					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

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	

1. Purpose

1.1 Strengthen the organization's supply chain security practices by establishing a process to identify and manage critical dependencies on suppliers and service providers, as required by NIS2 Article 21(3) and informed by Union-level supply chain risk assessments.

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 identified 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 critical suppliers and service providers on which the organization depends for critical operations, particularly within the ICT supply chain (hardware, software, cloud, telecommunications, managed services).

2.2 It applies to internal functions including Procurement, Vendor Management, Risk Management, and relevant operational departments. It also applies to suppliers themselves to the extent necessary to obtain risk information. "Critical suppliers" are those whose failure or compromise could significantly affect our ability to deliver services or meet legal or regulatory obligations.

3. Objectives

3.1 Establish visibility over supply chain dependencies, in particular by identifying single points of failure or high concentration risk within the 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 planning, or requiring stronger supplier controls, thereby improving resilience against supplier failure or attacks originating in the supply chain.

3.3 Align with NIS2 requirements by incorporating the results of any coordinated security risk assessments of critical supply chains (under Article 22) into organizational risk decisions, and by ensuring that 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 each key supplier is assessed for criticality and dependency level during onboarding and at defined intervals thereafter.

4.2 Risk Management (Enterprise Risk Committee): Reviews concentration risk and dependency analyses and approves risk treatment strategies (e.g., adding an alternate supplier or maintaining additional inventory for critical components). Incorporates supply chain risk into the enterprise Risk Register and reports to Top Management.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Monitoring and Audit

9.1 The dependency register and risk assessments shall be subject to annual internal audit. The Internal Audit function shall verify that all critical suppliers are recorded, that risk ratings are current, and that mitigation plans are in place and progressing. It shall also verify that external risk assessment inputs (Article 22 reports, etc.) have been properly considered.

9.2 The effectiveness of diversification and contingency measures shall be tested periodically. For example, a planned simulation may assume the failure of a major supplier in order to test continuity plans and alternative arrangements (similar to a Disaster Recovery (DR) exercise, but focused on supplier outage). The results of these tests shall be documented and any deficiencies remediated.

9.3 Metrics: The Risk Management function shall track metrics such as “% of critical services with at least one alternate supplier or solution available” and “Top 5 supplier dependencies and their risk trend.” These metrics shall be included in risk dashboards for leadership. A downward trend in dependency risk over time is an objective; where metrics indicate increasing dependency, this must trigger management review.

10. Review and Maintenance

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

10.2 Where sector authorities issue updated guidance, or where an incident reveals control gaps (for example, if a supplier outage has a greater impact than anticipated, indicating that the dependency was underestimated in the risk assessment), this policy shall be updated to refine criteria or mitigation strategies.

10.3 Revised versions of this policy must be approved by Top Management. Significant changes shall be communicated to all relevant departments, and training materials shall be updated accordingly to reflect new procedures or standards.

11. Related Policies and Linkages

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

11.2 P02 – Governance Roles and Responsibilities Policy. Clarifies ownership of supplier risk decisions.

11.3 P06 – Risk Management Policy. Incorporates concentration risk into enterprise Risk Registers.

11.4 P26 – Third-Party and Supplier Security Policy. Establishes the baseline security requirements; P41 adds dependency and concentration controls.

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

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

11.7 P32 – Business Continuity and Disaster Recovery Policy. Covers supplier outage and substitution scenarios.

11.8 P37 – Legal and Regulatory Compliance Policy. Ensures contracts and 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 the quality of their cybersecurity, including the results of coordinated supply chain risk assessments)

12.2 NIS2 Directive, Article 22(1) (Union-level coordinated security risk assessments of critical supply chains, informing 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 for identifying critical suppliers and managing related risks

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