					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P41					Názov dokumentu: **Politika riadenia rizík závislosti od dodávateľov**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
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	
Nariadenie EÚ GDPR	čl. 28, čl. 32 ods. 1 písm. d)	
Smernica EÚ NIS2	čl. 21 ods. 2 písm. d), čl. 21 ods. 3, čl. 22	
Nariadenie EÚ DORA	čl. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Účel

1.1 Zaviesť proces na identifikáciu a riadenie kritických závislostí od dodávateľov a poskytovateľov služieb s cieľom posilniť postupy bezpečnosti dodávateľského reťazca organizácie v súlade s článkom 21 ods. 3 smernice EÚ NIS2 a s posúdeniami rizík dodávateľského reťazca na úrovni Únie.

1.2 Zabezpečiť, aby riziká vyplývajúce z koncentrácie alebo závislosti od jedného dodávateľa boli identifikované a zmierňované a aby sa všetky odvetvovo špecifické riziká dodávateľského reťazca, ako ich identifikujú orgány podľa článku 22 smernice EÚ NIS2, začlenili do nášho riadenia rizík a plánovania kontinuity činností.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých kľúčových dodávateľov a poskytovateľov služieb, od ktorých je organizácia závislá pri zabezpečovaní kritických prevádzkových činností, najmä v dodávateľskom reťazci IKT (hardvér, softvér, cloudové služby, telekomunikačné služby, poskytovatelia riadených služieb).

2.2 Zahŕňa interné funkcie vrátane obstarávania, riadenia dodávateľov, riadenia rizík a príslušných prevádzkových útvarov. V rozsahu potrebnom na získavanie informácií o rizikách sa vzťahuje aj na samotných dodávateľov. „Kritickí dodávatelia“ sú tí, ktorých zlyhanie alebo kompromitácia by mohli významne ovplyvniť našu schopnosť poskytovať služby alebo plniť zákonné povinnosti.

3. Ciele

3.1 Získať prehľad o závislostiach v dodávateľskom reťazci, najmä identifikovať jednotlivé body zlyhania alebo vysoké riziko koncentrácie v našej dodávateľskej základni (napr. závislosť od jedného poskytovateľa cloudových služieb pre všetky služby).

3.2 Zaviesť opatrenia na zníženie a riadenie rizík súvisiacich s dodávateľmi, napríklad diverzifikáciu, plány pre mimoriadne situácie alebo požiadavku na zlepšenie kontrol u dodávateľov, a tým zvýšiť odolnosť voči zlyhaniam dodávateľov alebo útokom vychádzajúcim z dodávateľského reťazca.

3.3 Zabezpečiť súlad s požiadavkami smernice EÚ NIS2 začlenením výsledkov všetkých koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov podľa článku 22 do rozhodovania organizácie o rizikách a zabezpečiť, aby bol náš prístup k rizikám dodávateľského reťazca zdokumentovaný a preukázateľný.

4. Roly a zodpovednosti

4.1 Kancelária riadenia dodávateľov (VMO): zodpovedá za register závislostí od dodávateľov a koordinuje hodnotenia rizík. Zabezpečuje, aby bol pri zavedení dodávateľa a následne v pravidelných intervaloch každý kľúčový dodávateľ posúdený z hľadiska kritickosti a úrovne závislosti.

4.2 Útvar riadenia rizík (Výbor pre podnikové riziká): preskúmava riziko koncentrácie a analýzy závislostí, schvaľuje stratégie ošetrenia rizík (napr. schválenie pridania alternatívneho dodávateľa alebo vytvorenia dodatočných zásob kritických komponentov). Začleňuje riziká dodávateľského reťazca do celkového registra rizík a predkladá správy vrcholovému manažmentu.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Monitorovanie a audit

9.1 Register závislostí a posúdenia rizík budú každoročne predmetom interného auditu. Tím vnútorného auditu overí, že všetci kritickí dodávatelia sú evidovaní, že ich hodnotenia rizika sú aktuálne a že existujú plány zmierňovania rizík, ktoré sa priebežne realizujú. Overí tiež, že externé vstupy z posúdení rizík (správy podľa článku 22 a pod.) boli riadne zohľadnené.

9.2 Účinnosť diverzifikačných a kontingenčných opatrení sa bude pravidelne testovať. Napríklad sa môže vykonať plánovaná simulácia, v ktorej sa predpokladá zlyhanie významného dodávateľa, s cieľom otestovať naše plány kontinuity činností a alternatívne opatrenia (podobne ako pri cvičení obnovy po havárii, ale pre výpadok dodávateľa). Výsledky týchto testov sa dokumentujú a zistené nedostatky sa odstraňujú.

9.3 Metriky: útvar riadenia rizík bude sledovať metriky, ako sú „% kritických služieb, pre ktoré je dostupný aspoň jeden alternatívny dodávateľ alebo riešenie“ alebo „Top 5 závislostí od dodávateľov a ich trend rizika“. Tieto metriky budú zahrnuté do panelov rizík pre vedenie. Klesajúci trend rizika závislosti v čase je cieľom; ak metriky ukazujú rastúcu závislosť, musí to viesť k diskusii na úrovni manažmentu.

10. Preskúmanie a údržba

10.1 Túto politiku budú najmenej raz ročne preskúmavať tímy riadenia dodávateľov a riadenia rizík. Preskúmanie zohľadní všetky zmeny v prostredí dodávateľov (napr. ak sa nový dodávateľ stane kritickým alebo existujúci dodávateľ bude postupne vyradený) a všetky nové regulačné požiadavky týkajúce sa outsourcingu alebo rizika tretích strán.

10.2 Ak odvetvové orgány vydajú aktualizované usmernenia alebo ak incident odhalí nedostatky (napríklad ak mal výpadok dodávateľa väčší dopad, než sa predpokladalo, čo znamená, že naše posúdenie rizík nesprávne vyhodnotilo závislosť), politika sa aktualizuje s cieľom spresniť kritériá alebo stratégie zmierňovania rizík.

10.3 Revidované verzie politiky musí schváliť vrcholový manažment. Významné zmeny budú oznámené všetkým relevantným útvarom a školiace materiály budú primerane aktualizované tak, aby odrážali nové postupy alebo štandardy.

11. Súvisiace politiky a väzby

11.1 P01 – Politika informačnej bezpečnosti. Určuje zodpovednosť za správu a riadenie závislostí od dodávateľov.

11.2 P02 – Politika rolí a zodpovedností v oblasti správy a riadenia. Spresňuje vlastníctvo rozhodnutí o rizikách súvisiacich s dodávateľmi.

11.3 P06 – Politika riadenia rizík. Začleňuje riziko koncentrácie do podnikových registrov rizík.

11.4 P26 – Politika bezpečnosti tretích strán a dodávateľov. Stanovuje základnú bezpečnostnú úroveň; P41 dopĺňa kontroly závislosti a koncentrácie.

11.5 P27 – Politika používania cloudových služieb. Uplatňuje kritériá závislosti pri prijímaní cloudových služieb a plánovaní ukončenia.

11.6 P28 – Politika outsourcovaného vývoja. Pokrýva riziká závislosti pri externom vývoji.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Plánuje scenáre výpadku alebo nahradenia dodávateľa.

11.8 P37 – Politika právnych a regulačných požiadaviek súladu. Zabezpečuje, aby zmluvy a povinnosti zohľadňovali kontroly závislosti.

12. Referencie

12.1 Smernica NIS2 (EÚ 2022/2555), článok 21 ods. 3 (vyžaduje zohľadnenie zraniteľností špecifických pre každého priameho dodávateľa alebo poskytovateľa služieb a kvality ich kybernetickej bezpečnosti vrátane výsledkov koordinovaných posúdení rizík dodávateľského reťazca)

12.2 Smernica NIS2, článok 22 ods. 1 (koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie – informujú subjekty o rizikách dodávateľov v rámci celého odvetvia)

12.3 Vykonávacie nariadenie Komisie (EÚ) 2024/2690, príloha, oddiel 5 (požiadavky na bezpečnosť dodávateľského reťazca pre subjekty vrátane kritérií výberu dodávateľov, diverzifikácie a zmluvných povinností)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – odporúčania na identifikáciu kritických dodávateľov a riadenie súvisiacich rizík

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