöglichen Ihnen diese Pläne, vertragliche Vereinbarungen zu beenden, ohne Einschränkung der Einhaltung regulatorischer Anforderungen?	Ja		**28.8 b**
		28.3	Ermöglichen Ihnen diese Pläne, vertragliche Vereinbarungen zu beenden, ohne Beeinträchtigung der die Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen?	Ja		**28.8 c**
		28.4	Werden diese Exit-Pläne ausreichend getestet und regelmäßig überprüft?	Nein		**28.8**
		29.1	Haben Sie alternative Lösungen und Übergangspläne entwickelt, die es Ihnen ermöglichen, den IKT-Drittdienstleister die vertraglich vereinbarten IKT-Dienstleistungen und relevanten Daten zu entziehen und sicher und vollständig alternativen Anbietern zu übertragen oder wieder in die eigenen Systeme zu überführen?	Ja		**28.8**
		29.2	Verfügen Sie über angemessene Notfallmaßnahmen, um die Fortführung der Geschäftstätigkeit im Falle einer Störung aufrechtzuerhalten?	Ja		**28.8**
Artikel 29	**Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene**	1.1	Berücksichtigen Sie, bei IKT-Drittdienstleistungen die kritische oder wichtige Funktionen unterstützen, ob die IKT-Drittdienstleistung nicht oder nur ohne Weiteres ersetzbar sind?	Ja	N/A wenn IKT-Dienste Dritter keine kritischen oder wichtigen Geschäftsfunktionen unterstützen	**29.1 a**
		2.1	Berücksichtigen Sie, ob Sie bereits eine IKT-Dienstleistungsvereinbarung zur Unterstützung kritischer oder wichtige Funktionen mit demselben IKT-Drittdienstleister/Anbieter haben oder mit eng verbundenen IKT-Drittdienstleistern?	Ja	Konzentrationsrisiko	**29.1 b**
		3.1	Wägen Sie Nutzen und Kosten alternativer Lösungen ab?	Ja		**29.1**
		4.1	Wägen Sie die Vorteile und Risiken ab, wenn Verträge mit IKT-Drittdienstleistern zur Unterstützung kritischer oder wichtiger Funktionen, die Möglichkeit beinhalten, dass der IKT-Drittdienstleister an IKT-Unterauftragnehmer (Subunternehmer) vergibt, insbesondere wenn der IKT-Unterauftragsnehmer in einem Drittland niedergelassen ist?	Ja	N/A wenn die Verträge die Möglichkeit nicht enthalten	**29.2**
		5.1	Berücksichtigen Sie in den Verträgen mit IKT-Drittdienstleistern, die kritische oder wichtige Funktionen unterstützen, die insolvenzrechtlichen Bestimmungen die im Falle einer Insolvenz des IKT-Drittdienstleisters anwendbar wären, sowie jede Einschränkung, die sich im Zusammenhang mit der dringenden Wiederherstellung der Daten des Finanzunternehmens ergeben könnten.	Nein		**29.2**
		6.1	Berücksichtigen Sie bei der Beauftragung eines IKT-Dienstleisters der kritische oder wichtige Funktionen unterstützt mit Sitz in einem Drittland, die Einhaltung der EU-Datenschutzanforderungen und die Durchsetzung dieser Gesetze in diesem Drittland?	N/A	N/A wenn keine IKT-Dienstleisterverträge in einem Drittland abgeschlossen werden	**29.**
		7.1	Wenn IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen an Subunternehmer vergeben werden, berücksichtigen Sie, wie sich die potenziell lange und komplexe Ketten der Unterauftragsvergabe, auf Ihre Fähigkeit auswirken könnte, die vertraglich vereinbarten Funktionen zu überwachen?	Ja		**29**
		8.1	Wenn IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen an Subunternehmer vergeben werden, berücksichtigen Sie, ob die zuständige Behörde Ihre Vereinbarungen wirksam überwachen kann?	Ja		**29**

Artikel 30	**Wesentliche Vertragsbestimmungen**	1.1	Sind in Ihren Verträgen Ihre Rechte und Pflichten und die des IKT-Drittanbieters eindeutig zugewiesen und schriftlich dargelegt?	Ja		**30.1**
		2.1	Sind Ihre Vereinbarungen vollständig im Sinne dieser Verordnung?	Nein		**30.1**
		2.2	Steht dieses Dokument den relevanten Parteien entweder in gedruckter Form oder in einem herunterladbaren, dauerhaften und zugänglichen Format zur Verfügung?	Nein		**30.1**
		3.1	Enthalten Ihre Verträge eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Dienstleister bereitzustellen hat?	Ja		**30.2 a**
		4.1	Ist in Ihren Verträgen angegeben, ob externe IKT-Dienstleister, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, Unteraufträge an IKT-Dienstleistungen vergeben dürfen und welche Bedingungen dafür gelten?	Ja		**30.2 a**
		5.1	Enthalten Ihre Verträge die Regionen und Länder, in denen IKT-Dienstleistungen Dritter erbracht und Daten verarbeitet und gespeichert werden?	Ja		**30.2 b**
		6.1	Erfordern Ihre Verträge, dass dritte IKT-Dienstleister Sie über Änderungen an den Standorten, an denen diese Dienste bereitgestellt werden, vorab informieren?	Nein		**30.2 b**
		7.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten?	Nein		**30.2 c**
		8.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern Regelungen zum Zugriff, zur Wiederherstellung und Rückgabe von Daten im Falle einer Insolvenz, der Auflösung oder Einstellung des Geschäftsbetriebs des Dienstleisters oder einer Vertragsbeendigung?	Ja		**30.2d**
		9.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern Beschreibungen der Dienstleistungsgüte einschließlich Aktualisierungen oder Überarbeitungen?	Ja		**30.2 e**
		10.1	Sehen Ihre Verträge mit IKT-Drittdienstleistern vor, dass diese Sie bei einem IKT-Vorfall helfen, der mit dem für Ihr Unternehmen bereitgestellte IKT-Dienste in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten unterstützen?	Ja		**30.2 f**
		11.1	Sehen Ihre Verträge mit externen IKT-Drittdienstleistern vor, dass diese mit den zuständigen Behörden und Abwicklungsbehörden zusammenarbeiten, einschließlich der von diesen benannten Personen?	Ja		**30.2 g**
		12.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarung, entsprechend den Erwartungen der zuständigen Behörden und Abwicklungsbehörden?	Ja		**30.2 h**
		13.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern Bedingungen, für die Teilnahme an den von den Finanzunternehmen angebotenen Programmen zu Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz?	Ja		**30.2 i**
		14.1	Enthalten Ihre Verträge für IKT-Dienste, die **kritische oder wichtige Funktionen unterstützen**, eine Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen?	Ja		**30.3 a**
		14.2	Enthalten diese Verträge, die **kritische oder wichtige Funktionen unterstützen**, präzise quantitativen und qualitativen Leistungsziele , um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen, wenn eine vereinbarte Dienstleistungsgüte nicht erreicht wird?	Nein		**30.3 a**
		15.1	Enthalten Ihre Verträge für IKT-Dienstleistungen zur Unterstützung **kritischer oder wichtiger Funktionen** Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten?	Ja		**30.3 b**
		16.1	Enthalten Ihre Verträge für IKT-Drittdienste zur Unterstützung **kritischer oder wichtiger Funktionen** Anforderungen an den Dienstanbieter, Notfallpläne umzusetzen und zu testen?	Nein		**30.3 c**
		16.2	Enthalten diese Pläne Sicherheitsmaßnahmen, Tools, Kapazitäten und Richtlinien für IKT-Sicherheit, die es dem IKT-Drittdienstleister ermöglichen, ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen zu bieten?	Nein		**30.3 c**
		17.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern zur Unterstützung **kritischer oder wichtiger** Funktionen Anforderungen an den Drittdienstanbieter, an bedrohungsgesteuerten Penetrationstests (TLPT) teilzunehmen und uneingeschränkt mitzuwirken?	Ja		**30.3 d**
		18.1	Enthalten Ihre Verträge für IKT-Drittdienstleistungen zur Unterstützung **kritischer oder wichtiger Funktionen** das Recht, die Leistung des Dienstanbieters fortlaufend zu überwachen?	Ja		**30.3 e**
		18.2	Erlaubt diese Überwachung Ihnen, einem Dritten oder der zuständigen Behörde, uneingeschränkte Zugangs-, Inspektions- und Auditrechte?	Ja		**30.3.e i**
		18.3	Ermöglicht diese Überwachung Ihnen, einem Dritten oder der zuständigen Behörde, vor Ort Kopien relevanter Unterlagen anzufertigen, wenn diese für den Betrieb des IKT-Drittanbieters von entscheidender Bedeutung sind?	Ja		**30.3.e i**
		19.1	Haben Sie Ihr Recht erklärt, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind?	Ja		**30.3.e ii**
		20.1	Haben Sie vereinbart, dass IKT-Drittdienstleister bei den Vor-Ort-Inspektionen und Audits uneingeschränkt kooperieren müssen, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, Ihrer Organisation oder einem beauftragten Dritten durchgeführt werden?	Nein		**30.3.e iii**
		21.1	Haben Sie die Verpflichtung Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen, vereinbart?	Ja		**30.3.e iV**
		22.1	Enthalten Ihre Verträge mit IKT-Drittdienstleistern zur Unterstützung **kritischer oder wichtiger Funktionen** Ausstiegsstrategien?	Nein		**30.3 f**
		22.2	Sehen diese Ausstiegsstrategien eine verpflichtende Übergangsfrist vor, während derer der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen bzw. der IKT-Dienstleistung bereitstellt?	Nein		**30.3. f i**
		22.3	Gibt Ihnen diese Übergangsphase angemessen Zeit, einen alternativen Dienstleister zu finden oder eine interne Lösung einzuführen?	Nein		**30.3 f**
		23.1	Erwägen Sie bei der Aushandlung vertraglicher Vereinbarungen die Verwendung von Standardvertragsklauseln, die von Behörden für bestimmte Dienstleistungen entwickelt wurden?	Ja		**30.4**

Artikel	Handlungsfeld	Referenz	GAP-Analyse Frage	Antwort	Bemerkung/Dokumentation	DORA Referenz
		0	**Tauschen Sie Cyber-Bedrohungsinformationen und -informationen mit anderen Finanzunternehmen aus? Hierzu können Kompromittierungsindikatoren, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools gehören.**	**Ja**	Freiwillige Anforderung – wenn „Ja“ dann sind die Fragen 1.1 – 7.1 zu beantworten	
Artikel 45	**Vereinbarung über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen**	1.1	Verbessert dieser Informations- und Informationsaustausch die operationale digitale Resilienz Ihres Unternehmens?	Ja		**45.1 a**
		2.1	Findet dieser Informations- und Informationsaustausch innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen statt?	Nein		**45.1.b**
		3.1	Werden diese Informationen und Erkenntnisse durch Vorkehrungen umgesetzt, die den potenziell sensiblen Charakter der weitergegebenen Informationen schützen?	Nein		**45.1.c**
		4.1	Unterliegt dieser Informations- und Erkenntnisaustausch Verhaltensregeln Wahrung der Geschäftsgeheimnisse, des Schutzes personenbezogener Daten und Richtlinien zur Wettbewerbspolitik?	Ja		**45.1.c**
		5.1	Definieren Ihre Vereinbarungen zum Informationsaustausch die Bedingungen für die Teilnahme?	Ja		**45.1c**
		6.1	Erklären die Vereinbarungen zum Informationsaustausch, die sich auf Geschäftsgeheimnisse und Datenschutz beziehen, wann und in welcher Funktion öffentliche Behörden beteiligt werden könnten?	Nein		**45.1 c**
		7.1	Informieren Sie die zuständigen Behörden zu Beginn und am Ende Ihrer Mitgliedschaft über Ihre Teilnahme an Informationsaustauschvereinbarungen?	Ja		**45.3**

Unterschrift verantwortlicher GAP-Analyse: _____

Unterschrift verantwortlicher Vorstand: _____

Versionshistorie

Version	Datum	Dokumentation der Änderung / Neuerung
1.0	01.04.24	DORA GAP-Analyse auf Gesetzestext abgestimmt und visualisierte Elemente integriert
1.1	11.06.24	Tabellenblatt „Institutsstammdaten“ mit parametrisierbarer Verhältnismäßigkeitseinwertung integriert

Lizensiert für VR-Bank Must