PRAUDIT

FELKÉSZÜLÉSI SEGÉDLET A DORA RENDELETNEK TÖRTÉNŐ MEGFELELÉSHEZ

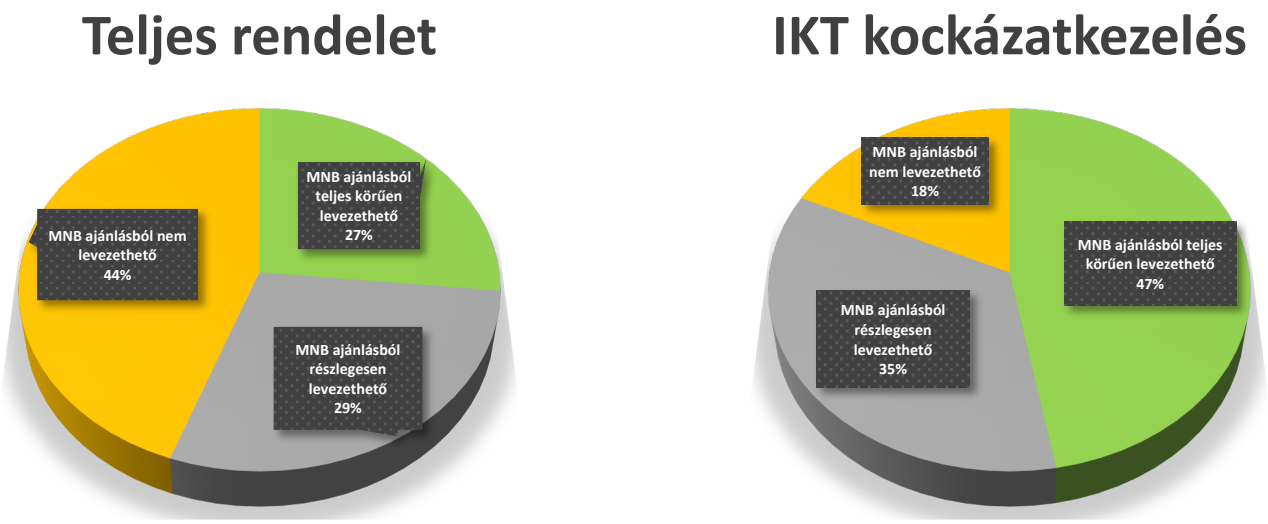
A pénzügyi ágazat digitális működési rezilienciájáról szóló (EU) 2022/2554 rendelet, közismertebb nevén DORA, 2023. január 17-én lépett hatályba és a tagországokban a két éve felkészülési időt követően, 2025. januártól lesz kötelezően alkalmazandó. A rendelet sajátossága, hogy kritikus részletszabályait jelentős részben szabályozástechnikai standardtervezeteket (Regulatory Technical Standard (RTS)) fogják megállapítani, melyek véglegesítésére a kijelölt szakhatóságoknak 12, illetve 18 hónap áll rendelkezésükre, így megjelenésük 2023. harmadik negyedévére és év végére várható.

A probléma a fentiekből adódik, mely szerint azoknak a pénzügyi szervezeteknek akik bevárják az RTS-ek és a kapcsolódó felügyeleti ajánlások aktualizálását, várhatóan kevesebb, mint egy év áll majd rendelkezésükre a megfelelés elérésére. Figyelembe véve a pénzügyi szervezetekre jelenleg is nehezedő megfelelőségi és audit terheket valamint, hogy a megfelelés elérése számos szervezet esetében csak új kontrollok, eszközök és folyamatok beszerzésével és fejlesztésével lesz várhatóan elérhető, az elképzelés nehezen megvalósítható feladatnak látszik. **Ügyfeleink részére ezért a jelen segédletben meghatározott pro-aktív megközelítést javasoljuk alkalmazni, mely alkalmas az új erőforrást, képességet és tapasztalatot igénylő hiányosságok korai azonosítására.** A teljes körű megfelelés eléréséhez hatékony segítséget nyújthat cégünk PCP üzletmenet-folytonosság tervezést és IT kockázatelemzést támogató alkalmazása, melynek részleteiről jelen dokumentum második részében írunk.

A megfelelés eléréshez javasolt eljárásrend:

01

Gap elemzés lefolytatása a rendelet II.-V. fejezeteiben foglalt követelményekre: bár az RTS-ek ismerete nélkül teljes körű gap-elemzés lefolytatása nem lehetséges, a rendelet maga is számos, a jogszabályokból és kapcsolódó MNB ajánlásokból (8/2020, 12/2020, 4/2019, 7/2020) nem vagy csak részben levezethető követelményt fogalmaz meg. A gap elemzés célszerűségét jól szemlélteti az alábbi két grafikon, mely a teljes rendelet valamint az RTS-ek ismerete nélkül leginkább feldolgozható IKT kockázatkezelés fejezet tekintetében mutatja be az MNB ajánlásokból részben vagy egészben levezethető előírások arányát a teljesen új követelményekhez viszonyítva.



A gap elemzés során javasolt azokra a követelményekre a hangsúlyt fektetni, melyek konkrét eredményterméket határoznak meg, így a felügyeleti szervek által is könnyedén számon kérhetőek. A teljesség igénye nélkül pár példa azon követelményekre, melyek várhatóan a legtöbb pénzügyi szervezetnél, mint feladatok fognak megjelenni:

Feladatok:

- Digitális rezilienciára vonatkozó stratégia megalkotása a rendelet szerinti tartalommal.
- Rendszeres (havi) vezetői jelentés a rendelet szerinti tartalommal (kockázatelemzésre kiterjedően is) a harmadik félnek minősülő IKT-szolgáltatókról.
- A harmadik félnek minősülő IKT-szolgáltatókkal kötött megállapodások keretében kiszervezett vagy megbízásba adott kulcsfontosságú vagy lényeges funkciókra vonatkozóan ÜMF tervek elkészítése.
- Digitális működési reziliencia tesztelését szolgáló program kialakítása a rendelet szerinti tartalommal.
- Harmadik félnek minősülő IKT-szolgáltatók pontosabb és szélesebb körű (nem csak kiszervezések és felhő szolgáltatások) nyilvántartása és kockázatainak elemzése.
- Ügyfelek, partnerek, valamint adott esetben a nyilvánosság felelős tájékoztatását lehetővé tevő kommunikációs eljárásrend kialakítása, valamint ehhez kapcsolódóan a nyilvános és médiaszóvivő szerepkör kialakítása.
- Kiber-fenyegetettségek és incidensek azonosításának, nyomon követésének és elemzésének (riportolásának) rendelet szerint megkövetelt érettségi szintjének eléréséhez szükséges feladatok.

02 **Road-map készítése a gap elemzés során feltárt eltérések megszüntetésére.**

03 **RTS-ek megjelenését követő legrövidebb időn belül gap-elemzés lefolytatása:** a tapasztalatok azt mutatják, hogy a szabályozástechnikai standardtervezetektől nem sokban térnek a végleges standardok, így a tervezetek megjelenését követően azonnal javasolt elkezdeni azok feldolgozását.

04 **Road-map kiegészítése, felülvizsgálata a gap elemzés során feltárt eltérések megszüntetésére.**

05 **Felügyeleti (MNB) ajánlások, útmutatók megjelenése, aktualizálása követő legrövidebb időn belül gap-elemzés lefolytatása:** az MNB ajánlások, útmutatók felülvizsgálata, kiegészítése az RTS-ek publikálását követően várható, mely a fenti eljárásrendet követve már csekély mennyiségű új feladat kell, hogy eredményezzen.

06 **Road-map kiegészítése, felülvizsgálata a gap elemzés során feltárt eltérések megszüntetésére.**

07 **Feltárt eltérések teljes körű megszüntetése:** a teljes körű megfelelés elérését a rendelet hatálya alá tartozó szervezeteknek 2025. január 17-ig kell biztosítaniuk.

Miben tud a PRAUDIT segíteni?

A PRAUDIT szakértői csapata a DORA rendeletnek történő teljes körű megfelelésig tartó út minden szakaszában támogatást tud nyújtani ügyfeleinek, egészen a gap elemzés lefolytatásától, a szabályozástechnikai standardtervezetek nyomon követésén át, az akciótervek elkészítéséig. Szakértőink támogatást tudnak nyújtani a jelenlegi szabályozó környezet átdolgozásában, illetve az új kontroll folyamatok, szabályozók és minta dokumentumok elkészítésében.

DORA felkészülés és megfelelés támogatása PCP alkalmazással:

praudit
continuity
planner

A digitális működési rezilienciáról szóló rendelet, közismertebb nevén DORA, az üzletmenet-folytonosság tervezés (BCM) és kockázatelemzés terén számos új és az eddigi jogszabályi és felügyeleti elvárásoknál szigorúbb kontrollt ír elő a pénzügyi szervezetek számára. **A megfelelés rendszerszemléletű módszertan és támogató célalkalmazás nélkül még nehezebben lesz véleményünk szerint megvalósítható.**

A PCP a PR-AUDIT Kft. évek óta sikerrel alkalmazott üzletmenet-folytonosság tervezést és információbiztonsági kockázatelemzést támogató alkalmazása, mely megoldást nyújt a DORA rendeletben az IKT kockázatkezelési keretrendszer részeként meghatározott alábbi követelmények rendszerszemléletű teljesítéséhez:

- Folyamatfelmérés, üzleti hatáselemzés és függőségelemzés végrehajtása, valamint az adatvagyon feltérképezése és osztályozása révén a pénzügyi szervezet kulcsfontosságú funkcióinak, szolgáltatásainak és erőforrásainak azonosítása.

- A harmadik félnek minősülő IKT-szolgáltatóktól függő folyamatok azonosítása, a harmadik félnek minősülő IKT-szolgáltatókkal meglévő kapcsolatok dokumentálása.

- Harmadik félnek minősülő IKT-szolgáltatókkal kötött megállapodások keretében kiszervezett vagy megbízásba adott kulcsfontosságú vagy lényeges funkciókra vonatkozóan ÜMF tervek elkészítése.

- Kulcsfontosságú (kritikus) IKT-rendszerek IKT-kockázatainak éves gyakoriságú, célzott értékelése, kockázatmenedzsment folyamatok széles körű támogatása.

- Kulcsfontosságú funkciók, szolgáltatások és erőforrások azonosításával a rendelet szerinti feladatok – pl. reziliencia tesztelése, kockázatértékelés, ÜMF tervezés - hatókörének pontosabb, így költséghatékonyabb meghatározása.

- IKT-vonatkozású üzletmenet-folytonossági tervek szükségességének azonosítása, a tervek létrehozása, melyek tartalmazzák a további károk megelőzéséhez szükséges eljárásrendeket, valamint a 11. cikkel összhangban kialakított célzott elhárítási és helyreállítási intézkedéseket.

- IKT-vonatkozású üzletmenet-folytonossági vonatkozású és katasztrófa utáni helyreállítási tervek, tesztelési és incidens jegyzőkönyvek és alapadatok egységes nyilvántartása.

További információkért, kérjük vegye fel a kapcsolatot velünk:

dr. Pataki-Vízi Linda
linda.vizi@praudit.hu

dr. Kőmíves Balázs
balazs.komives@praudit.hu

PR-AUDIT Kft.

A PR-AUDIT Professzionális Informatikai Kft. a hazai információbiztonsági piac megkerülhetetlen szereplője 2003 óta. A PR-AUDIT széleskörű auditori tapasztalattal rendelkező, informatikai, műszaki és jogi végzettségű szakemberekből áll, akik diplomájukon felül különböző minősítésekkel rendelkeznek. Minden átfogó audit projektünkön a különböző szakértelmet igénylő szakterületi részeken az erre szakosodott kolléga dolgozik.

Cégünk hosszú évek óta végez főként a pénzügyi szervezetek részére információbiztonsági, informatikai átvilágításokat és célauditokat, IT biztonsági kockázatelemzéseket és alakít ki átfogó szabályozó környezetet. Etikus hacker csapatunk évente több száz betörési tesztet, sérülékenységi vizsgálatot, alkalmazásbiztonsági auditot és forráskód elemzést végez. Ügyfeleink a kis cégektől a nagy multinacionális cégekig minden szegmensből évek óta visszatérő partnereink.