					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P41					Titlul documentului: **Politica de management al riscului de dependență față de furnizori**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
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 al UE	Art. 28, Art. 32(1)(d)	
Directiva NIS2 a UE	Art. 21(2)(d), Art. 21(3), Art. 22	
Regulamentul DORA al UE	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Scop

1.1 Consolidarea practicilor organizației privind securitatea lanțului de aprovizionare prin instituirea unui proces de identificare și gestionare a dependențelor critice față de furnizori și prestatori de servicii, în conformitate cu articolul 21 alineatul (3) din NIS2 și cu evaluările de risc la nivelul Uniunii privind lanțul de aprovizionare.

1.2 Asigurarea faptului că riscurile generate de concentrarea pe un singur furnizor sau de dependența de acesta sunt înțelese și atenuate și că orice riscuri sectoriale specifice lanțului de aprovizionare, evidențiate de autorități în temeiul articolului 22 din NIS2, sunt integrate în procesul de management al riscurilor și în planificarea continuității activității.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor furnizorilor critici și prestatorilor de servicii de care organizația depinde pentru activități critice, în special celor din lanțul de aprovizionare TIC (hardware, software, servicii cloud, telecomunicații, servicii gestionate).

2.2 Aceasta acoperă funcțiile interne, inclusiv Achiziții, managementul furnizorilor, managementul riscurilor și departamentele operaționale relevante. De asemenea, implică acești furnizori în măsura necesară colectării informațiilor privind riscurile. „Furnizori critici” sunt acei furnizori a căror indisponibilitate sau compromitere ar putea afecta semnificativ capacitatea noastră de a furniza servicii sau de a ne îndeplini obligațiile legale.

3. Obiective

3.1 Obținerea vizibilității asupra dependențelor din lanțul de aprovizionare, în special prin identificarea punctelor unice de eșec sau a riscului ridicat de concentrare în baza noastră de furnizori (de exemplu, dependența de un singur furnizor de servicii cloud pentru toate serviciile).

3.2 Implementarea unor măsuri de reducere și gestionare a riscurilor asociate furnizorilor, precum diversificarea, planurile de contingență sau impunerea unor controale consolidate la nivelul furnizorilor, sporind astfel reziliența la eșecul furnizorilor sau la atacurile provenite din lanțul de aprovizionare.

3.3 Alinierea la cerințele NIS2 prin integrarea rezultatelor oricăror evaluări coordonate ale riscurilor de securitate privind lanțurile de aprovizionare critice, conform articolului 22, în deciziile organizaționale privind riscul și prin asigurarea faptului că abordarea noastră privind riscul din lanțul de aprovizionare este documentată și demonstrabilă.

4. Roluri și responsabilități

4.1 Biroul de management al furnizorilor (VMO): deține registrul dependențelor față de furnizori și coordonează evaluările de risc. Se asigură că, la integrare și ulterior periodic, fiecare furnizor-cheie este evaluat din perspectiva criticității și a nivelului de dependență.

4.2 Funcția de management al riscurilor (Comitetul de risc la nivel de organizație): revizuiește riscul de concentrare și analizele de dependență, avizează strategiile de tratament al riscului (de exemplu, aprobarea adăugării unui furnizor alternativ sau menținerea unui stoc suplimentar pentru componente critice). Integrează riscul din lanțul de aprovizionare în registrul general de riscuri și raportează conducerii executive.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Monitorizare și audit

9.1 Registrul dependențelor și evaluările de risc vor fi supuse anual auditului intern. Auditul intern va verifica dacă toți furnizorii critici sunt incluși, dacă nivelurile lor de risc sunt actualizate și dacă planurile de atenuare sunt implementate sau în curs de implementare. De asemenea, va verifica dacă au fost luate în considerare în mod corespunzător sursele externe de evaluare a riscului (rapoarte aferente articolului 22 etc.).

9.2 Eficacitatea măsurilor de diversificare și de contingență va fi testată periodic. De exemplu, poate fi efectuată o simulare planificată în care se presupune că un furnizor major eșuează, pentru a testa planurile noastre de continuitate a activității și soluțiile alternative (similar unui exercițiu de recuperare în caz de dezastru, dar pentru indisponibilitatea unui furnizor). Rezultatele acestor teste sunt documentate, iar orice deficiențe de control sunt remediate.

9.3 Metrici: funcția de management al riscurilor va urmări metrici precum „% din serviciile critice pentru care există disponibil cel puțin un furnizor sau o soluție alternativă” sau „primele 5 dependențe față de furnizori și tendința lor de risc”. Aceste metrici vor fi incluse în tablourile de bord privind riscurile prezentate conducerii. O tendință descendentă a riscului de dependență în timp constituie un obiectiv; dacă metricile indică o creștere a dependenței, acest lucru trebuie să declanșeze o discuție la nivel de management.

10. Revizuire și mentenanță

10.1 Această politică va fi revizuită cel puțin anual de către echipele de management al furnizorilor și de management al riscurilor. Revizuirea va integra orice schimbări în peisajul furnizorilor (de exemplu, dacă un nou furnizor devine critic sau unul vechi este eliminat treptat) și orice noi cerințe de reglementare privind externalizarea sau riscul asociat terților.

10.2 Dacă autoritățile sectoriale emit ghiduri actualizate sau dacă un incident relevă lacune (de exemplu, dacă indisponibilitatea unui furnizor a avut un impact mai mare decât cel anticipat, indicând că evaluarea noastră de risc a apreciat eronat dependența), politica va fi actualizată pentru a rafina criteriile sau strategiile de atenuare.

10.3 Versiunile revizuite ale politicii trebuie aprobate de conducerea executivă. Schimbările semnificative vor fi comunicate tuturor departamentelor relevante, iar materialele de instruire vor fi actualizate în consecință pentru a reflecta noile proceduri sau standarde.

11. Politici conexe și interdependențe

11.1 P01 – Politica de securitate a informației. Atribuie responsabilitatea pentru guvernanța dependențelor față de furnizori.

11.2 P02 – Politica privind rolurile și responsabilitățile de guvernanță. Clarifică responsabilitatea pentru deciziile privind riscul asociat furnizorilor.

11.3 P06 – Politica de management al riscurilor. Integrează riscul de concentrare în registrele de riscuri la nivel de organizație.

11.4 P26 – Politica de securitate privind terții și furnizorii. Stabilește baza de referință a controalelor de securitate; P41 adaugă controale privind dependența și concentrarea.

11.5 P27 – Politica de utilizare a serviciilor cloud. Aplică criteriile de dependență la adoptarea serviciilor cloud și la planurile de ieșire.

11.6 P28 – Politica privind dezvoltarea externalizată. Acoperă riscurile de dependență în activitățile externe de inginerie.

11.7 P32 – Politica privind continuitatea activității și recuperarea în caz de dezastru. Planifică scenarii de indisponibilitate sau de substituire a furnizorilor.

11.8 P37 – Politica de conformitate juridică și de reglementare. Asigură că contractele și obligațiile reflectă controalele privind dependența.

12. Referințe

12.1 Directiva NIS2 (UE 2022/2555), articolul 21 alineatul (3) (impune luarea în considerare a vulnerabilităților specifice fiecărui furnizor direct/furnizor de servicii și a calității securității lor cibernetice, inclusiv a rezultatelor evaluărilor coordonate ale riscului din lanțul de aprovizionare)

12.2 Directiva NIS2, articolul 22 alineatul (1) (evaluări coordonate ale riscurilor de securitate la nivelul Uniunii pentru lanțuri de aprovizionare critice – informează entitățile cu privire la riscurile sectoriale asociate furnizorilor)

12.3 Regulamentul de punere în aplicare al Comisiei (UE) 2024/2690, anexa secțiunea 5 (cerințe privind securitatea lanțului de aprovizionare pentru entități, inclusiv criterii pentru selecția furnizorilor, diversificare și obligații contractuale)

12.4 Bune practici ENISA pentru securitatea cibernetică a lanțului de aprovizionare (2022) – recomandări privind identificarea furnizorilor critici și gestionarea riscurilor asociate

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