					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P41					Dokumentum címe: **Beszállítói függőségi kockázatkezelési szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
GDPR	28. cikk, 32. cikk (1) bekezdés d) pont	
NIS2 irányelv	21. cikk (2) bekezdés d) pont, 21. cikk (3) bekezdés, 22. cikk	
DORA-rendelet	28–30. cikk	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. cél

1.1 A szervezet ellátásilánc-biztonsági gyakorlatának megerősítése olyan folyamat bevezetésével, amely azonosítja és kezeli a beszállítóktól és szolgáltatóktól való kritikus függőségeket, összhangban a NIS2 irányelv 21. cikk (3) bekezdésével és az uniós szintű ellátásilánc-kockázatértékelésekkel.

1.2 Annak biztosítása, hogy az egy beszállítóra irányuló koncentrációból vagy az egy beszállítótól való függésből eredő kockázatok ismertek és kezeltek legyenek, továbbá hogy az ágazatspecifikus ellátásilánc-kockázatok – amelyeket a hatóságok a NIS2 22. cikke alapján kiemelnek – beépüljenek a kockázatkezelésbe és az üzletmenet-folytonossági tervezésbe.

2. hatály

2.1 Jelen szabályzat valamennyi olyan kiemelt beszállítóra és szolgáltatóra kiterjed, amelyre a szervezet kritikus működése során támaszkodik, különösen az IKT-ellátási láncban részt vevőkre (hardver, szoftver, felhőszolgáltatások, távközlés, menedzselt szolgáltatások).

2.2 Kiterjed a belső funkciókra, beleértve a Beszerzést, a beszállítókezelést, a Kockázatkezelést és az érintett operatív szervezeti egységeket. A szabályzat a kockázati információk gyűjtéséhez szükséges mértékben magukra a beszállítókra is vonatkozik. „Kritikus beszállítók” azok, amelyek kiesése vagy kompromittálódása jelentős hatással lehet a szolgáltatásnyújtási képességünkre vagy jogi kötelezettségeink teljesítésére.

3. célkitűzések

3.1 Átláthatóság biztosítása az ellátásilánc-függőségek felett, különös tekintettel az egyedi hibapontok vagy a magas koncentrációs kockázat azonosítására a beszállítói körben (például ha valamennyi szolgáltatás egyetlen felhőszolgáltatótól függ).

3.2 Intézkedések bevezetése a beszállítói kockázatok csökkentésére és kezelésére – például diverzifikáció, kerülőmegoldások és folytonossági tervek, illetve megerősített beszállítói kontrollok előírása – ezáltal növelve a rezilienciát a beszállítói kiesésekkel vagy az ellátási láncból eredő támadásokkal szemben.

3.3 A NIS2-követelményeknek való megfelelés biztosítása azáltal, hogy a kritikus ellátási láncokra vonatkozó koordinált biztonsági kockázatértékelések eredményeit (a 22. cikk szerint) beépítjük a

szervezeti kockázati döntésekbe, továbbá hogy saját ellátásilánc-kockázati megközelítésünk dokumentált és igazolható legyen.

4. szerepkörök és felelősségek

4.1 Beszállítókezelési iroda (VMO): felelős a beszállítói függőségi nyilvántartásért, és koordinálja a kockázatértékeléseket. Biztosítja, hogy a beléptetés során, valamint azt követően rendszeres időközönként minden kulcsfontosságú beszállító kritikussága és függőségi szintje értékelésre kerüljön.

4.2 Kockázatkezelés (vállalati kockázati bizottság): felülvizsgálja a koncentrációs kockázatot és a függőségi elemzéseket, támogatja a kockázatkezelési stratégiákat (például alternatív beszállító bevonásának jóváhagyása vagy biztonsági készlet fenntartása kritikus komponensekből). Az ellátásilánc-kockázatokat beépíti a teljes kockázati nyilvántartásba, és jelentést készít a felső vezetés részére.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. nyomon követés és audit

9.1 A függőségi nyilvántartást és a kockázatértékeléseket évente belső auditnak kell alávetni. A belső audit ellenőrzi, hogy minden kritikus beszállító szerepel-e a nyilvántartásban, kockázati besorolásuk naprakész-e, valamint hogy a kockázatcsökkentési tervek rendelkezésre állnak-e és megfelelően haladnak-e. Ellenőrzi továbbá azt is, hogy a külső kockázatértékelési bemeneteket (22. cikk szerinti jelentések stb.) megfelelően figyelembe vették-e.

9.2 A diverzifikációs és készenléti intézkedések hatékonyságát időszakosan tesztelni kell. Például végrehajtható olyan tervezett szimuláció, amelyben egy jelentős beszállító kiesését feltételezzük annak érdekében, hogy teszteljük üzletmenet-folytonossági terveinket és alternatív megoldásainkat (a DR-gyakorlathoz hasonlóan, de beszállítói kiesésre összpontosítva). A tesztek eredményeit dokumentálni kell, és a hiányosságokat helyesbíteni kell.

9.3 Mérőszámok: a Kockázatkezelési funkció olyan mérőszámokat követ nyomon, mint például „a kritikus szolgáltatások hány százalékához áll rendelkezésre legalább egy alternatív beszállító vagy megoldás”, illetve „az 5 legjelentősebb beszállítói függőség és azok kockázati trendje”. Ezeket a mérőszámokat a vezetés részére bemutatott kockázati irányítópultokon kell szerepeltetni. A függőségi kockázat időbeli csökkentése célkitűzés; ha a mérőszámok növekvő függőséget mutatnak, annak vezetői egyeztetést kell kiváltania.

10. felülvizsgálat és karbantartás

10.1 Jelen szabályzatot legalább évente felül kell vizsgálnia a beszállítókezelési és a Kockázatkezelési csapatnak. A felülvizsgálat során figyelembe kell venni a beszállítói környezetben bekövetkezett változásokat (például ha egy új beszállító kritikussá válik, vagy egy korábbi kivezetésre kerül), valamint a kiszervezésre vagy harmadik fél kockázataira vonatkozó új szabályozási követelményeket.

10.2 Ha az ágazati hatóságok frissített iránymutatást adnak ki, vagy egy incidens hiányosságokat tár fel (például ha egy beszállítói kiesés a vártnál nagyobb hatással jár, ami arra utal, hogy a kockázatértékelés alulbecsülte a függőséget), a szabályzatot frissíteni kell a szempontok vagy a kockázatcsökkentési stratégiák pontosítása érdekében.

10.3 A szabályzat módosított változatait a felső vezetésnek kell jóváhagynia. A jelentős változásokat minden érintett szervezeti egység felé kommunikálni kell, és a képzési anyagokat ennek megfelelően frissíteni kell az új eljárások vagy szabványok tükrözése érdekében.

11. kapcsolódó szabályzatok és összefüggések

11.1 P01 – Információbiztonsági szabályzat. Meghatározza a beszállítói függőségek irányításáért viselt elszámoltathatóságot.

11.2 P02 – Irányítási szerepkörök és felelősségek szabályzata. Egyértelművé teszi a beszállítói kockázatokkal kapcsolatos döntések tulajdonosi felelősségét.

11.3 P06 – Kockázatkezelési szabályzat. Beépíti a koncentrációs kockázatot a vállalati kockázati nyilvántartásba.

11.4 P26 – Harmadik felek és beszállítói biztonsági szabályzat. Alapszintű biztonsági követelményeket határoz meg; a P41 ehhez függőségi és koncentrációs kontrollokat ad hozzá.

11.5 P27 – Felhőszolgáltatások használatára vonatkozó szabályzat. A függőségi szempontokat alkalmazza a felhőszolgáltatások bevezetésére és a kilépési tervek kialakítására.

11.6 P28 – Kiszervezett fejlesztési szabályzat. Kezeli a külső fejlesztéssel kapcsolatos függőségi kockázatokat.

11.7 P32 – Üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzat. Tervezési keretet ad a beszállítói kiesési és helyettesítési forgatókönyvekhez.

11.8 P37 – Jogi és jogszabályi megfelelési szabályzat. Biztosítja, hogy a szerződések és kötelezettségek tükrözzék a függőségi kontrollokat.

12. hivatkozások

12.1 NIS2 irányelv (EU 2022/2555), 21. cikk (3) bekezdés (előírja az egyes közvetlen beszállítókra/szolgáltatókra jellemző sérülékenységek és kiberbiztonsági minőségük figyelembevételét, ideértve a koordinált ellátásilánc-kockázatértékelések eredményeit is)

12.2 NIS2 irányelv, 22. cikk (1) bekezdés (a kritikus ellátási láncok uniós szintű koordinált biztonsági kockázatértékelései – tájékoztatják a szervezeteket az ágazati szintű beszállítói kockázatokról)

12.3 A Bizottság (EU) 2024/2690 végrehajtási rendelete, 5. melléklet (az ellátási lánc biztonságára vonatkozó követelmények a szervezetek számára, beleértve a beszállítók kiválasztására, diverzifikálására és a szerződéses kötelezettségekre vonatkozó szempontokat)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – ajánlások a kritikus beszállítók azonosítására és a kapcsolódó kockázatok kezelésére

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022