PRAKTYCZNE WDROŻENIE ROZPORZĄDZENIA DORA

redakcja naukowa Bartosz Bacia

Bartosz Bacia, Wojciech Dańczyszyn, Piotr Filipowski
Anna Jędrej-Giluń, Arkadiusz Kawulski, Magdalena Matysiak
Michał Mostowik, Adam Rasiński, Rafał Rudzki
Witold Srokosz, Paweł Szulik, Adam Woźniak

Wolters Kluwer

Książka jest praktycznym przewodnikiem po najważniejszych aspektach wdrożenia w organizacji wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego („Rozporządzenie DORA") oraz towarzyszących temu aktowi prawnemu rozporządzeń delegowanych Komisji – Regulacyjnych Standardów Technicznych (RTS).

Każdy z rozdziałów zawiera omówienie konkretnego obszaru tematycznego odpowiadającego systematyce Rozporządzenia DORA, które skupia się na analizie wyzwań związanych z realizacją wymogów prawnych. Wskazuje również praktyczne rekomendacje rozwiązań przydatnych dla osób operacyjnie odpowiedzialnych za zgodność danej instytucji z przepisami tego Rozporządzenia.

Publikacja porusza m.in. takie kwestie jak:
- proces identyfikacji funkcji krytycznych lub istotnych;
- kształt i sposób wypełniania rejestru informacji;
- klasyfikacja usług ICT;
- raportowanie, proces testowania odporności cyfrowej;
- relacje kontraktowe i ocena ryzyka stron trzecich;
- identyfikacja oraz zapobieganie incydentom, wymiana informacji o cyberzagrożeniach między podmiotami sektora finansowego;
- zależność między wymogami norm ISO, BSI a wymogami Rozporządzenia DORA.

Sformułowane w książce opinie dotyczące sposobu wdrożenia wymogów regulacyjnych uwzględniają doświadczenia zdobyte przez autorów w projektach wdrożeniowych zrealizowanych w największych instytucjach finansowych w Polsce.

Opracowanie przeznaczone jest dla dyrektorów i menadżerów compliance, działów bezpieczeństwa i IT oraz dla przedsiębiorców branży finansowej i IT.

Bartosz Bacia – doktor nauk prawnych; radca prawny; członek Rady Nadzorczej Armenia Stock Exchange; ekspert Europejskiego Kongresu Finansowego; przewodniczący Komitetu Compliance przy Giełdzie Papierów Wartościowych w Warszawie; współautor „Standardu antykorupcyjnego dla biznesu" UN Global Compact. W przeszłości pełnił funkcję wiceprzewodniczącego Komitetu Ładu Korporacyjnego OECD.

ZAMÓWIENIA:
INFOLINIA: +48 801 044 545
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

PRAKTYCZNE WDROŻENIE ROZPORZĄDZENIA DORA

redakcja naukowa Bartosz Bacia

Bartosz Bacia, Wojciech Dańczyszyn, Piotr Filipowski
Anna Jędrej-Giluń, Arkadiusz Kawulski, Magdalena Matysiak
Michał Mostowik, Adam Rasiński, Rafał Rudzki
Witold Srokosz, Paweł Szulik, Adam Woźniak

Wolters Kluwer

WARSZAWA 2025

Stan prawny na 1 maja 2025 r.

Wydawca
Anna Kubuj-Kacperek

Redaktor prowadzący
Paulina Ambroży

Opracowanie redakcyjne
Katarzyna Świerk-Bożek

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

ISBN 978-83-8390-679-9 *ISBN PDF-a: 978-83-8390-680-5*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów 7

Wstęp 11

Rafał Rudzki
Ramy zarządzania ryzykiem ICT 15

Arkadiusz Kawulski
Rejestr informacji jako element zarządzania ryzykiem ICT ze strony zewnętrznych dostawców usług ICT 41

Wojciech Dańczyszyn
Funkcja krytyczna lub istotna 89

Michał Mostowik
Definicja „usług ICT" w DORA 109

Paweł Szulik
Raportowanie informacji na gruncie DORA 149

Piotr Filipowski, Magdalena Matysiak
Zewnętrzni dostawcy usług ICT i relacje kontraktowe. Ocena ryzyka stron trzecich 179

Anna Jędrej-Giluń, Adam Rasiński
Testowanie operacyjnej odporności cyfrowej 223

Adam Woźniak
Incydenty – identyfikacja, ochrona, zapobieganie i wykrywanie 303

Paweł Szulik
Współpraca podmiotów finansowych w zakresie wymiany informacji o cyberzagrożeniach na gruncie DORA oraz innych przepisów 325

Witold Srokosz
Nadzór KNF nad podmiotami finansowymi w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego 347

Bartosz Bacia
Budowanie operacyjnej odporności cyfrowej na gruncie DORA a cyberodporność według norm ISO, standardów NIST oraz BSI 363

Bibliografia 395

Orzecznictwo 397

Autorzy 399

WYKAZ SKRÓTÓW

Akty prawne

DORA	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.Urz. UE L 333, s. 1 ze sprost.)
dyrektywa 2014/59/UE	–	dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z 15.05.2014 r. ustanawiająca ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniająca dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady 2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (Dz.Urz. UE L 173, s. 190 ze zm.)
dyrektywa NIS 2	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz. UE L 333, s. 80)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2024 r. poz. 1061 ze zm.)
pr. bank.	–	ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2024 r. poz. 1646 ze zm.)

RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1 ze sprost.)
rozporządzenie 2019/881	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15 ze zm.)
rozporządzenie 2024/1772	–	rozporządzenie delegowane Komisji (UE) 2024/1772 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów (Dz.Urz. UE L 2024/1772)
rozporządzenie 2024/1774	–	rozporządzenie delegowane Komisji (UE) 2024/1774 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT (Dz.Urz. UE L 2024/1774 ze sprost.)
rozporządzenie 2024/2956	–	rozporządzenie wykonawcze Komisji (UE) 2024/2956 z 29.11.2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji (Dz.Urz. UE L 2024/2956)

rozporządzenie 2025/302	–	rozporządzenie wykonawcze Komisji (UE) 2025/302 z 23.10.2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych formularzy, wzorów i procedur stosowanych przez podmioty finansowe do celów zgłaszania poważnych incydentów związanych z ICT i powiadamiania o znaczących cyberzagrożeniach (Dz.Urz. UE L 2025/302)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
u.n.r.f.	–	ustawa z 21.07.2006 r. o nadzorze nad rynkiem finansowym (Dz.U. z 2025 r. poz. 640 ze zm.)
u.o.i.f.	–	ustawa z 29.07.2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2024 r. poz. 722 ze zm.)
u.u.p.	–	ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2025 r. poz. 611 ze zm.)

Inne

BSI	–	Federalny Urząd ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik)
CEDUR	–	Centrum Edukacji dla Uczestników Rynku
CSIRT	–	zespół reagowania na incydenty bezpieczeństwa komputerowego (*Computer Security Incident Response Team*)
EBA	–	Europejski Urząd Nadzoru Bankowego (European Banking Authority)
EBC	–	Europejski Bank Centralny
EIOPA	–	Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (European Insurance and Occupational Pensions Authority)
ENISA	–	Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency)
ESMA	–	Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (European Securities and Markets Authority)
ICT	–	technologie informacyjne i komunikacyjne (*Information and Communication Technology*)
ISO	–	Międzynarodowa Organizacja Normalizacyjna (International Standards Organization)
IT	–	technologia informacyjna (*information technology*)

KNF	–	Komisja Nadzoru Finansowego
NBP	–	Narodowy Bank Polski
NIST	–	Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology)
TSUE/TS	–	Trybunał Sprawiedliwości Unii Europejskiej (przed 1.12.2009 r. jako Trybunał Sprawiedliwości)
WSA	–	wojewódzki sąd administracyjny

WSTĘP

W epoce, w której technologia przenika każdy aspekt naszego życia, odporność operacyjna stała się fundamentem stabilności sektora finansowego. Czynności maklerskie lub bankowe, które niegdyś miały formę pisemną, od dłuższego czasu są realizowane i dokumentowane w sposób cyfrowy. Nie będzie zatem przesadą stwierdzenie, że *de facto* całość relewantnych regulacyjnie procesów zachodzących w instytucjach finansowych znajduje swoje odzwierciedlenie w wymiarze cyfrowym. Ludwig Wittgenstein poczynił kiedyś trafną uwagę dotyczącą relacji między rzeczywistością a jej odwzorowaniem, wskazując, że: „Tak właśnie obraz jest powiązany z rzeczywistością; dosięga jej. Jest jak miara przyłożona do rzeczywistości. Tylko skrajne punkty podziałki dotykają mierzonego przedmiotu”[1].

Obraz cyfrowy instytucji finansowej jest z natury dynamiczny i narażony na takie zagrożenia, jak jego deformacja, uszkodzenie, a nawet utrata. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (*Digital Operational Resilience Act*, DORA), wprowadzone przez Unię Europejską, jest odpowiedzią na rosnące ryzyko związane z cyfryzacją usług i postępującą integracją technologii informacyjnych i komunikacyjnych (ICT). Jego głównym celem jest zapewnienie, że instytucje finansowe nie tylko potrafią skutecznie reagować na cyberzagrożenia,

[1] L. Wittgenstein, *Tractatus logico-philosophicus*, tłum. B. Wolniewicz, Warszawa 1970, 2.1511–2.1512.

ale również utrzymać ciągłość działania w obliczu zakłóceń technologicznych.

W niniejszym opracowaniu przyglądamy się nie tylko technicznym aspektom DORA, ale także wpływowi tego rozporządzenia na zarządzanie oraz kulturę korporacyjną instytucji finansowych. Przepisy DORA wprowadzają przełomowe standardy, które wyznaczają nowe granice w podejściu do zarządzania ryzykiem ICT, a także podkreślają znaczenie współpracy międzysektorowej w zakresie cyberbezpieczeństwa.

Naszym celem jest dostarczenie kompleksowego przewodnika, który pozwoli zrozumieć, jak wymogi DORA mogą zostać zaimplementowane w praktyce. Przybliżamy kluczowe obszary regulowane rozporządzeniem i analizujemy praktyczne wyzwania stojące przed instytucjami finansowymi w kontekście poprawnego wdrożenia jego przepisów.

W opracowaniu wiele miejsca poświęcono na wyjaśnienie podstawowych dla DORA pojęć, takich jak „ramy zarządzania ryzykiem ICT", „usługi ICT" czy „operacyjna odporność cyfrowa". Dystynkcje wprowadzane bowiem przez rozporządzenie na poziomie definicyjnym mają istotny wpływ na sposób wykładni i stosowania poszczególnych norm tego aktu prawnego.

Przepisy DORA kładą szczególny nacisk na *outsourcing* ICT i ocenę ryzyka stron trzecich, ustanawiając wiele wymagań w tym obszarze. Zarządzanie ryzykiem stron trzecich musi być integralnym elementem ogólnego zarządzania ryzykiem ICT firmy. Spółki nie mogą delegować swojej odpowiedzialności w tym zakresie. W opracowaniu Czytelnicy znajdą przydatne wskazówki dotyczące oceny ryzyka stron trzecich oraz zgodnego z DORA kształtowania relacji kontraktowych z dostawcami usług ICT.

Jednym z kluczowych wyzwań stawianych przez DORA instytucjom finansowym jest testowanie operacyjnej odporności cyfrowej. Rozporządzenie wymaga, by spółki ustanowiły rzetelny i kompleksowy program testowania operacyjnej odporności cyfrowej jako część swoich

ram zarządzania ryzykiem ICT. Problem ten jest w tym opracowaniu przedmiotem wieloaspektowej analizy, która z pewnością okaże się przydatna przy projektowaniu wewnętrznych ram dla przeprowadzenia wymaganych tym aktem prawnym testów TLPT.

Przepisy DORA statuują wymaganie, by spółki wdrożyły proces zarządzania incydentami ICT w celu wykrywania, zarządzania i powiadamiania o incydentach ICT, w tym identyfikowania ich przyczyn źródłowych. Rozporządzenie delegowane Komisji (UE) 2024/1772 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów określa siedem kryteriów klasyfikacji, a także progi identyfikacji poważnych incydentów związanych z ICT. Na podstawie tej klasyfikacji wymagane jest raportowanie właściwym organom przy użyciu specjalnego szablonu. Ten aspekt wdrożenia jest szczegółowo omówiony w sposób praktyczny i przystępny dla osób odpowiedzialnych za proces wdrożenia DORA w danej organizacji.

Wiele miejsca poświęcono w opracowaniu zagadnieniu relacji między wymogami DORA a zaleceniami zawartymi w takich normach, jak ISO, NIST oraz BSI oraz przedstawiono zakres przydatności tych norm w procesie wdrożenia przepisów rozporządzenia.

Oddawana do rąk Czytelników książka została napisana wyłącznie przez praktyków. Jej autorzy kierowali projektami wdrożenia DORA w największych instytucjach finansowych w Polsce lub pełnili rolę kluczowych doradców w takich projektach. Dlatego w uwagach i ocenach w niej zawartych uwzględniono unikalną sumę doświadczeń zebranych w trakcie realizacji procesów wdrożeniowych, jak również perspektywę wyniesioną z dialogu z organami nadzoru zarówno na poziomie europejskim, jak i krajowym. Praktyka stosowania przepisów DORA dopiero się kształtuje, dlatego możliwe jest, że opinie wyrażone w opracowaniu w toku życia tego aktu prawnego mogą ulec zmianie. Autorzy dołożyli

jednak wszelkich starań, by były one aktualne w dacie publikacji książki i wpisywały się w *consensus* regulacyjny dotyczący wykładni przepisów DORA, biorący pod uwagę stanowiska Europejskich Organów Nadzoru, jak również wiodących organizacji branżowych w Unii Europejskiej.

Bartosz Bacia

Rafał Rudzki

RAMY ZARZĄDZANIA RYZYKIEM ICT

1. Wprowadzenie

„Ramy zarządzania ryzykiem ICT" to obok „operacyjnej odporności cyfrowej", użytej w samym tytule regulacji, kluczowe pojęcie dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011. Zarządzanie ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT) znalazło się na pierwszym miejscu ogólnej listy wymogów mających zastosowanie do podmiotów finansowych, o których mowa w art. 1 ust. 1 lit. a DORA, a następnie został mu poświęcony cały rozdział II regulacji, czyniąc z tego obszaru pierwszy z pięciu filarów rozporządzenia. Jednocześnie można zaryzykować stwierdzenie, że ten właśnie filar charakteryzuje się nie tylko największą złożonością, ale jednocześnie stanowi uogólnione „ramy" mieszczące w sobie również pozostałe obszary, tj. zarządzanie incydentami związanymi z ICT, testowanie operacyjnej odporności cyfrowej, zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT oraz ustalenia dotyczące wymiany informacji.

Przed rozważeniem tego, jak „ramy zarządzania ryzykiem związanym z ICT" powinny być skonstruowane, warto przywołać definicję „ryzyka związanego z ICT" zawartą w rozporządzeniu, zgodnie z którą pojęcie to oznacza każdą dającą się racjonalnie określić okoliczność związaną

z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, bezpieczeństwu operacji i procesów lub świadczeniu usług przez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym. Z perspektywy podmiotów finansowych tak opisany obszar bezpieczeństwa ICT i odporności cyfrowej stanowi część dobrze im znanego „ryzyka operacyjnego", które było przez lata definiowane jako ryzyko straty wynikające z nieodpowiednich lub zawodnych procedur wewnętrznych, błędów ludzi i systemów lub ze zdarzeń zewnętrznych[1]. Obszar „błędów systemów" niewątpliwie obejmował zawsze ryzyko związane z technologią informatyczną, bezpieczeństwem informacji i ciągłością funkcjonowania, a w warunkach postępującej cyfryzacji usług finansowych oraz stałego wzrostu poziomu zagrożeń w cyberprzestrzeni, z którymi mamy do czynienia na przestrzeni ostatnich lat, kwestie związane z ICT mogły nawet zyskać czołowe znaczenie w profilach ryzyka operacyjnego podmiotów finansowych.

Uzasadnienia zawarte w preambule DORA wydają się w pełni potwierdzać, że ryzyko związane z ICT było i jest częścią ryzyka operacyjnego,

[1] Przywołana definicja, która przez lata stanowiła najbardziej kanoniczne ujęcie ryzyka operacyjnego w sektorze finansowym, pochodzi z art. 4 ust. 1 pkt 52 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z 26.06.2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych, zmieniającego rozporządzenie (UE) nr 648/2012 (Dz.Urz. UE L 176, s. 1 ze zm.). Do przepisów unijnych została ona przeniesiona z wytycznych Komitetu Bazylejskiego ds. Nadzoru Bankowego, który na przełomie XX i XXI w. dostrzegł konieczność przywiązania większej uwagi do zarządzania innymi kategoriami ryzyka niż kredytowym i rynkowym, na których wówczas wyłącznie koncentrowały się instytucje finansowe. Obecnie mamy do czynienia z trochę analogiczną sytuacją opartą na przeświadczeniu, że w ramach ryzyka operacyjnego niewystarczająco skutecznie zarządzane było ryzyko związane z ICT, którego znaczenie istotnie wzrosło wraz z coraz większym wpływem technologii cyfrowych na sektor finansowy. Warto więc zaznaczyć, że w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1623 z 31.05.2024 r. w sprawie zmiany rozporządzenia (UE) nr 575/2013 w odniesieniu do wymogów dotyczących ryzyka kredytowego, ryzyka związanego z korektą wyceny kredytowej, ryzyka operacyjnego, ryzyka rynkowego oraz minimalnego progu kapitałowego (Dz.Urz. UE L 2024/1623 ze sprost.) definicja ryzyka operacyjnego została rozszerzona w ten sposób, że obejmuje w szczególności „ryzyko związane z technologiami informacyjno-komunikacyjnymi (ICT)".

natomiast jedną z kluczowych obaw tam wyrażonych jest to, że przepisy dotyczące ryzyka operacyjnego, jeżeli zostały szerzej rozwinięte w wybranych unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do zwalczania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie ukierunkowanym przepisom jakościowym dotyczącym zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania sprawności i odbudowy w odniesieniu do incydentów związanych z ICT lub zdolności w zakresie sprawozdawczości i testowania cyfrowego. Zrozumiałą tego konsekwencją jest zatem przepis art. 6 ust. 2 DORA, który „ramom zarządzania ryzykiem związanym z ICT" nakazuje obejmować co najmniej „strategie, polityki, procedury, protokoły i narzędzia ICT niezbędne do należytej i odpowiedniej ochrony wszystkich zasobów informacyjnych i zasobów ICT, w tym oprogramowania i sprzętu komputerowego, serwerów, a także wszystkich odpowiednich elementów fizycznych i infrastruktury, takich jak obiekty, ośrodki przetwarzania danych i wyznaczone obszary wrażliwe, w celu zapewnienia odpowiedniej ochrony wszystkich zasobów informacyjnych i zasobów ICT przed ryzykiem, w tym przed uszkodzeniem i nieuprawnionym dostępem lub użytkowaniem".

2. Ryzyko związane z ICT a ogólny system zarządzania ryzykiem

Zgodnie z przepisami DORA podmioty finansowe dysponują solidnymi, kompleksowymi i dobrze udokumentowanymi ramami zarządzania ryzykiem związanym z ICT jako częścią swojego ogólnego systemu zarządzania ryzykiem, który należy rozumieć jako obejmujący wszelkie rodzaje ryzyka, na które może być narażona działalność podmiotu finansowego.

Jednocześnie „ryzyko", które w kontekście kierowania i nadzorowania organizacją jest powszechnie definiowane jako „wpływ niepewności

na cele", zgodnie z powszechnie stosowanymi standardami[2] wymaga zastosowania następującego ramowego schematu działań składających się na proces zarządzania nim:

1) ustanawianie kontekstu (określanie strategicznych celów organizacji, realizowanych procesów, wewnętrznej struktury, wszelkich zewnętrznych uwarunkowań etc.);
2) szacowanie ryzyka, obejmujące kolejno:
   – identyfikowanie ryzyka (proces wyszukiwania, rozpoznawania i opisu ryzyka),
   – analizę ryzyka (proces określenia poziomu ryzyka, wyrażonego często jako kombinacja następstw oraz ich prawdopodobieństw),
   – ocenę ryzyka (proces porównania wyników analizy ryzyka z przyjętymi kryteriami w celu stwierdzenia, czy jego poziom jest akceptowany);
3) postępowanie z ryzykiem (m.in. akceptacja, ograniczanie, unikanie lub transfer ryzyka).

Po zastosowaniu określonych środków związanych z postępowaniem z ryzykiem pozostaje tzw. ryzyko rezydualne (zwane również szczątkowym), o którym będzie jeszcze mowa w dalszej części niniejszego opracowania z uwagi na konkretne wymogi przepisów DORA odnoszące się do tak nazwanego ryzyka. Tymczasem warto zauważyć, że sercem przedstawionego wyżej schematu zarządzania ryzykiem, realizowanego w zamkniętym cyklu wymienionych czynności poddanych regularnemu monitorowaniu i przeglądowi, jest proces szacowania ryzyka, który co do zasady pozwala danej organizacji ustalić poziom poszczególnych ryzyk z uwzględnieniem specyficznego dla siebie kontekstu i uwarunkowań,

[2] Mowa tu o międzynarodowej normie zarządzania ryzykiem ISO 31000 „Zarządzanie ryzykiem – wytyczne", której założenia zostały w szczególności przeniesione do rodziny norm bezpieczeństwa informacji zbudowanych wokół ISO/IEC 27001 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania". Do tej ostatniej powrócimy jeszcze w dalszej części niniejszego rozdziału, przywołując metodykę zarządzania ryzykiem w bezpieczeństwie informacji jako jedną z możliwych do wykorzystania na potrzeby szacowania ryzyka związanego z ICT.

a następnie dobrać mechanizmy postępowania z ryzykiem stosownie do dokonanych oszacowań.

Praktyczną implementację takiego sposobu myślenia o zarządzaniu ryzykiem w organizacji wydaje się na przykład rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zgodnie z którym administrator wdraża odpowiednie środki techniczne i organizacyjne uwzględniając charakter, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Jednocześnie same przepisy RODO bardzo niewiele mówią o szczegółach związanych z rodzajem dostępnych środków i sposobie ich doboru.

Na tym tle DORA przedstawia się jako rozbudowana lista szczegółowych wytycznych służących zapewnieniu bezpieczeństwa ICT i odporności cyfrowej. Co prawda w art. 4 DORA mowa jest o zasadzie proporcjonalności, zgodnie z którą podmioty finansowe stosują poszczególne przepisy, biorąc pod uwagę swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności swoich usług, działań i operacji, jednak trudno oprzeć się wrażeniu, że wymogi odnoszące się do „ram zarządzania ryzykiem związanym z ICT" koncentrują się wprost na określeniu zestawu mechanizmów postępowania z tym ryzykiem, które zostało niejako uniwersalnie oszacowane dla podmiotów finansowych podlegających pod rozporządzenie i w związku z tym dobór tych mechanizmów może być z góry określony.

3. Jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych

Sama treść DORA w art. 6–16 przedstawia jeszcze dość ogólne wymogi dotyczące sposobu postępowania z ryzykiem ICT, identyfikując już jednak konkretne obszary, takie jak: polityki i procedury tworzenia kopii zapasowych oraz metody i procedury przywracania oraz odzy-

skiwania danych czy ochrona i zapobieganie, obejmujące wdrażanie zautomatyzowanych mechanizmów izolowania zasobów informacyjnych na wypadek cyberataków oraz polityki i protokołów dotyczących silnych mechanizmów uwierzytelniania, opartych na odpowiednich standardach i specjalnych systemach kontroli oraz środkach ochrony kluczy kryptograficznych.

Kluczową kwestią jest jednak dalsza harmonizacja narzędzi, metod, procesów i polityk zarządzania ryzykiem związanym z ICT, przewidziana w art. 15 DORA, która została zrealizowana w rozporządzeniu delegowanym Komisji (UE) 2024/1774 z 13.03.2024 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT.

Wymogi zawarte we wskazanym akcie prawnym, obowiązujące podmioty finansowe nieobjęte tzw. uproszczonymi ramami zarządzania ryzykiem związanym z ICT, zostały ułożone w następującą strukturę odzwierciedloną w rozdziałach, sekcjach i artykułach:

1) Polityki, procedury, protokoły i narzędzia w zakresie bezpieczeństwa ICT:
   a) Ogólne elementy polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT,
   b) Zarządzanie ryzykiem związanym z ICT,
   c) Zarządzanie zasobami ICT:
      – Polityka zarządzania zasobami ICT,
      – Procedura zarządzania zasobami ICT,
   d) Szyfrowanie i kryptografia:
      – Mechanizmy kontroli szyfrowania i kryptograficznej,
      – Zarządzanie kluczami kryptograficznymi,
   e) Bezpieczeństwo operacji ICT:
      – Polityki i procedury dotyczące operacji ICT,
      – Zarządzanie pojemnością i wydajnością,
      – Zarządzanie podatnościami i poprawkami,
      – Bezpieczeństwo danych i systemów,
      – Rejestrowanie,

   f) Bezpieczeństwo sieci:
      – Zarządzanie bezpieczeństwem sieci,
      – Zabezpieczenie przesyłanych informacji,
   g) Zarządzanie projektami ICT i zmianą w systemach ICT:
      – Zarządzanie projektami ICT,
      – Pozyskiwanie, rozwój i utrzymanie systemów ICT,
      – Zarządzanie zmianą w systemach ICT,
   h) Bezpieczeństwo fizyczne i środowiskowe;
2) Polityka kadrowa i kontrola dostępu:
   – Polityka kadrowa,
   – Zarządzanie tożsamością,
   – Kontrola dostępu;
3) Wykrywanie incydentów związanych z ICT i reagowanie na nie:
   – Polityka zarządzania incydentami związanymi z ICT,
   – Wykrywanie nietypowych działań i kryteria wykrywania incydentów związanych z ICT oraz reagowania na nie;
4) Zarządzanie ciągłością działania w zakresie ICT:
   – Elementy strategii na rzecz ciągłości działania w zakresie ICT,
   – Testowanie planów ciągłości działania w zakresie ICT,
   – Plany reagowania i przywracania sprawności ICT;
5) Sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT (format i treść).

Dla pozostałych podmiotów finansowych, objętych uproszonymi ramami zarządzania ryzykiem związanym z ICT, przewidziano natomiast następującą strukturę wymogów zapisaną w rozdziałach i artykułach:

1) Uproszczone ramy zarządzania ryzykiem związanym z ICT:
   – Zarządzanie i organizacja,
   – Polityka i środki bezpieczeństwa informacji,
   – Klasyfikacja zasobów informacyjnych i zasobów ICT,
   – Zarządzanie ryzykiem związanym z ICT,
   – Bezpieczeństwo fizyczne i środowiskowe;
2) Dalsze elementy systemów, protokołów i narzędzi minimalizujących wpływ ryzyka związanego z ICT:
   – Kontrola dostępu,
   – Bezpieczeństwo operacji ICT,
   – Bezpieczeństwo danych, systemu i sieci,

   - Testy bezpieczeństwa ICT,
   - Pozyskiwanie, rozwój i utrzymanie systemów ICT,
   - Zarządzanie projektami ICT i zmianą w systemach ICT;
3) Zarządzanie ciągłością działania w zakresie ICT:
   - Elementy planu ciągłości działania w zakresie ICT,
   - Testowanie planów ciągłości działania;
4) Sprawozdanie z przeglądu uproszczonych ram zarządzania ryzykiem związanym z ICT (format i treść).

To, co powinno być widoczne na pierwszy rzut oka, to podobieństwo przedstawionych wyżej opisów do struktury znanych standardów lub wytycznych nadzorczych w zakresie bezpieczeństwa informacji. Jeśli chodzi o takie standardy, to niewątpliwie dobrym przykładem jest załącznik do normy ISO/IEC 27001 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania", zawierający wzorcowy wykaz zabezpieczeń (mechanizmów kontrolnych) i celów ich stosowania, których rozbudowany opis i specyfikację zawiera norma ISO/IEC 27002 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji"[3].

W zakresie przykładowych wytycznych nadzorczych, wykazujących zbieżność ze strukturą ram zarządzania ryzykiem ICT, można natomiast przytoczyć Rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, wydaną przez Komisję Nadzoru Finansowego wraz z zestawem analogicznych „Wytycznych" dotyczących tego samego obszaru, skierowanych do pozostałych grup nadzorowanych podmiotów

[3] W 2022 r. zostały opublikowane nowe edycje ISO/IEC 27001 i ISO/IEC 27002, w których dotychczasowa struktura wykazu zabezpieczeń (mechanizmów kontrolnych) i celów ich stosowania została całkowicie przebudowana i oparta już nie na kilkunastu grupach tematycznych (przypominających strukturę omawianego regulacyjnego standardu technicznego do DORA), tylko na cztery sekcje odpowiadające zabezpieczeniom: organizacyjnym (*organisational controls*), osobowym (*people controls*), fizycznym (*physical controls*) oraz technologicznym (*technological controls*). Należy jednak podkreślić, że zmiana dotyczy jedynie sposobu pogrupowania mechanizmów kontrolnych, których lista i zakres przedmiotowy nie uległy istotnym zmianom.

finansowych (spółdzielczych kas oszczędnościowo-kredytowych, firm inwestycyjnych, towarzystw funduszy inwestycyjnych, powszechnych towarzystw emerytalnych oraz podmiotów infrastruktury rynku kapitałowego). Jednocześnie, mając właśnie na względzie wspomnianą zbieżność z obowiązkami wynikającymi z DORA, Komisja Nadzoru Finansowego uchyliła wszystkie wymienione wyżej wytyczne, zanim 17.01.2025 r. rozporządzenie zaczęło być stosowane.

Z jednej więc strony zakres tematyczny objęty opisem ram zarządzania ryzykiem ICT zawartym w DORA oraz w powiązanym z nim aktem wykonawczym – rozporządzeniem 2024/1774 nie jest niczym nowym dla regulowanych podmiotów finansowych, które nierzadko latami budowały i doskonaliły swoje systemy zarządzania bezpieczeństwem informacji w oparciu o międzynarodowe standardy lub wytyczne organów nadzorczych. Z drugiej jednak strony szczegółowe wymogi zawarte w normach i wytycznych stanowiły dotychczas tzw. miękkie prawo, natomiast po wejściu w życie przepisów DORA mamy do czynienia z analogicznymi opisami wymaganych mechanizmów postępowania z ryzykiem związanym z ICT, które stały się już jednak tzw. twardym prawem.

Z powyższej obserwacji wyłania się fundamentalna refleksja dotycząca specyfiki DORA, którą można podsumować tak, że wymogi dotyczące bezpieczeństwa informacji zostały w rozporządzeniu potraktowane ze szczegółowością znacznie przekraczającą jakiekolwiek znane dotychczas przepisy prawa obowiązujące podmioty finansowe.

Co więcej, normy lub wytyczne, abstrahując od ich charakteru jako miękkiego prawa, formułowane były co do zasady dość elastycznie, zakładając konieczność ich implementacji z uwzględnieniem specyficznego kontekstu danej organizacji i dokonanego przez nią szacowania ryzyka. Dlatego szczególnym wyzwaniem wydają się twarde obecnie wymagania przepisów DORA, które bardzo sztywno regulują wiele elementów, czego dowodzą poniższe przykłady pochodzące z rozporządzenia 2024/1774:

– podmioty finansowe co najmniej raz w tygodniu przeprowadzają zautomatyzowane skanowanie pod kątem podatności oraz oceny

podatności zasobów ICT w odniesieniu do zasobów ICT wspierających krytyczne lub istotne funkcje (art. 10 ust. 2);
– w przypadku systemów ICT, które wspierają krytyczne lub istotne funkcje, podmioty finansowe weryfikują adekwatność obowiązujących reguł zapory sieciowej i filtrów połączeń co najmniej raz na 6 miesięcy (art. 13);
– podmioty finansowe przynajmniej raz na 6 miesięcy dokonują aktualizacji praw dostępu w odniesieniu do systemów ICT wspierających krytyczne lub istotne funkcje (art. 21 lit. e).

Podsumowując, przepisy DORA nie tylko zamieniają wiele dotychczasowych standardów dostępności, autentyczności, integralności i poufności danych w twarde przepisy prawa, ale w wielu miejscach idą nawet o krok dalej, sztywno określając pewne parametry dotyczące stosowania poszczególnych mechanizmów kontroli ryzyka związanego z ICT.

Praktyczna wskazówka
Przepisy DORA stanowią obecnie źródło wymogów, których zaimplementowanie staje się konieczne w ramach systemu zarządzania bezpieczeństwem informacji podmiotu finansowego podlegającego pod rozporządzenie, jednak nie oznacza to, że standardy takie jak ISO/IEC 27001 przestają być wyznacznikiem ogólnych ram budowania takich systemów. Jeśli dany podmiot finansowy opiera się od lat na ISO (lub analogicznym standardzie), to warto przy nim pozostać, ale mieć na ten standard zmapowane wymogi DORA. Wówczas przy przeglądzie systemu zarządzania bezpieczeństwem informacji (np. pod kątem nowej edycji standardu) można rozważać aktualizację poszczególnych mechanizmów kontrolnych co do zasady stosownie do własnych szacunków ryzyka, natomiast tam, gdzie dają o sobie znać przepisy DORA, przyjąć bardziej sztywne podejście.

4. Ryzyko rezydualne, tolerancja ryzyka oraz inne elementy dotyczące poziomu ryzyka ICT

Podtrzymując wcześniejsze stwierdzenie, że wymogi DORA odnoszące się do „ram zarządzania ryzykiem związanym z ICT" wydają się koncentrować głównie na określeniu zestawu konkretnych mechanizmów postępowania z poszczególnymi źródłami (czynnikami) tego ryzyka, nie można jednak pominąć tego, że szacowanie ryzyka związanego z ICT, w tym ewidencjonowanie jego zmian w czasie, jest również obowiąz-

kiem nałożonym na podmioty finansowe (w szerszym zakresie na te niebędące mikroprzedsiębiorstwami).

Szczegółowo przedstawia to art. 3 rozporządzenia 2024/1774, zgodnie z którym polityki i procedury zarządzania ryzykiem związanym z ICT muszą obejmować wszystkie poniższe elementy:

1) wskazanie zatwierdzenia poziomu tolerancji ryzyka;
2) procedurę i metodykę przeprowadzania oceny ryzyka (w oparciu o podatności i zagrożenia) oraz pomiaru wpływu i prawdopodobieństwa ich wystąpienia (w oparciu o wskaźniki ilościowe lub jakościowe);
3) procedurę określania, wdrażania i dokumentowania środków traktowania ryzyka związanego z ICT;
4) w odniesieniu do rezydualnego ryzyka związanego z ICT:
   - sposób jego identyfikacji,
   - podział ról i obowiązków w procesie akceptacji rezydualnego ryzyka, które przekracza ustalony poziom tolerancji,
   - opracowanie wykazu akceptowalnego ryzyka wraz z uzasadnieniami jego akceptacji,
   - zasady dotyczące przeglądu akceptowalnego rezydualnego ryzyka co najmniej raz w roku;
5) zasady dotyczące monitorowania między innymi wszelkich zmian ryzyka związanego z ICT i krajobrazu cyberzagrożeń;
6) zasady dotyczące procesu zapewniającego uwzględnienie wszelkich zmian w strategii biznesowej i strategii operacyjnej odporności cyfrowej podmiotu finansowego.

Jedną z przykładowych metodyk, które nasuwają się w kontekście zarządzania ryzykiem związanym z ICT, jest zarządzanie ryzykiem w Systemach Bezpieczeństwa Informacji zgodnie z ISO/IEC 27005, tj. normą z tej samej rodziny co wspomniane już w tym opracowaniu ISO/IEC 27001 i ISO/IEC 27002. Podstawowe założenia dotyczące procesu zarządzania ryzykiem, leżące u podstaw tej metodyki, zostały już wcześniej przedstawione przy okazji rozważań nad osadzeniem zarządzania ryzykiem związanym z ICT w ogólnym systemie zarządzania ryzykiem. Bardziej szczegółowe postanowienia tam zawarte obejmują w szczególności: identyfikowanie aktywów, identyfikowanie zagrożeń,

identyfikowanie podatności, identyfikowanie następstw, szacowanie następstw, szacowanie prawdopodobieństwa incydentu, określanie poziomu ryzyka, postępowanie z ryzykiem w bezpieczeństwie informacji oraz kryteria akceptowania ryzyka rezydualnego. Lista ta wydaje się pokrywać wszystkie kluczowe elementy procesu zarządzania ryzykiem wymienione w art. 3 rozporządzenia 2024/1774.

Norma ISO/IEC 27005 zakłada również, że proces analizy ryzyka w wielu jego aspektach może być realizowany zarówno metodami jakościowymi, jak i ilościowymi, co pokrywa się z oczekiwaniami wskazanego wyżej rozporządzenia, które dopuszcza, aby pomiar wpływu i prawdopodobieństwa wystąpienia podatności i zagrożeń przeprowadzany był w oparciu o wskaźniki jakościowe lub ilościowe.

Co najmniej dwa argumenty przemawiają za tym, że bardziej praktyczne zastosowanie w analizie ryzyka ICT znajdą przede wszystkim metody jakościowe. Po pierwsze, ryzyko operacyjne (w tym ryzyko związane z ICT) należy co do zasady uznać za trudno mierzalne, w szczególności jeśli niezbędne jest zapewnienie analizy wielu indywidualnych źródeł (czynników) ryzyka, z których znaczna część charakteryzuje się bardzo niskim prawdopodobieństwem materializacji, a zatem trudno poddającym się analizie ilościowej wykorzystującej często dane historyczne o incydentach. Po drugie, wspomniane już we wprowadzeniu do tego opracowania uzasadnienia zawarte w preambule DORA sugerują niewystarczalność tradycyjnego ilościowego podejścia do zwalczania ryzyka oraz potrzebę zapewnienia w tym zakresie ukierunkowanych przepisów jakościowych.

Niewątpliwie każdy podmiot finansowy posiada swobodę wyboru konkretnej metodyki szacowania ryzyka związanego z ICT i w szczególności nie musi to być metodyka ściśle oparta na żadnym istniejącym standardzie (w tym ISO/IEC 27005 przywołanym tu jedynie jako przykład), tylko na przykład na wewnętrznie zbudowanym modelu, w tym stanowiącym część bardziej ogólnego modelu pokrywającego szerszy zakres czynników ryzyka operacyjnego, jeśli ten tylko pozwala realizować wymogi wskazane w przepisach DORA. Oznacza to również, że ilościowa analiza ryzyka, choć wyżej zasugerowano jej mniejsze praktyczne

zastosowanie w obszarze zarządzania ryzykiem związanym z ICT, może również okazać się efektywnym narzędziem, w tym zastosowanym jako składnik mieszanej metodyki analizy, czerpiącej to, co najlepsze z podejścia jakościowego i ilościowego.

Przykładową koncepcją zintegrowania obydwu tych podejść może być oparcie procesu szacowania wpływu i prawdopodobieństwa zdarzeń materializujących ryzyko na trzech elementach, które kolejno uzupełniają informację na temat poziomu ryzyka:

1) statystyce dotyczącej incydentów związanych z ICT w odniesieniu do danej kategorii zagrożeń i podatności, uwzględniającej liczbę tych incydentów w zadanym okresie i ich przeciętny wpływ na organizację;
2) kluczowych wskaźnikach ryzyka, dostarczających ilościowych informacji nie o zmaterializowanym ryzyku, ale na podstawie których można wnioskować o wysokości wpływu lub prawdopodobieństwa dla danego czynnika ryzyka związanego z ICT (takich jak liczba i klasyfikacja podatności wykrytych podczas skanowania infrastruktury IT, które mogą sugerować poziom ryzyka wystąpienia udanych cyberataków);
3) eksperckich (czyli typowo jakościowych) szacunkach wpływu i prawdopodobieństwa, uzupełniających lukę wynikającą z zakładanego braku wystarczających danych ilościowych, pozwalających określić poziom każdego ryzyka (tj. wskazanych w dwóch poprzednich punktach).

Integracja wymienionych wyżej podejść w jednym modelu może zostać osiągnięta dzięki konwersji ustaleń co do poziomu ryzyka na wspólną skalę wskaźników wpływu i prawdopodobieństwa, niezależnie którą z powyższych metod ustalenia te zostały dokonane. Przykładowo pięciostopniowa skala prawdopodobieństwa ujęta opisowo („bardzo niskie", „niskie", „średnie", „wysokie", „bardzo wysokie"), jeśli została zmapowana na wskaźniki ilościowe („raz na 25 lat", „raz na 10 lat", „raz na 4 lata", „raz na rok", „raz na kwartał"), pozwala na przyporządkowywanie prawdopodobieństwa oszacowanego w sposób ilościowy jednoznacznie do jednego ze swoich pięciu stopni. Jednocześnie tą samą skalą będzie można posługiwać się w ramach eksperckiej samooceny ryzyka, w której

wybór jednego ze stopni następuje w sposób bardziej intuicyjny. Stosując następnie powszechne podejście polegające na przypisaniu poszczególnym stopniom skali jakościowej wartości liczbowych (np. od 1 dla „bardzo niskie" do 5 dla „bardzo wysokie"), które ułatwiają dalszą obróbkę danych w ramach analizy ryzyka[4], otrzymujemy uniwersalny wskaźnik, pozwalający szacować prawdopodobieństwo zarówno subiektywnie, jak i w oparciu o dane ujęte bardziej obiektywnie. W analogiczny sposób możemy podejść do szacowania wpływu, przyjmując również pięciostopniową skalę opisową oraz odpowiadające im pomocnicze kategorie ilościowe (np. oparte na wysokości potencjalnych strat). Na koniec poziom ryzyka, tradycyjnie definiowany jako kombinacja następstw oraz ich prawdopodobieństw, obliczamy jako iloczyn wskaźników prawdopodobieństwa i wpływu, co przy zastosowaniu pięciostopniowej skali dla każdego z nich (przyjmującej wartości od 1 do 5), daje wskaźnik ryzyka przyjmujący wartości od 1 do 25.

Te co do zasady nieskomplikowane i powszechnie stosowane od lat koncepcje powinny okazać się całkowicie wystarczające na potrzeby szacowania ryzyka związanego z ICT, w tym ewidencjonowania jego zmian w czasie oraz ocenę względem ustalonych poziomów tolerancji, jeśli zostaną spełnione następujące warunki:

1) w ramach szacowania ryzyka zostaną uwzględnione działające mechanizmy kontrolne (środki postępowania z ryzykiem), które mitygują materializację danego czynnika ryzyka, tak aby w wyniku szacowania określić poziom ryzyka rezydualnego;
2) zostaną zidentyfikowane co do zasady wszystkie źródła (czynniki) ryzyka związanego z ICT, w tym przez analizę wpływu dających się racjonalnie określić zagrożeń i podatności na bezpie-

[4] Zabieg polegający na przypisaniu kategoriom jakościowym wartości liczbowych mógłby wydawać się formą zamiany podejścia jakościowego do analizy ryzyka na podejście ilościowe. W szczególności pozwala on na dalszą obróbkę danych na temat poziomu ryzyka poprzez operacje matematyczne, natomiast w istocie operacje te będą jedynie narzędziem ułatwiającym agregowanie, uśrednianie czy porównywanie poziomów ryzyka. Natomiast tak długo jak informacje na temat szacowanego wpływu czy prawdopodobieństwa są uzyskane w oparciu o przypisanie do skali opisowej, nawet wykonując później obliczenia na wartościach liczbowych odpowiadających poszczególnym poziomom skali, pozostajemy nadal w kręgu jakościowej analizy ryzyka.

czeństwo sieci i systemów informatycznych, które przekłada się na bezpieczeństwo operacji i procesów lub świadczenia usług;

3) identyfikacja i szacowanie ryzyk zostaną przeprowadzone względem wszystkich procesów realizowanych przez podmiot finansowy z uwzględnieniem wyników analizy wpływu na działalność (*Business Impact Analysis*, BIA), co powinno korespondować z ustaleniami dotyczącymi określenia funkcji krytycznych lub istotnych podmiotu, zgodnie z ich definicją zawartą w art. 3 pkt 22 DORA;
4) uzyskana macierz oszacowanych poziomów ryzyka, domyślnie zbudowana w oparciu o listę procesów biznesowych (lub opcjonalnie o listę aktywów ICT, od których zależy realizacja tych procesów) oraz listę źródeł (czynników) ryzyka, będzie charakteryzowała się możliwie najbardziej optymalnym poziomem granulacji (zarówno procesów, jak i ryzyk), tak aby zapewnić zarówno prawidłowe zaadresowanie i zarządzanie konkretnymi zagadnieniami, ale też zbyt dużym poziomem szczegółowości nie sprawić, że przyjęty model okaże się dla organizacji praktycznie nieużyteczny;
5) wdrożona koncepcja określania wysokości wskaźników prawdopodobieństwa i wpływu, a na ich podstawie poziomu ryzyka, będzie w maksymalnym stopniu wolna od wad prowadzących do tworzenia fałszywego obrazu ryzyka, w tym ze względu na błędy w samej koncepcji kalkulacji wskaźników lub też typowe tendencje do jego niedoszacowania bądź przeszacowania w procesie samooceny.

Praktyczna wskazówka
Jeden z najbardziej powszechnych błędów w koncepcjach kalkulacji poziomu ryzyka jako iloczynu wskaźników prawdopodobieństwa i wpływu powstaje wówczas, gdy użycie tej prostej formuły nałoży się na nieodpowiednio dobrane skale tych wskaźników. Przyjmijmy, że w pięciostopniowej skali prawdopodobieństwa na najniższym stopniu (oznaczonym wartością 1) mamy „raz na 25 lat", a na najwyższym stopniu (oznaczonym wartością 5) mamy „kilka razy w roku". Jednocześnie w pięciostopniowej skali wpływu na najniższym stopniu (oznaczonym wartością 1) mamy „znikomy wpływ", a jej najwyższemu stopniowi (oznaczonemu wartością 5) przypiszemy „katastrofalne skutki". Wówczas poziom ryzyka równy 5 uzyskamy zarówno dla incydentów o katastrofalnych skutkach mogących wystąpić raz na 25 lat (jako iloczyn 1 x 5), jak i dla powtarzających się kilka razy w roku zdarzeń pozostających bez praktycznego wpływu na działalność (jako iloczyn 5 x 1). W rezultacie musielibyśmy traktować tak samo istotne ryzyka, z których wiele charakteryzuje się bardzo niskim prawdopodobieństwem wystąpienia i bardzo dotkliwymi skutkami, jak niegroźne sytuacje obserwowane na co dzień. Ten konkretny błąd można usunąć przez odpowiednie dobranie skal prawdopodobieństw i wpływu, ewentualnie przez modyfikację wzoru na wyliczenie poziomu ryzyka (tak aby wpływ odegrał w nim większe znaczenie). Przede wszystkim zaś należy pamiętać, że jeśli nie wyeliminujemy takiej lub innej wady przyjętego modelu szacowania, proces zarządzania ryzykiem związanym z ICT nie będzie skupiał się na realnych celach zapewniania cyfrowej odporności.

Przywołując ponownie potrzebę wyrażoną w preambule DORA, dotyczącą zapewnienia ukierunkowanych przepisów jakościowych na potrzeby mitygowania ryzyka związanego z ICT, oszacowany w przyjętym modelu poziom danego ryzyka może jeszcze wymagać typowo jakościowej (merytorycznej) weryfikacji. Przeprowadzenie takiej szczegółowej weryfikacji może być trudne dla wszystkich elementów macierzy ryzyka, ale wydaje się ona generalnie nieunikniona nie tylko wobec przypadków, w których wskaźniki sygnalizują przekroczenie poziomów tolerancji (gdzie trzeba zdecydować o akceptacji lub określeniu środków traktowania ryzyka), ale również w sytuacjach, w których wyniki szacowania w określonych punktach macierzy ryzyka mogą wydawać się zaniżone.

5. Funkcja kontroli odpowiedzialna za zarządzanie ryzykiem związanym z ICT

Zgodnie z art. 6 ust. 4 zdanie pierwsze DORA podmioty finansowe inne niż mikroprzedsiębiorstwa powierzają obowiązek zarządzania ryzykiem związanym z ICT i nadzór nad nim funkcji kontroli oraz zapewniają odpowiedni poziom niezależności takiej funkcji kontroli w celu uniknięcia konfliktów interesów. Jednocześnie zdanie drugie tego artykułu stanowi, że podmioty finansowe zapewniają odpowiednie rozdzielenie i niezależność funkcji zarządzania ryzykiem związanym z ICT, funkcji kontroli oraz funkcji audytu wewnętrznego, zgodnie z modelem trzech linii obrony lub wewnętrznym modelem zarządzania ryzykiem i kontroli ryzyka.

Sposób sformułowania wspomnianego przepisu, w szczególności potencjalne sprzeczności w opisach relacji między „funkcją zarządzania ryzykiem związanym z ICT" a „funkcją kontroli", mogą wprowadzać nieco zamieszania w rozważaniach nad koncepcją właściwej organizacji zarządzania ryzykiem związanym z ICT w podmiocie finansowym. Warto jednak spróbować w miarę możliwości rozwiać ewentualne wątpliwości co do rozumienia powyższych zapisów.

Po pierwsze, należy przywołać wytyczne w sprawie zarządzania wewnętrznego (*internal governance*) wydane przez Europejski Urząd Nadzoru Bankowego (EBA/GL/2021/05)[5], w których użyta terminologia wydaje się pokrywać z tą zastosowaną w art. 6 ust. 4 DORA. Zgodnie z pkt 169 wytycznych wśród komórek kontroli wewnętrznej (*internal control functions*) powinna znaleźć się komórka ds. zarządzania ryzykiem (*risk management function*), komórka ds. zgodności z przepisami (*compliance function*) oraz komórka audytu wewnętrznego (*internal audit function*). Wcześniej w pkt 33 wstępnego uzasadnienia („Background and rationale") znajduje się informacja, że instytucje mogą utworzyć dodatkowe, specyficzne funkcje kontroli, na przykład funkcję odpo-

[5] Dokument dostępny pod adresem: https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-its-final-guidelines-internal-governance (dostęp: 6.06.2025 r.).

wiedzialną za bezpieczeństwo IT (*IT security control*). Dalej w pkt 175 wytycznych zostały wymienione warunki, które wszystkie komórki kontroli wewnętrznej muszą spełnić, aby zostać uznane za niezależne, co w szczególności obejmuje konieczność oddzielenia organizacyjnego od działalności, którą mają monitorować i kontrolować. W tym kontekście art. 6 ust. 4 zdanie drugie DORA należałoby przypisać dokładnie to samo znaczenie, zgodnie z którym tak rozumianą niezależność muszą zachować wszystkie funkcje kontroli, łącznie z wyróżnionymi funkcjami – audytu wewnętrznego (mającej w modelu trzech linii obrony nadaną odpowiedzialność za monitorowanie pozostałych funkcji kontroli) oraz funkcji zarządzania ryzykiem związanym z ICT (kluczowej dla ram zarządzania tym ryzykiem zgodnie z DORA).

Po drugie, warto wrócić do fragmentów dokumentu konsultacyjnego[6] dotyczącego projektu regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT, które co prawda nie znalazły się w przyjętym rozporządzeniu 2024/1774, natomiast dają pewien wgląd w oczekiwany zakres zadań funkcji zarządzania ryzykiem związanym z ICT wyznaczonej zgodnie z art. 6 ust. 4 DORA. W art. 2 projektu rozporządzenia 2024/1774 zawartym w dokumencie konsultacyjnym datowanym na 13.06.2023 r. znalazł się następujący zakres zadań i odpowiedzialności tej funkcji kontroli:

1) raportowanie i doradzanie organowi zarządzającemu, pod który funkcja podlega, włączając raportowanie o wynikach szacowania ryzyka związanego z ICT;
2) zarządzanie i monitorowanie ryzyka związanego z ICT ponoszonego przez podmiot finansowy zgodnie z wymogami sekcji II regulacyjnego standardu technicznego oraz rozdziału II DORA (obydwa zatytułowane: „Zarządzanie ryzykiem związanym z ICT");

[6] Dokument dostępny pod adresem: https://www.esma.europa.eu/document/consultation-paper-draft-rts-ict-risk-management-tools-methods-processes-and-policies (dostęp: 6.06.2025 r.).

3) określenie celów w zakresie bezpieczeństwa ICT i bezpieczeństwa informacji oraz ustalenie jakościowych i ilościowych wskaźników mierzących osiąganie tych celów;
4) pozostawanie niezależnym od funkcji odpowiedzialnych za rozwój, zarządzanie, zmiany i operacje związane z ICT;
5) monitorowanie prawidłowości klasyfikacji zasobów informacyjnych i zasobów ICT przez podmiot finansowy;
6) rozwój i monitorowanie skuteczności wdrożenia programu zwiększania świadomości w zakresie bezpieczeństwa ICT oraz operacyjnej odporności cyfrowej.

Próbując odszukać zbliżony zakres zadań w innych regulacjach lub wytycznych dotyczących sektora finansowego, można w szczególności natknąć się na wydany w grudniu 2018 r. przez EBC dokument „Cyber resilience oversight expectations for financial market infrastructures"[7]. Załącznik do tego dokumentu zawiera wytyczne dotyczące powołania funkcji odpowiedzialnej za odporność cybernetyczną, którą co do zasady jest Chief Information Security Officer (CISO), a więc rola dość powszechnie tworzona w wielu organizacjach. Przedstawiony tam zakres zadań jest nieco bardziej szczegółowy niż powyższa próba doprecyzowania charakteru funkcji zarządzania ryzykiem związanym z ICT, niemniej jednak pokrywa się w kluczowych punktach, takich jak w szczególności:

1) wsparcie organu zarządzającego w określaniu polityk w zakresie odporności cybernetycznej (tj. *cyber resilience*, które dla celów niniejszego porównania traktujemy jako odpowiadające *digital operational resilience*);
2) udział w zarządzaniu ryzykiem cybernetycznym (tj. *cyber risk*, które dla celów niniejszego porównania traktujemy jak odpowiadające *ICT risk*);
3) tworzenie wewnętrznych wytycznych dotyczących odporności cybernetycznej;

[7] Dokument dostępny pod adresem: https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr181203_1.en.html lub https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (dostęp: 6.06.2025 r.).

4) inicjowanie i koordynowanie środków podnoszenia świadomości w zakresie odporności cybernetycznej i zapewniania szkoleń w tym zakresie;
5) pozostawanie niezależnym od działów IT i bezpośrednie raportowanie do organu zarządzającego.

Powracając zaś do pierwotnej propozycji opisu zakresu zadań funkcji zarządzania ryzykiem związanym z ICT wyznaczonej zgodnie z DORA, to została ona w całości usunięta w ostatecznym projekcie regulacyjnego standardu technicznego określającego narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT, przedłożonego Komisji Europejskiej 17.01.2024 r. przez Europejskie Urzędy Nadzoru[8]. W sekcji opisującej przebieg publicznych konsultacji znalazła się informacja o tym, że wielu respondentów zwróciło uwagę na to, że rozporządzenie dało Europejskim Urzędom Nadzoru delegację do dalszego doprecyzowania polityk i narzędzi, ale nie zadań i odpowiedzialności funkcji realizujących je w organizacji. W odpowiedzi Europejskie Urzędy Nadzoru zwróciły uwagę, że zarządzanie wewnętrzne (*governance*) to aspekt fundamentalny dla ram zarządzania ryzykiem związanym z ICT i zaproponowane takiego szczegółowego zakresu zadań zapewniłoby większą przejrzystość co do procesu wdrażania wymogów DORA. Uznały jednak argumenty co do braku odpowiedniego mandatu do określenia takiego zakresu zadań w regulacyjnych standardach technicznych do rozporządzenia, natomiast nie wykluczyły wydania w przyszłości odrębnych wytycznych w tym obszarze.

Powyższe analizy nakreślają ogólną koncepcję organizacji procesu zarządzania ryzykiem związanym z ICT jako wymagającą wskazania funkcji podlegającej pod organ zarządzający podmiotem finansowym, niezależnej od zadań o charakterze operacyjnym, która zapewnia monitorowanie ryzyka związanego z ICT, określanie wewnętrznych polityk w zakresie bezpieczeństwa ICT czy dbanie o program podnoszenia świadomości w zakresie operacyjnej odporności cyfrowej. W to, jakiej

[8] Dokument dostępny pod adresem: https://www.esma.europa.eu/document/final-report-draft-rts-ict-risk-management-framework-and-simplified-ict-risk-management (dostęp: 6.06.2025 r.).

konkretnie jednostce organizacyjnej należy powierzyć zadania związane z zarządzaniem ryzykiem związany z ICT, przepisy DORA zdają się już nie ingerować, pozostawiając to decyzji podmiotu finansowego, który zgodnie ze swoją specyfiką i strukturą organizacyjną może te zadania alokować do odrębnej funkcji kontroli utworzonej ściśle na potrzeby bezpieczeństwa IT albo też do komórki ds. zarządzania ryzykiem, jeśli ta w sposób kompleksowy obejmuje obszar zarządzania ryzykiem operacyjnym z uwzględnieniem niezbędnych aspektów ryzyka ICT.

Praktyczna wskazówka
Prawidłowej odpowiedzi na pytanie, czy *Chief Information Security Officer* (CISO) jest naturalnie przeznaczony do pełnienia funkcji zarządzania ryzykiem związanym z ICT, nie można udzielić bez szczegółowego wniknięcia w to, jaki konkretnie zakres zadań on wykonuje i jak jego rola osadzona jest w danej organizacji. Kwestia, na którą należy zwrócić szczególną uwagę, to kryterium niezależności wymagające, aby pracownicy danej jednostki organizacyjnej (w tym wypadku kierowanej przez CISO) nie wykonywali zadań operacyjnych wchodzących w zakres działalności, którą mają monitorować i kontrolować. Tutaj warto przywołać art. 13 DORA, który m.in. mówi o tym, że podmiot finansowy zapewnia przegląd incydentów związanych z ICT, w tym np. pod względem szybkości reagowania na ostrzeżenia dotyczące bezpieczeństwa oraz w stosownych przypadkach jakości i szybkości przeprowadzania analizy śledczej. Zakładając, że tak rozumiany przegląd incydentów stanowi element procesu monitorowania ryzyka ICT, a zespół zarządzany przez CISO realizuje zadania związane z obsługą mechanizmów wykrywania nietypowych działań, w tym problemów związanych z bezpieczeństwem sieci ICT, należy przemyśleć kwestie organizacji procesu zarządzania ryzykiem związanym z ICT pod kątem możliwego naruszenia zasad niezależności.

6. Ramy zarządzania ryzykiem ICT a strategia operacyjnej odporności cyfrowej

Zgodnie z art. 6 ust. 8 DORA ramy zarządzania ryzykiem związanym z ICT obejmują strategię operacyjnej odporności cyfrowej, w której określono sposób wdrażania tych ram. W tym celu strategia ma zawierać metody przeciwdziałania ryzyku związanemu z ICT i osiągania szczególnych celów w dziedzinie ICT, w tym przez wyjaśnienie, w jaki sposób ramy zarządzania ryzykiem związanym z ICT wspierają strategię

biznesową i cele biznesowe podmiotu finansowego, jak również dzięki uwzględnieniu takich elementów jak:

1) ustalenie limitu tolerancji ryzyka;
2) określenie jasnych celów w zakresie bezpieczeństwa informacji;
3) mechanizmy wprowadzone w celu wykrywania incydentów związanych z ICT;
4) sposób testowania operacyjnej odporności cyfrowej;
5) przedstawienie strategii komunikacji w przypadku incydentów związanych z ICT.

Patrząc na powyższe, można odnieść wrażenie, że strategia operacyjnej odporności cyfrowej jest w art. 6 ust. 8 zdanie pierwsze DORA pomyślana jako składnik ram zarządzania ryzykiem związanym z ICT, a poprzez dalszy opis tego, co strategia ma zawierać – jako rodzaj konstytucji cyfrowej odporności operacyjnej, zawierającej w sobie całościowy opis tych ram.

W praktyce jednak obszary, które ramy ryzyka ICT i stosownie do tego strategia operacyjnej odporności cyfrowej muszą obejmować, są związane z odrębnie funkcjonującymi w wielu organizacjach systemami zarządzania (np. bezpieczeństwem informacji czy ciągłości działania), które opisane są w politykach, procedurach i innych dokumentach. Stąd w naturalny sposób wyłania się koncepcja strategii rozproszonej, która porządkuje wszystkie niezbędne elementy w spójne ramy zarządzania ryzykiem ICT, ale w szczegółach referuje do innych regulacji wewnętrznych, które są nadrzędne dla tych elementów składowych (dalej mogąc odsyłać do bardziej szczegółowej dokumentacji dla danego zagadnienia). W tym zakresie podmioty finansowe mogą zastosować różne podziały, natomiast przykładowo ramy te mogłyby zostać zbudowane w oparciu o poniższe główne składniki:

1) polityka zarządzania ryzykiem związanym z ICT (opcjonalnie jako integralna część polityki zarządzania ryzykiem operacyjnym i wkomponowana w ogólny system zarządzania ryzykiem), obejmująca metodykę pomiaru kombinacji wpływu i prawdopodobieństwa wystąpienia podatności i zagrożeń dla systemów ICT wspierających funkcje biznesowe;

2) polityka zarządzania ryzykiem ze strony zewnętrznych dostawców ICT (jako jednej z kategorii ryzyka związanego z ICT, ale wyodrębnionej z uwagi na rozbudowane wymogi stanowiące odrębny filar, któremu został poświęcony rozdział V DORA);
3) strategia na rzecz ciągłości działania w zakresie ICT (domyślnie jako integralna część ogólnej strategii na rzecz ciągłości działania), odpowiednio powiązana ze strategią komunikacji w przypadku poważnych incydentów związanych z ICT;
4) polityka bezpieczeństwa informacji, obejmująca w szczególności mechanizmy wprowadzone w celu monitorowania i wykrywania incydentów związanych z ICT oraz systematycznego testowania operacyjnej odporności cyfrowej;
5) ogólne elementy ram, w tym zasady ich przeglądu, o których mowa w art. 6 ust. 5 DORA (w odniesieniu do podmiotów finansowych innych niż mikroprzedsiębiorstwa)[9] oraz w art. 16 ust. 2 DORA (w odniesieniu do mikroprzedsiębiorstw).

Praktyczna wskazówka
Opisane w strategii operacyjnej odporności cyfrowej elementy, takie jak polityka bezpieczeństwa informacji czy strategia na rzecz ciągłości działania, to co do zasady wdrożone składniki ram zarządzania ryzykiem związanym z ICT, które na bieżąco mają zapewniać bezpieczeństwo sieci i systemów informatycznych wspierających ciągłe świadczenie usług przez podmiot finansowy. Niezbędnym tego uzupełnieniem wydaje się określenie na przyszłość pewnych celów strategicznych podmiotu finansowego w zakresie operacyjnej odporności cyfrowej, dzięki którym odporność ta byłaby wzmacniania lub przynajmniej skutecznie zachowywana w warunkach rozwoju technologii informacyjno-komunikacyjnych i innych zmian w otoczeniu. Takie właśnie cele, materializujące się przez konkretne przedsięwzięcia zaplanowane do realizacji w krótszym lub dłuższym terminie, mają szansę stać się kluczowe, aby pokazać, jak strategia operacyjnej odporności cyfrowej podmiotu finansowego realnie wspiera jego strategię biznesową i cele biznesowe.

[9] Należy zwrócić uwagę, że niezależnie od przeglądu ram zarządzania ryzykiem, o którym mowa w art. 6 ust. 5 DORA, zgodnie z kolejnym ustępem tego artykułu podmioty finansowe inne niż mikroprzedsiębiorstwa muszą regularnie poddawać swoje ramy zarządzania ryzykiem związanym z ICT audytom wewnętrznym przeprowadzanym przez audytorów zgodnie z planami tych podmiotów dotyczącymi audytów.

7. Podsumowanie

Podsumowując dotychczasowe rozważania, można sformułować następujące najważniejsze spostrzeżenia dotyczące budowania ram zarządzania ryzykiem związanym z ICT zgodnie z DORA:

1) ramy te powinny stanowić część ogólnego systemu zarządzania ryzykiem, co należy przede wszystkim rozumieć jako konieczność uczynienia ich elementem widocznym w całościowym systemie zarządzania, w tym przez zapewnienie, aby wszystkie ustalenia dotyczące wskazanych ram określał, zatwierdzał i nadzorował organ zarządzający podmiotu finansowego;
2) ramy ryzyka związanego z ICT to przede wszystkim zapewnienie wdrożenia bardzo konkretnych wytycznych w zakresie bezpieczeństwa sieci i systemów informatycznych, obejmujących szczegółowy zestaw środków postępowania z ryzykiem, których wymóg implementacji w ograniczonym stopniu podlega zasadzie proporcjonalności czy poziomowi oszacowanego ryzyka;
3) szacowanie ryzyka związanego z ICT, w tym ewidencjonowanie jego zmian w czasie, stanowi element ram, natomiast wydaje się, że nie stanowi głównej osi, na której ramy mają być zbudowane (szacowanie ryzyka jest wymagane, ale sposób stosowania mechanizmów postępowania z ryzykiem wydaje się i tak z góry narzucony przepisami rozporządzenia);
4) zarządzanie ryzykiem ICT w organizacji może zostać powierzone funkcjom kontroli o różnych nazwach i przedmiotowych zakresach zadań w danej organizacji, natomiast kluczowe wydaje się, aby monitorując ryzyka związane z ICT, unikały wykonywania zadań o charakterze operacyjnym (np. w obszarze cyberbezpieczeństwa);
5) strategia operacyjnej odporności cyfrowej doskonale nadaje się do tego, aby stanowić nadrzędny opis ram zarządzania ryzykiem związanym z ICT w organizacji, również w rekomendowanym tutaj modelu strategii rozproszonej, która w szczegółach referuje do innych regulacji wewnętrznych, zawierających w sobie poszczególne elementy tych ram, a które zostały równolegle dostosowane do wymogów DORA.

Generalnie wymóg DORA dotyczący dysponowania solidnymi, kompleksowymi i dobrze udokumentowanymi ramami zarządzania ryzykiem związanym z ICT nie stawia przed podmiotami finansowymi, funkcjonującymi od lat na rynku, zadania wymagającego w tym zakresie zbudowania od nowa wszystkich rozwiązań. Raczej chodzi tu o dokładny przegląd funkcjonujących mechanizmów na potrzeby zarządzania ryzykiem, bezpieczeństwem informacji i ciągłością działania pod kątem dostosowania ich do przepisów, których poziom szczegółowości znacznie przekroczył jakiekolwiek znane dotychczas przepisy prawa w dziedzinie zarządzania technologiami informacyjno-komunikacyjnymi lub cyberbezpieczeństwem obowiązujące podmioty finansowe.

Ogólne myślenie o zagadnieniu, które zyskało teraz miano ram zarządzania ryzykiem związanym z ICT, może być zatem oparte na wypracowanych wcześniej rozwiązaniach i doświadczeniach, pod warunkiem że zostaną na to nałożone niezbędne szczegóły i niuanse zawarte w przepisach DORA, które w niniejszym opracowaniu starano się wyłowić i zwrócić na nie uwagę.