					[Insert Registered Legal Entity Name Here]							
Document number: P41					Document Title: Supplier Dependency Risk Management Policy							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
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	
EU GDPR	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	

NOTE:

This policy addresses the supply chain dependency and concentration risks highlighted by NIS2 Article 21(3) and Article 22. NIS2 Article 21(3) mandates that entities account for each supplier's specific vulnerabilities and overall product/service quality, including considering results of coordinated supply chain risk. Our add-on establishes processes to identify critical suppliers and mitigate single points of failure, aligning with ENISA's supply chain good practices that emphasize having strategies for ICT supply chain risks (like diversification, monitoring). Moreover, if authorities flag certain suppliers or technologies as high-risk (under Article 22 assessments), P41 ensures those warnings feed into our risk management. This policy is "optional" in that it goes beyond minimum compliance for some sectors, but it provides a competitive and resilience advantage. It could be used as an add-on service to clients by showing advanced supply chain risk governance.

1. **Purpose**
   1.1 1.1 Augment the organization's supply chain security practices by instituting a process to identify and manage critical dependencies on suppliers and service providers, as prompted by NIS2 Article 21(3) and Union-level supply chain risk assessments.
   1.2 1.2 Ensure that risks arising from concentration or reliance on single suppliers are understood and mitigated, and that any sector-specific supply chain risks (as highlighted by authorities under NIS2 Article 22) are incorporated into our risk management and business continuity planning.
2. **Scope**
   2.1 This policy applies to all essential suppliers and service providers that the organization relies on for critical operations, especially those in the ICT supply chain (hardware, software, cloud, telecom, managed services).
   2.2 It covers internal functions including Procurement, Vendor Management, Risk Management, and relevant operational departments. It also involves those suppliers themselves to the extent of gathering risk information. "Critical suppliers" are those whose failure or compromise could significantly impact our ability to deliver services or meet legal obligations.
3. **Objectives**
   3.1 Gain visibility over supply chain dependencies, particularly identifying single points of failure or high concentration risk in our supplier base (e.g., dependency on one cloud provider for all services).
   3.2 Implement measures to reduce and manage supplier-related risks – such as diversification, contingency plans, or requiring improved supplier controls – thereby enhancing resilience against supplier failures or attacks originating in the supply chain.
   3.3 Align with NIS2 requirements by integrating results of any coordinated security risk assessments of critical supply chains (per Article 22) into organizational risk decisions, and by ensuring our own supply chain risk approach is documented and demonstrable.
4. **Roles and Responsibilities**
   4.1 Vendor Management Office (VMO): Owns the supplier dependency register and coordinates risk evaluations. Ensures that during onboarding and periodically thereafter, each key supplier is assessed for criticality and dependency level.
   4.2 Risk Management (Enterprise Risk Committee): Reviews concentration risk and dependency analyses, endorses risk treatment strategies (e.g., approve adding an alternate supplier or holding extra inventory for critical components). Incorporates supply chain risk into the overall risk register and reports to top management.
   4.3 Procurement Department: During procurement and contract renewal, follows this policy to avoid undue dependency (e.g., include requirements for redundancy or second-source options in contracts when feasible). Escalates to Risk Management if a proposed sole-source scenario creates high risk.
   4.4 IT/Operations Departments: Identify operational single points of failure in technology or services. Develop and maintain contingency plans for quick replacement or workaround if a key supplier fails. They also monitor supplier performance and incidents and inform Vendor Management of any changes in risk (e.g., repeated outages of a vendor).

[……..
……
…….
……
……]

10. **Review and Maintenance**

10.1 This policy will be reviewed at least annually by the Vendor Management and Risk Management teams. The review will incorporate any changes in the supplier landscape (e.g., if a new supplier becomes critical or an old one is phased out) and any new regulatory requirements on outsourcing or third-party risk.

10.2 If sectoral authorities issue updated guidance or if an incident reveals gaps (for instance, if a supplier outage had greater impact than anticipated, indicating our risk assessment misjudged the dependency), the policy will be updated to refine criteria or mitigation strategies.

10.3 Revised versions of the policy must be approved by senior management. Significant changes will be communicated to all relevant departments, and training materials will be updated accordingly to reflect new procedures or standards.

11. Related Policies and Linkages

11.1 P01 – Information Security Policy. Assigns accountability for supplier dependency governance.

11.2 P02 – Governance Roles & Responsibilities Policy. Clarifies ownership for supplier risk decisions.

11.3 P06 – Risk Management Policy. Embeds concentration risk into enterprise risk registers.

11.4 P26 – Third-Party and Supplier Security Policy. Baseline security; P41 adds dependency/concentration controls.

11.5 P27 – Cloud Usage Policy. Applies dependency criteria to cloud service adoption and exit plans.

11.6 P28 – Outsourced Development Policy. Covers dependency risks in external engineering.

11.7 P32 – Business Continuity and Disaster Recovery Policy. Plans for supplier outage/substitution scenarios.

11.8 P37 – Legal and Regulatory Compliance Policy. Ensures contracts/obligations reflect dependency controls.

12. References

12.1 NIS2 Directive (EU 2022/2555), Article 21(3) (requiring consideration of vulnerabilities specific to each direct supplier/service provider and quality of their cybersecurity, including results of coordinated supply chain risk assessments)

12.2 NIS2 Directive, Article 22(1) (Union-level coordinated security risk assessments of critical supply chains – informs entities of sector-wide supplier risks)

12.3 Commission Implementing Regulation (EU) 2024/2690, Annex Section 5 (Supply chain security requirements for entities, including criteria for supplier selection, diversification, and contractual obligations)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – recommendations on identifying critical suppliers and managing related risks

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