BITSIGHT

LÖSUNGSKONZEPT

DORA-konform mit Bitsight

Die Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, kurz: DORA) ist eine Verordnung, die einen umfassenden Rahmen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT) für den Finanzsektor in der Europäischen Union (EU) schafft. DORA umfasst eine Reihe technischer Standards, die Finanzinstitutionen und ihre kritischen Drittanbieter bis zum 17. Januar 2025 in ihre IKT-Systeme übernehmen müssen. Hier erfahren Sie, was Sie wissen müssen, um die Frist einzuhalten.

Nach Jahren une inheitlicher, individueller Regelungen, die von EU-Mitgliedstaaten vorangetrieben wurden, harmonisiert DORA die Bemühungen, einen universellen Rahmen für die Bewältigung und Eindämmung von IKT-Risiken im Finanzsektor zu schaffen. Mit einem EU-weit einheitlichen Regelwerk schafft DORA ein umfassendes Konzept, das sicherstellt, dass Unternehmen den Folgen von IKT-Vorfällen standhalten, auf diese reagieren und sich von diesen erholen können, um dadurch die Erfüllung kritischer und wichtiger Funktionen aufrechtzuerhalten und Störungen für Kunden und das Finanzsystem auf ein Minimum reduzieren zu können.

DORA unterstreicht die Notwendigkeit, robuste Maßnahmen und Kontrollen für Systeme, Tools und Dritte einzuführen, über die richtigen Pläne zur Aufrechterhaltung des Geschäftsbetriebs zu verfügen und deren Wirksamkeit zu testen.

Die fünf Säulen von DORA

01 IKT-Risikomanagement

02 Berichterstattung über IKT-Vorfälle

03 Prüfung der digitalen operationalen Resilienz

04 Austausch von Informationen und Erkenntnissen

05 IKT-Risikomanagement für Drittparteien

Die fünf Säulen von DORA

1. IKT-Risikomanagement

Anwendungsbereich	• Governance (rechenschaftspflichtiges Leitungsorgan) • Rahmen für das Risikomanagement und damit verbundene Aktivitäten (Identifizierung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernen und Weiterentwicklung, Krisenkommunikation)
Wie wir Ihnen helfen	Bitsight unterstützt Unternehmen bei der Einhaltung der Governance-Grundsätze bei IKT-Risiken. Dazu gehört die Ermittlung der Risikotoleranz für IKT-Risiken auf der Grundlage der Risikobereitschaft des Unternehmens und der Toleranz gegenüber den Auswirkungen von IKT-Störungen.
Lösungsansatz von Bitsight	• Die Sicherheitseinstufung bewertet das Risiko des Unternehmens und seiner Geschäftspartner für Finanzdienstleister und ihr IKT-Anbieter-Ökosystem • Zuordnung von Risikofaktoren zu Rahmenkategorien

2. Berichterstattung über IKT-Vorfälle

Anwendungsbereich	• Standardisierte Klassifizierung von Vorfällen • Verpflichtende und standardisierte Berichterstattung über schwere Vorfälle • Anonymisierte EU-weite Berichte
Wie wir Ihnen helfen	Bitsight hilft bei der Bewertung der Vorfallklassifizierung auf der Grundlage einer Reihe spezifischer Kriterien, etwa der Anzahl der betroffenen Benutzer, Dauer, geografischen Ausbreitung, Schwere der Auswirkungen auf IKT-Systeme, Kritikalität der betroffenen Dienste, wirtschaftlichen Auswirkungen und dem Datenverlust.
Lösungsansatz von Bitsight	• Warnhinweise zu Risikofaktoren basierend auf Geschäftskontext und/oder Services • Meldung und Klassifizierung von Datenschutzverletzungen • Aufspüren von Risiken mithilfe von Filtern

3. Prüfung der digitalen operationalen Resilienz

Anwendungsbereich	• Umfassendes Prüfprogramm, mit Schwerpunkt auf technischen Prüfungen • Groß angelegte, bedrohungsspezifische Live-Tests, die alle drei Jahre von unabhängigen Prüfern durchgeführt werden
Wie wir Ihnen helfen	Bitsight arbeitet mit Sicherheits- und Risikoverantwortlichen zusammen, die sich auf die Performance der Cybersicherheit konzentrieren, um das Risiko von Sicherheitsverletzungen im gesamten Ökosystem systematisch zu senken. Unsere Fähigkeiten im Cybersicherheits-Risikomanagement erstrecken sich über gesamte Unternehmen und ihre Dritt- und Viertanbieter und ermöglichen es den Mitarbeitern, die Wirksamkeit des Risikomanagementsystems zu testen und zu messen.
Lösungsansatz von Bitsight	• Bitsight erkennt Malware, Botnets und Informationen zu kompromittierten Systemen (auf Vorfallebene) von außen • Kontinuierliche Überwachung der mit dem Internet verbundenen Ressourcen auf der Grundlage potenzieller Risikofaktoren für Verstöße und risikobasierter Analysen • Die Bewertung korreliert mit der Wahrscheinlichkeit einer Datenschutzverletzung und ermöglicht eine umfassende Risikoquantifizierung • Daten von Viertanbietern ermöglichen die Ermittlung von Risikokonzentrationen (z. B. welche Cloud-Anbieter vorherrschend sind) • Umfassende Informationen über das IKT-/Anbieter-Ökosystem auf automatisierte Weise (einschließlich Warnmeldungen und Risikoeinstufung)

4. Austausch von Informationen und Erkenntnissen

Anwendungsbereich	• Richtlinien für Vereinbarungen zum Informationsaustausch über Cyber-Bedrohungen und -Schwachstellen
Wie wir Ihnen helfen	Bitsight erleichtert den Austausch von Informationen und Erkenntnissen über Cyber-Bedrohungen zwischen Finanzinstituten, damit diese besser auf digitale Schwachstellen reagieren können.
Lösungsansatz von Bitsight	• EVAs (Enable Vendor Access) ermöglichen den Informationsaustausch zwischen Stakeholdern

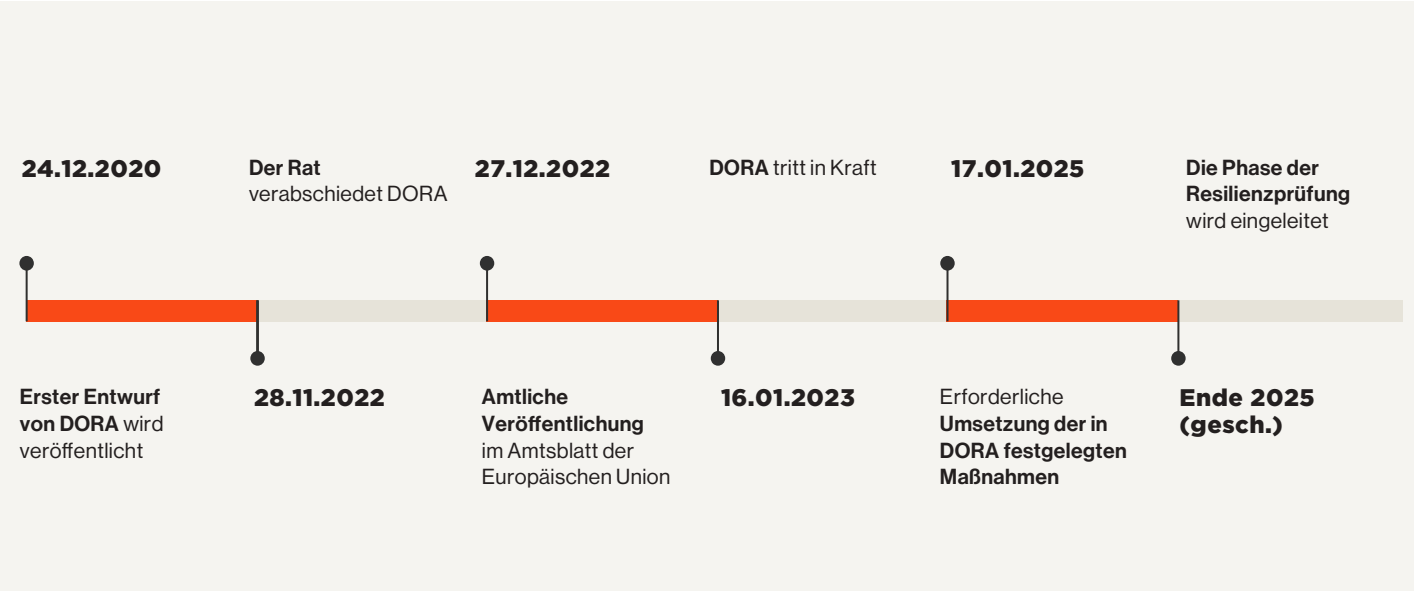
5. IKT-Risikomanagement für Drittparteien

Anwendungsbereich	• Strategie, Regelwerk und standardisiertes Informationsregister Richtlinien für die Bewertung vor Vertragsabschluss, den Vertragsinhalt, die Kündigung und den Ausstieg unter • Stressbedingungen (Konkurs/Insolvenz des Anbieters) • Schaffung eines Aufsichtsrahmens für kritische Anbieter innerhalb der EU mit klaren Anforderungen und Sanktionen
Wie wir Ihnen helfen	Bitsight unterstützt Unternehmen dabei, ein angemessenes Niveau an effektiven Sicherheitskontrollen und eine ausreichende Überwachung ihrer IKT-Drittanbieter sicherzustellen – insbesondere bei denjenigen, die als kritisch für ihre Lieferkette angesehen werden, sowie bei der Einführung von Maßnahmen zur Beaufsichtigung bestimmter Anbieter, die als kritisch für den globalen Markt angesehen werden.
Lösungsansatz von Bitsight	• Kontinuierliche Überwachung liefert sofortige Warnmeldungen über Veränderungen im Sicherheitsstatus von Anbietern anstelle von punktuellen jährlichen Bewertungen des Anbieterrisikos • Einstufung und Segmentierung von Anbietern nach Geschäftskontext, abgestimmt auf Inventar an Drittparteien • Bitsight VRM automatisiert und skaliert das Onboarding und die Risikobewertung von Anbietern mit kundenspezifischen Anforderungen • Verbesserte Zusammenarbeit durch EVAs zur Schaffung grundlegender Onboarding-Richtlinien • Kunden können Anbietern den Umgang mit KPIs für die Bewertung oder die Ereignis-/Risikoebene vorgeben (oder welche zusätzlichen Maßnahmen zulässig sind) • Die Schwachstellenerkennung und -behandlung bei Drittanbietern zeigt die Exposition von Anbietern gegenüber bekannten Schwachstellen und ermöglicht gemeinsame, evidenzbasierte Abhilfemaßnahmen • Bitsight verfügt standardmäßig über NIST-basierte Warnmeldungen und kann Risikofaktoren auf spezifische Rahmenwerke wie ISO 27001 oder allgemeine Anbieterfragebögen abbilden

Der Weg zu DORA

Die Europäische Kommission hat DORA im September 2020 als Teil eines größeren Pakets, das auch eine Strategie für ein digitales Finanzwesen mit Gesetzgebungsvorschlägen zu Krypto-Assets und digitaler Resilienz umfasst, vorgeschlagen. Der Rat der Europäischen Union und das Europäische Parlament haben DORA im November 2022 förmlich angenommen. Die Europäische Aufsichtsbehörde (ESA) arbeitet derzeit die technischen Regulierungsstandards (RTS) und technischen Durchführungsstandards (ITS) aus, die den Weg für die Einhaltung der Vorschriften ebnen werden. Diese Normen sowie ein Aufsichtsrahmen für kritische IKT-Anbieter werden voraussichtlich 2024 in ihrer endgültigen Form vorliegen.

Während die Uhr tickt, arbeiten Finanzinstitute und Drittanbieter von IKT-Dienstleistungen auf den bevorstehenden Stichtag am 17.01.2025 hin.



Einhaltung von DORA mithilfe von Bitsight

Bitsight ermöglicht Unternehmen, Cyberrisiken systematisch zu senken, indem es kritische Arbeitsabläufe hinsichtlich Risiko, Performance und Anfälligkeiten unterstützt. Sicherheitsverantwortliche können die Effektivität von Kontrollen, die von Best-Practice-Rahmenwerken empfohlen werden, kontinuierlich messen und die Daten von Risikofaktoren den Kontrollrahmen und fragebogenbasierten Bewertungen zuordnen. Dies stärkt das Vertrauen in die Antworten der Anbieter durch Überprüfungen und verbessert die Sichtbarkeit von Risiken.

Aufgrund der zunehmenden Abhängigkeit von der Cloud und Drittanbietern wird der Umgang mit Risiken von Seiten Dritter immer schwieriger. Mit seiner Gründung 2011 hat Bitsight eine neue Branche ins Leben gerufen und gibt Führungskräften das Vertrauen, schnellere und strategischere Entscheidungen beim Cyber-Risikomanagement zu treffen, und im großen Maßstab die Performance zu bewerten, Anbieter zu qualifizieren, Investitionen zu priorisieren und finanzielle Verluste zu minimieren.

Durch die aktive Überwachung von über 40 Millionen Unternehmen weltweit ermöglicht Bitsight den Sicherheitsteams, ein umfassendes Verständnis des Cyberrisikos zu gewinnen, das über Bewertungen hinausgeht und finanzielle und geschäftliche Zusammenhänge aufzeigt. Wir sorgen dafür, dass Unternehmen gemeinsam Risiken reduzieren, um die digitale operationale Resilienz zu stärken.

Bitsight, Ihr Partner auf Ihrem Weg zur Compliance →