TEMPLATE P27 · INCIDENT AND CHANGE LOG

Incident and change log

Records, with date and owner, every incident and every change to the AI system in production, how it was handled and its effect on risks, classification and evidence.

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

IN THIS DOCUMENT

01 Instructions for use

02 Identification

03 Incident log

04 Change log

05 Period indicators

06 Quality criteria

07 Approval and verification

08 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regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date.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	Throughout phase 6. It is opened at go-live and closed at retirement (P30).
Who completes it	AI Operations Owner (incidents and changes); the coordinator of each incident completes its record.
Who verifies it	AI Office at Lite intensity; AI Auditor at Enterprise intensity, by sampling and at each R6.
At which *gate* it is reviewed	R6 and G7. S1 and S2 incidents are also reviewed by the AI Committee.
Lite versus Enterprise	Lite may omit the fields marked **(Enterprise)**. No incident or relevant change may be left unrecorded.

Aspect	Guidance
Tool	T08 Nonconformity and incident register. If the company uses another incident or change tool, this log links its identifiers and adds the AI-specific fields.
Relationship	P16 Lineage · P19 Rollback · P24 Operations manual (types of change) · P25 Alerts · P26 Response plan · P12 Risk register · document 37.

Rules:

- **Every change is an event with a date, an author and a reason** (03 §2, principle 2).
- Incidents are coded **INC-AAAA-NNN** and nonconformities **NC-AAAA-NNN**; identifiers are not reused.
- Severity is classified using the criteria of document 37 and may be revised; both the initial and the final severity are kept.
- A relevant change executed without approval is a nonconformity (document 37).
- "No data" is not zero: if an impact is unknown, it is recorded as *No data*.

This template does not constitute legal advice.

02

Identification

Field	Content	Guidance
Use case code		IA-AAAA-NNN (T01).
AI system(s)		Identifier in the inventory (T02).
Intensity		Lite · Enterprise.
Period covered		From DD-MM-YYYY to DD-MM-YYYY.
Log owner		AI Operations Owner.
Document version		
Date of last update		DD-MM-YYYY.
Document status		Open · Closed on retirement.

03

Incident log

3.1 Summary

Type: Performance degradation · Erroneous output with impact · Discriminatory or biased output · Information leakage · Unauthorised action by an agent · Prompt injection or manipulation · Unavailability · Regulatory breach · Misuse of the system · Supplier incident. **Status:** Open · Contained · Resolved · Closed.

Code	Date and time of detection	Type	Initial / final severity	Brief description	Coordinator	Status	Closure date
INC-2026-007 ***(illustrative example)***	14-07-2026 10:42	Erroneous output with impact	S3 / S2	The assistant informed customers of a repealed return period	AI Operations Owner	Closed	02-08-2026

3.2 Incident record

One record per incident.

Field	Content	Guidance
Code		INC-AAAA-NNN.
Detected by		P25 alert (ID) · User · Affected person · Supplier · Audit · Other.
Estimated start date and time		May precede detection.
Affected system version		Model, instructions, knowledge base (P16).
Description		What happened, in plain language.
People and processes affected		Number and type; *No data* if unknown.
Initial and final severity, with justification		S1 · S2 · S3 · S4, using the criteria of document 37.
Containment actions and time		Kill switch, rollback, reduction of autonomy, etc.

Field	Content	Guidance
Time from detection to containment		In minutes or hours.
Reports checked		Result of the boxes in block 8 of P26: whether it applies, who reported, when and evidence, and P51 register.
Root cause		Technical, data, process, supplier or oversight (P52).
Corrective actions		What is changed, owner, date and verification. Changes are recorded in block 4.
Linked nonconformity		NC-AAAA-NNN (P50) if the incident reveals a breach of the framework.
Effect on the risk register		Risks reviewed in P12 and change in level.
Effect on classification or intensity (Enterprise)		Does it require P04 or P11 to be reviewed?
Economic impact		Amount with formula and status (validated · declared · estimated), or *No data*.
Human review of affected outputs		How affected decisions or actions were identified and corrected.
Lessons learned		What will be done differently; carried over to P30 and to C5.
Closed by		Role; in S1 and S2 the closure is verified by the AI Risk Owner.

04

Change log

4.1 Summary

Type: Minor · Relevant · Emergency (defined in P24). **Component:** Model · System instructions · Knowledge base · Training data · Agent tools or permissions · Autonomy level · Monitoring thresholds · Integration or infrastructure · Supplier · Population or purpose. **Status:** Requested · Approved · Executed · Rolled back · Rejected.

Change identifier	Date	Type	Component	Description	Approved by	Status	Related incident
(identifier from the change tool) (illustrative example)	20-07-2026	Relevant	Knowledge base	Replacement of the returns policy with the version in force and withdrawal of repealed documents	Technical owner with risk clearance	Executed	INC-2026-007

Changes use the identifier from the company's change management tool; this log does not create its own coding.

4.2 Record of a relevant or emergency change

Field	Content	Guidance
Identifier		From the change tool.
Reason		Improvement · Incident correction · Regulatory requirement · Change of supplier · Other.
Previous and new version		Updates P16.
Tests performed and result		Regression, bias, security, injection, depending on the component.
Applicable rollback plan		Reference to P19; has it been updated?
Does it change the autonomy level, the purpose or the population?		Yes · No. If Yes, it requires verification and a decision equivalent to G4/G5 and a new sign-off (P23).
Does it require reviewing the regulatory classification, intensity or risks?		Yes · No, with justification.
Updated evidence		Templates modified and new version.
Approval		Role, name and date, prior to execution except in an emergency.
Subsequent emergency recording		Date and time of recording and of the after-the-fact approval.

05

Period indicators

They are incorporated into the R6 continuity review.

Indicator	Value for the period	Previous period	Observations
Incidents by severity (S1 · S2 · S3 · S4)			
Median time from detection to containment (S1–S2)			
Incidents with regulatory reporting			
Incidents open at the end of the period			
Relevant changes executed			
Emergency changes			
Changes executed without prior approval (should be zero)			
Rollbacks executed			
Linked open nonconformities			

06

Quality criteria

Formal R6 and G7 criteria in document 21; process in document 37.

#	Check	Status (Met · Not met · Not applicable · Pending)
1	All incidents have a code, justified severity and status.	
2	S1 and S2 incidents have a complete record, root cause and reports checked.	
3	Relevant changes have tests, prior approval and an updated P16.	

#	Check	Status (Met · Not met · Not applicable · Pending)
4	Changes in autonomy, purpose or population have gone through verification and a decision equivalent to G4/G5.	
5	Detected breaches have an open nonconformity.	
6	The period indicators have been calculated for R6.	

07

Approval and verification

Function	Role	Name	Date	Signature or reference
Log owner	AI Operations Owner			
Verification of S1–S2 closures	AI Risk Owner			
Period verifier	AI Office (Lite) · AI Auditor (Enterprise)			
Review	R6 decision-maker (recorded in P29)			

Segregation of duties: the operations owner does not verify the evidence of their own operation (01 §8.1).

08

Version control

Version	Date	Changes
0.1	16-09-2026	First version of the template.