

Rozporządzenie DORA

Rewolucja czy ewolucja
w polskim sektorze
bankowym?

13 grudnia 2022

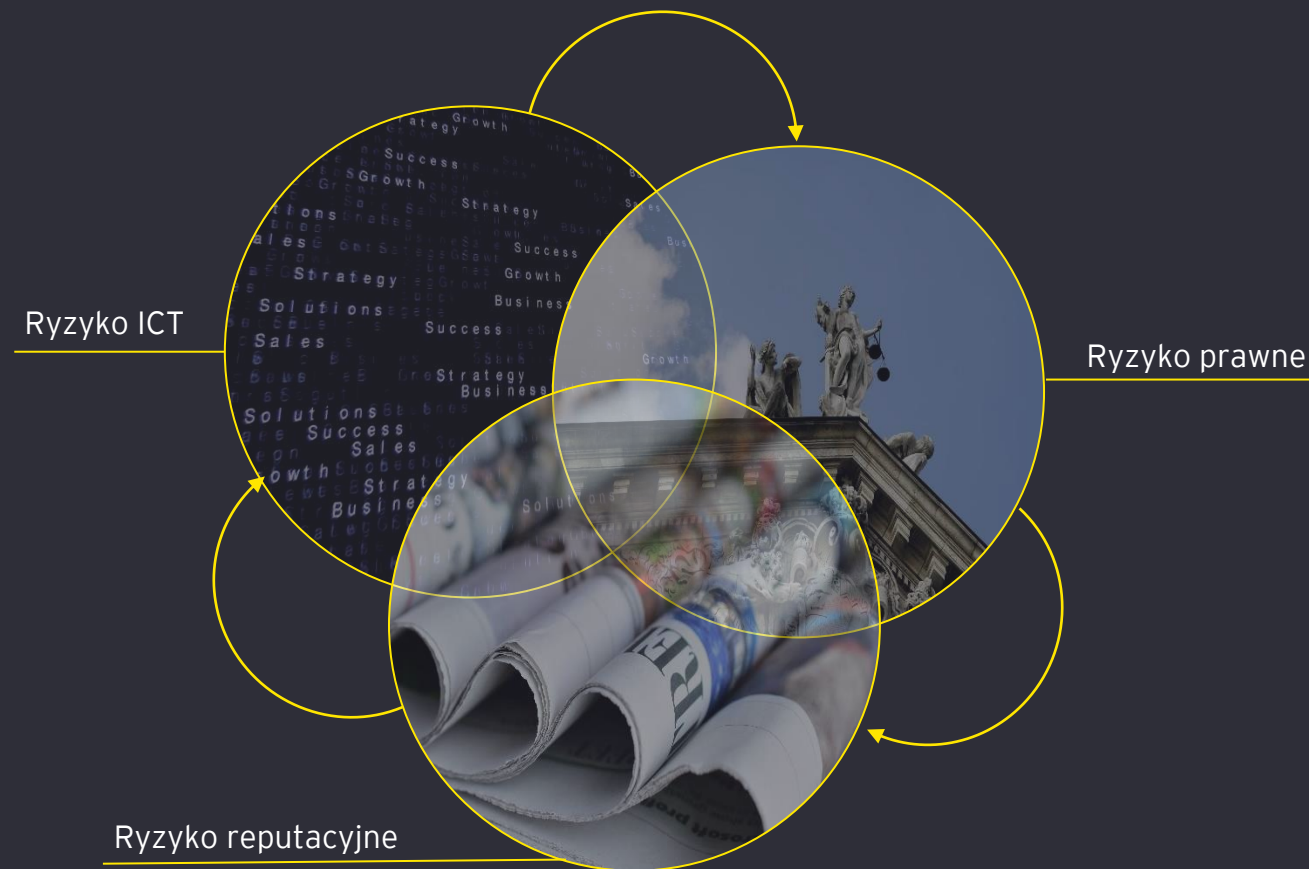


ZWIĄZEK BANKÓW POLSKICH



Building a better
working world

KNF wskazuje na silne powiązanie trzech rodzajów ryzyka:



DORA jest punktem przełomowym z wielu względów:

- 1 | Jest rozporządzeniem, a więc będzie obowiązywać bezpośrednio w Państwach Członkowskich UE
- 2 | Należy spodziewać się, że zostanie dodatkowo uzupełniona przez stanowiska organów nadzoru i rozporządzenia techniczne
- 3 | Będzie przedmiotem zainteresowania wszystkich aktorów w organizacji - ze względu na zasadę pełnej odpowiedzialności organu zarządzającego organizacją za ryzyko ICT

Cel badania polskiego sektora bankowego



1 |

Zarekomendowanie działań w zakresie wdrożenia obowiązków DORA

2 |

Ocena dojrzałości polskiego sektora bankowego w zakresie cyfrowej odporności

3 |

Wskazanie i omówienie obszarów w zakresie technologii informacyjnych i telekomunikacyjnych, które wymagają dostosowania do DORA, w oparciu o analizę obecnej praktyki banków

Digital Operational Resilience Act (DORA)

01

DORA jest rozporządzeniem Parlamentu Europejskiego i Rady UE przygotowaną w ramach unijnej strategii finansów cyfrowych.

1. Odpowiedź na rosnące cyber zagrożenia
2. Harmonizacja regulacji i standardów dotyczących ICT w UE

02

DORA ma na celu wzmocnienie odporności cyfrowej na zagrożenia wynikające z wykorzystywania nowoczesnej technologii. DORA

Koncentruje się na:

1. **Odporności na cyber zagrożenia**
2. **Zdolności do szybkiego powrotu do sprawności operacyjnej**

03

Zakresem DORA ma zostać objętych szereg instytucji oraz podmiotów sektora finansowego.

Rozporządzenie dotyczy nie tylko szeroko rozumianych instytucji finansowych, ale również dostawców krytycznych usług z obszaru ICT.

Należy pamiętać, że wymagania DORA mają formę **rozporządzenia** Parlamentu i Rady i jako takie muszą być bezwzględnie stosowane, oczywiście z uwzględnieniem zasady proporcjonalności

Kogo dotyczy?



DORA - perspektywa czasowa

01

Rozporządzenie opublikowane przez Komisję Europejską
24 września 2020
Od tego czasu na etapie negocjacji i poprawek w ramach instytucji UE oraz państw członkowskich

02

10 listopada 2022
PE ostatecznie zatwierdził przepisy **Rozporządzenia DORA**, a Rada przyjęła akt 28 listopada

03

Publikacja w **Dzienniku Urzędowym Unii Europejskiej**

Tu jesteśmy 20 dni

04

Wejście w życie:
DORA wejdzie w życie 20 dnia po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej i będzie bezpośrednio stosowana od 24 miesiąca od dnia publikacji

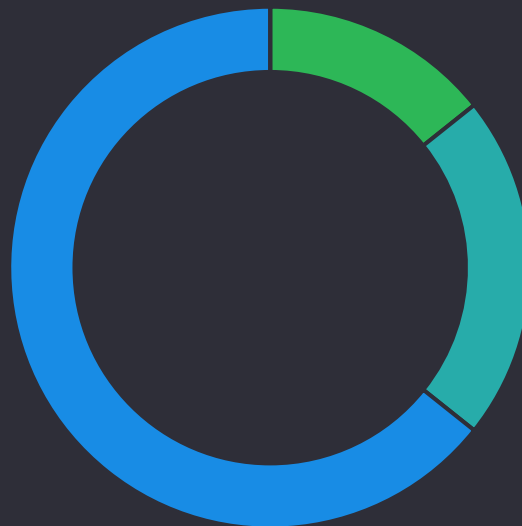
Gotowość sektora bankowego na DORA

Dla sektora bankowego DORA nie stanowi rewolucji a raczej ewolucję istniejącego systemu zarządzania bezpieczeństwem informacji i systemu kontroli wewnętrznej w obszarze ICT

Wnioski z badania

- 1 | Polski sektor bankowy jest przygotowany na nowe regulacje
- 2 | Konieczność podjęcia działań dostosowawczych
- 3 | Brak wykwalifikowanych zasobów ludzkich zarówno w ujęciu ilościowym, jak i kompetencyjnym

Jak Państwo oceniają przygotowanie Państwa organizacji na wymagania wynikające z DORA?



- Niezbędne będzie opracowanie programu mającego na celu dostosowanie do wymogów DORA
- Konieczne będą istotne zmiany w wybranych procesach cyberbezpieczeństwa / opracowanie nowych procesów cyberbezpieczeństwa
- Konieczne będą drobne zmiany wynikające z wymogów DORA
- Jesteśmy w Pełni zgodni z wymaganiami wynikającymi z DORA

EY | Building a better working world

Celem działalności EY jest budowanie lepiej funkcjonującego świata - poprzez wspieranie klientów, pracowników i społeczeństwa w tworzeniu trwałych wartości - oraz budowanie zaufania na rynkach kapitałowych.

Wspomagane przez dane i technologię, zróżnicowane zespoły EY działające w ponad 150 krajach, zapewniają zaufanie dzięki usługom audytorskim oraz wspierają klientów w rozwoju, transformacji biznesowej i działalności operacyjnej.

Zespoły audytorskie, consultingowe, prawne, strategiczne, podatkowe i transakcyjne zadają nieoczywiste pytania, by móc znaleźć nowe odpowiedzi na złożone wyzwania, przed którymi stoi dziś świat.

Nazwa EY odnosi się do firm członkowskich Ernst & Young Global Limited, z których każda stanowi osobny podmiot prawny. Ernst & Young Global Limited, brytyjska spółka z odpowiedzialnością ograniczoną do wysokości gwarancji (company limited by guarantee) nie świadczy usług na rzecz klientów. Informacje na temat sposobu gromadzenia przez EY i przetwarzania danych osobowych oraz praw przysługujących osobom fizycznym w świetle przepisów o ochronie danych osobowych są dostępne na stronie [ey.com/pl/pl/home/privacy](https://www.ey.com/pl/pl/home/privacy). Firmy członkowskie EY nie prowadzą praktyki prawniczej, jeśli jest to zabronione przez prawo lokalne.

Aby uzyskać więcej informacji, wejdź na www.ey.com/pl

© 2022 EYGM Limited.
Wszelkie prawa zastrzeżone.

Niniejsza publikacja została sporządzona z należytą starannością, jednak z konieczności pewne informacje zostały podane w skróconej formie. W związku z tym publikacja ma charakter wyłącznie orientacyjny, a zawarte w niej dane nie powinny zastąpić szczegółowej analizy problemu lub profesjonalnego osądu. EY nie ponosi odpowiedzialności za jakiegokolwiek straty powstałe w wyniku czynności podjętych lub zaniechanych na podstawie niniejszej publikacji. Zalecamy, by wszelkie przedmiotowe kwestie były konsultowane z właściwym doradcą.

