kancelarie rp

Poradnik

Nawigator Prawny

WIĘCEJ PORAD NA KANCELARIE.

FINANSE

Rok stosowania Rozporządzenia DORA – nadchodzące wyzwania

Wejście w życie rozporządzenia DORA zapoczątkowało nowy etap w zarządzaniu bezpieczeństwem informacji w sektorze finansowym. Po pierwszym roku kluczowe stają się już nie same procedury, lecz ich realizacja, regularne testowanie, audyty oraz odpowiedzialność najwyższego kierownictwa za zarządzanie ryzykiem związanym z ICT.

ADW. TOMASZ KAMIŃSKI

Wspólnik w Kancelarii Krzysztof Rożko i Wspólnicy

DANIEL NIWIŃSKI

Prawnik, Ekspert ds. cyberbezpieczeństwa w Kancelarii Krzysztof Rożko i Wspólnicy

W dobie postępującej cyfryzacji Rozporządzenie (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA) stanowi jeden z najważniejszych filarów unijnej strategii wzmacniania odporności systemu finansowego. Od 17 stycznia 2025 r. DORA jest bezpośrednio stosowana we wszystkich państwach członkowskich, wprowadzając jednolite ramy zarządzania ryzykiem ICT dla szerokiego spektrum podmiotów finansowych. Celem Rozporządzenia jest zapewnienie, aby wszystkie podmioty objęte zakresem stosowania DORA były zdolne do prawidłowego funkcjonowania nawet w warunkach poważnych incydentów związanych z ICT, awarii systemów informatycznych, czy zakłóceń w usługach świadczonych przez zewnętrznych dostawców usług ICT.

DORA okazała się być istotną zmianą dotychczasowego podejścia do cyberbezpieczeństwa nie tylko dla podmiotów bezpośrednio objętych zakresem jej stosowania, lecz również dla zewnętrznych dostawców usług ICT. Dostawcy świadczący usługi na rzecz podmiotów z sektora finansowego w pierwszym roku stosowania DORA stanęli przed dużym wyzwaniem dostosowania swoich procesów do restrykcyjnych wymagań podmiotów finansowych. Wielu dostawców usług ICT zdecydowało się na rozpoczęcie wdrożenia wymagań takich standardów jak ISO 27001 czy też ISO 22301

Doświadczenia i wyzwania

Pierwszy rok stosowania DORA przyniósł wiele wyzwań, a kolejne lata zapowiadają się równie pracowicie. Po opracowaniu procesów, dokumentacji i ich początkowym wdrożeniu nadszedł czas na realizację cyklicznych obowiązków związanych z doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Obowiązki te będą dotykały takich obszarów, jak audyty wewnętrzne, przeglądy (w tym przegląd ram zarządzania ryzykiem ICT), audyty i kontrole zewnętrznych dostawców usług ICT, szkolenia, a także cykliczna analiza ryzyka związanego z ICT.

DORA to regulacja, która wykracza daleko poza tradycyjnie pojmowane cyberbezpieczeństwo, stając się fundamentem dla nowego paradygmatu zarządzania ryzykiem operacyjnym w sektorze finansowym, który w najbliższych latach będzie generował zarówno istotne wyzwania regulacyjne, jak i organizacyjne.

W reżimie DORA audyt wewnętrzny jest jednym z kluczowych mechanizmów zapewnienia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji. Rozporządzenie wymaga, aby podmioty finansowe posiadały niezależną funkcję audytu wewnętrznego obejmującą wszystkie elementy ram zarządzania ryzykiem związanym z ICT, w tym polityki, procedury, systemy, mechanizmy kontroli oraz sposób zarządzania relacjami z dostawcami usług ICT.

Audyt wewnętrzny musi być prowadzony w sposób regularny, oparty na analizie ryzyka oraz adekwatny do profilu działalności i złożoności technologicznej danego podmiotu. Jego zakres powinien obejmować nie tylko bezpieczeństwo techniczne systemów, ale również zgodność organizacyjną i kontraktową. DORA kładzie również nacisk na raportowanie wyników audytu do organu zarządzającego. Najwyższe kierownictwo musi mieć realny wgląd w poziom ryzyka ICT oraz w skuteczność środków zaradczych. Ustalenia audytowe powinny prowadzić do konkretnych planów naprawczych, a ich realizacja powinna podlegać monitorowaniu.

Co istotne, audyt wewnętrzny w rozumieniu DORA nie jest jednorazowym przeglądem „na potrzeby zgodności", lecz elementem ciągłego cyklu doskonalenia SZBI. Ma on zapewniać, że instytucja nie tylko formalnie spełnia wymogi regulacyjne, ale faktycznie jest przygotowana na wystąpienie poważnych incydentów związanych z ICT.

Realna odpowiedzialność

DORA nakłada na podmioty finansowe obowiązek ciągłego utrzymywania i regularnego przeglądu ram zarządzania ryzykiem związanym z ICT. Nie mogą mieć one charakteru czysto formalnego i nie powinny polegać jedynie na pozornym odznaczeniu checklisty. Zgodnie z DORA, powinny one być prowadzone cyklicznie, a ich celem jest weryfikacja, czy przyjęte polityki, procedury, role i mechanizmy kontroli pozostają adekwatne do aktualnego profilu ryzyka oraz stopnia zależności od technologii i dostawców zewnętrznych.

Kluczową rolę w tym procesie odgrywa organ zarządzający, który odpowiada za zatwierdzanie wyników przeglądów oraz zapewnienie wdrożenia działań korygujących. DORA wymaga, aby najwyższe kierownictwo posiadało wystarczającą wiedzę i informacje umożliwiające realną ocenę poziomu ryzyka ICT, a nie jedynie akceptację dokumentacji przygotowanej przez osoby wyznaczone do obsługi procesów technicznych lub compliance.

> DORA czyni zarząd realnie odpowiedzialnym za poziom ryzyka związanego z ICT, a nie jedynie za podpisanie dokumentów.

W praktyce oznacza to konieczność tworzenia wskaźników ryzyka możliwych do realnego zbadania, regularnych raportów zarządczych oraz ścieżek eskalacji dla słabości wykrytych w ramach przeglądów. Przeglądy służą przede wszystkim poprawie bezpieczeństwa podmiotu oraz realizacji procesów związanych z ciągłym doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

Dostawcy usług ICT

Jednym z najbardziej przełomowych elementów DORA jest nałożenie na podmioty finansowe obowiązku realnego nadzoru nad zewnętrznymi dostawcami usług ICT, w szczególności tymi, od których zależy ciągłość krytycznych lub istotnych funkcji. Regulacja odchodzi od modelu opartego wyłącznie na zaufaniu do certyfikatów czy standardowych klauzul umownych, wprowadzając wymóg aktywnych audytów i kontroli dostawców.

Podmioty finansowe muszą zapewnić w umowach z dostawcami usług ICT skuteczne prawa audytowe, obejmujące dostęp do informacji, dokumentacji, systemów, obiektów oraz personelu dostawcy, w zakresie niezbędnym do oceny bezpieczeństwa, ciągłości działania i zgodności z DORA. Audyty te mogą być prowadzone samodzielnie, przez audytorów zewnętrznych lub w formie audytów wspólnych, jeżeli kilku klientów korzysta z tego samego dostawcy.

DORA wymaga także, aby wyniki audytów i kontroli były systematycznie analizowane i wykorzystywane w procesach zarządzania ryzykiem – w szczególności przy ocenie poziomu ryzyka koncentracji, planowaniu działań naprawczych lub podejmowaniu decyzji o zmianie dostawcy. Niedopuszczalne jest ograniczanie się do „tick-box compliance" polegającego na formalnym posiadaniu klauzul audytowych bez ich faktycznego wykonywania.

DORA ustanawia obowiązek prowadzenia cyklicznej i udokumentowanej analizy ryzyka związanego z ICT jako fundamentu całego systemu operacyjnej odporności cyfrowej. Podmioty finansowe muszą regularnie identyfikować i oceniać wszystkie ryzyka, które mogą wpływać na poufność, integralność, dostępność i autentyczność systemów oraz danych, w tym zarówno ryzyka wewnętrzne, jak i wynikające z zależności od zewnętrznych dostawców usług ICT.

Analiza ryzyka nie może ograniczać się do jednorazowego ćwiczenia. Zgodnie z DORA powinna być przeprowadzana cyklicznie i musi obejmować mapowanie krytycznych procesów biznesowych na wspierające je systemy informatyczne oraz ocenę, jakie skutki dla działalności, klientów i stabilności finansowej miałyby potencjalne incydenty.

DORA wymaga również, aby wyniki analizy ryzyka były wykorzystywane w sposób operacyjny – do określania priorytetów inwestycji w bezpieczeństwo, doboru środków bezpieczeństwa, opracowywania planów ciągłości działania oraz określania zakresu przyszłych testów odporności cyfrowej, a także szkoleń personelu. Organ zarządzający powinien otrzymywać regularne raporty z tych analiz i na ich podstawie podejmować decyzje strategiczne.

W praktyce cykliczna analiza ryzyka ICT staje się narzędziem zarządczym, które łączy perspektywę technologiczną, biznesową i regulacyjną, zapewniając, że odporność cyfrowa nie jest celem samym w sobie, lecz warunkiem stabilnego i bezpiecznego świadczenia usług finansowych.

Zarządzanie ryzykiem

Pierwszy rok stosowania DORA jasno pokazuje, że nie jest to regulacja „do wdrożenia", lecz jest to źródło trwałej zmiany kultury zarządzania ryzykiem w sektorze finansowym. Podmioty, które wykorzystają projekty wdrożenia wymogów DORA, jako impuls do realnego wzmocnienia odporności cyfrowej, zyskają nie tylko większe bezpieczeństwo, ale również przewagę organizacyjną i zaufanie rynku w coraz bardziej cyfrowym świecie.