					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P41					Заглавие на документа: **Политика за управление на риска, свързан със зависимостта от доставчици**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Правна бележка (авторски права и ограничения за ползване)

(C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никоя част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

Съответствие със стандарти и нормативни изисквания

Стандарт/регулация	Клауза/член	Коментар
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 на ЕС	Чл. 28, чл. 32(1)(d)	
NIS2 на ЕС	Чл. 21(2)(d), чл. 21(3), чл. 22	
DORA на ЕС	Чл. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Цел

1.1 Да се разширят практиките на организацията за сигурност на веригата на доставки чрез въвеждане на процес за идентифициране и управление на критични зависимости от доставчици и външни доставчици на услуги в съответствие с член 21, параграф 3 от NIS2 и оценките на риска за веригата на доставки на равнище Съюз.

1.2 Да се гарантира, че рисковете, произтичащи от концентрация или зависимост от един-единствен доставчик, са разбрани и смекчени и че всички специфични за сектора рискове по веригата на доставки, както са посочени от компетентните органи съгласно член 22 от NIS2, са включени в управлението на риска и в планирането на непрекъсваемостта на дейността при извънредни ситуации.

2. Обхват

2.1 Тази политика се прилага за всички съществени доставчици и външни доставчици на услуги, на които организацията разчита за критични операции, особено в ИКТ веригата на доставки (хардуер, софтуер, облачни услуги, телекомуникации, управлявани услуги).

2.2 Тя обхваща вътрешни функции, включително Закупуване и надлежна проверка на доставчици, Управление на доставчици, Управление на риска и съответните оперативни звена. В обхвата попадат и самите доставчици, доколкото това е необходимо за събиране на информация за риска. „Критични доставчици“ са тези, чийто отказ или компрометиране може съществено да повлияе на способността ни да предоставяме услуги или да изпълняваме правните си задължения.

3. Цели

3.1 Да се осигури видимост върху зависимостите по веригата на доставки, включително чрез идентифициране на единични точки на отказ или висок риск от концентрация в базата от доставчици (например зависимост от един доставчик на облачни услуги за всички услуги).

3.2 Да се въведат мерки за намаляване и управление на рисковете, свързани с доставчици, като диверсификация, планове за извънредни ситуации или изискване за засилени контроли при доставчика, като по този начин се повишава устойчивостта срещу откази на доставчици или атаки, произтичащи от веригата на доставки.

3.3 Да се постигне съответствие с изискванията на NIS2 чрез интегриране на резултатите от всички координирани оценки на риска за сигурността на критични вериги на доставки съгласно член 22 в организационните решения по отношение на риска и чрез гарантиране, че подходът ни към риска по веригата на доставки е документиран и доказуем.

4. Роли и отговорности

4.1 Офис за управление на доставчици (VMO): Поддържа регистъра на зависимостите от доставчици и координира оценките на риска. Осигурява всеки ключов доставчик да бъде оценяван по критичност и степен на зависимост при въвеждане и периодично след това.

4.2 Управление на риска (Комитет по корпоративен риск): Преглежда риска от концентрация и анализите на зависимостите, одобрява стратегиите за третиране на риска (например одобрение за включване на алтернативен доставчик или поддържане на допълнителни наличности за критични компоненти). Включва риска по веригата на доставки в Регистъра на риска и докладва на висшето ръководство.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Мониторинг и одит

9.1 Регистърът на зависимостите и оценките на риска подлежат на вътрешен одит ежегодно. Вътрешният одит проверява дали всички критични доставчици са включени, дали техните оценки на риска са актуални и дали са въведени планове за смекчаване и по тях има напредък. Проверява се и дали външните входни данни за оценка на риска (доклади по член 22 и др.) са били надлежно взети предвид.

9.2 Ефективността на мерките за диверсификация и мерките при извънредни ситуации се тества периодично. Например може да се проведе планирана симулация, при която се приема отказ на основен доставчик, с цел да се тестват нашите планове за непрекъсваемост и алтернативните механизми (подобно на учение по аварийно възстановяване, но за недостъпност на доставчик). Резултатите от тези тестове се документират и всички дефицити в контролите се отстраняват.

9.3 Показатели: Функцията по Управление на риска ще проследява показатели като „% от критичните услуги с поне един наличен алтернативен доставчик или решение“ или „Топ 5 зависимости от доставчици и тенденция на риска при тях“. Тези показатели ще бъдат включвани в таблото за управление на риска за ръководството. Намаляването на риска от зависимост във времето е цел; ако показателите показват нарастваща зависимост, това трябва да предизвика обсъждане от ръководството.

10. Преглед и поддръжка

10.1 Тази политика ще бъде преглеждана най-малко веднъж годишно от екипите по Управление на доставчици и Управление на риска. Прегледът ще отчита всички промени в средата на доставчиците (например ако нов доставчик стане критичен или стар бъде поетапно изведен) и всички нови регулаторни изисквания относно аутсорсинг или риск от трети страни.

10.2 Ако секторните органи издадат актуализирани указания или ако инцидент разкрие пропуски (например ако недостъпност на доставчик има по-голямо въздействие от очакваното, което показва, че оценката на риска е подценила зависимостта), политиката ще бъде актуализирана с цел прецизиране на критериите или стратегиите за смекчаване.

10.3 Преработените версии на политиката трябва да бъдат одобрени от висшето ръководство. Съществените промени ще бъдат комуникирани до всички относими звена, а материалите за обучение ще бъдат актуализирани по съответния начин, за да отразяват новите процедури или стандарти.

11. Свързани политики и връзки

11.1 P01 – Политика за информационна сигурност. Определя отчетността за управлението на зависимостите от доставчици.

11.2 P02 – Политика за роли и отговорности в управлението. Уточнява собствеността върху решенията за риска, свързан с доставчици.

11.3 P06 – Политика за управление на риска. Включва риска от концентрация в корпоративните регистри на риска.

11.4 P26 – Политика за сигурност на доставчиците и трети страни. Определя базовите изисквания за сигурност; P41 добавя контроли за зависимост и концентрация.

11.5 P27 – Политика за използване на облачни услуги. Прилага критериите за зависимост при приемане на облачни услуги и планове за изход.

11.6 P28 – Политика за външно възложена разработка. Обхваща рисковете от зависимост при инженерни дейности, възложени на външен изпълнител.

11.7 P32 – Политика за непрекъсваемост на дейността и аварийно възстановяване. Планира сценарии при недостъпност/замяна на доставчик.

11.8 P37 – Политика за правни въпроси и регулаторно съответствие. Осигурява договорите и задълженията да отразяват контролите за зависимост.

12. Референции

12.1 Директива NIS2 (ЕС 2022/2555), член 21, параграф 3 (изисква отчитане на уязвимостите, специфични за всеки пряк доставчик/доставчик на услуги, и качеството на тяхната киберсигурност, включително резултатите от координирани оценки на риска за веригата на доставки)

12.2 Директива NIS2, член 22, параграф 1 (координирани оценки на риска за сигурността на критични вериги на доставки на равнище Съюз – информира организациите за специфичните за сектора рискове, свързани с доставчици)

12.3 Регламент за изпълнение (ЕС) 2024/2690 на Комисията, приложение, раздел 5 (изисквания за сигурност на веригата на доставки за организациите, включително критерии за избор на доставчици, диверсификация и договорни задължения)

12.4 Добри практики на ENISA за киберсигурност на веригата на доставки (2022) – препоръки за идентифициране на критични доставчици и управление на свързаните рискове

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