TEMPLATE P50 · NONCONFORMITY REGISTER

Nonconformity register

Records each nonconformity with the framework and tracks it from detection to closure by the AI Auditor, with type, containment, root cause, actions, effectiveness verification and time limits.

Fernando García Varela Version 0.1 (working draft) 19-09-2026 Draft for review

IN THIS DOCUMENT

01 Instructions for use

02 Identification

03 Requirement not met and description

04 Type

05 Containment

06 Root cause and action plan

07 Time limits

08 Effectiveness verification, closure and re-audit

09 Status and history

10 Company register

11 Quality criteria

12 Approval and verification

13 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regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date.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.

Why it matters. A framework that does not record its own breaches cannot demonstrate that it is being complied with. The nonconformity record forces the event to be separated from its cause, the effectiveness criterion to be set before it is verified, and closure to be carried out by someone other than whoever gave rise to it. The company register allows the AI Committee and the board committee to see what is open, what is overdue and what keeps recurring; without it, critical nonconformities can remain buried in emails and the framework audit (document 38) has nothing to sample.

01

Instructions for use

Aspect	Guidance
When it is used	From the moment a possible nonconformity is detected (37 §3.1): in a *gate* verification, an R6, an audit, a use case register alert, a control test, an incident or a report from anyone. The record remains open until closure and, for critical and major nonconformities, until the re-audit.
Who completes it	The AI Office records and keeps it. Whoever detects the nonconformity proposes the type; the action owner documents containment, root cause and actions.
Who verifies it	The AI Auditor confirms the type, verifies effectiveness and closes it. At Lite intensity, the AI Auditor may close minor nonconformities on the basis of the AI Office's documentary verification (37 §3.8).
Who decides or approves	The action plan is approved by the AI Committee (critical), the AI Risk Owner (major) or the AI Office (minor). Disagreements about the type are resolved by the AI Committee.
Stage, *gate* or moment	At any point in the use case lifecycle and the corporate cycle. It is reviewed at R6 (R6.15), at G7 (G7.04), in the C4 quarterly report and in the C5 annual review.
Tool	T08 · Nonconformity and incident register (T01 module), with statuses, time limits, overdue alerts and links. This template is its equivalent in document or spreadsheet format.
Reference document	Document 37 §3 (process), §6 (relationship with incidents) and §8–9 (indicators and reporting to the board); 01 §12.
Lite versus Enterprise	The process is the same. Lite may omit the fields marked **(Enterprise)**; the root cause for major and critical nonconformities and closure by the AI Auditor are never omitted.

Completion rules:

- Code **NC-AAAA-NNN**: year of detection and a sequential number that does not restart within the year. Codes are not reused.
- A nonconformity is a failure to meet a mandatory requirement ("must"). Unmet "should" requirements are recorded as observations, not as nonconformities.
- The root cause analysis is documented in P52; this record captures its conclusion.
- The effectiveness criterion is set when the plan is approved, not at verification (37 §3.7).
- A closed nonconformity that reappears due to the same cause within twelve months is **reopened**; it is not recorded as a new one.
- "No data" is not zero: if a date or an effect is unknown, write *No data*.

02

Identification

Field	Content	Guidance
Code		NC-AAAA-NNN.
Title		One line the AI Committee can understand.
Detection date		DD-MM-AAAA. The time limits in section 7 run from this date.
Detection source		*Gate* verification · R6 · Internal audit · External audit · Register alert · Control test · Incident · Unauthorised use of AI · Report from an employee, customer, supplier or supervisor.
Detected by		Role and name.
Recorded by		AI Office; date of recording.
Scope		Use case (IA-AAAA-NNN), system (SIA-AAAA-NNN), supplier, area or corporate process.
Intensity of the affected use case		Lite · Enterprise · Not applicable (corporate process).
Action owner		Named person, other than the auditor who will close it.

03

Requirement not met and description

Field	Content	Guidance
Requirement not met		Document, section and verbatim text of the requirement.
Criterion or control affected		*Gate* criterion (G*n.nn* of document 21), SEG or AG control of document 35, contractual clause or other.
Description of the finding		What has been observed, with objective evidence. Facts, not opinions.
Evidence		Reference to the documents, logs or screenshots preserved.

Field	Content	Guidance
Does it invalidate a *gate*?		Yes · No. If Yes, the use case returns to the status prior to that *gate* until it is corrected (37 §3.4).
Linked incident		INC-AAAA-NNN (P27), if any. The type of the nonconformity is determined by the requirement not met, not by the severity of the incident (37 §6).
Other links (Enterprise)		Risks (IA-AAAA-NNN · R*nn*), *gate* decisions (P29), board recommendations (REC-AAAA-NNN).

04

Type

Type	Criterion (any one suffices)	Tick
Critical	Exposes the company or people to immediate serious harm or to a serious legal infringement, or nullifies the framework's control over a system in production.	☐
Major	Affects the validity of a decision, the segregation of duties or a relevant control, without immediate serious harm.	☐
Minor	One-off breach with no impact on decisions or on relevant controls.	☐

Field	Content	Guidance
Justification of the type		Using the examples in 37 §3.3.
Rule applied		None · Recurrence (third minor nonconformity in twelve months becomes major; a major one recurring within twelve months becomes critical if it affects production) · Accumulation (same cause as another NC; single analysis) · Unauthorised use of AI (at least major if personal or confidential data are involved).
Related nonconformities		Codes of those sharing the cause or of previous ones in the event of recurrence.
Type proposed by		Whoever detects it.
Type confirmed by		AI Auditor; date.
Disagreement resolved by		AI Committee; date and reference of the minutes, if there was a disagreement.

05

Containment

Mandatory for critical and major nonconformities. Options from lowest to highest intensity: restriction of use or scope · additional temporary human validation · lowering of the autonomy level (A0–A3) · suspension of a capability with the kill switch · suspension of the system with a fallback process (P19) · withdrawal from production.

Date and time	Containment action	Decision-maker	Effect observed	Evidence
(illustrative example) **03-11-2026 16:00**	Suspension of the agent's refund capability with the kill switch	AI Sponsor	No automatic refunds since 16:05; manual process active	Kill switch and fallback process logs

06

Root cause and action plan

6.1 Root cause

Field	Content	Guidance
Method		Five whys · Ishikawa · Both (P52).
Immediate cause		What directly produced the event.
Root cause		Cause in the management system that can be acted upon. "Human error" is not a final root cause.
Does it meet the four validity conditions?		Explains all the facts · had it been eliminated the failure would not have occurred or would have been detected · is actionable · does not merely point at a person. Yes · No.
Does the same failure exist in other systems or use cases?		Systems reviewed and result.
Reference of the worksheet		P52, version and date.

6.2 Actions

Type: Correction · Corrective action · Preventive action. **Status:** Pending · In progress · Executed · Verified effective · Not effective.

No.	Type	Action	Owner	Time limit	Effectiveness criterion	Expected evidence	Status
A01							
A02							
***(illustrative example)* A01**	Corrective action	Add the relevant-change criterion to P24 and T03	AI Operations Owner	15-12-2026	No relevant change without a *gate* in the following three months	Sample of changes from P27	In progress

Field	Content	Guidance
Plan approved by		AI Committee (critical) · AI Risk Owner (major) · AI Office (minor).
Approval date		
Agreements with other areas		Head of the area with whom each action that depends on it has been agreed.

07

Time limits

Reference time limits from 37 §3.10, running from detection unless otherwise indicated. The company may adjust them in C2 without exceeding those set by the applicable regulation; record here those approved.

Step	Critical	Major	Minor	Deadline for this NC	Actual date	On time?
Recording	Same day	2 working days	5 working days			
Containment	Immediate, within 48 hours at most	Within 10 days at most	Not required			
Root cause and action plan	Within 10 days at most	Within 30 days at most	Before the next *gate* or review			

Step	Critical	Major	Minor	Deadline for this NC	Actual date	On time?
Execution of actions	As per plan; as a guide, 60 days	As per plan; as a guide, 90 days	Before the next *gate* or review			
Effectiveness verification	Within the time limit in the plan	Within the time limit in the plan	At the next *gate* or review			
Re-audit	Mandatory	Mandatory	By sampling			
Reports to	AI Committee and board committee	AI Committee	AI Office			

Any status other than Closed with a time limit exceeded generates the **Overdue** flag. An overdue minor nonconformity is escalated to the AI Committee; an overdue major one, to the board committee.

08

Effectiveness verification, closure and re-audit

Field	Content	Guidance
Period of operation observed		Next *gate* or R6, sample of operations or test of the control.
Result against the effectiveness criterion		Effective · Not effective. If not effective, the NC returns to **Under analysis**.
Evidence of the verification		
Closure checks		Containment carried out · root cause documented (major and critical) · actions executed · effectiveness verified with evidence · register updated.
Closure date		
Closed by		AI Auditor. Never whoever gave rise to the NC or the action owner.
Re-audit date (Enterprise)		As a guide, between three and six months after closure for critical and major nonconformities (37 §3.9).
Result of the re-audit		The correction is still operating · Reopened.

09

Status and history

Statuses: Open · Contained · Under analysis · Plan approved · In progress · Awaiting verification · Closed · Reopened. **Flag:** Overdue.

Date	Previous status	New status	Author	Reason
	Open			

10

Company register

Aggregated view kept by the AI Office. One row per nonconformity; sorted by type and age.

Code	Title	Scope	Type	Source	Detection	Action owner	Status	Next deadline	Overdue	Lir inc
NC-2026-014 ***(illustrative example)***	Relevant change in production without a *gate*	IA-2026-003	Major	Register alert	03-11-2026	AI Operations Owner	In progress	15-12-2026	No	—

Indicators for the period (37 §8):

Indicator	Value	Previous period	Remarks
Open nonconformities by type and age			
Overdue nonconformities by type			
First-time effectiveness (% closed without returning to analysis)			
Reopenings in twelve months			

Indicator	Value	Previous period	Remarks
Average time to closure by type (days)			
Nonconformities in incident management			Late report, evidence not preserved, post-incident analysis omitted.

11

Quality criteria

Formal criteria in document 21 (R6.06, R6.15 and G7.04) and process in document 37.

#	Check	Status
1	The requirement not met is a "must", is quoted verbatim and there is objective evidence.	Met · Not met · Not applicable · Pending
2	The type is justified with the criteria in 37 §3.3 and confirmed by the AI Auditor; the recurrence and accumulation rules have been applied.	
3	Critical and major nonconformities have containment recorded with date, decision-maker and effect.	
4	Critical and major nonconformities have a valid root cause (P52) and it has been checked whether the failure exists in other systems.	
5	Each action has an owner, a time limit, an effectiveness criterion set at approval and expected evidence.	
6	The plan is approved by the body that corresponds to the type.	
7	The time limits are met or the NC is flagged as Overdue and escalated.	
8	The AI Auditor closes it, with effectiveness verified; critical and major nonconformities have a scheduled re-audit.	

12

Approval and verification

Function	Role in SEVEN-G	Name and position	Date	Signature or reference
Records and keeps	AI Office			
Detects and proposes the type	Any role			
Executes the action	Action owner			
Confirms the type, verifies effectiveness and closes	AI Auditor			
Approves the plan	AI Committee · AI Risk Owner · AI Office, according to type			

Segregation of duties: whoever gave rise to the nonconformity does not verify its correction, and the action owner does not close it; only the AI Auditor closes it (37 §2, principle 5).

13

Version control

Completed document

Version	Date	Author	Changes

Template

Version	Date	Changes
0.1	19-09-2026	First version. Record and company register of NC-AAAA-NNN nonconformities with the full process of 37 §3 and the time limits of 37 §3.10.