Risk matrix 5×5 with assessment criteria

Note
How to use this template: describe for each level what likelihood and impact mean in your company, and have top management approve the acceptance rules. Then rate every risk scenario in the risk register, before and after the controls. Levels, classes and rules match the default method "ISO 27005 Standard 5×5" in Complass.

Risk matrix

Likelihood	1 minor	2 limited	3 noticeable	4 severe	5 existence-threatening
5 frequent more than 3 times a year	5 medium	10 high	15 high	20 critical	25 critical
4 likely 1 to 3 times a year	4 low	8 medium	12 high	16 critical	20 critical
3 possible about every 1 to 3 years	3 low	6 medium	9 medium	12 high	15 high
2 rare about every 3 to 10 years	2 low	4 low	6 medium	8 medium	10 high
1 very rare less often than every 10 years	1 low	2 low	3 low	4 low	5 medium

low (1–4) medium (5–9) high (10–15) critical (16–25)

Risk score = likelihood × impact (1 to 25). Rate the impact per protection goal (confidentiality, integrity, availability) and take the highest value. The amounts are example values for a manufacturing company with 150 to 500 employees; adapt them to your size.

Likelihood levels

Level	Name	Description	Your definition
1	very rare	less often than every 10 years	
2	rare	about every 3 to 10 years	
3	possible	about every 1 to 3 years	

Level	Name	Description	Your definition
4	likely	1 to 3 times a year	
5	frequent	more than 3 times a year	

Impact levels

Level	Name	Description	Financial (example)	Your definition
1	minor	barely noticeable, internal with no external effect	up to €10,000	
2	limited	limited damage, quickly remedied	€10,000 to €50,000	
3	noticeable	noticeable damage, customers or partners affected	€50,000 to €250,000	
4	severe	severe damage, reporting duties, contract penalties	€250,000 to €1,000,000	
5	existence-threatening	threatens the existence of the company	over €1,000,000	

Risk classes and acceptance

Class	Risk score	Who may accept	Review
low	1–4	Risk owner with a justification	every 24 months
medium	5–9	Risk owner with a justification	every 12 months
high	10–15	Top management, with a justification and for a limited time	every 6 months
critical	16–25	not acceptable, treatment required	every 3 months

Risk register

ID	Risk scenario	Risk owner	L	I	Score / class	Treatment and controls	Residual risk
R01							
R02							
R03							
R04							
R05							
R06							
R07							
R08							
R09							
R10							

About this template

Template version 1.0-2cb82620
Content as of 26 September 2026
Published by Made with Complass, https://complass.eu

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

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en