					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P41					Documenttitel: **Beleid inzake risicobeheer van leveranciersafhankelijkheid**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)

(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.
Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.
Neem voor licentiëring contact op via: info@clarysec.com

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
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	
AVG	Art. 28, Art. 32(1)(d)	
EU NIS2	Art. 21(2)(d), Art. 21(3), Art. 22	
EU DORA	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Doel

1.1 De beveiligingspraktijken binnen de toeleveringsketen van de organisatie versterken door een proces in te richten voor het identificeren en beheersen van kritieke afhankelijkheden van leveranciers en dienstverleners, zoals vereist op grond van artikel 21, lid 3, van NIS2 en risicobeoordelingen van de toeleveringsketen op Unieniveau.

1.2 Waarborgen dat risico's die voortvloeien uit concentratie of afhankelijkheid van individuele leveranciers worden begrepen en beperkt, en dat sectorspecifieke risico's in de toeleveringsketen, zoals onder artikel 22 van NIS2 door bevoegde autoriteiten benadrukt, worden opgenomen in ons risicobeheer en onze continuïteits- en herstelplanning.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle essentiële leveranciers en dienstverleners waarvan de organisatie afhankelijk is voor kritieke activiteiten, in het bijzonder binnen de ICT-toeleveringsketen (hardware, software, cloud, telecommunicatie en managed services).

2.2 Dit beleid heeft betrekking op interne functies, waaronder Inkoop, Leveranciersmanagement, Risicobeheer en relevante operationele afdelingen. Het omvat tevens de betreffende leveranciers, voor zover dit nodig is om risico-informatie te verzamelen. Onder "kritieke leveranciers" worden leveranciers verstaan waarvan uitval of compromittering aanzienlijke gevolgen kan hebben voor ons vermogen om diensten te leveren of aan wettelijke verplichtingen te voldoen.

3. Doelstellingen

3.1 Inzicht verkrijgen in afhankelijkheden in de toeleveringsketen, in het bijzonder door single points of failure of een hoog concentratierisico binnen onze leveranciersbasis te identificeren, bijvoorbeeld afhankelijkheid van één cloudprovider voor alle diensten.

3.2 Maatregelen implementeren om leveranciersgerelateerde risico's te beperken en te beheersen, zoals diversificatie, continuïteitsmaatregelen of het eisen van versterkte beheersmaatregelen bij leveranciers, en daarmee de weerbaarheid tegen leveranciersuitval of aanvallen via de toeleveringsketen vergroten.

3.3 Afstemming op de vereisten van NIS2 door de resultaten van gecoördineerde risicobeoordelingen van kritieke toeleveringsketens, conform artikel 22, te integreren in organisatorische risicobesluiten, en

door te waarborgen dat onze aanpak voor risico's in de toeleveringsketen is gedocumenteerd en aantoonbaar is.

4. Rollen en verantwoordelijkheden

4.1 Vendor Management Office (VMO): beheert het register van leveranciersafhankelijkheden en coördineert risicobeoordelingen. Borgt dat iedere sleutelleverancier tijdens onboarding en periodiek daarna wordt beoordeeld op criticaliteit en afhankelijkheidsniveau.

4.2 Risicobeheer (Enterprise Risk Committee): beoordeelt concentratierisico en afhankelijkheidsanalyses, bekrachtigt risicobehandelingsstrategieën, bijvoorbeeld het goedkeuren van een alternatieve leverancier of het aanhouden van extra voorraad voor kritieke componenten, neemt risico's in de toeleveringsketen op in het centrale risicoregister en rapporteert aan het hoger management.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Monitoring en audit

9.1 Het register van leveranciersafhankelijkheden en de risicobeoordelingen worden jaarlijks intern geaudit. De interne audit- en compliancefunctie verifieert dat alle kritieke leveranciers zijn opgenomen, dat hun risicoclassificaties actueel zijn en dat risicobehandelingsplannen bestaan en voortgang laten zien. Ook wordt gecontroleerd of externe input uit risicobeoordelingen, zoals artikel 22-rapporten, naar behoren is meegewogen.

9.2 De doeltreffendheid van diversificatie- en continuïteitsmaatregelen wordt periodiek getest. Zo kan bijvoorbeeld een geplande simulatie worden uitgevoerd waarbij wordt uitgegaan van uitval van een majeure leverancier, om onze continuïteitsplannen en alternatieve regelingen te testen, vergelijkbaar met een hersteloefening, maar dan voor leveranciersuitval. De resultaten van deze tests worden gedocumenteerd en eventuele tekortkomingen worden gecorrigeerd.

9.3 Metrieken: de risicobeheerfunctie volgt metrieken zoals "% van kritieke diensten waarvoor ten minste één alternatieve leverancier of oplossing beschikbaar is" of "Top 5 leveranciersafhankelijkheden en hun risicotrend". Deze metrieken worden opgenomen in risicodashboards voor het management. Een dalende trend in afhankelijkheidsrisico in de tijd is een doelstelling; indien metrieken een toenemende afhankelijkheid laten zien, moet dit leiden tot bespreking door het management.

10. Herziening en onderhoud

10.1 Dit beleid wordt ten minste jaarlijks beoordeeld door de teams voor Leveranciersmanagement en Risicobeheer. In de beoordeling worden wijzigingen in het leverancierslandschap meegenomen, bijvoorbeeld als een nieuwe leverancier kritisch wordt of een bestaande leverancier wordt uitgefaseerd, evenals eventuele nieuwe wettelijke of regelgevende vereisten voor uitbesteding of risico's van derde partijen.

10.2 Indien sectorale autoriteiten geactualiseerde richtsnoeren uitbrengen of indien een incident hiaten aan het licht brengt, bijvoorbeeld wanneer uitval van een leverancier een grotere impact had dan voorzien en erop wijst dat onze risicobeoordeling de afhankelijkheid onjuist heeft ingeschat, wordt het beleid geactualiseerd om criteria of risicobehandelingsstrategieën te verfijnen.

10.3 Herziene versies van het beleid moeten worden goedgekeurd door het hoger management. Significante wijzigingen worden gecommuniceerd aan alle relevante afdelingen en trainingsmaterialen worden dienovereenkomstig bijgewerkt om nieuwe procedures of standaarden weer te geven.

11. Gerelateerde beleidslijnen en samenhang

11.1 P01 – Informatiebeveiligingsbeleid. Wijst verantwoordingsplicht toe voor de governance van leveranciersafhankelijkheden.

11.2 P02 – Beleid inzake governancerollen en -verantwoordelijkheden. Verduidelijkt eigenaarschap voor besluiten over leveranciersrisico.

11.3 P06 – Beleid inzake risicobeheer. Verankert concentratierisico in het Enterprise Risk Register.

11.4 P26 – Beleid inzake beveiliging van derde partijen en leveranciers. Bevat de baseline voor beveiliging; P41 voegt beheersmaatregelen voor afhankelijkheid en concentratie toe.

11.5 P27 – Beleid inzake gebruik van cloudservices. Past afhankelijkheidscriteria toe op de adoptie van cloudservices en exitplannen.

11.6 P28 – Beleid inzake uitbestede ontwikkeling. Behandelt afhankelijkheidsrisico's binnen uitbestede engineering.

11.7 P32 – Beleid voor bedrijfscontinuïteit en herstel na verstoringen. Voorziet in scenario's van leveranciersuitval of vervanging.

11.8 P37 – Beleid inzake juridische en regelgevende naleving. Borgt dat contracten en verplichtingen beheersmaatregelen voor afhankelijkheden weerspiegelen.

12. Referenties

12.1 NIS2-richtlijn (EU 2022/2555), artikel 21, lid 3 (vereist dat rekening wordt gehouden met kwetsbaarheden die specifiek zijn voor iedere directe leverancier/dienstverlener en met de kwaliteit van hun cyberbeveiliging, inclusief de resultaten van gecoördineerde risicobeoordelingen van de toeleveringsketen)

12.2 NIS2-richtlijn, artikel 22, lid 1 (gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens op Unieniveau – informeert entiteiten over sectorbrede leveranciersrisico's)

12.3 Uitvoeringsverordening (EU) 2024/2690 van de Commissie, bijlage sectie 5 (vereisten inzake beveiliging van de toeleveringsketen voor entiteiten, inclusief criteria voor leveranciersselectie, diversificatie en contractuele verplichtingen)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – aanbevelingen voor het identificeren van kritieke leveranciers en het beheersen van gerelateerde risico's

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