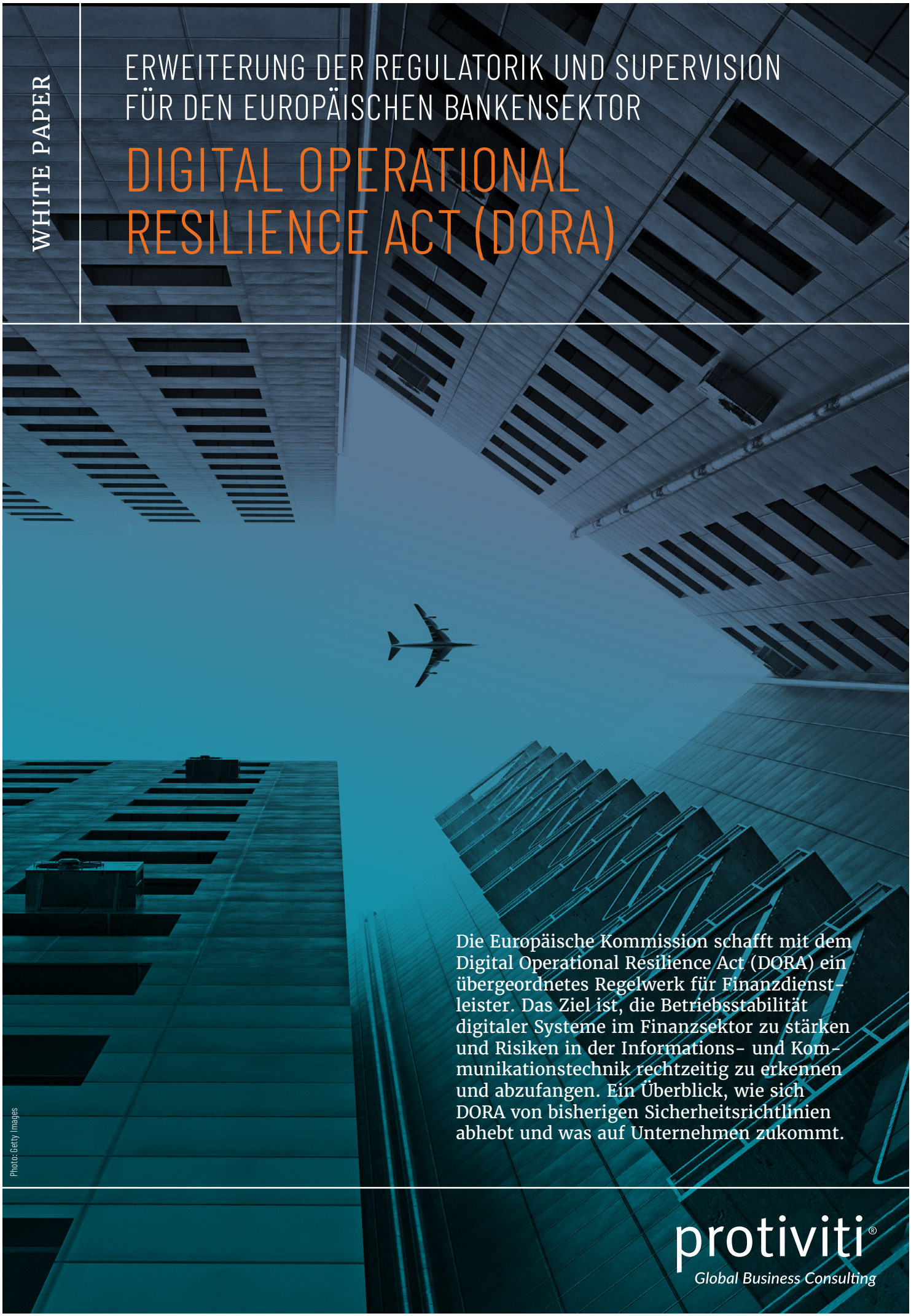
WHITE PAPER

ERWEITERUNG DER REGULATORIK UND SUPERVISION FÜR DEN EUROPÄISCHEN BANKENSEKTOR

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)



Die Europäische Kommission schafft mit dem Digital Operational Resilience Act (DORA) ein übergeordnetes Regelwerk für Finanzdienstleister. Das Ziel ist, die Betriebsstabilität digitaler Systeme im Finanzsektor zu stärken und Risiken in der Informations- und Kommunikationstechnik rechtzeitig zu erkennen und abzufangen. Ein Überblick, wie sich DORA von bisherigen Sicherheitsrichtlinien abhebt und was auf Unternehmen zukommt.

Photo: Getty Images

protiviti®
Global Business Consulting

WHITE PAPER

ERWEITERUNG DER REGULATORIK UND SUPERVISION FÜR DEN EUROPÄISCHEN BANKENSEKTOR

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

INHALTE

EINLEITUNG

Cyberattacken und ihre Folgen sind schon lange keine Randerscheinung mehr und das Ausmaß von potenziellen Cyberbedrohungen nimmt stetig zu. Die jährlichen Schäden für die Weltwirtschaft haben sich allein im Zeitraum von 2015 bis 2020 nahezu verdoppelt und liegen derzeit auf einem Niveau von fast 5,5 Billionen Euro.[1]

Allein in Deutschland belief sich der jährliche wirtschaftliche Schaden für das Jahr 2022 bereits auf 203 Milliarden Euro im Vergleich zum Jahr 2018/19 mit rund 103 Milliarden Euro.[2] Das entspricht einem Anstieg von knapp 100 Prozent. In einer Umfrage der Bitkom (Stand August 2022) gingen rund 42 Prozent der befragten Unternehmen davon aus, dass die auf sie getätigten Cyberangriffe in den nächsten zwölf Monaten stark zunehmen würden.[2]

Die voranschreitende Digitalisierung von Dienstleistungen jeglicher Art sowie die zunehmende Abhängigkeit der Unternehmen von ihrer IT bei ihrer operationalen Geschäftstätigkeit erweitern die potenziellen Angriffsflächen für Cyberattacken. Darüber hinaus haben sich in etlichen Branchenzweigen spezifische IKT-Anwendungen (Informations- und Kommunikationstechnologien) und IKT-Dienstleister durchgesetzt, die den Markt mit ihren Dienstleistungen dominieren. Eine detektierte Sicherheitslücke betrifft somit direkt eine Vielzahl von Unternehmen, welche die betroffenen Dienstleistungen in Anspruch nehmen. Dieses Klumpenrisiko, verbunden mit interdependenten Wertschöpfungsketten, multipliziert im schlimmsten Fall die möglichen Schäden, die mit einer Sicherheitslücke im IKT-System und einer erfolgreichen Cyberattacke einhergehen könnten. Dies trifft besonders auf die Finanzbranche zu, die durch die Pandemie einen weiteren Schub in der Digitalisierung ihrer Geschäftsprozesse erfahren hat und somit auch eine größere Angriffsfläche für mögliche Cyberattacken bietet. Cybersicherheitsrisiken für Finanzunternehmen werden derzeit auf EU-Ebene nicht einheitlich geregelt, sodass das Niveau der Sicherheitsvorkehrungen, die im EU-Raum Cyberattacken gegenüber ergriffen werden, stark divergiert.

Das „Digital Finance Package“ der EU (2020) stellt eine übergeordnete Leitlinie dar, wie die EU die digitale Transformation des Finanzwesens in den kommenden Jahren einheitlicher gestalten möchte. Dies dient dazu, die Wettbewerbsfähigkeit des europäischen Finanzsektors zu stärken und gleichzeitig die damit verbundenen Risiken zu regulieren. Die Strategie beinhaltet – neben der Beseitigung der Fragmentierung des digitalen Binnenmarkts – die Anpassung des EU-Rechtsrahmens, um digitale Innovationen zu erleichtern, sowie die Förderung eines datengesteuerten Finanzwesens. Ziel ist es, die digitale operationale Resilienz und gleichzeitig die Wettbewerbsfähigkeit des europäischen Finanzsystems zu stärken.

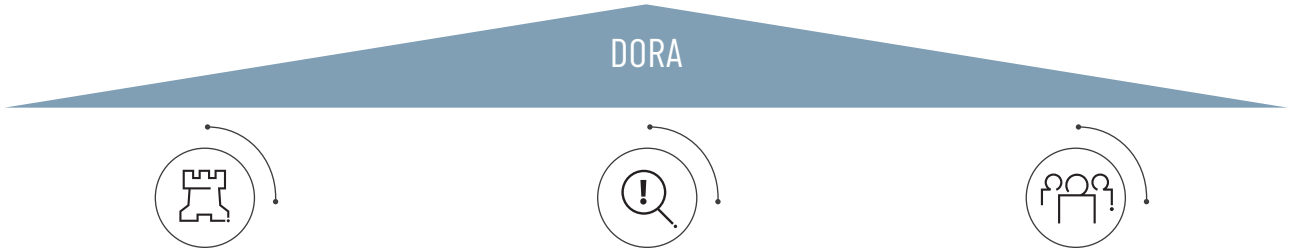
Letzterer Punkt fußt auf der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors, kurz DORA (Digital Operational Resilience Act). Mit DORA intendiert die Europäische Kommission eine Harmonisierung der Rahmenbedingungen der digitalen und betrieblichen Widerstandsfähigkeit von Banken und Dienstleistern (IKT-Drittanbietern) und somit die Etablierung und Konsolidierung eines europäischen Cybersecurity-Standards.

> »Mit DORA und der Vereinheitlichung von Regularien und Berichtspflichten entsteht endlich ein homogenes Bild der Cybersicherheitslage in der EU.«
>
> ANDREJ GREINDL, MANAGING DIRECTOR

[1] Vgl. EU Agency for Cybersecurity (data from July 2021 to July 2022): Infografik „Top Cyber Threats in the EU“. Online verfügbar unter: Top Cyber Threats in the EU - Consilium (europa.eu)

[2] Vgl. Bitkom e. V. (2022): „203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen“. Online verfügbar unter: 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen | Presseinformation | Bitkom e.V.

DORA umfasst dabei thematisch drei Säulen. Zum einen sollen die Finanzunternehmen ein angemessenes Rahmenwerk für IKT-Governance- und & -Risikomanagement etablieren, das potenzielle IKT-Risiken frühzeitig identifiziert und geeignete Wiederherstellungsmaßnahmen vorgibt, um im Falle eines Cyberangriffs die Funktionsfähigkeit des Finanzunternehmens schnellstmöglich wiederherzustellen. Die zweite Säule behandelt die Vereinheitlichung des Meldewesens von kritischen IKT-Vorfällen und gibt vor, welche Mindestangaben im Falle eines Cybersecurity-Incidents an die jeweilige verantwortliche ESA (European Supervisory Authority) verpflichtend gemeldet werden müssen. Darüber hinaus sind Vorgaben für verpflichtende Resilienztests enthalten, mit denen im regelmäßigen Turnus die digitale operationale Resilienz der jeweiligen Finanzinstitute überprüft werden soll. Die dritte Säule enthält Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos für die Finanzinstitute. Dieser Abschnitt nennt die wesentlichen Bestandteile, die ein Vertrag zur Erbringung von IKT-Dienstleistungen beinhalten muss, um das mit der Beanspruchung, aber auch der Entlassung der IKT-Dienstleister einhergehende Risiko adäquat steuern zu können. Zudem soll ein Überwachungsrahmen (Oversight Framework) für als kritisch eingestufte IKT-Dienstleister eingeführt werden, welcher Informations-, Kontroll- und Überprüfungsrechte der ESA diesen gegenüber beinhaltet. Im folgenden Abschnitt werden die drei Säulen von DORA und ihre Vorgaben für die Finanzinstitute sowie die Maßnahmen beschrieben, die seitens der Finanzinstitute ergriffen werden müssen, um die Vorgaben von DORA zu erfüllen. Abschließend erfolgt je Säule ein inhaltlicher Abgleich von Vorgaben der DORA mit bereits bestehenden EU-Regularien wie der MaRisk, dem IT-Sicherheitsgesetz sowie den Inhalten der BAIT, VAIT, KAIT und ZAIT (kurz: xAIT) und welche Handlungsempfehlungen daraus für betroffene Finanzinstitute resultieren, um insbesondere neue Regulierungsvorgaben von DORA in Zukunft erfüllen zu können.



IKT-Governance- & -Risikomanagementrahmen

- Vereinheitlichung von Geschäftsstrategien mit IKT-Risikomanagement durch Schaffung einer verantwortlichen Stelle im Topmanagement
- Kontinuierliche Überwachung und Weiterentwicklung des IKT-Risikomanagements anhand der sich stetig verändernden Cyberrisiken
- Konzipierung von risikobasierten Maßnahmenplänen zur Identifikation, Prävention, Detektion, Reaktion und Regeneration von Cyberbedrohungen

IKT-Vorfallsmeldepflicht und Testen der digitalen operationalen Resilienz

- Einführung einer standardisierten Meldepflicht für kritische IKT-Vorfälle an die Aufsichtsbehörden
- Standardisierung der Klassifizierung von IKT-Vorfällen
- Vorgabe von einzuhaltenden Testkriterien und Inhalten für die Tester durch die ESAs und EZB mittels risikobasierter Testpläne
- Informationsaustausch & Anerkennung von Testergebnissen zwischen den ESAs

IKT-Drittparteienrisikomanagement

- Ausweitung des internen Risikomanagementprozesses von Finanzinstituten auf ihre IKT-Dienstleister
- Definition von Mindestvorgaben zu Vertragsinhalten zwischen dem Finanzinstitut und ihren IKT-Dienstleistern
- Festlegung von kritischen IKT-Dienstleistern durch die ESA, welche dann Informations-, Kontroll- und Überprüfungsrechten der ESA unterliegen

Ziel: Stärkung der Zusammenarbeit zwischen aufsichtsrechtlichen Behörden und Finanzinstituten durch Informations- und Erkenntnisaustausch, um wachsenden IKT-Risiken entgegenzuwirken.

DIE DREI SÄULEN VON DORA

Das primäre Ziel von DORA ist die Harmonisierung von Sicherheitsvorkehrungen für Finanzinstitute gemäß europäischen und nationalen Standards zum Schutz vor Cyberangriffen im gesamten EU-Bereich. Hierfür wurden die folgenden Vorgaben definiert:

SÄULE 1: ANGEMESSENES RAHMENWERK FÜR IKT-GOVERNANCE- & -RISIKOMANAGEMENT

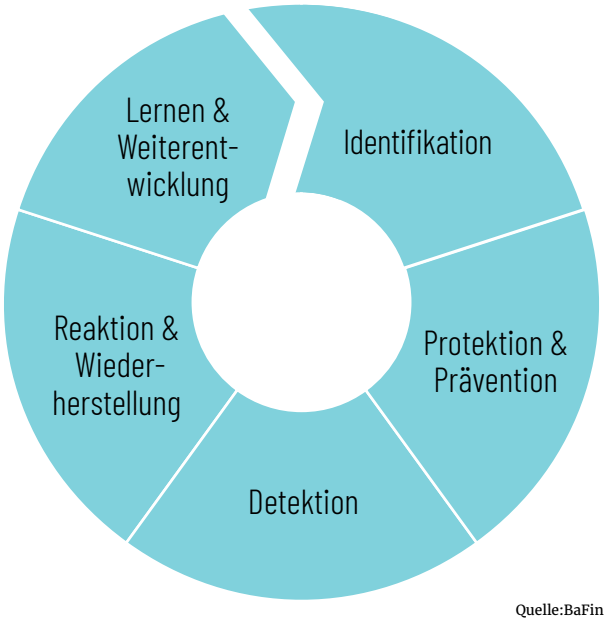
Zukünftig sollen die Geschäftsstrategie und das IKT-Risikomanagement von Finanzunternehmen besser aufeinander abgestimmt sein. Hierfür werden die Leitungsorgane betroffener Unternehmen in die Verantwortung genommen, in der Entwicklung des IKT-Risikomanagements und der Gesamtstrategie für die digitale operationale Resilienz eine zentrale und aktive Rolle einzunehmen. Dazu gehört neben der Steuerung und der Bereitstellung entsprechender Ressourcen auch die Definition, Genehmigung, Überwachung und Rollenzuweisung im Zusammenhang mit dem IKT-Risikomanagement. Die durch das Leitungsorgan definierte Gesamtstrategie ist zunächst in einem übergeordneten Grundsatz festzuhalten, der dann in eine Reihe spezifischer Anforderungen aufzuspalten ist. Inhaltlich soll der Umgang mit unternehmensinternen IKT-Systemen und -Datenbeständen festgelegt werden, inklusive deren kontinuierlicher Überwachung. Es sind Regelungen für den Aufbau und die stetige Weiterentwicklung des IKT-Risikomanagements zu definieren sowie Melde-, Genehmigungs- und Kontrollverfahren festzulegen. Dies inkludiert auch IKT-Reaktions- und -Wiederherstellungspläne. Die erstellte Leitlinie soll auch als Grundlage für die Nutzung von IKT-Dienstleistungen, zur Schulung von IKT-Prozessen inklusive damit verbundener Rollen und Verantwortlichkeiten sowie für die Erstellung von Revisionsplänen herangezogen werden. Letztere müssen dann durch das zuständige Leitungsorgan genehmigt und fortlaufend überprüft werden

Im Rahmen eines IKT-Risikomanagements sollen IKT-Risiken und deren Ursachen zunächst identifiziert und passende Schutz- und Präventionsmaßnahmen definiert werden. Um den Geschäftsbetrieb zu gewährleisten, gilt es, anormale Aktivitäten zeitnah aufzudecken und dedizierte Strategien für die Fortführung des Geschäftsbetriebs und das Notfallmanagement zu entwickeln. Dies gilt nicht nur für die logische IKT-Infrastruktur, sondern auch für die Integrität, Sicherheit und Robustheit physischer Infrastrukturen und Einrichtungen. Das IKT-Risikomanagement soll durch geeignete Überprüfungs- und Überwachungsverfahren stets weiterentwickelt werden, um die digitale Betriebsstabilität auch in einer sich dynamisch ändernden Bedrohungslage zu sichern (siehe auch Abbildung 2). Die Verordnung selbst gibt bei der Umsetzung und Entwicklung eines Risikomanagements keinen Standard vor. Die Komponenten des IKT-Risikomanagements können in bereits etablierte operative Gesamtrisikomanagementsysteme eingegliedert werden.

Vergleich von DORA mit MaRisk, xAIT und dem IT-Sicherheitsgesetz

Für bereits regulierte Unternehmen ergeben sich verglichen mit bestehenden EU-Regularien wie der MaRisk, dem IT-Sicherheitsgesetz 2.0 oder den xAIT-Regelungen in Bezug auf die IKT-Governance und das IKT-Risikomanagement kaum neue Anforderungen aus der DORA. Die Anforderungen sollten bereits in bestehenden Organisationsstrukturen und Gesamtrisikomanagementsystemen etabliert sein. Ein detaillierterer Abgleich der DORA-Verordnung mit den bereits existierenden Regularien im Hinblick auf die Einführung einer angemessenen IKT-Governance und eines IKT-Risikomanagements ist im Anhang aufgeführt.

ELEMENTE DES IKT-RISIKOMANAGEMENTS



Quelle:BaFin

SÄULE 2: HARMONISIERTE IKT-VORFALLS-MELDEPFLICHT UND TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ

Neben der Definition und Einführung eines angemessenen IKT-Risikomanagements auf der Grundlage einheitlicher Vorgaben soll auch die Berichterstattung an die Aufsichtsbehörden mit der Einführung von DORA harmonisiert und vereinheitlicht werden. Zudem sollen regelmäßige Funktionstests sicherstellen, dass das IKT-Risikomanagement und damit einhergehende implementierte Sicherheitsvorkehrungen auch tatsächlich effektiv sind und der Betrieb und die Funktionsweise des Finanzunternehmens stets sichergestellt ist. DORA fordert somit implizit einen auf EU-Ebene harmonisierten Business-Continuity-Management-Standard.

»Viele Inhalte von DORA sind bereits mit bestehenden EU-Regularien abgedeckt. Trotzdem ist DORA nicht zu unterschätzen.«

SEBASTIAN MAYER, MANAGING DIRECTOR

Im Interesse einer einheitlichen Berichterstattung bzw. Vorfallsmeldung sind Finanzunternehmen zukünftig verpflichtet, einen Prozess zur Überwachung und Protokollierung von IKT-bezogenen Vorfällen zu etablieren. Alle protokollierten Vorfälle sind zu klassifizieren und als schwerwiegend geltende IKT-Vorfälle fristgerecht und unverzüglich[3,4] unter der Verwendung einer einheitlichen Formatvorlage an die zuständigen Behörden[5] zu melden. Die Klassifizierung erfolgt anhand festgeschriebener Kriterien wie beispielsweise der Dauer des Vorfalls, der Anzahl betroffener Kunden oder der geografischen Ausbreitung der vom IKT-Vorfall betroffenen Gebiete. Die genauen Kriterien inklusive der Wesentlichkeitskriterien werden durch die ESA in Abstimmung mit der EZB und der ENISA präzisiert und veröffentlicht. Zusätzlich sollen Finanzunternehmen über eine regelmäßige Berichterstattung in Form von Erst-, Folge- und Abschlussberichten auch ihre Kunden*innen oder Nutzer*innen informieren, sofern die Vorfälle Auswirkungen auf deren finanzielle Interessen haben. Sobald die Erstmeldung oder sonstige Meldungen bei den Behörden eingegangen sind, wird dies bestätigt und, wenn möglich, eine Rückmeldung mit sachdienlichen Orientierungshilfen aus ähnlichen Bedrohungslagen anderer, anonymisierter Finanzinstitute gegeben.

Durch die Meldung von schwerwiegenden IKT-Vorfällen wird es für die ESA möglich, jährlich in anonymisierter und aggregierter Form über solche Vorfälle zu berichten. Dadurch können Finanzinstitute von den Erfahrungen anderer Finanzunternehmen profitieren und im besten Fall vorbeugende Sicherheitsmaßnahmen zur Vermeidung ähnlicher Vorfälle etablieren. Zusätzlich gibt die ESA Warnungen heraus und erstellt allgemein gehaltene Statistiken, um die Bewertungen von Bedrohungen und Schwachstellen im IKT-Bereich zu unterstützen.

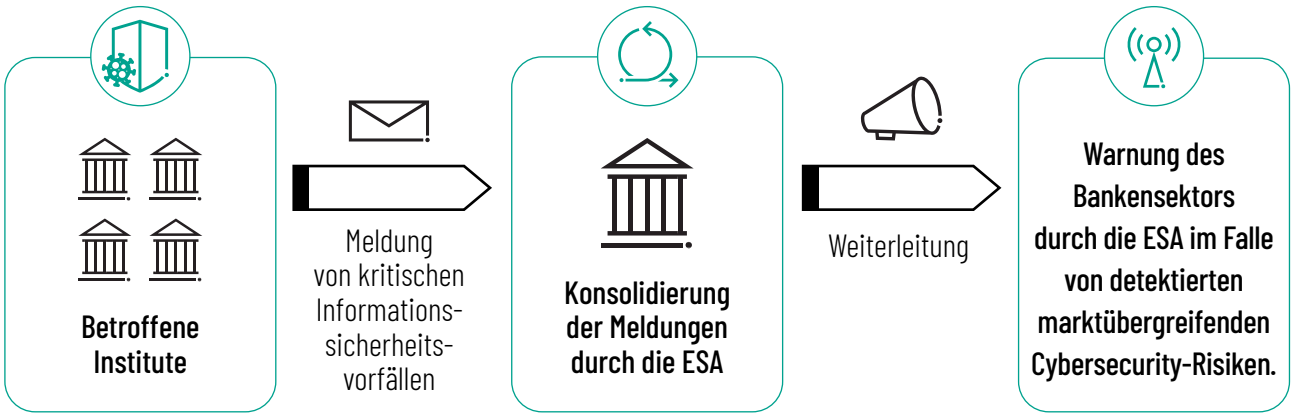
Funktionstest der digitalen operationalen Resilienz

Zur Sicherstellung der Funktionsweise und Angemessenheit des etablierten IKT-Risikomanagements, der IKT-Systeme und zugehöriger Kontrollen sollen einzelne kritische Komponenten regelmäßig – mindestens jährlich – durch angemessene Tests

[3] Art. 19 Abs. 1, S. 3 – gem. VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) Nr. 2016/1011.

[4] Zwar macht DORA hierzu bisher keine konkreten Angaben, zieht man jedoch vergleichbare Rahmenwerke und Gesetze wie bspw. die EU-DSGVO heran, dann gilt bspw. gem. Art. 33 DSGVO: Der Verantwortliche hat im Falle einer Verletzung des Schutzes personenbezogener Daten diesen Vorfall unverzüglich, d. h. möglichst binnen 72 Stunden an die jeweilige Aufsichtsbehörde zu melden, nachdem ihm die Verletzung bekannt wurde […].

[5] Gemäß Art. 19 Abs. 6 EBA, ESMA, EIOPA oder EZB.



überprüft werden. DORA sieht dabei nicht nur das Testen organisatorischer Kontrollen vor, sondern explizit auch das Prüfen technischer Komponenten, zum Beispiel durch Penetrationstests, Open-Source-Tests oder Netzwerksicherheitsbewertungen. Die ESA erarbeitet im Einvernehmen mit der EZB gemeinsame technische Regulierungsstandards[6]. In diesen wird präzisiert, inwieweit Tests durch interne oder externe Tester durchgeführt werden, welcher Umfang und welche Testmethodik für Tests notwendig sind, welche Anforderungen an das Testkonzept und für die einzelnen Testphasen gelten und wie die Behebungsphasen für die Schwachstellen, die potenziell durch den Test identifiziert wurden, zu gestalten sind.

Für die Umsetzung der Anforderungen können Unternehmen einen risikobasierten Testplan etablieren. Hierbei gilt es, verschiedene Bedrohungsszenarien zu simulieren und die Abwehrbereitschaft zu testen. Sofern von Bedrohungsszenarien betroffene Prozesse und Systeme ausgelagert sind, kann es notwendig werden, diese Tests auch bei externen IKT-Dienstleistern durchzuführen. Deren Kooperation in Bezug auf verpflichtende Tests wird künftig erforderlich sein. Dies sollte im besten Fall vertraglich festgehalten sein (siehe hierzu auch Kapitel zu „Ausgereiftes IKT-Risikomanagement für Drittparteien“). Die bei den Tests ermittelten Schwachstellen, Mängel oder Lücken sind umgehend durch Korrekturmaßnahmen zu schließen. Die Testergebnisse sollen protokolliert und an die europäischen Aufsichtsbehörden übermittelt werden.

Zusammenfassend kommen mit der zweiten Säule von DORA neue Anforderungen an die Protokollierung und Meldung von signifikanten IKT-Vorfällen auf betroffene Unternehmen zu. Des Weiteren soll ein festes Rahmenwerk für die Durchführung von Resilienztests deren Qualität erhöhen. Der Austausch von Protokollen zu Testergebnissen soll zudem den Informationsaustausch des Finanzmarktes auf EU-Ebene fördern. Ziel ist es, auf diese Weise zeitnahe und einheitliche Maßnahmen zum Schutz vor Cyberangriffen auf EU-Ebene einführen zu können.

Vergleich von DORA mit MaRisk, xAIT und dem IT-Sicherheitsgesetz

Bestehende EU-Regularien beinhalten bereits Anforderungen an die Berichterstattung über Informationssicherheitsvorfälle und die Durchführung von Stresstests. Mit der Einführung von DORA werden diese nun spezifiziert. Die Berichtsvorgaben und die Verpflichtung zur Durchführung regelmäßiger Stresstests gelten zudem bis dato nur für unternehmensinterne Bereiche. Externe IKT-Dienstleister unterlagen bisher nicht diesen Vorgaben. Mit DORA werden die geltenden Anforderungen nun auch für externe IKT-Dienstleister rechtskräftig. Als Folge der neuen Regelungen zur verpflichtenden IKT-Vorfallsmeldepflicht sollten Finanzunternehmen ihr aktuell implementiertes

[6] Als Orientierungsmaßstab für das Testkonzept zum Testen der digitalen operationalen Resilienz eines Unternehmens dient das europäische Rahmenwerk TIBER-EU (Threat Intelligence Based Ethical Red Teaming). Der Leitfaden gibt vor, wie Behörden, Einrichtungen und Anbieter von Bedrohungsdaten und Red-Teams zusammenarbeiten sollten, um die Cyberresilienz von Einrichtungen durch die Durchführung eines kontrollierten Cyberangriffs zu testen und zu verbessern. Online verfügbar unter:

https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.de.html

https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_220621_IT-Aufsicht_VA_Vortrag_Brueggemann.pdf;jsessionid=1BE6A788B12BC0453A8B-CB557F4AAB9A.1_cid502?__blob=publicationFile&v=2

Meldewesen für Informationssicherheitsvorfälle erweitern, um den Meldepflichten an die Behörden nachzukommen. Des Weiteren sollten die aktuellen unternehmensinternen Vorgaben zur Durchführung und Protokollierung von Stresstests darauf geprüft werden, ob sie dem neuen Rahmenwerk vollständig entsprechen, und ein Prozess zur fristgerechten Meldung der Stresstestergebnisse etabliert werden. Eine detaillierte Gegenüberstellung bereits bestehender Anforderungen für Vorfallsmeldepflichten und an die Durchführung von Tests zur Betriebsstabilität geknüpfter Vorgaben aus der MaRisk, xAIT und dem IT-Sicherheitsgesetz im direkten Vergleich zu DORA ist im Anhang aufgeführt.

»Die Ausweitung von Prüf-, Informations- und Kontrollrechten gegenüber kritischen IKT-Dienstleistern und die Unterstützung der ESA bei deren Überwachung bietet Finanzinstituten eine Chance für mehr Cybersicherheit.«

CHRISTOPHER CHASSÉE, DIRECTOR

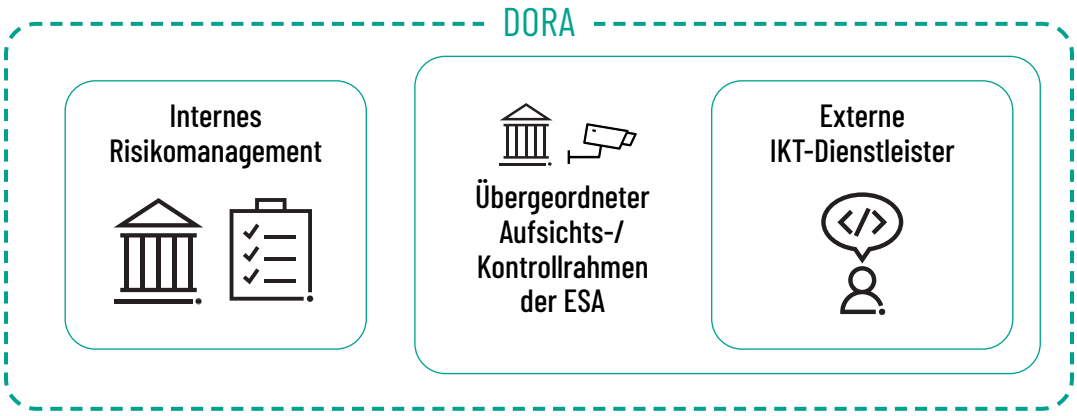
SÄULE 3: AUSGEREIFTES IKT-RISIKOMANAGEMENT FÜR DRITTPARTEIEN

Die dritte Säule des DORA spezifiziert Anforderungen an das IKT-Risikomanagement für Drittparteien. Für einen ausgereiften Schutz vor Cyberangriffen soll das interne Risikomanagement von Finanzinstituten auf ihre IKT-Dienstleister ausgeweitet werden.

Gefordert ist ein Überwachungsprozess, der das ganzheitliche Management von IKT-Risiken, die durch die Auslagerung von Services an Dritte entstehen, möglich macht – während der Vertragsverhandlungen, des Vertragsabschlusses, der Leistungserfüllung und der Nachvertragsphase. Wichtig ist hierbei, dass die Verantwortung für das IKT-Risikomanagement auch bei der Auslagerung von Prozessen an Dienstleister stets bei dem Finanzinstitut verbleiben muss. Um dies standardisiert umsetzen zu können, definiert DORA verpflichtende Mindestvorgaben zu Vertragsinhalten zwischen Finanzinstitut und IKT-Dienstleistern. So müssen Verträge neben einer vollständigen Beschreibung der Leistungen inklusive Leistungszielen auch Angaben zu den Orten enthalten, an denen die Daten verarbeitet werden. Darüber hinaus müssen Berichtspflichten, insbesondere die Gewährleistung des Vertragspartners, bei IKT-Vorfällen Unterstützung zu leisten, sowie eine Exit-Strategie schriftlich in den Dienstleistungsverträgen vereinbart werden. Zukünftig fallen auch IKT-Dienstleister aus dem eigenen Unternehmensverbund, also beispielsweise Tochter- oder Muttergesellschaften betroffener Finanzinstitute, unter diese Regelungen.

DORA soll dafür sorgen, dass kritische IKT-Dienstleister einem durch die ESA verantworteten Aufsichtsrahmen unterworfen werden. Welche IKT-Dienstleister als kritisch eingestuft sind, legt die ESA fest und veröffentlicht jährlich eine entsprechende Liste. Ein neues Überwachungsgremium, bestehend aus den Vorsitzenden der ESA, Exekutivdirektor*innen von europäischen Aufsichtsbehörden und anderen Vertreter*innen, erhält ein weitreichendes Informations-, Kontroll- und Überprüfungsrecht gegenüber diesen kritischen IKT-Dienstleistern. Das Überwachungsgremium bewertet, ob kritische IKT-Dienstleister über fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen zum IKT-Risikomanagement verfügen. Sollten Standards und Vorgaben durch die kritischen IKT-Dienstleister nicht eingehalten werden, kann das Gremium eingreifen und Finanzinstitute als letzte Konsequenz auch auffordern, nicht mehr mit bestimmten Dienstleistern zusammenzuarbeiten.

AUSWEITUNG DES RISIKOMANAGEMENTS AUF EXTERNE IKT-DIENSTLEISTER



Zusammenfassend soll DORA durch die Anforderungen an die Vertragsinhalte zwischen Finanzinstituten und IKT-Dienstleistern sowie die Einführung eines Kontroll- und Überwachungsrahmens für als kritisch definierte IKT-Dienstleister eine ganzheitliche Überwachung von IKT-Dienstleistern auf gesamteuropäischer Ebene fördern.

Vergleich von DORA mit MaRisk, xAIT und dem IT-Sicherheitsgesetz

Bereits in bestehenden EU-Regularien werden Unternehmen verpflichtet, die Auslagerung von IKT-Prozessen oder die Bereitstellung von IKT-Komponenten durch Drittparteien in ihr IKT-Risikomanagement einzubeziehen, Mindestinhalte in Dienstleistungsverträgen aufzunehmen und deren Einhaltung sicherzustellen. Mit DORA werden die Mindestinhalte für die Dienstleistungsverträge erweitert. Die Tatsache, dass zukünftig auch IKT-Dienstleister aus dem eigenen Unternehmensverbund den gleichen Anforderungen wie das regulierte Finanzinstitut unterliegen, erhöht die Reichweite entsprechender Anforderungen an das IKT-Risikomanagement und damit verbundener Prozesse. Neu ist außerdem die Schaffung des Kontrollgremiums für als kritisch festgelegte IKT-Dienstleister. Einen detaillierteren Vergleich finden Sie im Anhang. Als Maßnahme zur Umsetzung der neuen DORA-Regelungen sollten Finanzinstitute daher für ihre bestehenden IKT-Dienstleistungsverträge überprüfen, inwieweit diese die Mindestinhalte gemäß DORA abdecken, und die Verträge ggf. nachschärfen. Mittelfristig haben Finanzinstitute zukünftig die Möglichkeit, bei der Auswahl ihrer IKT-Dienstleister auf die Liste der von der ESA als kritisch klassifizierten Dienstleister zurückzugreifen. Deren Risikomanagement wird durch das Aufsichtsgremium der ESA regelmäßig auf seine Angemessenheit und Wirksamkeit geprüft, was sich wiederum positiv auf die Risikomanagement- und Überwachungspflichten der beauftragenden Finanzinstitute auswirkt.

FAZIT – DORA FÖRDERT DIE ZUSAMMENARBEIT

DORA schafft eine Grundlage, um die Zusammenarbeit zwischen den Finanzinstituten sowie den aufsichtsrechtlichen Behörden und sonstigen vertrauenswürdigen Gemeinschaften innerhalb der Finanzbranche zu fördern. Es wird ein adäquater Austausch entsprechender Informationen unter der Berücksichtigung ihrer Sensibilität ermöglicht.

Zusammenfassend sind die Regelungen und Anforderungen von DORA für regulierte Unternehmen zu einem Großteil bereits in anderen europäischen Regularien enthalten (siehe Anhang). Die größten Veränderungen stellen das erweiterte IKT-Risikomanagement von Drittparteien inklusive der Einführung des Kontrollgremiums dar. Neu sind auch die Vorgaben zu den einheitlichen Klassifizierungen und Protokollierung von IKT-Vorfällen sowie das Rahmenwerk für die Resilienztests inklusive der standardisierten Meldung von Testergebnissen. Es gilt, pro Institut individuell zu betrachten, wie sich DORA im Kontext mit anderen Regularien ausschlägt und welche Maßnahmen ergriffen werden sollten, um die Anforderungen vollumfänglich abzudecken.

Das Gesetz wurde am 11. November 2022 vom EU-Parlament mit großer Mehrheit bestätigt und ist am 16. Januar 2023 in Kraft getreten. Betroffene

Finanzunternehmen haben nun eine Umsetzungsfrist von zwei Jahren, sodass die neuen Regelungen Anfang 2025 abschließend wirksam werden und angemessen in den Unternehmen umgesetzt sein müssen. DORA gilt für alle Unternehmen, die der Aufsicht der ESMA oder EIOPA unterliegen, ebenso für Banken, die bereits die bestehenden EBA-Leitlinien einhalten mussten, und auch für andere Akteure des Finanzsektors, die bisher keiner umfassenden Regulierung zur IKT-Sicherheit unterlagen. Eine genaue Auflistung der Institute und Unternehmen ist in der Verordnung aufgeführt. Hinsichtlich der Anforderungen gibt es zudem Unterscheidungen je nach Größe und Aufbau von Finanzunternehmen.

UNSERE TOP-5-HANDLUNGSEMPFEHLUNGEN

Abschließend möchten wir Ihnen unsere Top 5 der Handlungsempfehlungen darstellen, die Ihrem Unternehmen einen Rahmen für die Umsetzung der DORA-Anforderungen geben können:

1. Durchführung eines DORA-Gap-Assessments

Wir empfehlen Unternehmen, zunächst ein Gap-Assessment auf der Grundlage der DORA-Anforderungen durchzuführen. Wesentliche Aspekte des DORA-Gap-Assessments umfassen dabei die drei vorgestellten Domänen von DORA (IKT-Governance- & -Risikomanagementrahmen, IKT-Vorfallsmeldepflicht und Testen der digitalen operationalen Resilienz sowie IKT-Risikomanagement für Drittparteien). Unternehmen, die bereits reguliert sind, können sich hierbei auf die Neuerungen konzentrieren, die mit DORA aus einer IKT-Compliance-Perspektive eingeführt wurden. Ziel des DORA-Gap-Assessments ist die Identifizierung von Gaps, die Priorisierung der identifizierten Gaps sowie die Ableitung von Maßnahmen zu deren Behebung.

2. Ableitung einer DORA-Roadmap

Basierend auf den Ergebnissen des DORA-Gap-Assessments ist in einem zweiten Schritt eine Roadmap abzuleiten. Diese soll auf den im Gap-Assessment

ermittelten Prioritäten basieren. Unternehmen sollten insbesondere sicherstellen, dass der Zeitplan mit den in der DORA-Verordnung festgelegten Fristen übereinstimmt und dass Zuständigkeiten den verantwortlichen Personen bzw. Funktionen innerhalb der Organisation klar zugewiesen werden.

3. Umsetzung benötigter Veränderungen

Zu den Änderungen, die erforderlich sind, um die DORA-Verordnung zu erfüllen, können u. a. die Verbesserung von Prozessen und Kontrollen für die betriebliche Widerstandsfähigkeit, die Aktualisierung der Reaktionspläne für Cybervorfälle und die Einführung geeigneter Governance- und Überwachungsregelungen gehören. So müssen Unternehmen beispielsweise robuste Cybersicherheitsmaßnahmen einführen, ihr Risikomanagement für Dritte verbessern und sicherstellen, dass sie über wirksame Verfahren zur Datensicherung und -wiederherstellung verfügen.

4. Test und Validierung

Unternehmen sollten anschließend szenariobasierte Tests durchführen, um die Wirksamkeit ihrer Verbesserungen zu validieren. Diese Tests sollten unterschiedlichste Szenarien abdecken, darunter Cyberangriffe, Systemausfälle und andere Betriebsunterbrechungen. Die Tests sollten so konzipiert sein, dass sie etwaige Schwachstellen in Notfall- und/oder Reaktionsplänen aufdecken.

5. Kontinuierliche Verbesserung

Unternehmen sollten abschließend einen Prozess zur kontinuierlichen Verbesserung einführen, sodass Prozesse und Kontrollen zur Gewährleistung der operationellen Resilienz laufend überwacht, überprüft und verbessert werden. Nur so ist sichergestellt, dass operationelle und digitale Risiken fortlaufend wirksam adressiert werden. Dazu gehört die Überprüfung und Aktualisierung von Notfallplänen sowie von Governance- und Aufsichtsregelungen auf der Grundlage der Ergebnisse szenariobasierter Tests. Hierbei sollten insbesondere Änderungen der Bedrohungslandschaft oder des Risikoprofils des Unternehmens berücksichtigt werden. Darüber hinaus ist fortlaufend zu überprüfen, dass alle bedeutenden (Sicherheits-)Vorfälle gemäß den Anforderungen der DORA-Verordnung an die nationalen Aufsichtsbehörden gemeldet werden.

KONTAKTIEREN SIE UNS!

CHRISTOPHER CHASSÉE
Director
+49 172 621 73 01
christopher.chassee@protiviti.de

SEBASTIAN MAYER
Managing Director
+49 162 276 58 55
sebastian.mayer@protiviti.de

ANDREJ GREINDL
Managing Director
+49 172 698 30 53
andrej.greindl@protiviti.de

www.protiviti.de

© 2024 PROTIVITI GMBH

ANHANG: DORA IM VERGLEICH MIT BISHERIGEN REGULARIEN

	DORA	MaRisk	xAIT	IT-Sicherheitsgesetz
SÄULE 1 IKT-Governance- & - Risikomanagementrahmen	Die Geschäftsführung soll eine aktive und zentrale Rolle für das IKT-Risikomanagement übernehmen. Es ist neben der Bereitstellung von Mitteln und Ressourcen eine übergeordnete Leitlinie zu schaffen, die in spezifische Unternehmensbereiche heruntergebrochen wird. IKT-Risiken sollen sich hierbei nicht nur auf logische Infrastrukturelemente beziehen, sondern auch physische Aspekte beinhalten.	Die Geschäftsführung ist verantwortlich für die ordnungsgemäße Geschäftsorganisation und ein wirksames Risikomanagement (vgl. AT 3). Die Geschäftsführung hat sicherzustellen, dass die Geschäftsaktivitäten auf der Grundlage von Organisationsrichtlinien betrieben werden, die schriftlich fixiert sind, den betreffenden Mitarbeitenden in geeigneter Weise bekannt gemacht werden und die u. a. Inhalte wie die Regelungen hinsichtlich der Ausgestaltung der Risikosteuerungsprozesse enthalten (vgl. AT 5). Für IT-Risiken sind angemessene Steuerungs- und Überwachungsprozesse einzurichten (vgl. AT 7.2. TZ 2).	Das Institut hat die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen (vgl. BAIT Tz. 3.1). Zur Steuerung des IT-Betriebs sind durch die Geschäftsführung angemessene qualitative und quantitative Kriterien festzulegen und Ressourcen bereitzustellen (vgl. BAIT Tz. 2.5 und Tz. 8.1 ff.). Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und innerhalb des Instituts zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien des Instituts zu stehen und ist bei wesentlichen Veränderungen der Rahmenbedingungen zu überprüfen und bei Bedarf zeitnah anzupassen (vgl. BAIT Tz. 4.2).	Betreiber kritischer Infrastrukturen sind verpflichtet, […] angemessene Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind (vgl. BSIG § 8a & § 8c Abs. 1-2). Es gilt, organisatorische und technische Sicherheitsvorkehrungen zu treffen – dies umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen […] (vgl. BSIG § 8a Abs. 1a).

ANHANG: DORA IM VERGLEICH MIT BISHERIGEN REGULARIEN

	DORA	MaRisk	xAIT	IT-Sicherheitsgesetz
SÄULE 2 IKT-Vorfallsmeldepflicht & Testen der operationalen Resilienz	Verpflichtung der Finanzunternehmen, einen Prozess zur Überwachung, Klassifizierung und Meldung von IKT-Vorfällen an die Behörden und an ihre Kunden und Nutzer zu etablieren. Die Klassifizierung der Vorfälle soll anhand festgeschriebener Komponenten erfolgen. Verpflichtung der Finanzunternehmen zur Durchführung regelmäßiger Resilienztests, die die Angemessenheit der Ausgestaltung des IKT-Risikomanagements und Kontrollrahmens sicherstellen. Die Tests sind unter Einhaltung der Vorgaben der ESA durchzuführen und Ergebnisse an die europäischen Aufsichtsbehörden zu übermitteln.	Die Geschäftsleitung ist mindestens jährlich über bedeutende Schadensfälle aus operationellen Risiken zu unterrichten (vgl. BT 3.2. Tz. 6). Für wesentliche Risiken des Unternehmens sind regelmäßige Stresstests durchzuführen (vgl. AT 4.5 Tz. 5). Die Ergebnisse der Stresstests sind kritisch zu reflektieren. Dabei ist zu ergründen, ob ein Handlungsbedarf besteht (vgl. AT 4.3.3 Tz. 6). Die Geschäftsleitung hat sich regelmäßig über die Risikosituation berichten zu lassen. In den Risikoberichten sind insbesondere auch die Ergebnisse der Stresstests und deren potenzielle Auswirkung auf die Risikosituation aufzuführen (vgl. BT 3.1 Tz. 1.2).	Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zeitnah zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen (vgl. BAIT Tz. 4.7, VAIT Tz. 4.4). Die Sicherheit der IT-Systeme ist regelmäßig und anlassbezogen zu überprüfen (vgl. BAIT Tz. 5.6). Die Wirksamkeit der IT-Notfallpläne ist durch mindestens jährliche IT-Notfalltests zu überprüfen. Die Tests müssen IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, vollständig abdecken (vgl. BAIT Tz. 10.4). Der oder die Informationssicherheitsbeauftragte hat der Geschäftsleitung mindestens vierteljährlich und ggf. ad hoc über den Status der Informationssicherheit zu berichten (vgl. VAIT Tz. 4.10). Die inhaltlichen Berichtspflichten des oder der Informationssicherheitsbeauftragten an die Geschäftsführung orientieren sich an BT 3.2. Tz. 1 der MaRisk.	Das BSI fungiert als zentrale Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der IT (vgl. BSIG § 8b Abs. 1). Die Betreiber kritischer Infrastrukturen haben dem BSI eine Kontaktstelle für die Kommunikationsstrukturen [...] zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das BSI erfolgt an diese benannte Kontaktstelle (vgl. BSIG § 8b Abs. 3). Störungen sind von der jeweiligen Kontaktstelle unverzüglich an das BSI zu melden (vgl. BSIG § 8b Abs. 4). Anbieter digitaler Dienstleistungen müssen diese vor etwaigen Cyberrisiken schützen. Dies beinhaltet die Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen und die Umsetzung und Testung getroffener Sicherheitsvorkehrungen unter der Wahrung internationaler Normen (vgl. BSIG § 8c Abs. 2).

ANHANG: DORA IM VERGLEICH MIT BISHERIGEN REGULARIEN

	DORA	MaRisk	xAIT	IT-Sicherheitsgesetz
SÄULE 3 IKT-Drittparteien-risikomanagement	Ausweitung der internen Risikomanage-mentprozesse von Finanzinstituten auf ihre IKT-Dienstleister. Definition von Mindestvorgaben zu Vertrags-inhalten zwischen dem Finanzinstitut und ihren IKT-Dienstleistern, die eine konti-nuierliche Überwachung der Dienstleister möglich machen. Ausweitung der Regulatorik auf IKT-Dienst-leister aus dem eigenen Unternehmensver-bund des Finanzinstitutes. Festlegung von kritischen IKT-Dienstleistern durch die ESA, welche dann Informations-, Kontroll- und Überprüfungs-rechten der ESA unterliegen.	Risiken sind auf Ebene des gesamten Instituts zu erfassen, unabhängig davon, in welcher Organisationseinheit die Risiken verursacht werden (vgl. AT 2.2 Tz. 1). Das Unternehmen muss anhand einer Risiko-analyse bewerten, welche Risiken mit einer Auslagerung verbunden sind (vgl. AT 9 Tz. 2). Mindestvorgaben für Vertragsinhalte zwischen Finanzinstituten und Auslagerungs-unternehmen (vgl. AT 9 Tz. 7). Das Institut hat die mit der Auslagerung verbundenen Risiken angemessen zu steuern und die Ausführung der ausgelagerten Aktivitäten ordnungsgemäß zu überwachen (vgl. AT 9 Tz. 9).	Die Auslagerung von IT-Dienstleistungen haben den Anforderungen nach MaRisk AT 9 zu entsprechen (vgl. BAIT Tz. 9.1, VAIT Tz. 9.1). Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden Fremd-bezug von IT-Dienstleistungen vorab eine Risikoanalyse durchzuführen (vgl. Tz. 9.2). Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen (AT 9 Tz. 11 - Risikoanalyse gem. AT9 Tz.2).	Das BSI kann zur Erfüllung seiner Aufgaben [...] auf dem Markt bereitgestellte infor-mationstechnische Produkte und Systeme untersuchen (vgl. BSIG § 7a Abs. 1) und bei Bedarf technische Details vom Anbieter verlangen (vgl. BSIG § 7a Abs. 2). Das BSI darf Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder anderen Angriffsmethoden zu erheben und auszuwerten. Das BSI darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten (vgl. BSIG § 7b Abs. 4).