					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P41					Dokumenttitel: **Richtlinie zum Management von Lieferantenabhängigkeitsrisiken**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Vorschrift	Klausel/Artikel	Anmerkung
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-DSGVO	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. Zweck

1.1 Diese Richtlinie stärkt die Sicherheitspraktiken der Organisation in der Lieferkette, indem sie ein Verfahren zur Identifizierung und Steuerung kritischer Abhängigkeiten von Lieferanten und Dienstleistern festlegt, wie es durch Artikel 21 Absatz 3 NIS2 sowie unionsweite Bewertungen von Lieferkettenrisiken veranlasst ist.

1.2 Sie stellt sicher, dass Risiken aus der Konzentration auf einzelne Lieferanten oder aus Abhängigkeiten von ihnen verstanden und gemindert werden und dass sektorspezifische Risiken der Lieferkette, wie sie von Behörden nach Artikel 22 NIS2 hervorgehoben werden, in unser Risikomanagement und die Planung zur Aufrechterhaltung des Geschäftsbetriebs einfließen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle wesentlichen Lieferanten und Dienstleister, auf die die Organisation für kritische Betriebsabläufe angewiesen ist, insbesondere in der IKT-Lieferkette (Hardware, Software, Cloud, Telekommunikation, Managed Services).

2.2 Sie gilt für interne Funktionen einschließlich Einkauf, Lieferantenmanagement, Risikomanagement und relevanter operativer Bereiche. Soweit dies zur Einholung von Risikoinformationen erforderlich ist, bezieht sie auch diese Lieferanten selbst ein. „Kritische Lieferanten“ sind solche, deren Ausfall oder Kompromittierung unsere Fähigkeit zur Leistungserbringung oder zur Erfüllung rechtlicher Verpflichtungen erheblich beeinträchtigen könnte.

3. Ziele

3.1 Transparenz über Abhängigkeiten in der Lieferkette schaffen, insbesondere durch die Identifizierung von Single Points of Failure oder hohen Konzentrationsrisiken im Lieferantenbestand (z. B. Abhängigkeit von einem einzigen Cloud-Anbieter für alle Services).

3.2 Maßnahmen zur Reduzierung und Steuerung lieferantenbezogener Risiken umsetzen, etwa durch Diversifizierung, Notfallpläne oder die Anforderung verbesserter Kontrollen bei Lieferanten, und damit die Resilienz gegenüber Lieferantenausfällen oder aus der Lieferkette stammenden Angriffen erhöhen.

3.3 Die Anforderungen der NIS2 erfüllen, indem Ergebnisse koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 in organisatorische Risikoentscheidungen integriert werden und unser eigener Ansatz zum Management von Lieferkettenrisiken dokumentiert und nachweisbar ist.

4. Rollen und Verantwortlichkeiten

4.1 Lieferantenmanagement Office (VMO): Verantwortet das Register für Lieferantenabhängigkeiten und koordiniert Risikobewertungen. Stellt sicher, dass jeder Schlüssellieferant beim Onboarding und danach in regelmäßigen Abständen hinsichtlich Kritikalität und Abhängigkeitsgrad bewertet wird.

4.2 Risikomanagement (Enterprise Risk Committee): Überprüft Konzentrationsrisiken und Abhängigkeitsanalysen, befürwortet Strategien zur Risikobehandlung (z. B. Genehmigung eines alternativen Lieferanten oder zusätzlicher Lagerbestände für kritische Komponenten). Nimmt Lieferkettenrisiken in das zentrale Risikoregister auf und berichtet an die oberste Leitung.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Überwachung und Audit

9.1 Das Register für Lieferantenabhängigkeiten und die Risikobewertungen werden jährlich intern auditiert. Die Interne Revision und die Compliance-Funktion prüfen, ob alle kritischen Lieferanten erfasst sind, ob ihre Risikoeinstufungen aktuell sind und ob Minderungspläne vorhanden sind und Fortschritte zeigen. Außerdem wird geprüft, ob externe Eingaben aus Risikobewertungen (Berichte nach Artikel 22 usw.) ordnungsgemäß berücksichtigt wurden.

9.2 Die Wirksamkeit von Diversifizierungs- und Notfallmaßnahmen wird regelmäßig getestet. Beispielsweise kann eine geplante Simulation durchgeführt werden, in der der Ausfall eines wesentlichen Lieferanten angenommen wird, um unsere Pläne zur Aufrechterhaltung des Geschäftsbetriebs und alternativen Regelungen zu testen (ähnlich einer Disaster-Recovery-Übung, jedoch bezogen auf Lieferantenausfälle). Die Ergebnisse dieser Tests sind zu dokumentieren und festgestellte Mängel zu beheben.

9.3 Kennzahlen: Die Risikomanagement-Funktion verfolgt Kennzahlen wie „% der kritischen Services, für die mindestens ein alternativer Lieferant oder eine alternative Lösung verfügbar ist“ oder „Top 5 der Lieferantenabhängigkeiten und deren Risikotrend“. Diese Kennzahlen werden in Risiko-Dashboards an die Führungsebene berichtet. Ein sinkender Trend beim Abhängigkeitsrisiko über die Zeit ist das Ziel; zeigen die Kennzahlen eine wachsende Abhängigkeit, muss dies eine Managementdiskussion auslösen.

10. Überprüfung und Pflege

10.1 Diese Richtlinie wird mindestens jährlich durch die Teams für Lieferantenmanagement und Risikomanagement überprüft. Die Überprüfung berücksichtigt alle Änderungen in der Lieferantenlandschaft (z. B. wenn ein neuer Lieferant kritisch wird oder ein bisheriger ausläuft) sowie neue regulatorische Anforderungen an Auslagerungen oder Drittparteienrisiken.

10.2 Wenn sektorale Behörden aktualisierte Leitlinien veröffentlichen oder ein Vorfall Lücken aufdeckt (beispielsweise wenn ein Lieferantenausfall größere Auswirkungen hatte als erwartet und damit zeigt, dass unsere Risikobewertung die Abhängigkeit falsch eingeschätzt hat), wird die Richtlinie aktualisiert, um Kriterien oder Strategien zur Risikominderung zu präzisieren.

10.3 Überarbeitete Fassungen der Richtlinie müssen von der obersten Leitung genehmigt werden. Wesentliche Änderungen werden allen relevanten Bereichen mitgeteilt, und Schulungsmaterialien werden entsprechend aktualisiert, um neue Verfahren oder Standards abzubilden.

11. Verwandte Richtlinien und Verknüpfungen

11.1 P01 – Informationssicherheitsrichtlinie. Weist Rechenschaftspflicht für die Governance von Lieferantenabhängigkeiten zu.

11.2 P02 – Richtlinie zu Governance-Rollen und Verantwortlichkeiten. Stellt die Verantwortlichkeit für Entscheidungen zu Lieferantenrisiken klar.

11.3 P06 – Risikomanagement-Richtlinie. Verankert Konzentrationsrisiken in unternehmensweiten Risikoregistern.

11.4 P26 – Richtlinie zur Sicherheit von Lieferanten und Drittparteien. Sicherheitsbasislinie; P41 ergänzt Kontrollen zu Abhängigkeiten und Konzentration.

11.5 P27 – Richtlinie zur Nutzung von Cloud-Diensten. Wendet Abhängigkeitskriterien auf die Nutzung von Cloud-Services und Exit-Pläne an.

11.6 P28 – Richtlinie zur ausgelagerten Entwicklung. Behandelt Abhängigkeitsrisiken in externer Entwicklung.

11.7 P32 – Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery. Plant für Szenarien zu Lieferantenausfall und Ersatz.

11.8 P37 – Richtlinie zur rechtlichen und regulatorischen Compliance. Stellt sicher, dass Verträge und Verpflichtungen Kontrollen zu Abhängigkeiten berücksichtigen.

12. Referenzen

12.1 NIS2-Richtlinie (EU 2022/2555), Artikel 21 Absatz 3 (verlangt die Berücksichtigung von Schwachstellen, die für jeden direkten Lieferanten/Dienstleister spezifisch sind, sowie der Qualität ihrer Cybersicherheit, einschließlich der Ergebnisse koordinierter Bewertungen von Lieferkettenrisiken)

12.2 NIS2-Richtlinie, Artikel 22 Absatz 1 (unionsweite koordinierte Sicherheitsrisikobewertungen kritischer Lieferketten – informiert Einrichtungen über sektorweite Lieferantenrisiken)

12.3 Durchführungsverordnung (EU) 2024/2690 der Kommission, Anhang Abschnitt 5 (Anforderungen an die Sicherheit der Lieferkette für Einrichtungen, einschließlich Kriterien für Lieferantenauswahl, Diversifizierung und vertragliche Verpflichtungen)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – Empfehlungen zur Identifizierung kritischer Lieferanten und zur Steuerung der damit verbundenen Risiken

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