TEMPLATE P13 · MITIGATION AND CONTINGENCY PLAN

Mitigation and contingency plan

Turns the response to each risk into actions with an owner, deadline, cost and effectiveness test, and defines what is done if the risk materialises.

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

IN THIS DOCUMENT

01 Instructions for use

02 Identification

03 Summary of risks requiring treatment

04 Mitigation actions

05 Risk transfer

06 Contingency plans

07 Risks accepted without actions

08 Plan monitoring (Enterprise)

09 Total cost of the plan

10 Quality criteria

11 Approval and verification

12 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regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date.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	In phase 3, together with the risk matrix and register (P12), before G3. It is followed up in phases 4 and 5 (controls must be designed at G4 and operating at G5) and updated in phase 6.
Who completes it	The AI Risk Owner coordinates. Each action is proposed and carried out by its owner (usually the AI Technical Owner or the AI Product Owner).
Who verifies it	Lite: the AI Risk Owner at G3; if the AI Risk Owner has prepared the plan, the AI Office or the AI Auditor verifies it. Enterprise: AI Auditor.

Aspect	Guidance
Who decides	It is approved with G3: AI Sponsor with risk clearance (Lite) · AI Committee (Enterprise). Funding for the actions forms part of the decision.
Gate at which it is reviewed	Feasibility; follow-up at G4, G5 and R6. (G3)
Tool	T06 · Risk matrix and register: records the response, controls and contingency plan of each risk; treatment actions with owner, deadline and status are tracked in this template. The Excel of the use case generated by T06 proposes, for each registered risk, mitigation actions (section 4) and a contingency plan (section 6) from the catalogue in document 33 §9, with the columns of this template to be completed: it is the starting point, not the approved plan.
Lite versus Enterprise	Lite may omit the columns and blocks marked **(Enterprise)**. Every Medium, High or Critical residual risk must have actions and, if High or Critical, a contingency plan, under both intensities.

Completion rules:

- Each action is linked to a risk in P12 and states **what it reduces**: likelihood, impact or both.
- An action does not reduce residual risk until there is **evidence of effectiveness**.
- Critical security, legal compliance and human oversight controls do not allow "Proceed with conditions" (01 §7.3).
- The costs of the actions are incorporated into the feasibility assessment (P10) under their category.

02

Identification

Field	Content	Guidance
Use case code		IA-AAAA-NNN.
Associated P12 version		The plan corresponds to a specific version of the register.
Document version		
Date		DD-MM-AAAA.
Author		Name and role.
Intensity		Lite · Enterprise.

03

Summary of risks requiring treatment

No. (P12)	Risk	Inherent level	Response	Target residual level	Target date
			Avoid · Mitigate · Transfer · Accept	Low · Medium · High · Critical	
(illustrative example) **R01**	Leakage of another customer's data through prompt injection	16 Critical	Mitigate	8 Medium	Before G5

04

Mitigation actions

Action no.	Risk	Action	Control type	Reduces	Owner	Deadline	Estimated cost (€) and category	Evidence of effectiveness
A01			Preventive · Detective · Corrective	Likelihood · Impact · Both				
(illustrative example) **A01**	R01	Isolate the context of each conversation and limit queries to the authenticated customer's orders.	Preventive	Likelihood	AI Technical Owner	15-12-2026	8,000 · Build people	Test of 300 injection attacks with no leaks
(illustrative example) **A02**	R01	Output filter that blocks personal data not belonging to the customer.	Preventive	Impact	AI Technical Owner	15-12-2026	4,000 · Licences	Filter test report

Action no.	Risk	Action	Control type	Reduces	Owner	Deadline	Estimated cost (€) and category	Evidence of effectiveness
***(illustrative example)* A03**	R01	Operational alert when the filter blocks a response.	Detective	Impact	AI Operations Owner	31-01-2027	1,500 · Control and compliance	Alert configured and tested (P25)

Cost categories: licences · model consumption · compute and infrastructure · data · build people · operations people · suppliers and services · control and compliance · adoption and training.

05

Risk transfer

Complete if any response is "Transfer".

Risk	Mechanism	Counterparty	Coverage and limits	Annual cost (€)	Part of the risk that is not transferred
	Insurance · Contractual clause · Supplier warranty				Reputational, regulatory or people-related risk that remains with the company

06

Contingency plans

One for each High or Critical residual risk and for each risk with impact 5 even if its level is lower.

Field	Content	Guidance
Risk		No. from P12.
Scenario		What happens when the risk materialises.
Trigger		Indicator and threshold that activate the plan. It must be observable in monitoring (P25).

Field	Content	Guidance
Immediate actions		Containment in the first hours, including shutting down the system if appropriate.
Use of the rollback plan		Whether P19 is activated and how the previous process is restored.
Owner responsible for activating the plan		Person with authority to stop the system.
Maximum reaction time		Hours from the trigger to containment.
Communication		Who is informed: AI Committee, data protection, customers, supervisors.
Regulatory notifications		If it may be a serious incident or a personal data breach, the incident response plan (P26) is followed with its time limits.
Recovery		Conditions for resuming operation.

(illustrative example) Risk R01. Trigger: a single confirmed response containing another customer's data. Actions: deactivate the assistant on the web channel and route enquiries to agents; preserve logs; open an S1 or S2 incident depending on scope. Owner: AI Operations Owner. Maximum reaction time: 1 hour. Communication: AI Committee and data protection officer immediately.

07

Risks accepted without actions

Risk	Residual level	Reason for acceptance	Accepted by (P12 §6)	Condition that would require it to be reviewed

08

Plan monitoring (Enterprise)

Review date	Actions implemented	Actions with verified effectiveness	Overdue actions	Risks that change level	Decision

Overdue actions on relevant controls are treated as an expired condition and may constitute a nonconformity (01 §12).

09

Total cost of the plan

Category	One-off investment (€)	Annual recurring cost (€)
Control and compliance		
Build people		
Operations people		
Licences		
Suppliers and services		
Other categories		
Total		

The total must be shown in P10 §6.1.

10

Quality criteria

The formal criteria are in document 21 (see criteria G3.xx, G4.xx and G5.xx).

#	Check	Status
1	Every Medium, High or Critical residual risk in P12 has actions or documented acceptance.	Met · Not met · Not applicable · Pending
2	Each action has an owner, date, cost and planned evidence of effectiveness.	
3	High and Critical residual risks, and those with impact 5, have a contingency plan with an observable trigger.	
4	The contingency plans link to P19 (rollback) and P26 (incidents).	

#	Check	Status
5	Transfers indicate what is not transferred.	
6	The cost of the plan is incorporated into P10.	
7	No conditions are proposed on critical security, legal compliance or human oversight controls.	

11

Approval and verification

Function	Role in SEVEN-G	Name and position	Date	Signature or reference
Coordinates	AI Risk Owner			
Answers for the actions	Owners of each action			
Verifies	AI Office or AI Auditor (Lite, if the AI Risk Owner prepares the risks) · AI Auditor (Enterprise)			
Decides and funds	AI Sponsor with risk clearance (Lite) · AI Committee (Enterprise)			

Segregation of duties: whoever carries out an action does not verify its effectiveness.

12

Version control

Completed document

Version	Date	Author	Changes

Template

Version	Date	Changes
0.1	16-09-2026	First version. Mitigation actions linked to P12, transfer, contingency and cost by category of the common specification §5.1 and §5.7.