

Microsec zrt.

**Segédlet a DORA szerinti besoroláshoz,
az előzetes kockázatértékeléshez és
átvilágításhoz**

V1.2



Tartalom

1	Bevezetés.....	3
2	Besorolási szintek ismertetése	3
2.1	Alap	3
2.2	Kritikus vagy fontos funkciót támogató IKT szolgáltatás	4
2.3	Kritikus harmadik fél IKT-szolgáltató	4
3	A módszertan kidolgozása és a besorolás	5
3.1.1	Alap kategóriába javasolt sorolni	5
3.1.2	Kritikus vagy fontos funkciót támogató IKT szolgáltatás kategóriába javasolt sorolni	6
3.1.3	Miért nem javasolt bármit besorolni indokolatlanul magasabb szintre?.....	6
4	A Microsec zrt. által elvégzett és ügyfelei számára javasolt termékbesorolás	7
5	Segédlet az Előzetes kockázatértékeléshez és az Átvilágításhoz.....	8
6	Dokumentum verzió kezelés	12

1 Bevezetés

A DORA rendelet¹ (Digital Operational Resilience Act) egy olyan EU-s pénzügyi szabályozás, amely a pénzügyi szektor működési biztonságára összpontosít.

Szabályokat és előírásokat határoz meg a pénzügyi szervezetek számára információs és kommunikációs technológiával kapcsolatos események észlelésére, védelmére, helyreállítására és javítására a pénzügyi szervezeteken belül. Ennek a szabályozásnak része, hogy a harmadik feles IKT szolgáltatók (tehát olyan szolgáltatók, akik a pénzügyi szervezet részére szolgáltatnak) tevékenységet is nyomon kövesse a pénzügyi szervezet, biztos lehessen ezen szolgáltatók biztonságában is.

2 Besorolási szintek ismertetése

A harmadik feles IKT szolgáltatók tevékenységének nyomon követéséhez a pénzügyi szervezetnek be kell sorolnia azokat. Három besorolási szint létezik, és ezek különböző követelményeket várnak el:

2.1 Alap

Sajnos a DORA nem adott nevet a kategóriának, de a következőkben Alap szintként hivatkozunk rá.

Ez esetben harmadik féllel kötött szerződésnek a Rendelet 30. cikk (2) paragrafusában leírtakat kell tartalmaznia, és annak kell meg is felelni.

Ezek nagyon röviden:

- Szolgáltatás teljes körű leírása (dokumentáció),
- Alvállalkozó igénybevételének szabályai,
- Szolgáltatás földrajzi helyének megjelölése,
- Adatvédelmi rendelkezések,
- Adatvisszaszolgáltatási rendelkezések,
- Hatósági együttműködési kötelezettség,
- Szerződés megszüntetési rendelkezések,
- Részvételi kötelezettség a pénzügyi szervezet biztonságtudatossági képzésein.

¹ <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2554>

2.2 Kritikus vagy fontos funkciót támogató IKT szolgáltatás

A rendelet definíciója szerint a „kritikus vagy fontos funkció”: olyan funkció, amelynek zavara lényegesen rontaná a pénzügyi szervezet pénzügyi teljesítményét, vagy szolgáltatásai és tevékenységei megbízhatóságát vagy folytonosságát, vagy az említett funkció kiesése, hibás vagy meghíúsult működése lényegesen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére.

A kritikus vagy fontos funkciót támogató IKT szolgáltatás esetben harmadik féllel kötött szerződésnek tartalmaznia mindent, ami Alap szintnél szükséges, valamint két további lényeges dolgot:

- A harmadik feles IKT szolgáltató vezessen be a DORA-nak megfelelő vészhelyzeti terveket, és olyan IKT biztonsági intézkedéseket, mint a sérülékenység vizsgálat, penetrációs vizsgálat és a kódelemzés.
- Vegyen rész a veszély alapú (TLPT) behatolás tesztelésben.

2.3 Kritikus harmadik fél IKT-szolgáltató

Ezt a besorolást az erre feljogosított hatóság osztja ki. Jelenleg nincs ilyen.

3 A módszertan kidolgozása és a besorolás

A 2024/1773/CID 3. cikk (2) bekezdése alapján a pénzügyi szervezet által kidolgozott módszertanon kell alapulnia a harmadik feles IKT szolgáltatások besorolásának. Ennek alapján a következőképpen érdemes eljárni, figyelembe véve a kockázatkezelés alapelveit.

3.1.1 Alap kategóriába javasolt sorolni

Az itt felsorolt esetek mindegyikére jellemző, hogy a termék/szolgáltatás kiváltása piaci termékkel rövid idő alatt biztosítható:

- Minden olyan szolgáltatást, amely használata során nem integrált, és aminek van alternatív lehetséges forrása.
- Nyílt, szabványos felülettel integrált szolgáltatásokat
- Ezek esetében a szabványos felület lehetővé teszi, hogy egy ugyanezen interfészt támogató alternatív szolgáltatóhoz a szolgáltatás átvihető legyen.
- Nem egyedi fejlesztésű szoftvereket.

Az Alap szintre besorolásban továbbá segíthet a Bizottság (EU) 2017/565 felhatalmazáson alapuló rendelet 30. cikk (1) és (2) is, amely a következőt mondja:

(1) A 2014/65/EU irányelv 16. cikke (5) bekezdése első albekezdésének alkalmazásában az operatív funkció akkor tekintendő kritikusnak vagy fontosnak, ha a teljesítésében bekövetkezett hiányosság vagy hiba lényegesen gyengítené a befektetési vállalkozás folyamatos megfelelését az engedélyezéséhez szükséges feltételeknek és kötelezettségeknek vagy a 2014/65/EU irányelvből eredő egyéb kötelezettségeinek, illetve gyengítené pénzügyi teljesítményét és befektetési szolgáltatásainak és tevékenységeinek megalapozottságát vagy folyamatosságát.

(2) A többi funkció státusának sérelme nélkül a következő funkciók nem tekinthetők kritikusnak vagy fontosnak az (1) bekezdés alkalmazásában:

a) a vállalkozásnak nyújtott tanácsadói szolgáltatások és egyéb, a vállalkozás befektetési tevékenységének részét nem képező szolgáltatások, beleértve a vállalkozásnak nyújtott jogi tanácsadást, a vállalkozás alkalmazottainak képzését, a számlázási szolgáltatásokat és a vállalkozás helyiségeinek és alkalmazottainak biztonságát is;

b) szabványosított szolgáltatások megvásárlása, beleértve a piaci információs szolgáltatásokat és árfolyamok szolgáltatását.

Ez alapján számos szolgáltatás minősíthető Alap szintre.

3.1.2 Kritikus vagy fontos funkciót támogató IKT szolgáltatás kategorizálás

Az itt felsorolt esetek mindegyikére jellemző, hogy a termék/szolgáltatás kiváltása piaci termékkel rövid idő alatt gyorsan nem megoldható:

- Minden olyan szolgáltatást, amely használata során nem nyílt, szabványos felülettel integrált, és kiváltása hosszabb ideig tartana.
- Egyedi szoftverfejlesztés szolgáltatás keretében fejlesztett szoftver

3.1.3 Miért nem javasolt bármit besorolni indokolatlanul magasabb szintre?

Az indokolatlanul kritikus vagy fontossá minősítés ellen az szól, hogy az Alap szinthez képest a következő követelményeket (amelyekhez erőforrást is kell rendelni) rója a pénzügyi szervezetre:

- A 28. cikk (8) szerint a kritikus vagy fontos funkciókat támogató szolgáltatások esetében kilépési stratégiákat is ki kell dolgoznia és be kell vezetnie a pénzügyi szervezetnek, és ezt TESZTELNI is kell.

Ez gyakorlatban azt jelentheti, hogy egy kritikus és fontos funkciót támogató IKT rendszer esetében egy másik szolgáltatótól is szükséges lehet beszerezni és tesztelni is egy ekvivalens szolgáltatást, hogy az arra történő átállás feltételei teljesülhessenek.

- A 29. cikk szerint a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások esetén szükséges az IKT-koncentrációs kockázat értékelése, és az eredményének megfelelő kontroll intézkedések végrehajtása.

4 A Microsec zrt. által elvégzett és ügyfelei számára javasolt termék-besorolás

A Microsec zrt., hogy üzletfelei számára megkönnyítse a DORA megfelelést, elvégezte saját maga is termékei/szolgáltatása DORA szerinti besorolását, melyet javasol használni.

A besorolást az alábbi táblázat tartalmazza.

Kategória	Csoport	Termékek
Alap	Nem integráltan használt szolgáltatások	Aláíró tanúsítványok Tárolt kulcsos távoli aláíró szolgáltatás (web-szignó vagy mobil app felülettel) Bélyegző tanúsítványok SSL tanúsítványok PSD2 tanúsítványok Időbélyegzés Archiválás OCCR
Alap	Nyílt, szabványos felülettel integrált szolgáltatások	Tárolt kulcsos távoli aláíró szolgáltatás, CSC interfészen
Alap	Nem egyedi fejlesztésű szoftverek	e-Szignó Desktop e-Szignó SDK e-Szignó Hitelesítő Szerver e-Szignó PDF Autosigner Microsigner Microsigner SDK web-Szignó on-premise MicroCA/MicroAC Suite Scan & Sign – offline és online
Kritikus vagy fontos funkciót támogató IKT szolgáltatás	Nem nyílt, szabványos felülettel integrált szolgáltatás (A kiváltása hosszabb ideig tartana.)	Tárolt kulcsos távoli aláíró szolgáltatás, a pénzügyi szervezetnél telepített Webszignó alkalmazással (aláíró felülettel)

5 Segédlet az Előzetes kockázatértékeléshez és az Átvilágításhoz

A pénzügyi szervezett számára a 2024/1773/CID 5. cikke szerinti szükséges előzetes kockázatértékelés, valamint a 6. cikk szerinti átvilágítás a harmadik feles IKT szolgáltatókkal kapcsolatosan.

Ezen feladatok megkönnyítéséhez összegyűjtöttük az alábbi táblázatba a Microsec bizalmi szolgáltatásával kapcsolatosan az előre megválaszolható kérdésekre a válaszokat.

Röviden összefoglalva: a bizalmi szolgáltatások esetében javasoljuk a pénzügyi szervezetek felé, hogy a kockázatértékeléshez és az átvilágításhoz használják fel tanúsításainkat, mint harmadik féltől származó vizsgálat eredményét.

Jogszábai szakasz	Vizsgálandó rész	Válasz	Igazolás
5. cikk (2) a)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] működési kockázatok;	Lásd 6. cikk (1) b) és 5. cikk (2) b)	-
5. cikk (2) b)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] jogi kockázatok;	A Szolgáltató bizalmi szolgáltatóként kötelezett, hogy a 24/2016 BM. rendelet 5. §-a szerint és célokra rendelkezzen felelősségbiztosítással, valamint a Szolgáltató megszűnésével kapcsolatos kockázatokra a 19-22. § szerint pénzügyi garanciával.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.
5. cikk (2) c)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] IKT-kockázatok;	Lásd 6. cikk (1) b)	-

Jogsabályi szakasz	Vizsgálandó rész	Válasz	Igazolás
5. cikk (2) d)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] reputációs kockázatok;	Lásd 6. cikk (1) a) 1	-
5. cikk (2) e)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] a bizalmas vagy személyes adatok védelméhez kapcsolódó kockázatok;	A Szolgáltató bizalmi szolgáltatóként az adatokat a Dáptv. 88. § (1) előírásai szerint kezeli, őrzi meg, és törli.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.
5. cikk (2) f)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] az adatok rendelkezésre állásával kapcsolatos kockázatok;	Lásd 5. cikk (2) e)	-
5. cikk (2) g)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] az adatkezelés és az adattárolás helyéhez kapcsolódó kockázatok;	A Szolgáltató adatkezelésének országai: Magyarország, Spanyolország	Az Adakezelési tájékoztató tartalmazza ezt: https://www.microsec.hu/api/?func=cms.media&file=/pdf/microsec-adatkezelesi-tajekoztato-v1.14.pdf
5. cikk (2) h)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] a harmadik fél IKT-szolgáltató helyéből eredő kockázatok;	A Szolgáltató telephelyének országa: Magyarország.	A cégnyilvántartásból ellenőrizhető: https://www.e-cegjegyzek.hu/

Jogszábai szakasz	Vizsgálandó rész	Válasz	Igazolás
6. cikk (1) a) 1	Rendelkezik-e üzleti hírnévvel?	Igen, a Szolgáltató 40 éves és több mint 20 éve nyújt bizalmi szolgáltatásokat.	https://www.microsec.hu/hu/cegtortenet
6. cikk (1) a) 2	[Rendelkezik-e] megfelelő képességekkel, szakértelemmel és kellő pénzügyi, humán és technikai erőforrásokkal, információbiztonsági előírásokkal, megfelelő szervezeti felépítéssel, kockázatkezeléssel és belső kontrollokkal	A Szolgáltatóra az eIDAS és a Dáptv. továbbá a vonatkozó szabványok kifejezetten előírásokat támasztanak ezekre vonatkozóan, ezek alapján évente megfelelőség értékelésre kerül A Szolgáltató továbbá ISO 9001 és ISO 27001 tanúsításokkal is rendelkezik. Ezen felül a Szolgáltató tovább alanya a NIS2 tanúsításnak, amely hamarosan lehetségessé válik	A Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt, mely folyamatosan elérhető az alábbi linkeken: eIDAS és Dáptv. szerinti megfelelőség értékelés https://e-szigno.hu/eidas-megfeleles ISO 9001 és ISO 27001 tanúsítások https://www.microsec.hu/hu/minosegbiztonsag-es-audit NIS2 tanúsítás Amint lehetséges a tanúsítás, azok eredménye is közzétételre kerül.

Jogsabályi szakasz	Vizsgálandó rész	Válasz	Igazolás
6. cikk (1) a) 3	[Rendelkezik-e] IKT-szolgáltatások megbízható és professzionális nyújtásához szükséges engedélyekkel vagy regisztrációval	A Szolgáltató bizalmi szolgáltatóként nyilvántartásba vett az NMHH-nál. A Szolgáltató NIS2/kiberbiztonsági törvény alanyként nyilvántartásba vett az SZTFH-nál.	A Szolgáltató ezen követelménynek történő megfelelésének ellenőrzésére a nyilvántartások ellenőrzése javasolt: NMHH https://esign.nmhh.hu/bszny/ SZTFH Jelenleg nem ismert kereshető nyilvántartás.
6. cikk (1) b)	képes-e arra, hogy nyomon kövesse a releváns technológiai fejleményeket, azonosítsa az IKT-biztonsággal kapcsolatos legfontosabb gyakorlatokat, és adott esetben alkalmazza azokat annak érdekében, hogy a digitális működési rezilienciára vonatkozóan hatékony és megbízható keretet biztosítson;	A Szolgáltató bizalmi szolgáltatóként kötelezett arra, hogy a technológia fejleményeket kövesse. A bizalmi szolgáltatásokra előírt az üzletmenet folytonossági tervek létezése és tesztelése, valamint a penetrációs és sérülékenységi tesztelés.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelésének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.

6 Dokumentum verzió kezelés

Verzió	Dátum	Módosítás
V1.0	2024-11-26	Első verzió
V1.1	2024-12-03	A besorolásból még hiányzó termékek hozzáadása