					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P41					Titolo del documento: **Politica di gestione del rischio di dipendenza dai fornitori**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineamento a standard e normative applicabili

Standard/Regolamento	Clausola/Articolo	Commento
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 UE	Art. 28, Art. 32(1)(d)	
NIS2 UE	Art. 21(2)(d), Art. 21(3), Art. 22	
DORA UE	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Finalità

1.1 Rafforzare le pratiche di sicurezza della catena di fornitura dell'organizzazione mediante l'istituzione di un processo volto a identificare e gestire le dipendenze critiche da fornitori e prestatori di servizi, in linea con l'articolo 21(3) della NIS2 e con le valutazioni coordinate dei rischi della catena di fornitura a livello dell'Unione.

1.2 Assicurare che i rischi derivanti dalla concentrazione o dalla dipendenza da singoli fornitori siano compresi e mitigati e che gli eventuali rischi della catena di fornitura specifici di settore, come evidenziati dalle autorità ai sensi dell'articolo 22 della NIS2, siano integrati nella gestione del rischio e nella pianificazione della continuità operativa.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i fornitori essenziali e ai prestatori di servizi dai quali l'organizzazione dipende per le operazioni critiche, con particolare riferimento a quelli della catena di fornitura ICT (hardware, software, cloud, telecomunicazioni, servizi gestiti).

2.2 La politica riguarda le funzioni interne, tra cui Approvvigionamenti, gestione dei fornitori, Gestione del rischio e i dipartimenti operativi pertinenti. Coinvolge inoltre i fornitori stessi nella misura necessaria alla raccolta delle informazioni di rischio. Per "fornitori critici" si intendono quelli il cui guasto o la cui compromissione potrebbe incidere in modo significativo sulla capacità dell'organizzazione di erogare servizi o di adempiere agli obblighi di conformità.

3. Obiettivi

3.1 Ottenere visibilità sulle dipendenze della catena di fornitura, in particolare identificando singoli punti di guasto o livelli elevati di concentrazione del rischio nella base fornitori (ad esempio, dipendenza da un unico fornitore cloud per tutti i servizi).

3.2 Attuare misure per ridurre e gestire i rischi connessi ai fornitori, quali diversificazione, piani di continuità o richiesta di rafforzamento dei controlli del fornitore, aumentando così la resilienza rispetto ai guasti dei fornitori o ad attacchi originati nella catena di fornitura.

3.3 Allinearsi ai requisiti della NIS2 integrando nelle decisioni organizzative sul rischio i risultati di eventuali valutazioni coordinate dei rischi di sicurezza delle catene di fornitura critiche, ai sensi dell'articolo 22, e assicurando che l'approccio al rischio della catena di fornitura sia documentato e dimostrabile.

4. Ruoli e responsabilità

4.1 Vendor Management Office (VMO): è titolare del registro delle dipendenze dai fornitori e coordina le valutazioni del rischio. Assicura che, durante l'onboarding e successivamente con periodicità definita, ciascun fornitore chiave sia valutato in termini di criticità e livello di dipendenza.

4.2 Gestione del rischio (Enterprise Risk Committee): riesamina il rischio di concentrazione e le analisi di dipendenza, approva le strategie di trattamento del rischio, ad esempio l'introduzione di un fornitore alternativo o il mantenimento di scorte aggiuntive di componenti critici. Integra il rischio della catena di fornitura nel Registro dei rischi complessivo e riferisce all'alta direzione.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Monitoraggio e audit

9.1 Il registro delle dipendenze e le valutazioni del rischio devono essere sottoposti annualmente ad audit interno. La funzione di audit interno/conformità verifica che tutti i fornitori critici siano elencati, che i relativi livelli di rischio siano aggiornati e che i piani di mitigazione siano in essere e in avanzamento. Verifica inoltre che gli input derivanti da valutazioni esterne del rischio, quali i rapporti ai sensi dell'articolo 22, siano stati debitamente considerati.

9.2 L'efficacia delle misure di diversificazione e continuità deve essere verificata periodicamente. Ad esempio, può essere condotta una simulazione pianificata in cui si assume il guasto di un fornitore rilevante, al fine di testare i piani di continuità e le soluzioni alternative predisposte, analogamente a un'esercitazione di disaster recovery ma riferita all'indisponibilità del fornitore. I risultati di tali test devono essere documentati e le eventuali carenze corrette.

9.3 Metriche: la funzione di Gestione del rischio monitora metriche quali "% di servizi critici con almeno un fornitore o una soluzione alternativa disponibile" oppure "Top 5 delle dipendenze dai fornitori e relativo andamento del rischio". Tali metriche devono essere incluse nelle dashboard di rischio destinate alla direzione. La riduzione nel tempo del rischio di dipendenza costituisce un obiettivo; se le metriche mostrano un aumento della dipendenza, ciò deve innescare una discussione a livello direzionale.

10. Riesame e manutenzione

10.1 La presente politica deve essere riesaminata almeno annualmente dai team di Vendor Management e Gestione del rischio. Il riesame tiene conto di eventuali cambiamenti nel panorama dei fornitori, ad esempio se un nuovo fornitore diventa critico o uno precedente viene dismesso, nonché di eventuali nuovi requisiti normativi in materia di esternalizzazione o rischio di terze parti.

10.2 Se le autorità settoriali emettono linee guida aggiornate o se un incidente evidenzia lacune, ad esempio se l'indisponibilità di un fornitore ha avuto un impatto maggiore del previsto, indicando che la valutazione del rischio ha sottostimato la dipendenza, la politica deve essere aggiornata per affinare i criteri o le strategie di mitigazione.

10.3 Le versioni aggiornate della politica devono essere approvate dall'alta direzione. Le modifiche significative devono essere comunicate a tutti i dipartimenti pertinenti e i materiali formativi devono essere aggiornati di conseguenza per riflettere nuove procedure o nuovi requisiti.

11. Politiche correlate e collegamenti

11.1 P01 – Politica per la sicurezza delle informazioni. Assegna la responsabilità per la governance della dipendenza dai fornitori.

11.2 P02 – Politica sui ruoli e sulle responsabilità di governance. Chiarisce la titolarità delle decisioni sul rischio dei fornitori.

11.3 P06 – Politica di gestione del rischio. Integra il rischio di concentrazione nei registri dei rischi aziendali.

11.4 P26 – Politica di sicurezza delle terze parti e dei fornitori. Definisce la baseline di sicurezza; la P41 aggiunge controlli su dipendenza e concentrazione.

11.5 P27 – Politica di utilizzo del cloud. Applica i criteri di dipendenza all'adozione dei servizi cloud e ai piani di uscita.

11.6 P28 – Politica sullo sviluppo esternalizzato. Copre i rischi di dipendenza nell'ingegneria esterna.

11.7 P32 – Politica di continuità operativa e disaster recovery. Definisce la pianificazione per scenari di indisponibilità o sostituzione del fornitore.

11.8 P37 – Politica di conformità legale e normativa. Assicura che contratti e obblighi riflettano i controlli sulla dipendenza.

12. Riferimenti

12.1 Direttiva NIS2 (UE 2022/2555), articolo 21(3) (richiede di considerare le vulnerabilità specifiche di ciascun fornitore diretto/prestatore di servizi e la qualità della relativa cibersicurezza, inclusi i risultati delle valutazioni coordinate del rischio della catena di fornitura)

12.2 Direttiva NIS2, articolo 22(1) (valutazioni coordinate dei rischi di sicurezza delle catene di fornitura critiche a livello dell'Unione – informa i soggetti sui rischi dei fornitori a livello settoriale)

12.3 Regolamento di esecuzione della Commissione (UE) 2024/2690, Allegato Sezione 5 (requisiti di sicurezza della catena di fornitura per i soggetti, inclusi criteri per la selezione dei fornitori, la diversificazione e gli obblighi contrattuali)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – raccomandazioni sull'identificazione dei fornitori critici e sulla gestione dei rischi correlati

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