Umsetzung in der Bank DORA

Der **D**igital **O**perational **R**esilience **A**ct **(DORA)** ist ab dem 17. Januar 2025 verbindlich anzuwenden. Allerdings sind noch viele Fragen offen: Für wen gilt DORA? Wie sind die BAIT hinsichtlich DORA zu berücksichtigen? Und vor allem: Wie sieht die praktische Umsetzung aus? Mit welchem Aufwand ist zu rechnen und welche Sanktionen drohen bei Nicht-Einhaltung?

Die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) ist als Antwort auf den digitalen Wandel und die zunehmende Gefahr von Cyberbedrohungen im Finanzsektor zu verstehen. Sie setzt ihren Fokus auf einen angemessenen Umgang mit der zunehmenden Abhängigkeit des Finanzsektors von Drittanbietern. Die Finanzsysteme der Europäischen Union sollen in die Lage versetzt sein, die Betriebsstabilität im Falle einer schwerwiegenden Störung aufrechtzuerhalten.

Entsprechend ist der Geltungsbereich von DORA geregelt. Es fallen nicht nur die typischen Finanzunternehmen unter die EU-Verordnung, sondern auch Dienstleister, die Informations- und Kommunikationstechnologie-Dienstleistungen (IKT) Unternehmen im Finanzsektor anbieten und durchführen (Art. 2 Abs. 1 lit. u DORA).

DORA stellt eine EU-Verordnung dar und ist gemäß der anzuwendenden Normenhierarchie höherrangig als Gesetzgebungen und Verordnungen auf nationaler Ebene. Insofern sind beispielsweise die nationalen Gesetze wie das KWG, ZAG, KAGB und VAG sowie diverse Verwaltungsanweisungen, wie z. B. MaRisk, BAIT, VAIT, KAIT und ZAIT, der DORA untergeordnet.

Im Folgenden setzen wir den Schwerpunkt auf die bankspezifische Sichtweise.

Mit der Einführung einer EU-Verordnung müssen die nationalen Gesetze mit dem höherrangigen internationalen Recht harmonisiert werden. Nationale Regelungen können über die Öffnungsklauseln das internationale Recht nur ergänzen oder erweitern – nicht aber einschränken. So werden beispielsweise die BAIT in Teilen angepasst werden müssen. So sehen die BAIT noch eine Beschränkung der Auslagerungsfähigkeit des Informationssicherheitsbeauftragten vor (BAIT Tz. 4.6). Diese Beschränkung ist mit Anwendung von DORA (Art. 6 Abs. 10 DORA) in der bisherigen Form jedoch nicht mehr anwendbar. Insofern ist eine allgemeine Überprüfung bzw. Überarbeitung der BAIT vorgesehen.[1]

Dessen ungeachtet stellen jedoch die BAIT in der Fassung vom 16. August 2021 ein gutes Fundament zur Umsetzung von DORA dar.

In der Praxis ergeben sich folgende Umsetzungsschritte:

- Durchführung als Projekt und Aufwandsschätzung
- Durchführung einer Gap Analyse
- Beseitigung der Gaps gemäß der Gap-Analyse
- Beendigung des Projektes und Überführung in den Regelkreislauf

Durchführung als Projekt und Aufwandsschätzung

Die Umsetzung von DORA sollte als Projekt in der Bank erfolgen. Wir empfehlen, folgende Punkte zu klären:

- Aufwandsabschätzung (eigener Personalaufwand, Schulungs- und Fortbildungskosten für die Mitarbeiterinnen und Mitarbeiter, ggf. Beratungsunterstützung weiterer Dienstleister)
- Festlegung des Projektziels
- Festlegung des Projektanfangs und -endes sowie der Meilensteine, der Projektleitung und der einzelnen Verantwortlichkeiten
- Ermittlung des möglichen Mehraufwands zur nachhaltigen Anwendung von DORA im Regelkreislauf

Der Aufwand zur Umsetzung der vier unten genannten Handlungsfelder kann bankindividuell ausfallen. Hierbei spielt u. a. auch die Heterogenität der IT-Landschaft, der Umfang selbst betriebener und ausgelagerter IT-Systeme eine Rolle.

Durchführung einer Gap-Analyse

Die Gap-Analyse bzw. Analyse der strategischen Lücke ist ein wichtiger Schritt, um den Ist-Zustand Ihrer Bank zu ermitteln. Die konkreten Handlungsempfehlungen zeigen Ihnen, welche operativen Maßnahmen Sie ergreifen müssen, um diese Lücken zu schließen. Hierzu empfehlen wir u. a. die Hilfstabelle des BVR zu nutzen.[2]

Die Gap-Analyse erstreckt sich auf vier Handlungsfelder:

1. IKT-Risikomanagement
2. Management IKT-bezogene Vorfälle
3. Testen der digitalen operationalen Resilienz
4. IKT-Drittparteien-Risikomanagement

Beseitigung der Gaps gemäß der Gap-Analyse

Nach der Durchführung der Gap-Analyse ergeben sich konkrete Handlungsbedarfe, die in der Bank umgesetzt werden müssen.

1. Monitoring: IKT-Risikomanagement (Kapitel 2, Art. 5–16 DORA)

Um IKT-Risiken schnell, effizient und umfassend zu erkennen und ein hohes Maß an digitaler Widerstandsfähigkeit zu gewährleisten, fordert DORA nach Kapitel 2, Art. 6 einen soliden, umfassenden und gut dokumentierten Rahmen für das IKT-Risikomanagement.

Dieser Rahmen umfasst u. a. folgende Punkte:

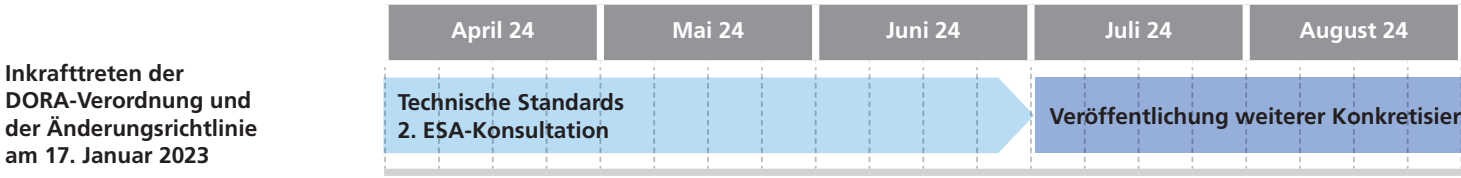
- Ergänzung der IT-Strategie durch eine DORA-Strategie
- Überprüfung und Anpassung des Governance- und Kontrollrahmens (Einrichtung einer IKT-Risikokontrollfunktion) inkl. des Berichtswesens
- Durchführung der erforderlichen Anpassungen im Informationsverbund
- Identifizierung und Klassifizierung der IKT-Systeme und IKT-Dienstleister nach dem neuen Begriff „kritische oder wichtige Funktion“ sowie nach den Abhängigkeiten und Risiken
- Anpassung der Sicherheitsmaßnahmen (z. B. System-, Netzwerk- und Datensicherheit, Schwachstellen- und Patchmanagement, IKT-Änderungsmanagement)
- Überarbeitung des bisherigen Notfallmanagements
- Überprüfung und Anpassung der schriftlich fixierten Ordnung (interne Arbeitsanweisungen)
- Einführung von nachhaltigen Schulungsprogrammen (z. B. Awareness-Maßnahmen)

2. Management IKT-bezogener Vorfälle (Kapitel 3, Art. 17–23 DORA)

Das Management von IKT-bezogenen Vorfällen bezieht sich auf die proaktive Planung, Organisation und Koordination von Maßnahmen zur Reaktion auf und Bewältigung von Vorfällen. Dies umfasst die Erkennung, Bewertung, Eindämmung und Wiederherstellung nach Vorfällen wie Cyberangriffen, Datenlecks, Systemausfällen oder anderen Sicherheitsverletzungen. Das Ziel ist es, die Auswirkungen zu minimieren, die Geschäftskontinuität aufrechtzuerhalten und die Sicherheit der digitalen Infrastruktur zu gewährleisten. Dies beinhaltet auch die Dokumentation von Vorfällen, um aus ihnen zu lernen und zukünftige Sicherheitsmaßnahmen zu verbessern.

Dieser Rahmen umfasst u. a. folgende Punkte:

- Klassifizierung aller IKT-bezogenen Vorfälle und Anpassung des damit verbundenen Meldewesens/ der Meldeverpflichtungen



- Anwendung von Lernprozessen aus IKT-bezogenen Vorfällen und Kommunikationspläne
- Freiwilliger Informationsaustausch zwischen Finanzunternehmen für bessere Sicherheits- und Abwehrmaßnahmen

3. Testen der digitalen operationalen Resilienz (Kapitel 4, Art. 24–27 DORA)

Das Testen der digitalen operationalen Resilienz bezieht sich darauf, wie gut die Bank auf digitale Bedrohungen und Herausforderungen vorbereitet ist und wie effektiv hier reagiert werden kann. Dabei werden verschiedene Aspekte der digitalen Infrastruktur und Sicherheitsmaßnahmen überprüft, um die Widerstandskraft gegen Cyberangriffe, Datenverlust und weitere digitale Risiken zu bewerten. Das Testen der digitalen operationalen Resilienz hilft dabei, Schwachstellen zu identifizieren und Maßnahmen zur Stärkung der Sicherheit und des Schutzes digitaler Ressourcen zu entwickeln.

Dabei können auch Lösungen Dritter in die Tests einbezogen werden.

DORA – Position und Unterstützungsangebot der DZ CompliancePartner GmbH

1. Wir werden die IKT-Risikokontrollfunktion (Art. 6 Abs. 4 DORA) als Auslagerungsdienstleistung anbieten (Art. 6 Abs. 10 DORA):
   – präferiert in Form der Weiterentwicklung der heutigen Funktion des/r Informationssicherheitsbeauftragten (ISB)
   – oder alternativ als ergänzende Funktion.
2. Wir setzen uns in den Gremien der Genossenschaftlichen FinanzGruppe für die Weiterentwicklungslösung des/r ISB ein.
3. Wir unterstützen unsere Kunden in der Implementierung von DORA durch Umsetzungsprojekte mit Augenmaß. Dabei werden wir die Auslagerungskunden in der Informationssicherheit priorisieren.

4. IKT-Drittparteien-Risikomanagement (Kapitel 5, Abschnitt 1, Art. 28–30 DORA)

Das IKT-Drittparteienrisiko bezieht sich auf die Gefahr, die von externen Parteien ausgeht. Dazu gehören Risiken wie Datenlecks, Cyberangriffe oder Sicherheitslücken, die durch Drittanbieter von Software, Dienstleistungen oder Infrastruktur verursacht werden.

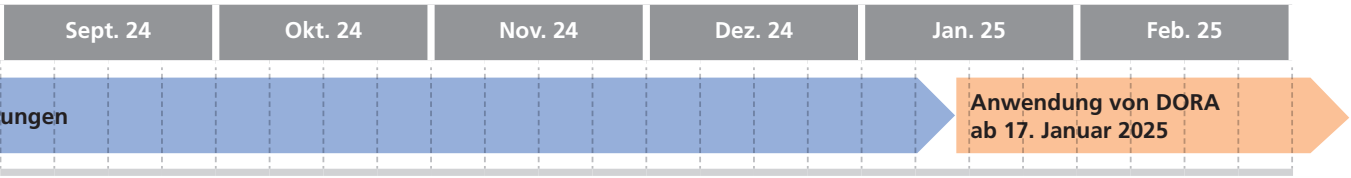
Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Systemen. Durch angemessene Risikominderung und -kontrolle kann sichergestellt werden, dass externe Anbieter keine unangemessenen Risiken für Ihre IKT-Infrastruktur darstellen und die Kontinuität Ihrer Geschäftsprozesse gewährleistet bleibt.

Unter anderem werden folgende Punkte vorgesehen:

- Implementierung eines Prozesses für den Einsatz von IKT-Dienstleistern
- Implementierung eines Prozesses zur Ermittlung und Überprüfung der entsprechenden Risiken
- Anpassung der Verträge mit IKT-Drittparteien auf DORA-Konformität inkl. Aufnahme einer Exit-Strategie
- Sicherstellung der DORA-Anforderungen durch das Auslagerungsmanagement
- Identifikation und Dokumentation des IKT-Drittparteienrisikos durch Ausübung der Zugangs-, Inspektions- und Auditrechte
- Erstellung eines Informationsregisters, welches die vollständige Übersicht aller in der Bank enthaltenen IKT-Dienstleistungen beinhaltet etc.

Beendigung des Projektes und Überführung in den Regelkreislauf

Nach erfolgter DORA-Umsetzung empfehlen wir, den Projektabschluss zu dokumentieren und in den Regelkreislauf überzugehen. Hierbei ist z. B. die Planung von IKS-Aufgaben vorzunehmen, damit die Aktualität der Governance und des Kontrollrahmens, der Durchführung der erforderlichen IKT-Notfallübungen etc. nachhaltig sichergestellt ist.



Sanktionen

Können Sanktionen bei Nicht-Einhaltung von DORA drohen? Die Umsetzung und Anwendung von DORA kann gem. Art. 50 DORA durch die zuständige Aufsicht kontrolliert werden. Auch Sanktionen können gem. Art. 50 Abs. 1 DORA verhängt werden. Dabei werden Kriterien zum Sanktionsumfang gem. Art. 51 Abs. 2 DORA entsprechend berücksichtigt (z. B. Wesentlichkeit, Schwere und Dauer des Verstoßes, Finanzkraft der verantwortlichen natürlichen oder juristischen Person).

Hinsichtlich der Umsetzungsphase werden weitere technische Regulierungs- und Implementierungsstandards (Regulatory Technical Standards – RTS und Implementing Technical Standards – ITS) im Laufe des Jahres 2024 veröffentlicht.[3]

Einige Entwürfe zu den technischen Regulierungs- und Implementierungsstandards liegen bereits vor. Einige weitere werden noch veröffentlicht.

Dennoch ist es ratsam, die Veröffentlichung nicht abzuwarten, sondern zeitnah mit der Umsetzung zu beginnen, da Umfang und Komplexität nicht unterschätzt werden sollten. ▬

Weiterführende Infos zu DORA und unserem Leitfaden für Banken: https://www.dz-cp.de/informationssicherheit/dora

Katja Schlüter
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: katja.schlueter@dz-cp.de

Benjamin Wellnitz
Bereichsleiter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

[1] https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait-dora-598580 (abgerufen am 09.04.2024)

[2] BVR-Rundschreiben „Umsetzung der EU-Verordnung ‚Digitale operationale Resilienz im Finanzsektor (DORA)': Handlungsempfehlungen und Unterstützungsleistungen für 2024" vom 08.01.2024

[3] https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (abgerufen am 09.04.2024)