Deloitte.

DORA: Oboznámte sa s nariadením o digitálnej prevádzkovej odolnosti

Ako by mali finančné inštitúcie zohľadniť nové pravidlá vo svojich stratégiách?

Zákonodarcovia EÚ ratifikovali nariadenie o digitálnej prevádzkovej odolnosti (známe ako DORA). Nariadenie bolo zverejnené v Úradnom vestníku Európskej únie 27. decembra 2022 a nadobudlo účinnosť 16. januára 2023. Od tohto dátumu sa musia finančné inštitúcie, na ktoré sa nariadenie vzťahuje, začať riadiť novými pravidlami v praxi najneskôr do 24 mesiacov. Tento čas by mali využiť nielen na prípravu na výzvy, ktoré prináša aktuálne znenie nariadenia, ale aj na zhodnotenie širších strategických dôsledkov tejto regulácie.

DORA je kľúčovou iniciatívou EÚ v oblasti digitálnej prevádzkovej a kybernetickej odolnosti v sektore finančných služieb. Nariadenie zavádza jednotný súbor pravidiel regulácie a dohľadu na prevádzkovú odolnosť informačných a komunikačných technológií vo finančnom sektore. Okrem iného od finančných inštitúcií vyžaduje, aby uskutočnili významné investície na zlepšenie svojej odolnosti voči digitálnym a kybernetickým rizikám.

Nové povinnosti si budú vyžadovať najmä zmenu prístupu riadiacich orgánov, ktorých úlohou bude posilniť odolnosť inštitúcií voči digitálnym hrozbám, ktoré sa budú dynamicky vyvíjať, a minimalizovať zraniteľnosť obchodných modelov. Riadiace orgány finančných inštitúcií, riadenie rizík v oblasti informačných a komunikačných technológií (IKT) a ďalší lídri finančných inštitúcií budú zohrávať dôležitú úlohu pri zavádzaní interných zmien v reakcii na požiadavky nariadenia DORA, ich implementácii a pri prijímaní strategických investičných rozhodnutí potrebných na budovanie odolnosti.

Detailnú technickú dohodu o obsahu DORA dosiahli vyjednávači EÚ v lete 2022. Našu analýzu tejto dohody v rámci tzv. „piatich pilierov" DORA nájdete v našom článku z júla 2022, v ktorom sa dočítate o piatich strategických bodoch, ktoré budú musieť finančné inštitúcie zvážiť pri implementácii a zavádzaní DORA do praxe.

Strategické oblasti pre finančné inštitúcie vyplývajúce z nariadenia DORA

1. Koncepcia „prevádzkovej odolnosti" bude pre finančné inštitúcie znamenať zmenu prístupu

Nariadenie DORA po prvýkrát prináša do regulačného rámca EÚ v oblasti FSI hľadisko prevádzkovej odolnosti. Nahrádza existujúcu mozaiku pokynov zameraných na kybernetické a IT riziká novým, holistickým prístupom k budovaniu odolnosti voči digitálnym hrozbám. Ide však o viac než len zmenu terminológie – prevádzková odolnosť presahuje tradičné prístupy k riadeniu rizík používané v oblastiach kybernetických rizík, IT rizík a kontinuity podnikania. Núti totiž finančné inštitúcie predpokladať, že závažným narušeniam sa nedá vyhnúť (bez ohľadu na to, aká silná je ochrana inštitúcie), a integrovať vyššiu úroveň odolnosti voči takýmto narušeniam do prevádzkového modelu svojich najdôležitejších služieb alebo funkcií. Tento prístup bude viesť k nastaveniu priebežného dialógu medzi inštitúciami, regulátormi a orgánmi dohľadu.

Vývoj uvedeného prístupu v Spojenom kráľovstve (ktoré zaviedlo svoj regulačný rámec pre prevádzkovú odolnosť v marci 2022) znamenal, že inštitúcie si museli stanoviť vysoké referenčné hodnoty pre svoju budúcu odolnosť. A na splnenie týchto cieľov sa budú musieť pripraviť na značné investície. Príklad Spojeného kráľovstva tiež ukázal, že na riešenie globálnych otázok v súvislosti s prevádzkovou odolnosťou, ktoré nie je možné efektívne riešiť na úrovni jednotlivých inštitúcií, bude potrebné posilniť (prípadne vytvoriť) medzisektorovú spoluprácu. Finančný sektor preto bude musieť prevziať iniciatívu pri vývoji metód na riešenie rizík expozície voči tretím stranám, postupov testovania tretích strán a zdieľania informácií o hrozbách v reálnom čase.

2. Posilnenie zodpovednosti vedúcich orgánov za prevádzkovú odolnosť

Nariadenie DORA stanovuje, že za prevádzkovú odolnosť inštitúcie je zodpovedné jej predstavenstvo. Vrcholový manažment preto bude musieť prevziať vedúcu úlohu pri implementácii najdôležitejších zložiek DORA. V praxi teda budú členovia predstavenstva a vrcholového vedenia musieť schváliť súbor kľúčových plánov, ako je napríklad stratégia digitálnej prevádzkovej odolnosti firmy a jej politika týkajúca sa tretích strán v oblasti IKT. Okrem toho budú vedúce orgány zodpovedné aj za prijímanie rozhodnutí o prevádzkovom modeli, ktoré sú nevyhnutné na integráciu požiadaviek DORA do každodennej činnosti inštitúcií. Konkrétne bude po novom v ich kompetencii stanovenie úrovne tolerancie rizík a rozhodovanie o tom, ako stanoviť priority nápravných opatrení na riešenie zistených prevádzkových nedostatkov.

Po zavedení DORA bude pre vedúce orgány čoraz dôležitejšie preukázať orgánom dohľadu, že ich inštitúcia je odolná voči hrozbám špecifickým pre danú inštitúciu, ako aj voči všeobecným hrozbám v danom odvetví. Budú musieť dobre pochopiť pripravenosť firmy na zvládnutie možných narušení IKT a zároveň zachovať kontinuitu služieb. Budú musieť preukázať, že: prijali správne manažérske rozhodnutia, riadne preskúmali plány odolnosti a následne posilnili odolnosť inštitúcie. Pravidelné informácie pre vedúce orgány o hrozbách a zraniteľnostiach pochádzajúcich z vonkajšieho prostredia bude potrebné dynamicky zohľadňovať v celkovej odolnosti firmy.

3. Priebežné povinnosti budú mať vplyv na opatrenia inštitúcií aj po skončení obdobia implementácie

Implementačné obdobie 24 mesiacov bude pre väčšinu finančných inštitúcií (vrátane tých veľkých a sofistikovaných) výzvou v mnohých oblastiach, okrem iného v otázkach pokročilého testovania, hlásenia incidentov, impact assessment a pod. Nariadenie DORA však zavádza aj priebežný spôsob riadenia odolnosti založený na priebežných previerkach. Finančné inštitúcie tak budú mať povinnosť vykonávať priebežné testovanie odolnosti a hodnotenie rizík a vhodnosti svojich plánov odolnosti. Budú tiež musieť priebežne zhromažďovať informácie o hrozbách, aby splnili novú povinnosť hlásenia hrozieb a incidentov, ako aj vypracúvať vlastné rizikové scenáre. Nariadenie DORA od inštitúcií vyžaduje, aby určili kritické alebo významné funkcie (CIF) ako ústredný bod stratégie hodnotenia, ktorú musia realizovať pri budovaní svojej odolnosti, najmä pokiaľ ide o identifikáciu hrozieb a testovanie scenárov.

Hlavným zámerom nariadenia DORA je zaviesť trvalú regulačnú povinnosť firiem dosiahnuť prevádzkovú odolnosť, ktorá sa dokáže prispôsobovať neustále sa meniacim nárokom podľa toho, ako sa budú formovať hrozby a oblasti zraniteľnosti. Vďaka investíciám do strategických schopností, ako je zisťovanie hrozieb a testovanie odolnosti, budú vedúce orgány lepšie vybavené, aby pochopili, ako môžu scenáre ovplyvniť kritické funkcie ich firmy a viesť k ďalším následným dopadom, ale aj to, aké investície budú potrebné na dosiahnutie dostatočnej úrovne pripravenosti. Strategické schopnosti tohto druhu budú navyše kľúčové aj pri efektívnej reakcii na prípadné nepredvídané narušenia, pretože vedúce orgány budú mať hlbšie a podrobnejšie znalosti o základnej štruktúre a fungovaní svojej inštitúcie.

4. Predpokladaný dopad na stratégie firiem v oblasti outsourcingu

Riešenie zraniteľností tretích strán je hlavnou výzvou pri posilňovaní prevádzkovej odolnosti aj pre britské firmy, ktoré sú na ceste k prevádzkovej odolnosti ďalej. Nariadenie DORA zavádza ako prvé na svete rámec dohľadu nad kritickými tretími stranami (CTP), rozširuje rozsah perimetra finančnej regulácie a dáva európskym orgánom dohľadu (ESA) nové právomoci v oblasti dohľadu nad CTP a riešenia rizík pre odolnosť finančného sektora EÚ. Regulačné orgány EÚ však jasne uviedli, že to v žiadnom prípade neznižuje individuálnu zodpovednosť finančných inštitúcií, pokiaľ ide o outsourcing. Nariadenie DORA finančným inštitúciám naozaj ukladá niekoľko nových požiadaviek na riadenie rizík tretích strán, ktoré budú ešte prísnejšie, ak tretie strany podporujú poskytovanie kritickej funkcie alebo služby. To sa môže stať zvlášť dôležité pre poskytovateľov spomedzi FinTech alebo digitálnych spoločností, ktorých závislosť od určitých digitálnych platforiem ich môže vystaviť väčším rizikám v oblasti IKT tretích strán a vyvolať prísnejší dohľad nad týmto rizikom.

Finančné inštitúcie by tiež mali venovať osobitnú pozornosť požadovanému posúdeniu rizika koncentrácie. Oblasti zraniteľnosti, ktoré môžu byť identifikované na základe týchto hodnotení (nadmerná závislosť od jedného externého poskytovateľa, kritickosť obsluhovaných funkcií atď.), môžu pre finančné inštitúcie znamenať zvýšenú intenzitu kontrol zo strany orgánov dohľadu. Táto situácia môže následne vyvolať tlak na vedúce orgány, aby prehodnotili svoje strategické rozhodnutia týkajúce sa ich ochoty podstupovať riziko pri nadväzovaní vzťahov s tretími stranami. Lídri firiem by sa mali zamerať aj na roly interných oddelení a zamestnancov zodpovedných za riadenie rizík a zadávanie zákaziek s ohľadom na ich ochotu podstupovať riziko v prevádzkových modeloch inštitúcie. Vedúce orgány tiež môžu zvážiť riešenie identifikovaných rizík koncentrácie tým, že prijmú nápravné opatrenia, ako napríklad prijatím stratégie pre viacerých dodávateľov.

5. Oblasť prevádzkovej odolnosti ako kľúčový faktor investičných rozhodnutí na úrovni vedúcich orgánov inštitúcie

Budovanie prevádzkovej odolnosti v inštitúcii si vyžaduje, aby bola táto oblasť zakotvená ako kľúčový faktor pri rozhodovaní o biznis stratégii a pri navrhovaní zmien obchodného modelu. Presnejšie povedané, finančné inštitúcie budú mať za úlohu určiť požadovanú úroveň odolnosti v rámci vypracovania stratégie digitálnej prevádzkovej odolnosti, ktorú vyžaduje DORA, vďaka čomu sa budú môcť vedúce orgány viac zapojiť do rozhodovania o rizikách a odolnosti. Vedúce orgány a riaditelia obchodných oddelení budú musieť pochopiť obchodné dôvody pre investície do kapacít prevádzkovej odolnosti a zároveň budú musieť byť schopní vyjadriť, ako sa počiatočné náklady vyvážia tým, že nastavia prevádzkový model, ktorý v priebehu času obstojí pri rastúcej regulačnej kontrole. Aby to bolo uskutočniteľné v praxi, vedúce orgány by mali uprednostniť tie oblasti, ktoré budú v priebehu implementácie DORA v popredí záujmu orgánov dohľadu. Ide napríklad o požiadavky, ktoré si vyžadujú pravidelné výstupy (napr. výber CIF, impact assessment, postupy testovania odolnosti, výstupy z rámca na hlásenie incidentov atď.).

Vedúce orgány by mali mať na pamäti, ako by orgány dohľadu mohli interpretovať zásadu proporcionality obsiahnutú v DORA. Je pravdepodobnejšie, že väčšie podniky budú mať v určitých oblastiach pokročilejšie schopnosti (napr. testovanie odolnosti), ale budú tiež podliehať oveľa širšej úrovni kontroly vzhľadom na potenciálny systémový význam ich kľúčových služieb. Naopak, menšie podniky môžu mať prospech z menej prísnych požiadaviek (napr. nemusia vykonávať pokročilé testovanie TLPT, používať zjednodušený rámec riadenia rizík v oblasti IKT atď.), ale napriek tomu môžu čeliť značným investičným nárokom na vybudovanie kapacít potrebných na dosiahnutie súladu s tými časťami nariadenia, ktoré sa uplatňujú jednotne v celom sektore (napr. požiadavka na hlásenie incidentov v oblasti IKT a ustanovenia o riadení rizík tretích strán).

Záver

Nariadenie DORA nie je len „jednorazovým compliance cvičením na dodržiavanie predpisov". Naopak, jeho cieľom je pomôcť finančným inštitúciám, aby zostali dlhodobo odolné voči neustále sa meniacim hrozbám v čoraz zložitejšom technologickom prostredí.

Hoci európske orgány dohľadu musia počas dvojročného implementačného obdobia ešte zapracovať značnú časť sekundárnych predpisov DORA a objasniť očakávania týkajúce sa odolnosti, už teraz je jasné, že od vedúcich orgánov firiem sa očakáva, že prevezmú kľúčovú úlohu pri budovaní odolnosti a väčší podiel zodpovednosti za zásadné rozhodnutia. Bude dôležité nastaviť silný „tone from the top" – signál, ktorý jasne definuje dôležitosť prevádzkovej odolnosti a ktorý regulačné orgány, investori a ďalšie zainteresované strany vezmú na vedomie, pretože prevádzkové hrozby v sektore finančných služieb sú na vzostupe.

Ako vám môžeme pomôcť?

Odborníci Deloitte sú pripravení podporiť finančné inštitúcie pri budovaní pevných pilierov prevádzkovej odolnosti podľa požiadaviek nariadenia DORA. Ponúkame komplexné služby, ktoré zahŕňajú kompletný proces od readiness analýzy až po jej implementáciu, a to všetko presne podľa vašich potrieb.

- Rámec riadenia rizík. Na splnenie požiadaviek nariadenia DORA budú inštitúcie potrebovať spoľahlivé procesy riadenia rizík. Deloitte vám pomôže zosúladiť obchodné stratégie a (nielen) kybernetické riziká vašej organizácie a udržiavať komplexný a účinný rámec ich riadenia.
- Hlásenie incidentov. Cieľom nariadenia DORA je harmonizovať procesy klasifikácie a hlásenia incidentov. Včasné odhalenie incidentov a rýchla reakcia sú nevyhnutné. Našim klientom preto pomáhame prispôsobiť sa novým pravidlám EÚ na hlásenie incidentov a zosúladiť interné procesy v tomto smere s cieľom optimalizovať prideľovanie zdrojov.
- Testovanie odolnosti. Nariadenie DORA vyžaduje, aby finančné inštitúcie testovali svoje systémy na základe súvisiacich rizík. Zahŕňa to skríning zraniteľností a penetračné testovanie, ako aj robustné testovanie kontinuity podnikania.
- Penetračné testovanie na základe hrozieb (TLPT) pre kritických hráčov. Kybernetická prax Deloitte v strednej Európe umožňuje poskytovanie najkvalitnejších služieb penetračného testovania svojho druhu vďaka vysokokvalifikovaným odborníkom a technologickému zázemiu.
- Zdieľanie analýzy hrozieb. Aktivity v oblasti kybernetických hrozieb sa často týkajú viacerých organizácií vo finančnom sektore súčasne. Nariadenie DORA, ktoré sa zameriava na zdieľanie informácií o hrozbách, pomôže celému sektoru stať sa zodpovednejším a aktívnejším pri obrane proti rastúcemu počtu kybernetických útokov. Našim klientom preto pomáhame s vývojom a integráciou procesu zdieľania informácií o týchto hrozbách.
- Riadenie rizík tretích strán (TPRM) a monitorovanie. Inštitúcie by mali posúdiť, či ich stratégie a plány reakcie a obnovy relevantným spôsobom zohľadňujú rozšírené pravidlá riadenia rizík v oblasti IKT. Rámec TPRM od Deloitte je založený na špičkových postupoch a vychádza z globálnych regulačných požiadaviek. Našim klientom tak poskytujeme komplexné riešenie na riadenie procesov, postupov a činností v rámci ekosystémov tretích strán. Vďaka implementácii TPRM budú naši klienti využívať všetky výhody komplexnej technologickej platformy, ktorá kombinuje mobilný zber údajov, nástroje na zlepšovanie výkonnosti na úrovni podniku a útvarov a analytický reporting.

Viac informácií o našich službách nájdete na našich webových stránkach

Kontaky

Martin Kubačka
Partner
mkubacka@deloittece.com
+420 776 306 694

Jakub Holl
Director
jholl@deloittece.com
+420 734 353 815

Tomáš Mihóčik
Director
tmihocik@deloittece.com
+421 910 820 005

Martin Antos
Manager
mantos@deloittece.com
+420 734 783 919