DIGITAL OPERATIONAL RESILIENCE ACT

AAMCONSULTING

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE
a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról

Általános Információk

A rendelet célja: A kiberfenyegetések elleni védekezés, kockázatkezelés, adat- és információbiztonság koordinálása és összehangolása az EU-n belül.

Felkészülési határidő: 2025. január 17. (további szabályozástechnikai standardok 2024. január 17-ig és 2024. július 17-ig lesznek elérhetőek).

Érintett szervezetek: A rendelet a pénzügyi szervezetekre (hitelintézetek, pénzforgalmi intézmények, biztosítótársaságok, befektetési társaságok stb.) és a harmadik félként igénybe vett IKT szolgáltatókra vonatkozik.

Büntetések: A tagállamok által kerülnek meghatározásra a rendelet megsértése esetén alkalmazandó közigazgatási szankciók és korrekciós intézkedések. A „kritikus IKT harmadik fél szolgáltatók" esetében a lehetséges büntetés mértéke az előző üzleti év átlagos napi világméretű forgalmának legfeljebb 1 százaléka.

A DORA RENDELETBEN MEGHATÁROZOTT FŐBB KÖVETELMÉNYEK

IKT Kockázatkezelés

- Folyamatos részvétel az IKT-kockázatok nyomon követésében, az irányítási és ellenőrzési keretrendszer fejlesztése (ideértve a politikákat és eljárásokat, szerepeket és felelősségi köröket, kockázati tűréshatárokat, fő teljesítménymutatókat, üzletmenet-folytonossági tervet, üzleti hatáselemzést, a digitális működés ellenálló képességére vonatkozó képzést).
- IKT incidensek felülvizsgálati folyamatának végrehajtása (tanulságok levonása, elemzés) és IKT tudatossági programok bevezetése.

Digitális működési ellenállókészség tesztelése

- A pénzügyi funkciók folyamatos digitális működési ellenálló képességének tesztelése, a felkészültség figyelemmel kísérése, a gyengeségek és hiányosságok azonosítása, valamint a korrekciós intézkedések végrehajtása.
- A digitális működési ellenálló képesség tesztelése szoftveres megoldások alkalmazásával (Threat Lead Pen Testing (TLPT), stb.)

IKT-val kapcsolatos incidensek kezelése, osztályozása és jelentése

- A biztonsági események megfigyelési és jelentési folyamatainak harmonizálása és a jelentési módszer szabványosítása.

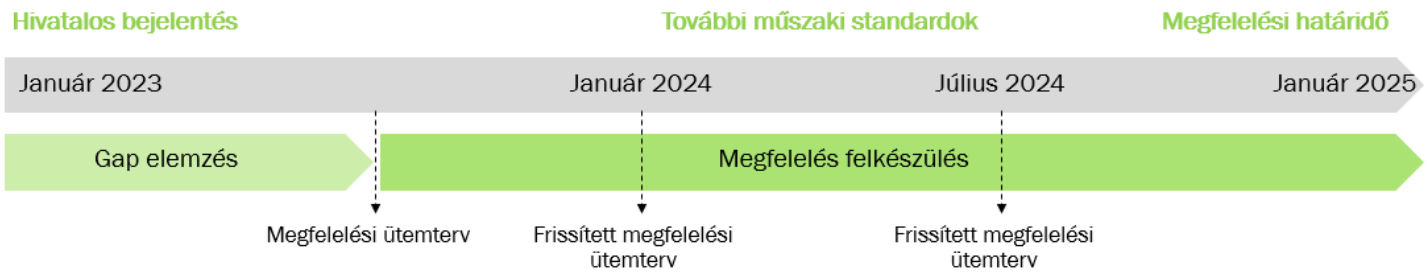
IKT harmadik féllel szembeni kockázatok kezelése

- Harmadik fél szolgáltatókkal kapcsolatos IKT kockázatok monitorozása, ellenőrzése, mérése.

Információmegosztási megállapodások

- Szabványosított formában történő jelentés készítése az illetékes pénzügyi hatóságok felé . Az információkat továbbítani kell az Európai Felügyeleti Hatóság által felügyelt vizsgálati csoportnak.

Az AAM megközelítése



Gap elemzés szakasz— Az AAM elvégzi a szervezet rendelet követelményeinek való megfelelésének kezdeti értékelését, valamint javaslatokat tesz a szükséges javításokra és változtatásokra. A fázis végén az AAM helyzetfelmérési jelentést és a megfelelésre vonatkozó ütemtervet készít.

Megfelelés felkészülés szakasz — Az AAM segítséget nyújt a kontroll hiányosságok értékelése során feltárt meg nem felelések kezelésében. Az AAM folyamatosan frissíti a végrehajtási ütemtervet, amint további hivatalos műszaki standardok kerülnek közzétételre.

AAMCONSULTING

1133 Budapest, Hungary,
Capital Square Office, Váci út 76.
Telephone: +36 1 465 2070
Web: www.aam.hu

1000 Sofia, Bulgaria,
17 Moskovska St., 3rd floor
Telephone: +359 883 22 54 77
Web: www.aamconsulting.bg

DIGITAL OPERATIONAL RESILIENCE ACT

AAMCONSULTING

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

Elvégzendő megfelelési feladatok és kapcsolódó AAM-szolgáltatások

Az IKT kockázatkezelés keretrendszer fejlesztése és testre szabása

Az IKT-val kapcsolatos üzleti funkciók (vezetői ellenőrzés, belső ellenőrzés stb.) azonosítása, osztályozása és dokumentálása, valamint a kapcsolódó IKT-rendszerek konfigurálása.

FŐBB SZOLGÁLTATÁSAINK

- A digitális ellenálló képességre vonatkozó stratégia kidolgozása;
- Irányítás - az IT-biztonsági követelmények integrálása a szervezeten belül;
- Kockázatkezelési módszertan és kockázatkezelési terv kidolgozása;
- Belső és külső eljárások és szabályzatok kidolgozása;

Digitális ellenállóképesség vizsgálata

A kulcsfontosságú IKT-rendszerek, dokumentumok és alkalmazások legalább évente egyszeri tesztelése és felülvizsgálata. A szervezet kulcsfontosságú funkcióit és szolgáltatásait háromévente kell tesztelni, olyan fejlett módszerekkel, mint a fenyegetésalapú behatolásvizsgálat.

FŐBB SZOLGÁLTATÁSAINK

- Tesztelési stratégia és forgatókönyvek meghatározása;
- Tesztelési módszertanok és eljárások kidolgozása
- Teszttervek elkészítése, a terjedelem meghatározása;
- A tesztelési folyamat koordinálása;
- Tesztjelentési struktúrák kidolgozása;
- Iránymutatás nyújtása a hatóságoknak történő digitális jelentéstételhez;

A harmadik felek IKT-kockázatainak nyomon követésére vonatkozó feltételek meghatározása

Harmadik felekkel való együttműködés kezdetétől fogva, a beszállítóval szembeni követelmények meghatározása, dokumentációk, szolgáltatások, kockázatértékelések vizsgálata

FŐBB SZOLGÁLTATÁSAINK

- IKT kockázatikezelési stratégia és szabályozás kidolgozása/felülvizsgálata;
- Harmadik félre vonatkozó kockázatok felmérése / harmadik fél auditálása
- Harmadik fél IKT kockázati eljárásainak integrálása a vállalat kockázatkezelési keretrendszerébe;
- A megfelelés és a harmadik féllel kötött szerződések értékelése;
- Kilépési stratégia és átmeneti terv meghatározása;

Az IKT-keretrendszer és az eseménykezelés felülvizsgálata

Az IKT-rendszerek információbiztonságának a rendeletben előírt rendszeres felülvizsgálatának megtervezése, koordinálása, észrevételek dokumentálása és cselekvési tervek készítése. A jelentős kockázatok figyelemmel kísérése, nyilvántartása a hatóságoknak történő jelentése, valamint a felügyeleti ellenőrzésekből származó visszajelzések kezelése.

FŐBB SZOLGÁLTATÁSAINK

- A terv felülvizsgálatának előkészítése;
- A felülvizsgálati folyamat koordinálása;
- A kapott eredmények rögzítése és értékelése;
- Megelőző és javító intézkedések meghatározása;
- Az események azonosítása, a kapott eredmények nyomon követése és kezelése, naplóelemzés és az eseménykezelési folyamat támogatása;

AAMCONSULTING

1133 Budapest, Hungary,
Capital Square Office, Váci út 76.
Telephone: +36 1 465 2070
Web: www.aam.hu

1000 Sofia, Bulgaria,
17 Moskovska St., 3rd floor
Telephone: +359 883 22 54 77
Web: www.aamconsulting.bg