HADRIAN

Die Kurzanleitung zur Vorbereitung auf den Digital Operational Resilience Act

Was ist der Digital Operational Resilience Act?

Der Digital Operational Resilience Act (DORA), der am 16. Januar 2023 offiziell in Kraft trat, markiert einen entscheidenden Moment in der Cybersicherheit und Finanzregulierung. DORA hat sich zum Ziel gesetzt, die Risikoprotokolle im gesamten Spektrum der Informations- und Kommunikationstechnologie (IKT) in der Finanzwelt der Europäischen Union zu verbessern und zu vereinheitlichen. Das Hauptaugenmerk liegt dabei auf der Vereinheitlichung und Stärkung des Rahmens für die digitale operative Widerstandsfähigkeit.

Die DORA legt einheitliche Kriterien für die Sicherung von Netzwerken und Informationssystemen von Unternehmen und Einrichtungen des Finanzsektors sowie von wichtigen Drittanbietern fest, die IKT-bezogene Dienstleistungen wie Cloud-Plattformen oder Datenanalysedienste anbieten. Sie schafft eine Regulierungsstruktur, die sich auf die digitale betriebliche Widerstandsfähigkeit konzentriert und verlangt, dass alle Unternehmen ihre Fähigkeit sicherstellen, verschiedenen Störungen und Bedrohungen im Zusammenhang mit IKT standzuhalten, darauf zu reagieren und sich davon zu erholen. Diese Anforderungen sind in allen Mitgliedsstaaten der Europäischen Union standardisiert, wobei das Hauptziel die Prävention und Abschwächung von Cyber-Bedrohungen ist.

Die schnelle Antwort

Wie können sich Führungskräfte im Bereich Sicherheits- und Risikomanagement (SRM) auf die digitalen Operationen der EU vorbereiten?

- Bestimmen Sie, ob Ihre Organisation die Anforderungen von DORA erfüllen muss
- Erster Schwerpunkt auf IKT-Risikomanagement, Drittparteirisiko, Informationsaustausch, Meldung von Zwischenfällen und Prüfung der betrieblichen Widerstandsfähigkeit
- Entwicklung eines umfassenden Plans zur Schließung von Compliance-Lücken

Erhöhte Sicherheitspraktiken

Die breite Anwendbarkeit von DORA führt zu Anfragen von Unternehmen sowohl innerhalb als auch außerhalb der EU. Die von DORA geforderte Ausfallsicherheit erstreckt sich auf verschiedene Abteilungen und Führungspositionen, einschließlich des Chief Information Security Officer (CISO), des Chief Information Officer (CIO) und des Enterprise Risk Teams. Faktoren wie Recovery Point Objectives (RPO) und Recovery Time Objectives (RTO) für Service Level Agreements (SLAs) rücken in den Fokus.

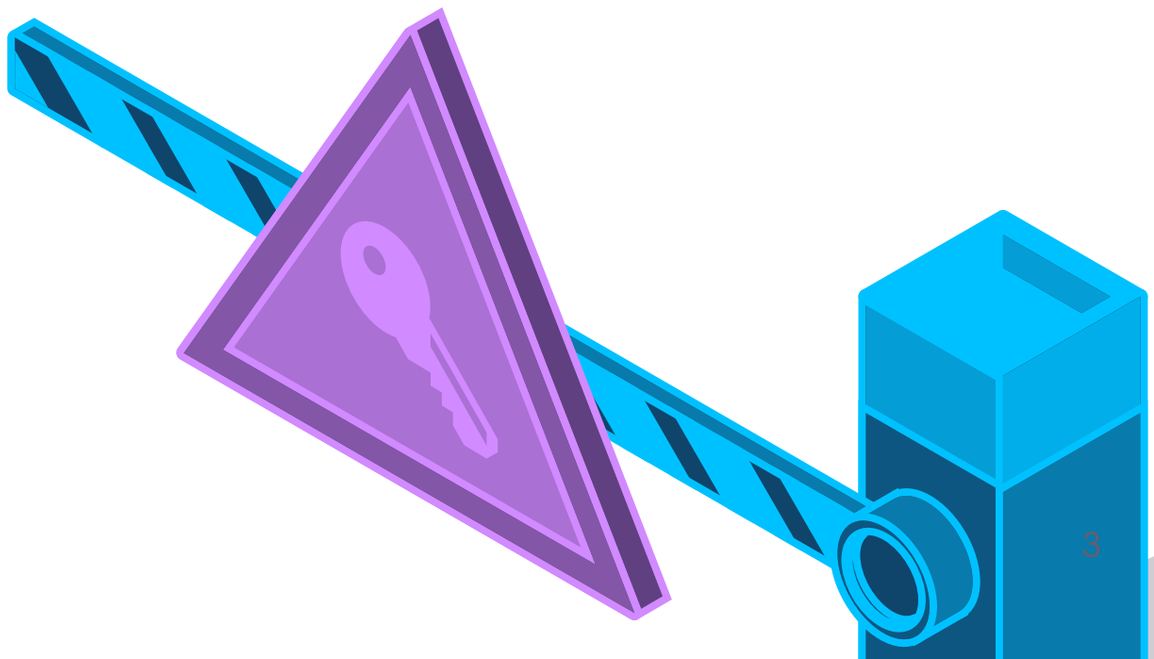
In den letzten zehn Jahren haben die ESAs Leitlinien für das IKT-Risikomanagement bereitgestellt und Regulierungsbehörden wie die Europäische Zentralbank (EZB) und De Nederlandsche Bank (DNB) beeinflusst. Jetzt, wo die DORA in Kraft ist, ist es an der Zeit, Ihre IKT-Risikopraktiken zu bewerten. Untersuchen Sie Ihre aktuelle Situation, identifizieren Sie Lücken und passen Sie sie an DORA an. Dies ist kein bürokratisches Kontrollkästchen, sondern eine Chance, die Kontrollen zu verbessern. Standardisieren und automatisieren Sie für ein kosteneffizientes IKT-Risikomanagement. Bereiten Sie sich auf von DORA initiierte Audits und Inspektionen vor.

Für die einen ist DORA der Beginn einer beschleunigten Reifungsreise, für die anderen eine Gelegenheit, ihre Fähigkeiten zu verbessern. In einer Welt, die digitale Widerstandsfähigkeit schätzt, ist DORA Ihr Wegweiser. Es geht um mehr als nur die Einhaltung von Vorschriften - es geht um die Schaffung eines widerstandsfähigen Finanzökosystems.

Why is the Digital Operational Resilience Act a game-changer?

2 minuten gelesen

Blogbeitrag lesen



Wer ist drin und wer ist draußen: der Anwendungsbereich von DORA

Lesen Sie Artikel 2 der DORA, um ihre Reichweite zu verstehen

In Reichweite:

- Kreditinstitut
- Zahlungsinstitut
- Anbieter von Kontoinformationsdiensten
- Investmentgesellschaft
- Krypto-Asset-Dienstleister
- Versicherungs- und Rückversicherungsunternehmen

...und viele mehr, insgesamt 21 Arten von Einrichtungen. (Siehe Artikel 2 für die vollständige Liste).

Außerhalb des Geltungsbereichs:

- Verwalter eines bestimmten alternativen Investmentfonds
- Bestimmte Versicherungs- und Rückversicherungsunternehmen
- Kleine Rentenversicherung
- Kleinstunternehmen oder kleine bis mittlere Versicherungsvermittler
- Postscheckämter

> **Hinweis**
> In den Mitgliedstaaten gelten möglicherweise besondere Ausnahmen. Genaue Angaben finden Sie immer in den Originalrichtlinien.

Die Rolle der ESAs bei der Marktresilienz

Wenn Sie sich mit den 64 Artikeln der DORA befassen, wird die größere Rolle, die die europäischen Aufsichtsbehörden (ESAs) bei der Überwachung der lokalen Durchsetzung spielen werden, wesentlich. Unternehmen sollten sich auf eine verstärkte Überwachung und strenge Kontrollen einstellen, einschließlich Verpflichtungen wie:

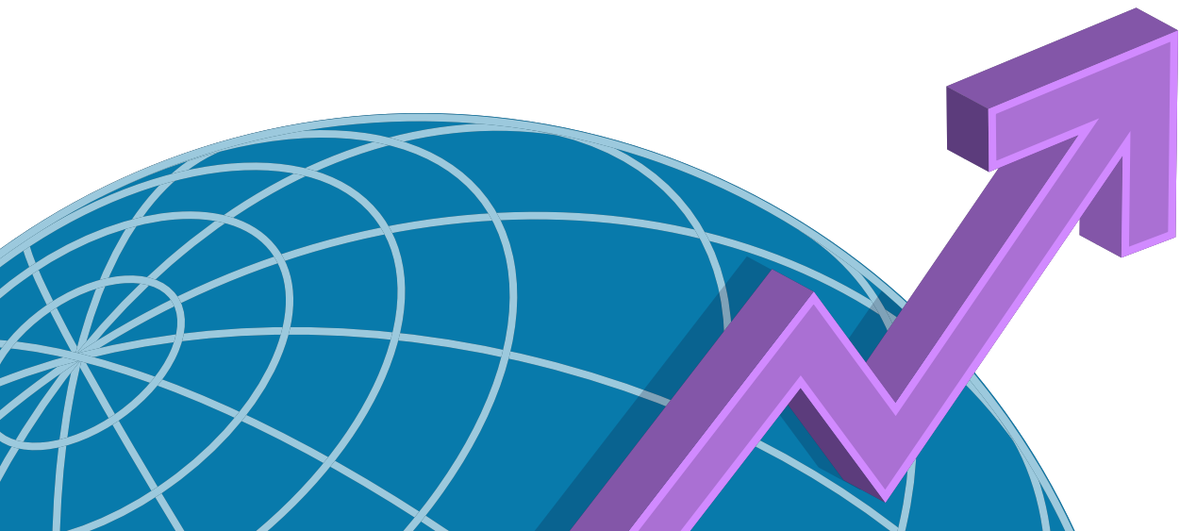
- Ausarbeitung eines soliden, umfassenden und gut dokumentierten Rahmens für das IKT-Risikomanagement (Artikel 6 Absatz 1), der zumindest die Strategien, Politiken, Verfahren, IKT-Protokolle und -Werkzeuge umfassen muss, die zum Schutz aller Informationen und IKT-Vermögenswerte erforderlich sind
- Gemeinsame Nutzung der vorgeschriebenen Berichte über größere IKT-bezogene Vorfälle
- Entwicklung belastbarer Pläne zur Aufrechterhaltung des Geschäftsbetriebs (BCP) und Pläne zur Wiederherstellung im Katastrophenfall (DRP)
- Testen von IKT-Betriebskontinuitätsplänen und IKT-Reaktions- und Wiederherstellungsplänen mindestens einmal pro Jahr

Was sind ESAs?

Die europäischen Finanzaufsichtsbehörden (ESAs) sind integraler Bestandteil des 2011 eingerichteten europäischen Finanzaufsichtssystems (ESFS).

Mit Einrichtungen wie der europäischen Bankenaufsichtsbehörde (EBA) in Paris, der europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) in Paris und der europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) in Frankfurt spielen die ESAs eine entscheidende Rolle bei der mikroprudenziellen Aufsicht auf EU-Ebene.

Sie wurden von der Europäischen Kommission im Jahr 2009 als Reaktion auf die Finanzkrise 2007-08 vorgeschlagen.



Geldbußen und Auswirkungen

Finanzinstitute, die sich nicht an die Verordnung halten, müssen mit verschiedenen Konsequenzen rechnen, unter anderem:

Ordnungsgelder

Schwere Verstöße können zu Geldbußen von bis zu 10 Millionen Euro oder 5 % des gesamten Jahresumsatzes führen, je nachdem, welcher Betrag höher ist.

Abhilfemaßnahmen

Die Aufsichtsbehörden können den Instituten auferlegen, Abhilfemaßnahmen zu ergreifen, um Schwächen in der operationellen Widerstandsfähigkeit zu beheben.

Öffentliche Rügen

Aufsichtsorgane können Finanzinstitute, die die Anforderungen der Verordnung nicht erfüllen, öffentlich anprangern.

Entzug der Zulassung

Wiederholte Verstöße gegen die Vorschriften können zum Entzug der Zulassung des Organs führen.

Schadensersatz

Die Institute können verpflichtet sein, Kunden oder Dritte für Schäden zu entschädigen, die durch die Nichteinhaltung von Vorschriften entstehen.

Identifizierung von Hürden am DORA-Horizont

Verabschiedung des Gesetzes, das den Unternehmen eine Frist bis 2025 für die Umsetzung von DORA einräumt. Während der zweijährigen Vorbereitungszeit (2023 und 2024) sollte die Governance an die Säulen von DORA angepasst werden. Durchführung einer Lückenanalyse für eine digitale Resilienzstrategie. Ab 2025 sind obligatorische Berichte, Tests und jährliche Bewertungen erforderlich. Penetrationstests und ESA-Zertifizierung werden bis Ende 2025 obligatorisch.

24. September 2020: Veröffentlichung des DORA-Vorschlags durch die Europäische Kommission

23. Juli 2022: Vorläufige Einigung über DORA erzielt

10. November 2022: Ratifizierung der DORA-Verordnung durch das Europäische Parlament

Q4 2022 (Nov./Dez.): Veröffentlichung der DORA im Amtsblatt der EU

17. Januar 2023: Tag der Verabschiedung
DORA tritt in Kraft

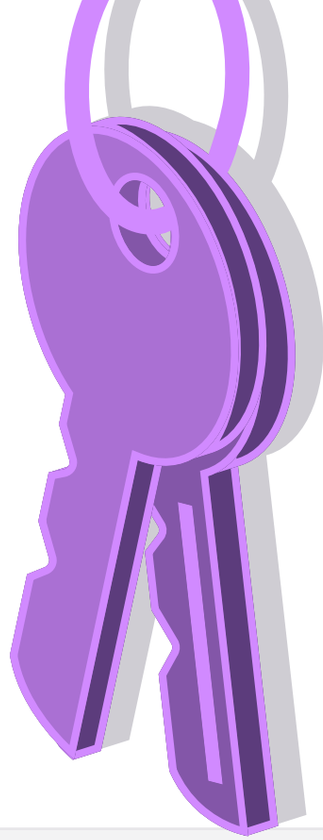
Q3 2023 - Q4 2024: Vorlage der technischen Standards durch die ESAs

17. Januar 2025: Anwendbarkeit von DORA
Volle Übereinstimmung mit DORA und seinen technischen Standards erforderlich

Aufgepasst!

Die DORA hat Vorrang vor sich überschneidenden Texten wie den NIS- oder ESA-Leitlinien und ist damit die wichtigste Referenz für die Überprüfung der Einhaltung von Vorschriften, um Lücken zu vermeiden, wenn sie 2025 in Kraft tritt.

DORA navigieren - Schlüsselkomponenten



Der von der Europäischen Union entworfene Rechtstext von DORA beschreibt die Bestimmungen der Gesetzgebung und zielt auf fünf Kernsäulen der Cybersicherheit ab, die verbessert werden sollen. Von den Cybersicherheitsanforderungen bis hin zum Risikomanagement spielt jedes Element eine entscheidende Rolle bei der Gestaltung der Zukunft der Cybersicherheit im Finanzsektor.

5 Kernsäulen

IKT-Risikomanagement

Nachweis interner Verwaltungs- und Kontrollrahmen, die ein wirksames Management aller IKT-Risiken gewährleisten.

IKT-Risiko gegenüber Dritten

Effizientes Management von IKT-Risiken gegenüber Dritten, einschließlich der Risiken, die sich aus der Beauftragung von IKT-Dienstleistern gegenüber Dritten ergeben.

Informationsaustausch

Erleichterung des Austauschs von Informationen und Erkenntnissen über Cyber-Bedrohungen zwischen Finanzunternehmen.

Meldung von IKT-bezogenen Vorfällen

Entwicklung der Fähigkeit, größere Vorfälle den zuständigen Behörden zu melden und die Nutzer und Kunden der Dienste zu informieren.

Digital Operational Resilience Testing

Implementierung, Pflege und Überprüfung von Testprogrammen für die digitale Betriebsfestigkeit.

Voraussetzungen für eine erfolgreiche DORA-Konformität

Die Einführung des Digital Operational Resilience Act (DORA) stellt einen entscheidenden Moment für den Finanzsektor dar, da die Institute nun nicht mehr in erster Linie das operationelle Risiko durch Kapitalzuweisung steuern, sondern auch Regeln für umfassende IKT-bezogene Schutz-, Erkennungs-, Eindämmungs-, Wiederherstellungs- und Reparaturfunktionen einhalten müssen. Diese Änderung der Vorschriften stellt die betroffenen Organisationen jedoch vor Herausforderungen bei der Einhaltung der Vorschriften:

Weitreichender Anwendungsbereich: Der breite Anwendungsbereich von DORA erstreckt sich auf verschiedene Finanzinstitute und kritische Drittdienstleister (Critical Third-Party Service Providers, CTPS), was eine genaue Abgrenzung des Anwendungsbereichs schwierig macht.

Komplexe Anforderungen: Die komplizierten Mandate von DORA erfordern ein detailliertes Verständnis und eine strategische Planung, was sowohl das Verständnis als auch die Ausführung komplexer macht.

Finanzielle Belastung: Die Einhaltung von DORA ist mit spürbaren finanziellen Auswirkungen verbunden, da die Institutionen in die Stärkung der IKT-Systeme und die Umstrukturierung der Prozesse investieren.

Kulturwandel: Die operationelle Resilienz erfordert einen Mentalitätswandel und stellt eine große Herausforderung beim Übergang von konventionellen Operationen zu einem resilienzorientierten Ansatz dar.

Stärken Sie
Regeln für das IKT-Risikomanagement

Erweitern Sie
IKT-Regulierung für alle Beteiligten

Harmonisieren Sie
Berichterstattung und Informationsaustausch

Standardisieren Sie
Belastbarkeitstests und Überwachung

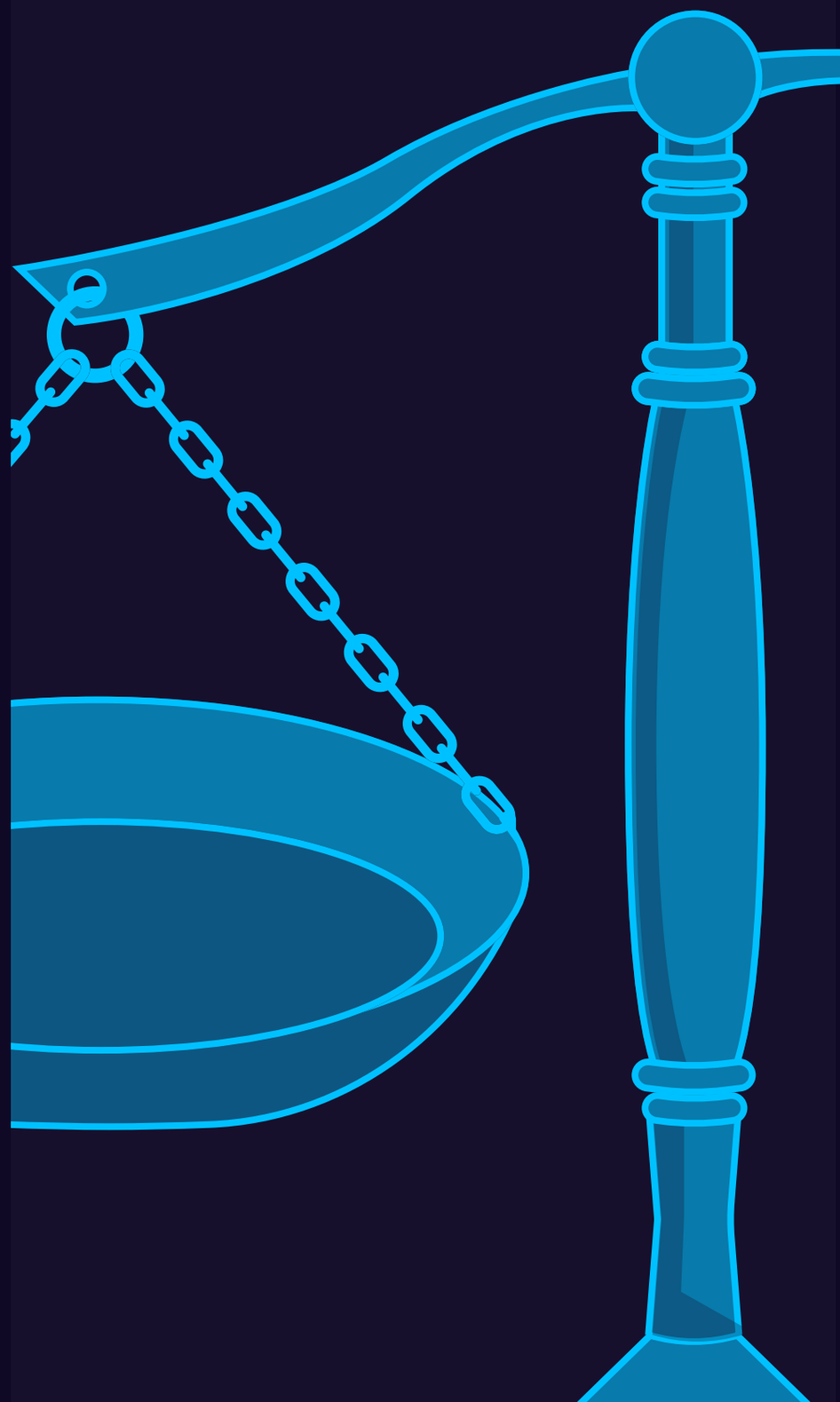
Voraussetzungen für die erfolgreiche Erfüllung der DORA-Anforderungen (Forts.)

Ressourcenbeschränkungen: Ressourcenknappheit, einschließlich Budgetbeschränkungen, Qualifikationsdefizite und Personalknappheit, kann die umfassende Umsetzung von DORA behindern, insbesondere bei kleineren Einrichtungen.

Herausforderungen bei der Zusammenarbeit: Kooperationsbemühungen, vor allem mit Dritten, sind im Rahmen von DORA oft notwendig. Es kann jedoch mühsam sein, eine konsequente Zusammenarbeit zu erreichen, insbesondere von Stellen, die nicht in den Zuständigkeitsbereich von DORA fallen.

Dynamische Regulierungslandschaft: Die sich ständig verändernde Regulierungslandschaft im Finanzsektor stellt eine ständige Herausforderung für die Einhaltung der DORA-Vorschriften dar.

Trotz dieser Hürden verspricht die Einhaltung der DORA-Vorschriften den Weg zu einem widerstandsfähigeren, sichereren und zuverlässigeren Finanzökosystem in der EU zu ebnen.



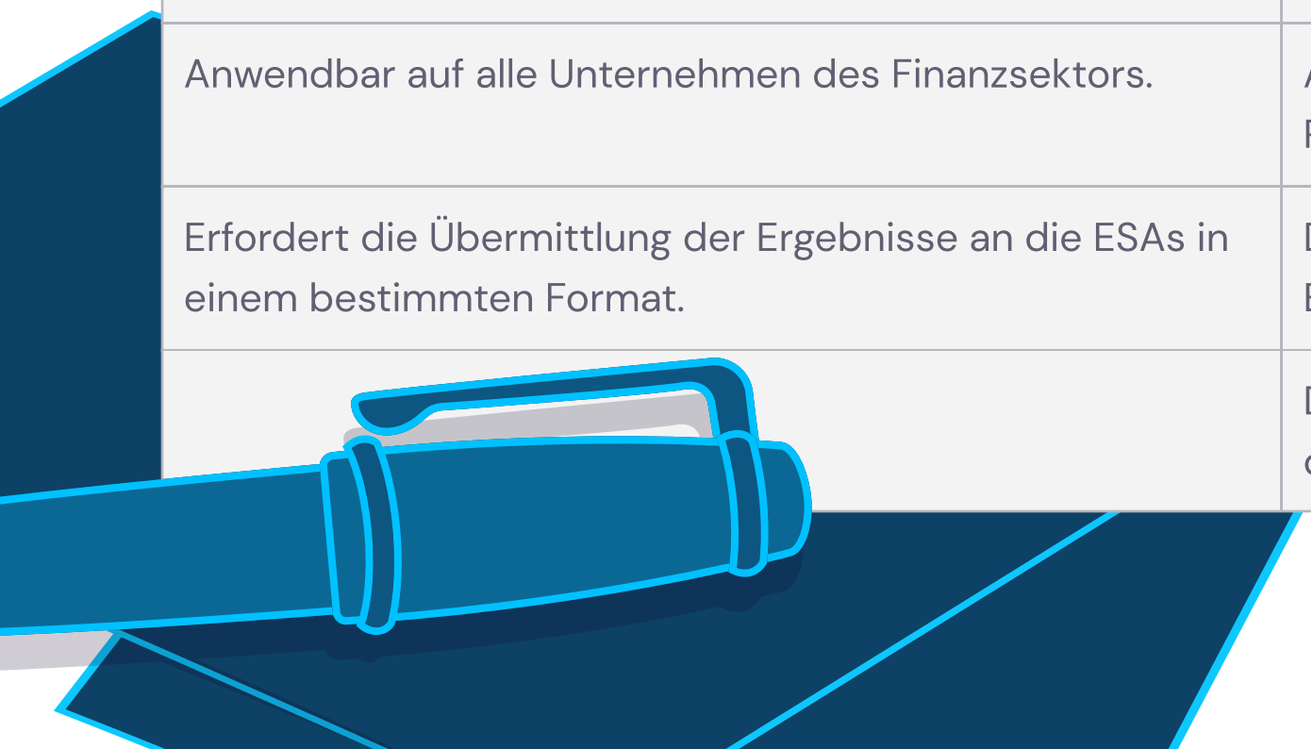
Anpassung an die DORA-Konformität

Die ESAs erwarten eine neue Ära der Berichterstattung und Kommunikation von Finanzinstituten, die wertvolle Erkenntnisse zur Verbesserung der Cyber-Intelligenz der EU liefern. Die ESAs werden in dieser Zeit die RTSs verfeinern und von den Unternehmen verlangen, dass sie ihre Governance und Praktiken an die DORA-Säulen der Widerstandsfähigkeit anpassen.

Um eine digitale Resilienzstrategie zu verwirklichen, können Unternehmen eine erste Lückenbewertung durchführen und ihren Reifegrad analysieren. Dazu gehört die Bewertung der Einhaltung bestehender Richtlinien (ESA, NIS, CROE) und IT-Risikomanagementstandards (ITIL, COBIT, NIST CSF, ISO). Durch die Identifizierung von Deltas kann eine Roadmap die Prioritäten für die DORA-Anforderungen festlegen. In dieser Phase werden die Regulierungsbehörden neue RTS und ITS definieren, was eine flexible Strategie erfordert.

Eine wichtige Änderung ist die Einführung von Tests der digitalen operationellen Belastbarkeit, die auf bedrohungsorientierten Penetrationstests basieren (Vorschlag von Artikel 23) und zwei Kategorien umfassen:

Obligatorische jährliche interne Tests	Erweiterte Prüfungen (alle drei Jahre)
Anwendbar auf alle Unternehmen des Finanzsektors.	Anwendbar auf Unternehmen, die die Kriterien der Regulierungsbehörde erfüllen.
Erfordert die Übermittlung der Ergebnisse an die ESAs in einem bestimmten Format.	Durchgeführt von einer externen Einrichtung, wobei die ESAs Konformitätsbescheinigungen ausstellen.
	Die Nichteinhaltung könnte zu einer möglichen Einstellung der Unternehmenstätigkeit führen.



Auf dem Weg zur DORA-Konformität

Bereiten Sie sich auf die vollständige Durchsetzung von DORA im Januar 2025 vor, indem Sie Projekte initiieren, den Budgetbedarf abschätzen und organisationsweite Initiativen umsetzen. Bauen Sie die Widerstandsfähigkeit auf und erreichen Sie die DORA-Konformität mit den folgenden Schritten:

Risikoermittlung durch Network Mapping

- Identifizierung von Risiken durch Abbildung der Anwendungsabhängigkeiten in der gesamten Infrastruktur.
- Nutzen Sie Sicherheitslösungen wie Hadrian, um diesen Zuordnungsprozess zu erleichtern, kritische und nicht kritische Prozesse aufzudecken und Abhängigkeiten von Dritten zu identifizieren.
- Gehen Sie bisher unbekannte Risiken sofort nach ihrer Entdeckung an.

Erhöhte Erkennungsfähigkeiten

- Nutzen Sie das verbesserte Verständnis Ihrer Umgebung, um die Erkennungsmöglichkeiten zu verbessern.

Proaktive Eindämmung von Sicherheitsverletzungen

- Anerkennung der Eindämmung von Sicherheitsverletzungen als wesentlicher Aspekt der Widerstandsfähigkeit gemäß DORA
- Implementierung von Technologien wie Mikro-Segmentierung (Zero Trust Segmentation), um das Netzwerk in Zonen zu unterteilen, die eine kontrollierte Kommunikation zwischen Arbeitslasten und Geräten ermöglichen.
- Isolieren Sie proaktiv hochwertige Anlagen oder grenzen Sie während eines aktiven Angriffs reaktiv kompromittierte Systeme ein, um die Ausbreitung eines Einbruchs zu verhindern.

Verständnis des DORA-Rahmens

DORA ist mehr als ein bloßes Compliance-Mandat. Es bietet die Chance, Ihr Unternehmen zukunftssicher zu machen, die Cybersicherheitspraktiken zu verbessern und Ihr Unternehmen für die kommenden Herausforderungen und Chancen der digitalen Finanzlandschaft zu rüsten. Hier erfahren Sie, wie Sie das tun können:

Risikobewältigung durch proaktive offensive Sicherheit

Nachweis interner Führungs- und Kontrollrahmen, die ein wirksames Management aller IKT-Risiken gewährleisten.

Wie kann Hadrian helfen?

Das Continuous Automated Red Teaming (CART) von Hadrian bietet kontinuierliche und automatisierte simulierte Angriffe auf Ihr System, um Schwachstellen und Sicherheitslücken zu ermitteln. Da es sich um ein kontinuierliches Verfahren handelt, können wir neue Bedrohungen und Schwachstellen erkennen, sobald sie auftauchen.

Effizientes Management von Risiken Dritter

Wenn es um Dritte geht, sind die entsprechenden rechtlichen Vereinbarungen zum Schutz der Cybersicherheit unerlässlich. Letztendlich müssen Sie aber alle Schwachstellen überwachen, die Ihre Dritten in Ihre Angriffsfläche einbringen. Das ist eine große Aufgabe und praktisch unmöglich von Hand zu überwachen.

Wie kann Hadrian helfen?

Die intelligente Sicherheitsplattform von Hadrian bewertet Ihre gesamte Angriffsfläche, identifiziert Schwachstellen aus Drittquellen, bewertet die Wahrscheinlichkeit und die Auswirkungen eines Angriffs, schlägt Abhilfemaßnahmen vor und validiert die Sicherheit nach der Behebung der Schwachstellen.

Bereiten Sie sich auf eine schnelle und genaue Meldung von Vorfällen vor.

DORA soll die Cybersicherheit in der gesamten Europäischen Union durch die schnelle und effektive Meldung von Vorfällen verbessern. Der Informationsaustausch trägt dazu bei, das Bewusstsein für Cyber-Bedrohungen zu schärfen und hilft, IKT-bezogene Vorfälle einzudämmen, so DORA.

Wie kann Hadrian helfen?

Herkömmlichen Compliance-Berichten fehlt es an Echtzeit-Updates, was zu einer verzögerten Wahrnehmung von Problemen führen kann. Hadrian liefert genaue und klare Berichte, die die DORA-Anforderungen für externe Stakeholder erfüllen und eine vertrauensvolle Kommunikation mit Führungskräften und Vorstandsmitgliedern gewährleisten.

Über Hadrian

Defensive Sicherheit sollte durch offensive Sicherheit bestätigt werden. Hadrian bietet die Hackerperspektive und zeigt die Ziele und Methoden auf, die bei einem realen Datenverstoß verwendet werden könnten. Die kontinuierlichen und umfassenden Tests von Hadrian entdecken und validieren Risiken völlig eigenständig.

Die Plattform von Hadrian kombiniert Technologien zur Erkennung von Angriffsflächen, automatisierte Penetrationstests und das Management von Bedrohungen in einer cloudbasierten und agentenlosen Plattform. Die hochmoderne Technologie wird von Hadrians internem Hacker-Team ständig aktualisiert und verbessert.

> „Das Aufregende an der Arbeit von Hadrian ist, dass sie ein scheinbar unmögliches Rätsel gelöst haben: das Auffinden von Schwachstellen in einem komplexen Netzwerk mit menschenähnlichen Details, in großem Maßstab, von außen und kontinuierlich. Wofür ein engagiertes Team von Sicherheitsingenieuren normalerweise einige Wochen braucht, um ein einziges System zu finden, kann Hadrian innerhalb von Minuten für Tausende von Systemen erledigen."
>
> **Tiago Teles - Sicherheitschef, ABN AMRO**

Vertraut von

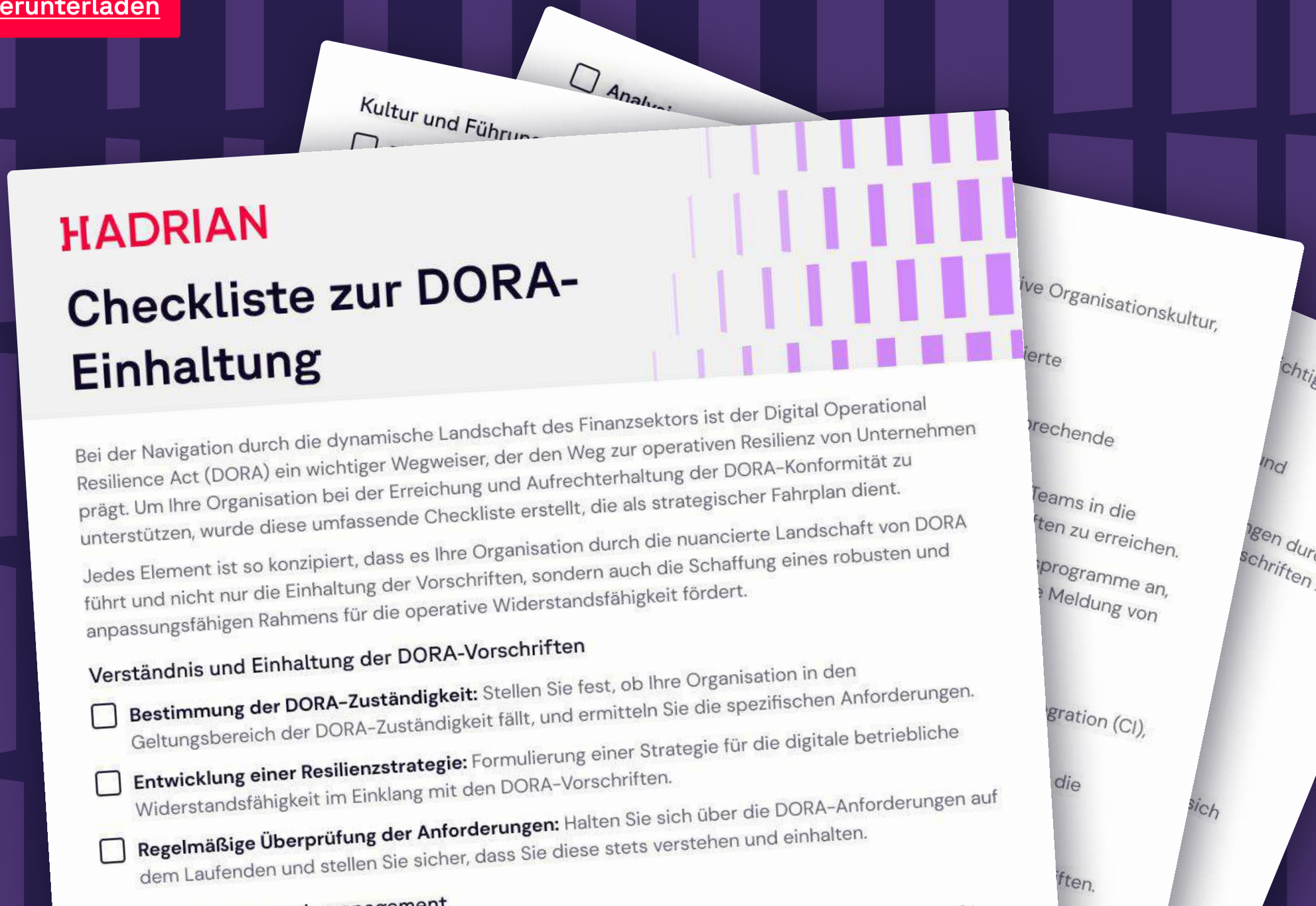
ABN·AMRO · SHV ENERGY · macmillan education · CTC GLOBAL

WeatherTech · LEROY MERLIN · LOTTOMATICA · Crédit Agricole

RITUALS... · BIOLANDES · nedap · Van Oord

Checkliste zur DORA-Einhaltung

Checkliste herunterladen



DORA: Wesentliche Begriffe, die Sie kennen sollten

Kontoinformationsdienstleister: Ein Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366;

Krypto-Asset-Dienstleister: Ein Krypto-Vermögenswert-Dienstleister gemäß der Definition in der einschlägigen Bestimmung der Verordnung über Märkte für Krypto-Vermögenswerte;

Cyberangriff: Ein böswilliger Vorfall im Zusammenhang mit IKT, der durch den Versuch eines Bedrohungsakteurs verursacht wird, einen Vermögenswert zu zerstören, bloßzustellen, zu verändern, zu deaktivieren, zu stehlen oder sich unbefugten Zugang zu ihm zu verschaffen bzw. ihn unbefugt zu nutzen;

Digitale operationelle Widerstandsfähigkeit: Die Fähigkeit eines Finanzunternehmens, seine betriebliche Integrität und Zuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch die Nutzung von Dienstleistungen, die von IKT-Drittanbietern erbracht werden, das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit des Netzes und der Informationssysteme, die ein Finanzunternehmen nutzt, zu gewährleisten, und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität zu unterstützen, auch bei Störungen;

Europäische Aufsichtsbehörden: Die im Rahmen des europäischen Finanzaufsichtssystems eingerichteten Regulierungsagenturen, die die Finanzstabilität gewährleisten sollen;

IKT-Vermögensbestandteil: Ein Software- oder Hardware-Vermögensbestandteil im Netzwerk und in den Informationssystemen, die vom Finanzinstitut genutzt werden;

IKT-Risiko: Jeder nach vernünftigem Ermessen erkennbare Umstand im Zusammenhang mit der Nutzung von Netz- und Informationssystemen, der, wenn er sich verwirklicht, die Sicherheit des Netzes und der Informationssysteme, von technologieabhängigen Werkzeugen oder Prozessen, von Abläufen und Prozessen oder von der Erbringung von Dienstleistungen gefährden kann, indem er nachteilige Auswirkungen auf die digitale oder physische Umgebung hat;

IKT-bezogener Vorfall: Ein einzelnes Ereignis oder eine Reihe miteinander verbundener, vom Finanzinstitut nicht geplanter Ereignisse, die die Sicherheit des Netzes und der Informationssysteme beeinträchtigen und negative Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzinstitut erbrachten Dienstleistungen haben;

Versicherungsunternehmen: Ein Versicherungsunternehmen im Sinne von Artikel 13, Punkt (1), der Richtlinie 2009/138/EG;

Technische Durchführungsstandards (ITS): Ein technischer Durchführungsrechtsakt, der die einheitliche Anwendung bestimmter Vorschriften des Basisrechtsakts vorsieht;

Verwalter von alternativen Investmentfonds: Ein Verwalter von alternativen Investmentfonds im Sinne von Artikel 4 Absatz 1 Buchstabe b der Richtlinie 2011/61/EU;

Mittelgroßes Unternehmen: Ein Finanzinstitut, das kein kleines Unternehmen ist, weniger als 250 Personen beschäftigt und einen Jahresumsatz von höchstens 50 Millionen Euro und/oder eine Jahresbilanz von höchstens 43 Millionen Euro aufweist;

Wichtige DORA-Begriffe
(Forts.)

Kleinstunternehmen: Ein Finanzunternehmen, bei dem es sich nicht um einen Handelsplatz, eine zentrale Gegenpartei, ein Transaktionsregister oder einen Zentralverwahrer handelt, das weniger als 10 Personen beschäftigt und einen Jahresumsatz und/oder eine Jahresbilanzsumme von höchstens 2 Mio. EUR aufweist;

Netz- und Informationssystem: Netz- und Informationssystem gemäß der Definition in 2022/2555;

Zahlungsinstitut: Ein Zahlungsinstitut gemäß der Definition in Artikel 4 Nummer 4 der Richtlinie (EU) 2015/2366;

Technische Regulierungsstandards (RTS): Ein delegierter technischer Rechtsakt, der von einer europäischen Aufsichtsbehörde ausgearbeitet wurde;

Rückversicherungsunternehmen: Ein Rückversicherungsunternehmen gemäß der Definition in Artikel 13, Punkt (4) der Richtlinie 2009/138/EG;

Kleines Unternehmen: Ein Finanzinstitut, das 10 oder mehr Personen, aber weniger als 50 Personen beschäftigt und einen Jahresumsatz und/oder eine Jahresbilanzsumme von mehr als 2 Mio. EUR, aber nicht mehr als 10 Mio. EUR hat;

Bedrohungsgesteuerte Penetrationstests: Ein Rahmenwerk, das die Taktiken, Techniken und Verfahren realer Bedrohungsakteure nachahmt, die als echte Cyber-Bedrohung wahrgenommen werden, und das einen kontrollierten, maßgeschneiderten, nachrichtendienstlich geleiteten (Red Team) Test der kritischen Live-Produktionssysteme des Finanzunternehmens liefert.