Risikomatrix 5×5 mit Bewertungskriterien

Hinweis
So nutzen Sie die Vorlage: Beschreiben Sie je Stufe, was Wahrscheinlichkeit und Auswirkung in Ihrem Unternehmen bedeuten, und lassen Sie die Akzeptanzregeln von der Geschäftsleitung freigeben. Dann bewerten Sie jedes Risikoszenario im Risikoregister, vor und nach den Maßnahmen. Stufen, Klassen und Regeln entsprechen der Standardmethode „ISO 27005 Standard 5×5“ in Complass.

Risikomatrix

Eintrittswahrscheinlichkeit	1 gering	2 begrenzt	3 spürbar	4 schwer	5 existenzbedrohend
5 häufig mehr als 3-mal im Jahr	5 mittel	10 hoch	15 hoch	20 kritisch	25 kritisch
4 wahrscheinlich 1- bis 3-mal im Jahr	4 niedrig	8 mittel	12 hoch	16 kritisch	20 kritisch
3 möglich etwa alle 1 bis 3 Jahre	3 niedrig	6 mittel	9 mittel	12 hoch	15 hoch
2 selten etwa alle 3 bis 10 Jahre	2 niedrig	4 niedrig	6 mittel	8 mittel	10 hoch
1 sehr selten seltener als alle 10 Jahre	1 niedrig	2 niedrig	3 niedrig	4 niedrig	5 mittel

niedrig (1–4) mittel (5–9) hoch (10–15) kritisch (16–25)

Risikowert = Eintrittswahrscheinlichkeit × Auswirkung (1 bis 25). Die Auswirkung bewerten Sie je Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit) und nehmen den höchsten Wert. Die Beträge sind Beispielwerte für ein produzierendes Unternehmen mit 150 bis 500 Beschäftigten; passen Sie sie an Ihre Größe an.

Stufen der Eintrittswahrscheinlichkeit

Stufe	Bezeichnung	Beschreibung	Ihre Festlegung
1	sehr selten	seltener als alle 10 Jahre	
2	selten	etwa alle 3 bis 10 Jahre	

Stufe	Bezeichnung	Beschreibung	Ihre Festlegung
3	möglich	etwa alle 1 bis 3 Jahre	
4	wahrscheinlich	1- bis 3-mal im Jahr	
5	häufig	mehr als 3-mal im Jahr	

Stufen der Auswirkung

Stufe	Bezeichnung	Beschreibung	Finanziell (Beispiel)	Ihre Festlegung
1	gering	kaum spürbar, intern ohne Außenwirkung	bis 10.000 €	
2	begrenzt	begrenzter Schaden, schnell behebbar	10.000 € bis 50.000 €	
3	spürbar	spürbarer Schaden, Kunden oder Partner betroffen	50.000 € bis 250.000 €	
4	schwer	schwerer Schaden, Meldepflichten, Vertragsstrafen	250.000 € bis 1.000.000 €	
5	existenzbedrohend	existenzbedrohend für das Unternehmen	über 1.000.000 €	

Risikoklassen und Akzeptanz

Klasse	Risikowert	Wer darf akzeptieren	Überprüfung
niedrig	1–4	Risikoeigner mit Begründung	alle 24 Monate
mittel	5–9	Risikoeigner mit Begründung	alle 12 Monate
hoch	10–15	Geschäftsleitung, mit Begründung und befristet	alle 6 Monate
kritisch	16–25	nicht akzeptierbar, Behandlung erforderlich	alle 3 Monate

Risikoregister

ID	Risikoszenario	Risikoeigner	W	A	Wert / Klasse	Behandlung und Maßnahmen	Restrisiko
R01							
R02							
R03							
R04							
R05							
R06							
R07							
R08							
R09							
R10							

Über diese Vorlage

Vorlagenversion 1.0-12c0f439
Stand der Inhalte 26.09.2026
Herausgeber Erstellt mit Complass, https://complass.eu

Bezug: ISO/IEC 27001:2022 6.1.2; ISO/IEC 27005:2022

Diese Vorlage ist keine Rechtsberatung. Sie ersetzt nicht die Prüfung, welche Anforderungen für Ihr Unternehmen gelten, und garantiert kein Prüfungs- oder Zertifizierungsergebnis.

Lizenz: Creative Commons Namensnennung 4.0 International (CC BY 4.0). Sie dürfen die Vorlage verwenden, ändern und weitergeben, auch kommerziell, wenn Sie die Quelle nennen. Namensnennung: „Vorlage: Complass (complass.eu), CC BY 4.0“. https://creativecommons.org/licenses/by/4.0/deed.de