| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P06 | | | | | 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** |
| | | | |
| | | | |

An relevanten Standards und Vorschriften ausgerichtet

| Standard/Vorschrift | Klausel/Artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klauseln 6.1, 8.32, 10 | Kernanforderungen an die Risikoidentifizierung und das Risikomanagement, Integration in das Änderungsmanagement, kontinuierliche Verbesserung |
| ISO/IEC 27005:2024 | Vollständige Methodik des Risikolebenszyklus | Vollständiger Risikomanagementprozess im Einklang mit dem Standard |
| ISO 31000:2018 | Grundsätze und Rahmenwerk des Risikomanagements | Übernommene Grundsätze des Risikomanagements im Rahmenwerk |
| NIST SP 800-30 Rev.1 | SP 800-30, SP 800-39 | Leitlinien und Struktur für Risikobewertungen, gestufte Risiko-Governance |
| DSGVO | Artikel 24, 25, 32 | Datenschutzbezogene Risikoprozesse und Kontrollen |
| EU NIS2 | Artikel 21(2)(a–d) | Verpflichtungen zur Risiko- und Sicherheitsbewertung |
| EU DORA | Artikel 5, 6 | IKT-Risikomanagement und operationelle Resilienz |
| COBIT 2019 | APO12, MEA | Struktur und Überwachung des Risikomanagements |

**1. Zweck**

1.1 Diese Richtlinie legt ein einheitliches und formalisiertes Rahmenwerk zur Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von Informationssicherheitsrisiken in der gesamten Organisation fest.

1.2 Sie gewährleistet die konsistente Anwendung risikobasierter Grundsätze zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Informationswerten im Einklang mit ISO/IEC 27001:2022, Klausel 6.1, und ISO 31000:2018.

1.3 Die Richtlinie verankert das Management von Informationssicherheitsrisiken in den Entscheidungsprozessen der Organisation, um interne strategische Ziele und externe regulatorische Anforderungen zu erfüllen.

**2. Geltungsbereich**

2.1 Diese Richtlinie gilt für alle Organisationseinheiten, Geschäftsprozesse, Systeme, alle Beschäftigten sowie Einbindungen Dritter, die an der Handhabung, Entwicklung, Speicherung oder Verwaltung von Informationswerten beteiligt sind.

2.2 Der Geltungsbereich erstreckt sich auf physische, digitale und cloudbasierte Systeme bzw. Werte, einschließlich strukturierter und unstrukturierter Daten, Anwendungen, Infrastruktur, Netzwerke und Dienste.

2.3 Sie umfasst Informationssicherheitsrisiken auf strategischer, operativer, Projekt- und technischer Ebene und ist für alle Mitarbeiter, Auftragnehmer und Dienstleister verbindlich, die in ISMS-Aktivitäten eingebunden sind.

**2.4 Das Risikomanagement ist auf die folgenden Szenarien anzuwenden:**

**2.4.1 Neue Projekte oder Systemeinführungen**

2.4.1.1 Wesentliche Änderungen (z. B. Architektur, Eigentümerschaft, Prozesse)

2.4.1.2 Onboarding von Lieferanten und Vereinbarungen mit Dritten

2.4.1.3 Reaktion auf Sicherheitsvorfälle und Überprüfungen nach Vorfällen

2.4.1.4 Regelmäßige organisatorische Risikoüberprüfungen oder Audits

## 3. Ziele

3.1 Einrichtung und operative Umsetzung eines wiederholbaren, organisationsweiten Risikomanagementprozesses auf Grundlage der Methoden nach ISO/IEC 27005 und ISO 31000.

3.2 Sicherstellung, dass Risiken mithilfe strukturierter und nachvollziehbarer Methoden identifiziert, analysiert, bewertet und behandelt werden, einschließlich der Zuordnung von Risikoverantwortung und der Verknüpfung mit Kontrollen.

3.3 Aufrechterhaltung eines zentralen und versionskontrollierten Risikoregisters und Risikobehandlungsplans, die den aktuellen Risikostatus, die Abdeckung durch Kontrollen und den Fortschritt risikomindernder Maßnahmen abbilden.

3.4 Ausrichtung von Risikoentscheidungen an dokumentierter Risikobereitschaft und festgelegten Toleranzwerten sowie Ermöglichung fundierter Governance-Entscheidungen zur Risikoakzeptanz, Risikominderung, Risikoübertragung oder Risikovermeidung.

3.5 Kontinuierliche Überwachung von Risikotrends und Sicherstellung der Wirksamkeit von Risikobehandlungen sowie Ermöglichung proaktiver Anpassungen auf Grundlage der Bedrohungslage oder geschäftlicher Veränderungen.

## 4. Rollen und Verantwortlichkeiten

**4.1 Geschäftsleitung / Leitungsorgan**

4.1.1 Genehmigt das Risikomanagement-Rahmenwerk und legt die akzeptable Risikobereitschaft sowie Toleranzschwellen fest.

4.1.2 Genehmigt Risikobehandlungsstrategien für Restrisiken, die die Toleranz überschreiten.

4.1.3 Stellt Ressourcen und Aufsicht für den wirksamen Betrieb des Risikomanagementprogramms bereit.

**4.2 ISMS-Manager / Risikobeauftragter**

4.2.1 Ist für diese Richtlinie verantwortlich und stellt ihre Konformität mit ISO/IEC 27001 und ISO/IEC 27005 sicher.

4.2.2 Leitet den unternehmensweiten Risikobewertungsprozess und pflegt das Risikoregister sowie den Risikobehandlungsplan.

4.2.3 Stellt regelmäßige Überprüfungen und die Eskalation wesentlicher Risiken an die Geschäftsleitung oder den Informationssicherheitslenkungsausschuss sicher.

[ ... 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 Diese Richtlinie und das zugehörige Rahmenwerk sind jährlich oder in den folgenden Fällen zu überprüfen:**

9.1.1 Nach einem wesentlichen Risikoereignis oder Informationssicherheitsvorfall

9.1.2 Nach einer erheblichen organisatorischen oder technischen Änderung

9.1.3 Als Reaktion auf Auditfeststellungen oder neue regulatorische Anforderungen

**9.2 Der ISMS-Manager, der Risikobeauftragte und das Compliance-Team sind gemeinsam verantwortlich für:**

9.2.1 die Einleitung des Überprüfungszyklus

9.2.2 die Einholung von Beiträgen aus den Geschäftsbereichen

9.2.3 die Überarbeitung von Verfahren und Schwellenwerten nach Bedarf

**9.3 Alle Überarbeitungen müssen:**

9.3.1 versionskontrolliert und protokolliert werden,

9.3.2 von der Geschäftsleitung genehmigt werden,

9.3.3 an relevante Interessengruppen kommuniziert werden,

9.3.4 für mindestens 5 Jahre im Audit-Repository aufbewahrt werden.

## 10. Zugehörige Richtlinien und Verknüpfungen

**10.1 Diese Richtlinie steht in wechselseitiger Abhängigkeit zu den folgenden Informationssicherheitsrichtlinien:**

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt das übergeordnete Governance-Modell für Informationssicherheit fest, innerhalb dessen diese Risikomanagement-Richtlinie gilt.

10.1.2 P2 – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert die verantwortlichen Stellen und Governance-Ebenen, auf die in der Risikoeskalationsmatrix Bezug genommen wird.

10.1.3 P5 – Änderungsmanagement-Richtlinie: Löst bei Infrastruktur- und Organisationsänderungen eine erneute Risikobewertung aus.

10.1.4 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Unterstützt die Auswirkungsbewertung bei der Risikoidentifizierung.

10.1.5 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Validiert die Einhaltung dieser Richtlinie, einschließlich der Vollständigkeit des Risikoregisters und der Nachweise zu Risikobehandlungen.

## 11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist ausdrücklich an den folgenden Standards und Rahmenwerken ausgerichtet, um sicherzustellen, dass sie internationalen Best Practices und regulatorischen Erwartungen für das Management von Informationssicherheitsrisiken entspricht:

**11.2 ISO/IEC 27001:**

11.2.1 Klausel 6.1: Legt die Anforderungen an die Identifizierung von Risiken und Chancen fest, einschließlich des vollständigen Lebenszyklus von Informationssicherheitsrisikobewertungen und -behandlungen. Diese Richtlinie setzt Klausel 6.1.2 und 6.1 durch ein strukturiertes Rahmenwerk operativ um, das dokumentierte Verfahren für Risikoidentifizierung, Analyse, Bewertung, Behandlung und Restrisikoakzeptanz verbindlich vorgibt.

11.2.2 Klausel 8.32: Die Integration risikobasierten Denkens in Änderungsmanagementprozesse stellt sicher, dass alle wesentlichen organisatorischen Änderungen formelle erneute Risikobewertungen auslösen.

11.2.3 Klausel 10: Kontinuierliche Verbesserung ist durch regelmäßige Richtlinienüberprüfungen, Trendanalysen von Risiken und risikobasierte Aktualisierungen der SoA verankert.

**11.3 ISO/IEC 27005:**

11.3.1 Bietet spezialisierte und detaillierte Leitlinien für das Management von Informationssicherheitsrisiken. Diese Richtlinie setzt das vollständige Risikoprozessmodell der

ISO/IEC 27005 um: Festlegung des Kontexts, Risikoidentifizierung, Risikoanalyse, Risikobewertung, Risikobehandlung, Risikoakzeptanz, Risikokommunikation sowie Risikoüberwachung und -überprüfung.

**11.4 ISO 31000:**

11.4.1 Diese Richtlinie integriert Grundsätze der ISO 31000 wie Führungsverantwortung, Integration in Entscheidungsprozesse und kontinuierliche Verbesserung. Sie stellt sicher, dass das Risikomanagement in Kultur und Betrieb der Organisation verankert ist.

**11.5 NIST SP 800-30 Rev.1:**

11.5.1 Entspricht dem NIST-Leitfaden zur Durchführung von Risikobewertungen, einschließlich Bedrohungsidentifizierung, Schwachstellenanalyse, Einschätzung der Eintrittswahrscheinlichkeit und Bestimmung der Auswirkungen. Die Struktur dieser Richtlinie spiegelt die von NIST definierten Schritte der Risikobewertung wider und passt sie sowohl auf technische als auch auf geschäftliche Prozesse an.

**11.6 NIST SP 800-39:**

11.6.1 Unterstützt die Risiko-Governance auf Unternehmensebene und betont ein gestuftes Risikomanagement auf Ebene der Organisation, der Mission/Geschäftsprozesse und der Informationssysteme. Die Richtlinie stellt sicher, dass die Risikoverantwortung auf allen Ebenen eindeutig definiert ist und Behandlungsstrategien auf Organisationsebene umfasst.

**11.7 DSGVO:**

11.7.1 Artikel 24: Verlangt die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um Datenschutzrisiken angemessen zu steuern – dies wird durch den strukturierten Risikoprozess dieser Richtlinie abgedeckt.

11.7.2 Artikel 25: „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ steht im Einklang mit der Verankerung der Risikobehandlung in System- und Prozessdesigns.

11.7.3 Artikel 32: Verlangt einen risikobasierten Ansatz für Sicherheitsmaßnahmen – erfüllt durch auswirkungsbasierte Risikobewertungen und die Auswahl von Kontrollen.

**11.8 EU NIS2-Richtlinie:**

11.8.1 Artikel 21(2)(a–d): Verlangt von Einrichtungen die Durchführung von Risikobewertungen, die Umsetzung von Richtlinien zur Risikoanalyse und die Sicherstellung verhältnismäßiger Sicherheitsmaßnahmen. Diese Richtlinie erfüllt diese Verpflichtungen durch die kontinuierliche Anwendung des Risikolebenszyklus und dokumentierte Governance.

**11.9 EU DORA:**

11.9.1 Artikel 5: Verlangt ein dokumentiertes IKT-Risikomanagement-Rahmenwerk – vollständig abgedeckt durch die Architektur dieser Richtlinie, einschließlich SoA-Zuordnung und KRIs.

11.9.2 Artikel 6: Verlangt die Integration des Risikomanagements in Strategien zur operationellen Resilienz; dies wird durch Eskalationsmatrizen und die Nachverfolgung kritischer Informationswerte adressiert.

**11.10 COBIT 2019:**

11.10.1 APO12 – Risiken managen: Entspricht unmittelbar der Einrichtung eines strukturierten Risikomanagementansatzes in der Organisation, einschließlich Rollenzuweisung, Nachverfolgung von Behandlungen und Sicherstellung der Rechenschaftspflicht auf Ebene des Leitungsorgans.

11.10.2 MEA01 – Leistung und Konformität überwachen, evaluieren und beurteilen: Spiegelt sich im Schwerpunkt dieser Richtlinie auf Trendanalysen, der Überwachung von KRIs und der Integration von Audit-Rückmeldungen in Zyklen der kontinuierlichen Verbesserung wider.