| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P06S | | | | | Dokumenttitel:<br>**Risikomanagement-Richtlinie** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>01.01.2025 | | | Dokumentenverantwortlicher: | | | | | | | |
| X | Richtlinie | | Standard | | Verfahren | | Formular | | Register | | Sonstiges | |

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

| **Genehmigungen** | | | |
|---|---|---|---|
| **Name** | **Position** | **Datum** | **Unterschrift** |
| | | | |
| | | | |

**Rechtlicher Hinweis (Urheberrecht und Nutzungsbeschränkungen)**

(C) 2025 Clarysec LLC. All rights reserved.

Dieses Dokument ist geistiges Eigentum der Clarysec LLC. Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Genehmigung für kommerzielle oder Implementierungszwecke kopiert, wiederverwendet, verbreitet oder verändert werden.
Die unbefugte Nutzung ist streng untersagt und kann rechtliche Schritte nach sich ziehen.
Für Lizenzierungsanfragen kontaktieren Sie bitte: info@clarysec.com

Ausgerichtet an anwendbaren Standards und regulatorischen Anforderungen

| Standard/Regelwerk | Klausel/Artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klauseln 6.1, 6.1.3 | |
| ISO/IEC 27002:2022 | 5.4, 5.25 | |
| NIST SP 800-53 Rev. 5 | RA-1 bis RA-7, PM-9 | |
| EU-NIS2-Richtlinie | Artikel 21(2)(a–d) | |
| EU DORA | Artikel 5 | |
| COBIT 2019 | APO12, MEA01 | |

**1. Zweck**

1.1 Diese Richtlinie legt fest, wie die Organisation Risiken im Zusammenhang mit Informationssicherheit, Betrieb, Technologie und Dienstleistungen Dritter identifiziert, bewertet und steuert.

1.2 Sie stellt sicher, dass das Risikomanagement ein aktiver Bestandteil der Planung, Projektdurchführung, Lieferantenauswahl und der Reaktion auf Sicherheitsvorfälle ist, im Einklang mit ISO 27001, ISO 31000 und regulatorischen Anforderungen.

1.3 Die Richtlinie unterstützt fundierte Entscheidungen, den Schutz von Informationswerten und die Resilienz wesentlicher Geschäftsprozesse.

**2. Geltungsbereich**

**2.1 Diese Richtlinie gilt für:**

2.1.1 alle Abteilungen, Systeme und Nutzer innerhalb der Organisation

2.1.2 sämtliche Informationen, Dienste und Werte, die intern oder durch Dritte verwaltet werden

2.1.3 risikobezogene Aktivitäten einschließlich Projektprüfungen, Systemaktualisierungen, Auslagerungen und regulatorischer Compliance

**2.2 Sie umfasst alle Arten von Risiken, insbesondere:**

2.2.1 Cybersicherheitsbedrohungen und Systemschwachstellen

2.2.2 betriebliche Störungen und Dienstausfälle

2.2.3 rechtliche, Compliance- oder Reputationsrisiken

2.2.4 Risiken im Zusammenhang mit Dritten und Lieferketten

2.3 Alle Mitarbeitenden, Auftragnehmer und Dienstleister müssen diese Richtlinie bei der Identifizierung oder Meldung von Risiken einhalten.

**3. Ziele**

3.1 Einfache und wiederholbare Verfahren zur Risikobewertung sind in die regulären Geschäftsabläufe zu integrieren.

3.2 Risiken, die sich auf Vertraulichkeit, Integrität, Verfügbarkeit (CIA) oder die Compliance auswirken können, sind zu identifizieren und zu priorisieren.

3.3 Für alle wesentlichen Risiken sind Verantwortlichkeiten festzulegen und Risikobehandlungsmaßnahmen zu definieren.

3.4 Zur Unterstützung der Auditfähigkeit und der Risikonachverfolgung ist ein korrektes und aktuelles Risikoregister zu führen.

3.5 Es ist sicherzustellen, dass das Management in die Genehmigung der Risikotoleranz und wesentlicher Risikobehandlungspläne eingebunden ist.

**4. Rollen und Verantwortlichkeiten**

**4.1 Geschäftsführung**

4.1.1 legt die Risikobereitschaft der Organisation fest und genehmigt das Risikomanagement-Rahmenwerk.

4.1.2 genehmigt wesentliche Entscheidungen zur Risikobehandlung und die hierfür erforderlichen Ressourcen.

4.1.3 überprüft gemeinsam mit dem Risikokoordinator vierteljährlich die wesentlichen Risiken.

**4.2 Risikokoordinator (oder ISMS-Verantwortlicher)**

4.2.1 koordiniert Risikobewertungen und pflegt das Risikoregister.

4.2.2 stellt sicher, dass Risikobewertung, Verantwortlichkeiten und Risikobehandlungsmaßnahmen dokumentiert sind.

4.2.3 organisiert mindestens einmal jährlich eine formale Risikoüberprüfung.

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

**9. Anforderungen an Überprüfung und Aktualisierung**

**9.1 Jährliche Richtlinienüberprüfung**

9.1.1 Diese Richtlinie muss mindestens einmal jährlich durch die Geschäftsführung und den Risikokoordinator überprüft werden, um Relevanz und Vollständigkeit sicherzustellen.

**9.2 Auslöser für Aktualisierungen**

**9.2.1 Eine vorgezogene Überprüfung und Aktualisierung muss erfolgen, wenn:**

9.2.1.1 ein wesentlicher Vorfall oder eine Auditfeststellung Risikolücken aufdeckt

9.2.1.2 neue Geschäftseinheiten, Technologien oder Partnerschaften eingeführt werden

9.2.1.3 sich eine regulatorische oder vertragliche Anforderung ändert

**9.3 Versionskontrolle**

**9.3.1 Alle Aktualisierungen dieser Richtlinie müssen mit den folgenden Metadaten versioniert werden:**

9.3.1.1 Versionsnummer und Inkrafttretensdatum

9.3.1.2 Zusammenfassung der Änderungen

9.3.1.3 Genehmiger (Geschäftsführung)

9.3.1.4 archivierte frühere Versionen zu Audit-Zwecken

**9.4 Kommunikation und Sensibilisierung**

9.4.1 Aktualisierte Versionen der Richtlinie und wesentliche Risikobehandlungspläne müssen den betroffenen Mitarbeitenden mitgeteilt werden. Die jährliche Sensibilisierungsschulung muss grundlegende Prinzipien des Risikobewusstseins enthalten.

**10. Zugehörige Richtlinien und Verknüpfungen**

**10.1 Diese Richtlinie wird in Abstimmung mit mehreren weiteren Richtlinien angewendet, um eine umfassende Sicherheitsgovernance sicherzustellen:**

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt fest, wer für Risikoverantwortung und Entscheidungsfindung rechenschaftspflichtig ist.

10.1.2 P5S – Änderungsmanagement-Richtlinie: Verlangt eine Risikobewertung vor der Umsetzung technischer oder prozessbezogener Änderungen.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Behandelt regulatorische Risiken im Zusammenhang mit dem Umgang mit personenbezogenen Daten.

10.1.4 P30S – Incident-Response-Richtlinie: Stellt sicher, dass die Risikobehandlung während und nach Sicherheitsvorfällen fortgeführt wird.

10.1.5 P33S – Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs: Identifiziert Restrisiken und Wiederherstellungsmaßnahmen für kritische Dienste.

## 11. Referenzstandards und Rahmenwerke

### 11.1 ISO/IEC 27001:

11.1.1 Klausel 6.1 – Legt einen formalen Risikomanagementprozess und die Planung der Risikobehandlung fest.

11.1.2 Klausel 6.1.3 – Verlangt von Organisationen die Aufbewahrung dokumentierter Behandlungspläne und Genehmigungen.

### 11.2 ISO/IEC 27002:

11.2.1 Maßnahmen 5.4, 5.25 – Geben Umsetzungshinweise zu Risikoverantwortung, Priorisierung und Lebenszyklusmanagement.

### 11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 bis RA-7 – Definieren Risikobewertung, Reaktionsstrategien, Dokumentation und Überprüfungsmechanismen.

11.4 PM-9 – Verlangt eine konsistente Überwachung organisatorischer Risiken auf Managementebene.

### 11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(a–d) – Verlangt verpflichtende Kontrollen zur Risikobewertung, Risikominderung und Governance für wesentliche und wichtige Einrichtungen.

### 11.6 EU DORA

11.6.1 Artikel 5 – Verlangt von regulierten Unternehmen, Rahmenwerke für das Management von IKT-Risiken festzulegen und zu steuern, einschließlich Identifizierung, Klassifizierung und Reaktion.

### 11.7 COBIT 2019

11.7.1 APO12 – Risiko steuern: Integriert Risiken in die strategische und operative Planung.

11.7.2 MEA01 – Überwachen, Evaluieren und Beurteilen: Stellt die Wirksamkeit und Compliance der Risikoprozesse und Maßnahmen sicher.