TEMPLATE P12 · RISK MATRIX AND REGISTER

Risk matrix and register

Identifies, assesses and monitors the use case's risks using common scales, inherent and residual levels, a response and acceptance by the competent body.

Fernando García Varela Version 0.1 (working draft) 16-09-2026 Draft for review

IN THIS DOCUMENT

01 Instructions for use

02 Identification

03 Scales

04 Risk register

05 Use case heat map

06 Acceptance of residual risk

07 Portfolio risks (Enterprise)

08 Review history

09 Quality criteria

10 Approval and verification

11 Version control

Legal notice and disclaimer. SEVEN-G is a reference methodological framework provided "as is" and for information purposes only. It does not constitute legal, regulatory, financial or professional advice, nor does it guarantee compliance with any law or standard. References to general regulation (such as the EU AI Act, the GDPR, DORA or NIS2), to technical standards and to regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date. **Each organisation that uses SEVEN-G is solely responsible for identifying the regulation that applies to it, verifying that it is current and certifying its own regulatory compliance**, with the appropriate qualified advice. This methodology is a generic, free aid shared with the community so that nobody has to start from scratch; each person or organisation can and should adapt it to its own use. It must not be inferred that its legally sensitive parts have been reviewed by legal counsel: those reviews, for each company or sector, are the ultimate responsibility of the company, consultant or organisation that uses it. Although every effort is made to keep it up to date, some regulation may have changed without being reflected here. To the fullest extent permitted by law, the author accepts no responsibility whatsoever for the effects of its application in any organisation or for its full applicability. The methodology does not grant certification of any kind. The author accepts no liability for any use made of this content or for any decisions taken on the basis of it. The data, figures, companies and cases in the examples are fictitious or illustrative.

01

Instructions for use

Aspect	Guidance
When it is used	It is created in phase 3 and is a living register: it is updated in phase 5 (updated risk register before G5), in phase 6 and at every R6, and whenever a risk materialises, the classification changes or a new risk emerges.
Who completes it	The AI Risk Owner coordinates and assesses; the AI Product Owner and the AI Technical Owner identify risks and propose controls; each risk has an owner.
Who verifies it	Lite: the AI Risk Owner at G3 and G5; if the AI Risk Owner has prepared the register, the AI Office or the AI Auditor verifies it. Enterprise: AI Auditor.

Aspect	Guidance
Who decides	Acceptance of residual risk is decided by the body in section 6 according to the level. The *gate* is decided by the body in 01 §7.5.
Gate at which it is reviewed	Feasibility, G5 · Go-live and R6 · Continuity review. (G3)
Tool	T06 · Risk matrix and register: "Risks" view and "Risks" record tab of the T01 register, with the same fields, scales, heat map and acceptance rules as this template, CSV export and Excel of the use case (matrix, register, mitigation and contingency plans proposed for P13 and typical risks to consider).
Lite versus Enterprise	Lite may omit the columns and blocks marked **(Enterprise)**. The scales, the inherent and residual levels, the response and the acceptance are mandatory in both.

Completion rules:

- The scales and levels are **those of the common specification §5.1 and document 33**. They are not modified per use case.
- Impact is assessed on **five axes** and the **highest** is taken.
- The level is calculated as **inherent** (without controls) and **residual** (with effective controls). A control only reduces the residual if it exists and works; planned controls are indicated separately.
- A **Critical** residual risk without approval from the board or its board committee **blocks G3 and G5**.
- The typical risks in the catalogue of document 33 (format RT-<CAT>-NN) are used as a starting point so that known risks are not omitted.

02

Identification

Field	Content	Guidance
Use case code		IA-AAAA-NNN.
AI systems covered		Codes from P05.
Regulatory classification		Taxonomy of 03 §3.3 (P11).
Intensity and ambition level		
Document version		
Date of last review		DD-MM-AAAA.

Field	Content	Guidance
Next review		Date of the next R6 or the next *gate*.
Applicable economic impact thresholds		Reference to those approved in C2 (document 13).

03

Scales

3.1 Likelihood

Value	Name	Indicative reference
1	Rare	Less than once in 5 years or < 5 % over the use case's horizon
2	Unlikely	Once every 2–5 years or 5–20 %
3	Possible	Once every 1–2 years or 20–50 %
4	Likely	Several times a year or 50–80 %
5	Almost certain	Monthly or more often, or > 80 %

3.2 Impact

Value	Name
1	Negligible
2	Minor
3	Moderate
4	Major
5	Critical

Assessment axes (the highest is taken):

Axis	What is assessed	Guidance
Economic	Losses, cost overruns, unrealised value.	Thresholds in euros set by the company in C2, in proportion to its size.
People and rights	Harm to customers, employees or other people; discrimination; physical safety.	
Regulatory	Non-compliance, sanctions, requests from the supervisor.	
Operational	Interruption or degradation of processes and services.	
Reputational	Loss of trust among customers, the market or society.	

3.3 Risk level

Level = Likelihood × Impact: **Low** 1–4 · **Medium** 5–9 · **High** 10–15 · **Critical** 16–25.

Likelihood \ Impact	1 Negligible	2 Minor	3 Moderate	4 Major	5 Critical
5 Almost certain	5 Medium	10 High	15 High	20 Critical	25 Critical
4 Likely	4 Low	8 Medium	12 High	16 Critical	20 Critical
3 Possible	3 Low	6 Medium	9 Medium	12 High	15 High
2 Unlikely	2 Low	4 Low	6 Medium	8 Medium	10 High
1 Rare	1 Low	2 Low	3 Low	4 Low	5 Medium

In a spreadsheet: `=IF(P*I>=16,"Critical",IF(P*I>=10,"High",IF(P*I>=5,"Medium","Low")))`.

04

Risk register

4.1 Identification

No.	Risk (cause, event and consequence)	Category	Reference typical risk	System or phase	Risk owner	Date added
R01		EST · TEC · DAT · ECO · LEG · ORG · REP · GEN · SEG · TER	Code from the catalogue of document 33, if one exists			
R02						
(illustrative example) **R01**	Through a prompt injection in a customer's message, the assistant reveals order data belonging to another customer, causing harm to the affected person and a possible breach of the GDPR.	GEN	GEN catalogue of document 33	Enquiries assistant · phases 5–6	AI Technical Owner	20-11-2026

Categories: EST strategic · TEC technical · DAT data · ECO economic · LEG legal and compliance · ORG organisational · REP reputational · GEN generative AI and agents · SEG security and offensive AI · TER third parties.

4.2 Inherent and residual assessment

No.	Inh. L	Inh. I	Dominant axis	Inherent level	Existing and effective controls	Res. L	Res. I	Residual level	Trend (Enterprise)
R01	1–5	1–5		Low · Medium · High · Critical					Rising · Stable · Falling
(illustrative example) **R01**	4	4	People and rights	16 Critical	Session isolation per customer; output filter for personal data; injection testing with 0 leaks	2	4	8 Medium	Falling

4.3 Response and monitoring

No.	Response	Planned controls (P13)	Accepted by	Acceptance date	Status	Next review
R01	Avoid · Mitigate · Transfer · Accept				Identified · Under treatment · Accepted · Materialised · Closed	
(illustrative example) **R01**	Mitigate	Output monitoring with alerting (P25)	AI Sponsor, with clearance from the AI Risk Owner	15-01-2027	Accepted	R6 in the second quarter of 2027

Responses: **Avoid** (the cause or the activity is eliminated) · **Mitigate** (controls that reduce likelihood or impact) · **Transfer** (insurance or contract; reputational and regulatory risk is not fully transferred) · **Accept** (the residual is assumed with approval). The list of statuses is proposed by this template, to be confirmed in document 33.

05

Use case heat map

In each cell, enter the risk numbers according to their **residual** assessment.

Likelihood \ Impact	1 Negligible	2 Minor	3 Moderate	4 Major	5 Critical
5 Almost certain					
4 Likely					
3 Possible					
2 Unlikely				R01 *(illustrative example)*	
1 Rare					

Summary	Inherent	Residual
Critical		

Summary	Inherent	Residual
High		
Medium		
Low		

06

Acceptance of residual risk

Residual level	Who may accept it	Requirement
Low (1–4)	AI Product Owner	With a record.
Medium (5–9)	AI Sponsor	With clearance from the AI Risk Owner.
High (10–15)	AI Committee	With clearance from the AI Risk Owner and a mitigation plan (P13). Also applies under Lite intensity.
Critical (16–25)	Not accepted	Exceptionally, only the board or its board committee, within the risk appetite approved in C2. Without that approval it blocks G3 and G5.

No.	Residual level	Accepting body	Date	Reference of the minutes or record	Validity of the acceptance
					Until the next R6 or until the change that invalidates it

07

Portfolio risks (**Enterprise**)

Field	Content	Guidance
Risks shared with other use cases		Same supplier, same model, same data or same critical function.

Field	Content	Guidance
Concentration		If the sum of exposures exceeds the risk appetite, the AI Committee is informed.
Risks to be escalated		High or Critical risks and concentrated risks.

08

Review history

Date	Moment	Main changes	New risks	Closed risks	Reviewed by
	G5 · R6 · Event (phase 3)				

09

Quality criteria

The formal criteria are in document 21 (see criteria G3.xx, G5.xx and R6.xx) and the methodology in document 33.

#	Check	Status
1	The register has been checked against the catalogue of typical risks, including GEN, SEG and TER where applicable.	Met · Not met · Not applicable · Pending
2	Each risk describes cause, event and consequence, and has an owner.	
3	The scales used are the common ones and impact takes the highest of the five axes.	
4	Inherent and residual levels are calculated; the residual only considers existing and effective controls.	
5	Each risk has a response; those marked Mitigate have controls in P13.	
6	Acceptance is signed by the body corresponding to the residual level.	
7	There are no Critical residual risks without approval from the board or its board committee.	

#	Check	Status
8	The register is up to date at the time of the *gate* or the review.	

10

Approval and verification

Function	Role in SEVEN-G	Name and position	Date	Signature or reference
Coordinates and assesses	AI Risk Owner			
Identifies and proposes controls	AI Product Owner and AI Technical Owner			
Verifies	AI Office or AI Auditor (Lite, if the AI Risk Owner prepares the risks) · AI Auditor (Enterprise)			
Accepts the residual	According to section 6			
Decides the *gate*	Body in 01 §7.5			

Segregation of duties: whoever accepts a risk has not assessed it; the AI Risk Owner issues clearance but does not accept risks of Medium level or above.

11

Version control

Completed document

Version	Date	Author	Changes

Template

Version	Date	Changes
0.1	16-09-2026	First version. Applies the scales, levels, responses, acceptance and categories of the common specification §5.1.

External sources cited

Links to the official or primary source, checked before publication. Always verify the version in force on the date of use.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng · Parlamento Europeo y Consejo de la UE · 27-04-2016