AI Change Accountability & Reauthorisation

A practitioner-derived method for tracing AI change from signal to decision, implementation and closure

Field-tested in one organisation, in facilitated mode, on a real AI change event.

Author: Maja Kurek, AIGP, CIPM, CIPP/E · RuleBridge Advisory

23 September 2026

One-page overview

From a visible signal to a completed governance outcome

AI systems do not remain fixed after approval. Models change. Providers retire or replace services. Hosting moves. Data sources, prompts and integrations evolve. Permissions expand. Human review is reduced or bypassed. Actual use can move away from the purpose that was approved.

A change can therefore invalidate the assumptions behind an earlier decision without automatically creating a new governance decision. This method gives an organisation one practical path from the first visible signal to an authorised decision, implemented action, evidenced closure and learning.

Central question

Which changes to an AI system, model, provider, platform, data basis, operating context, level of autonomy or human role should trigger renewed assessment, reauthorisation, restriction, suspension or exit - who has authority to decide, and how is implementation and closure evidenced?

Unit of analysis

One candidate AI change event or risk signal entering intake and materiality review. The event is not described as material before that review. The method does not assess the whole organisation, the whole AI lifecycle or a model in isolation.

Governance Outcome Trace

Signal → intake and classification → ownership → specialist inputs → actual decision authority → decision → changed practice, use, workflow or system → corrective-action ownership → evidence of completion → recurrence and organisational learning.

Three separate decisions

Decision layer	Question
Review route	How deeply must this event be reviewed?
Interim operating status	What is permitted while facts or formal approval remain open?
Final governance outcome	What does the actual authority decide should happen?

No review route or hard trigger predetermines the final outcome.

Core artefacts

Artefact	Purpose
Organisation Authority Map	A standing view of signal channels, ownership, specialist functions, formal and actual authorities, emergency authority, escalation, cumulation review and closure roles.
AI Change Event Sheet	A two-part record for one event, from signal and baseline to decision, action, closure and learning.
Event Register	A portfolio record across the six status axes, authority, review route, interim status, outcome, actions, evidence, recurrence and record version.
Closure & Learning Supplement	An optional record for events with multiple actions, complex evidence, affected-person remediation or extended recurrence review.
Boundary Record	A controlled record for a Pre-authorised Change Boundary and every event that invokes it.

Critical gate

Who can actually stop, restrict or reauthorise this use today - by name or decision forum?

How this guide is organised

Opening pages:

- One-page overview;
- How this guide is organised.

Main guide:

1. Why and when to use the method
2. Scope and boundaries
   - Proportionality note
3. The Governance Outcome Trace
4. Modes of use and Step 0
   - Readiness self-check
   - Quick Start - first event in ten steps
5. Intake, taxonomy and descriptors
6. Materiality and hard-escalation logic
7. Three-part decision architecture
8. Uncertainty, emergency change and legal escalation
9. Actual authority and specialist inputs
10. Decision, action, closure, reopen and learning
11. Evidence quality, transition ledger and six-axis status model
12. Using the toolkit
13. Synthetic examples - not field evidence
14. Assumptions, limitations, status, licence and citation

Reference material:

- Glossary and controlled vocabulary.

Appendices:

- Appendix A. Organisation Authority Map
- Appendix B. AI Change Event Sheet - Part 1
- Appendix C. AI Change Event Sheet - Part 2
- Appendix D. Closure & Learning Supplement
- Appendix E. Event Register field specification
- Appendix F. Boundary Record

1. Why and when to use the method

1.1 Why this method exists

AI systems do not create governance difficulty only at first deployment. They continue to change in ways that can alter capability, consequence, data use, dependency, human control and organisational responsibility.

A provider may replace a model. Engineering may move from an external API to self-hosting. A team may change a prompt, add a data source or connect the system to a new channel. A system that originally drafted advice may begin to make or execute decisions. Human review may become sampled rather than universal. A workflow may reach a new population, language, market or volume. Actual use may diverge from what the organisation approved. A supplier-side configuration may also diverge silently from the state the organisation believed it was operating.

Each of these changes can make the earlier decision unreliable. Yet many organisations have no single operational path for answering four linked questions:

1. What exactly changed against the approved or reconstructed baseline?
2. Does the earlier approval still apply, and what review is now required?
3. Who has the real authority to decide what happens while the review is open and what happens afterwards?
4. How will the organisation prove that the decision was implemented and know when the event is genuinely closed?

This method is designed for that gap between a visible signal and a confirmed governance outcome.

1.2 Intended users

The method is intended for people who own or govern AI-enabled products, services, workflows and dependencies, including:

- AI, product, system and workflow owners;
- business and process owners;
- COO, CTO, CIO, CDO and Head of AI offices;
- AI-governance, risk, compliance, privacy and transformation leads;
- decision forums with formal or actual authority;
- provider, platform and dependency relationship owners;
- qualified internal or external specialists contributing defined inputs.

It can be facilitated by RuleBridge Advisory or another facilitator, or run by the organisation itself. The facilitator never becomes the organisation's decision authority. The event owner runs the record and coordinates the work. Specialists join for identified questions; listing a specialist function in the Authority Map does not require that function to review every event.

1.3 Typical entry events

Use the method when one or more of the following becomes visible:

- a provider deprecation, update or change notice;
- a planned or completed model, prompt, hosting, platform or integration change;
- a new data source, data-use pattern, retention arrangement or processing location;
- a change in intended use or evidence that actual use has diverged;
- an increase in autonomy, permissions, tool access or transaction authority;
- a change to human review, intervention, override, workload, language capacity, domain capacity or escalation;
- a new population, language, geography, customer group, volume or operating context;

- a performance signal, incident, near miss, complaint or recurring exception;
- a contractual, regulatory or organisational change;
- evidence that the person or forum holding actual authority has changed;
- evidence that a provider did not give an expected change notice;
- several linked changes whose combined effect may invalidate the earlier baseline;
- a change whose prior approval cannot be identified, is contested or cannot be determined.

1.4 Entry criteria and parallel-response gate

Enter the method when…	**Do not use it as a substitute for…**
A planned or actual change, notice, incident, complaint, monitoring output or actual-use divergence becomes visible.	Detection tooling, technical monitoring, model evaluation, cybersecurity assessment, procurement due diligence or audit.
The organisation needs to decide whether an earlier approval still applies, whether a first authorisation is required, and who can decide what happens next.	A generic inventory exercise or whole-enterprise maturity assessment.
The event has enough organisational consequence to require a traceable decision, or a documented decision that no further route is needed.	A rule that every change is material or that every signal requires formal reauthorisation.
The organisation needs a record of implementation, closure evidence and future review.	A compliance certificate, risk score or assurance conclusion.

This method never delays or replaces any applicable incident, security, privacy, safety, employment, customer-remediation or regulatory response process. Record which parallel processes are activated, their owners and deadlines; this trace runs alongside them, never before them.

2. Scope and boundaries

In this method, reauthorisation means a renewed organisational decision by the relevant actual authority on whether, and under which conditions, an AI use, system, workflow or dependency may continue. It is not a regulatory approval, a legal qualification, a certification, or a technical revalidation.

2.1 What the method does

The method:

- structures one candidate event, its baseline status, verified delta and operating context;
- distinguishes a signal, verified change, incident, risk interpretation and governance trigger;
- applies a multi-label change-event taxonomy and cross-cutting descriptors;
- guides an organisation-side materiality review without producing a numerical risk score;
- identifies specialist questions and records how qualified inputs informed the decision;
- tests whether formal governance is matched by actual authority;
- separates review route, interim operating status and final governance outcome;
- records options, rationale, conditions, uncertainty, dissent and temporary measures;
- assigns corrective actions, owners, dependencies, dates and verifiers;
- requires closure criteria at decision time and evidence of implementation;
- creates a recurrence, reopen and organisational-learning loop.

2.2 What the method does not do

The method does not:

- provide legal advice or determine substantial modification, provider/deployer status, legal compliance or legal sufficiency;
- audit, assure, certify or conclude that controls are effective;
- perform technical model evaluation, bias testing, red teaming, performance validation or cybersecurity assessment;
- act as MLOps, model monitoring or deprecation-detection software;
- execute systems integration, migration, hosting, rollback or technical cutover;
- replace third-party risk management, procurement or vendor scoring;
- replace an enterprise operational-resilience programme;
- produce a maturity score, risk score, compliance score or regulator-approved result;
- replace qualified legal, technical, security, privacy, human-factors, sectoral or other specialist expertise.

The method may analyse the organisational materiality of provider, platform, model and dependency changes. It does not perform supplier due diligence or technical assessment.

2.3 Role-aware, not deployer-only

The method can be used when an organisation acts as a provider, deployer, product manufacturer, or in more than one role, however the organisation's roles are described under applicable law. Legal role is an input field and a possible legal-escalation question. It is not a conclusion of this method.

2.4 What a completed trace can establish

A completed trace can show:

- what entered the process;
- the baseline status and what was verified against the earlier baseline;
- who owned the system, affected consequence and event trace;

- which specialist inputs were sought and used;
- who held formal authority and actual decision authority;
- what was decided and under what conditions;
- what changed in practice or in the system;
- what evidence supported each named closure type;
- what was learned and what should reopen the event.

It does not establish that the decision was legally or technically correct, that risk was reduced, or that the system is safe, fair, effective or compliant.

Proportionality note

A smaller organisation may combine roles where the combination is explicit, workable and subject to proportionate challenge. It may, for example, combine system owner and event owner, or consequence owner and register-and-learning owner, where the scope is limited and the authority remains clear.

The following combinations are not permitted:

- actual authority and facilitator;
- a person confirming their own succession to actual authority;
- closure verifier and action owner, unless a documented exception records why no practical alternative exists, who authorised the exception and what compensating check applies.

Role compression does not remove the need to name the distinct responsibilities. A person may hold more than one role, but the record must show which role they were exercising at each decision point.

Documentation is also proportionate. Section 10.4 is the single rule for the records and closure required by each route. R0 uses the short R0 record in the editable templates. It may reference the current Authority Map, standing review cadence and source records rather than reproduce them. A conditional module is opened only when its stated condition applies. A blank required field is not the same as a reasoned finding that a module is not applicable.

3. The Governance Outcome Trace

All ten elements are required, subject to the element statuses in §3.1. An element that is missing without a recorded status is a governance finding, not permission to fill the gap by assumption.

No.	Trace element	Required question	Minimum evidence
1	Candidate change event or risk signal	What became visible, through which channel, and when?	Notice, request, monitoring output, incident record, complaint or planned-change record.
2	Intake and classification	How did the event enter, and how was it distinguished from a duplicate, incident or unverified signal?	Event ID, intake record, taxonomy classes, descriptors and linked-event decision.
3	Ownership	Who owns the system or workflow, business consequence and event trace?	Named system owner, consequence owner and event owner, with evidenced mandates or recorded limitations.
4	Specialist inputs	Which questions require qualified legal, technical, privacy, cyber, human-factors, sectoral or other input?	Defined questions, named input owners, qualification assessment, conclusions, limitations, status and date.
5	Actual decision authority	Who can actually continue, condition, restrict, pause, suspend, transition or exit?	Formal authority, actual authority, evidence of real authority and any succession or vacancy record.
6	Decision	Which options were considered, what was decided and why?	Route, interim status, outcome, rationale, conditions, constrained-option record, uncertainty and dissent.
7	Changed practice, use, workflow or system	What changed after the decision?	Implemented artefact, configuration, operating instruction or observed practice.
8	Corrective-action ownership	Who completes each action, by when, and with which dependencies?	Action plan, one accountable owner per action, dependencies, due date and verifier.
9	Evidence of completion	How is implementation and satisfaction of the closure criteria demonstrated?	Direct or corroborated evidence, evidence limitation, closure type and verifier.
10	Recurrence and organisational learning	Did the event recur, and what standing process, Authority Map, threshold or Boundary Record changed?	Event-specific review, learning note, linked event, process update or reopen transition record.

3.1 Trace-element status

Record all ten element statuses in field C16, including in the R0 short record. A reference to an existing record is sufficient; the content need not be copied. Each element carries one controlled status: **completed**, **pending**, **not required with rationale**, **unavailable**, **contested**, or **not within this trace**.

The following are invariants and cannot be marked **not required with rationale**:

- actual decision authority for any event that reaches a governance decision;
- an interim operating status while review remains open;
- closure evidence for any record whose workflow_phase is **Closed**.

A record_disposition of **cancelled** requires a named owner, a rationale and confirmation by a second person. Cancellation does not erase the signal or its route history.

3.2 Three governing rules

1. **Closure means confirmed closure.** An event is not closed because a message was sent, a ticket was marked complete or a policy was edited.
2. **A missing element is a result.** If the organisation cannot identify actual authority, specialist ownership or closure evidence, that gap is recorded rather than concealed.
3. **Simulated and reconstructed evidence remain visible.** Tabletop use never becomes field evidence. Retrospective reconstruction is never described as contemporaneous.

4. Modes of use and Step 0

4.1 Five modes of use

Mode	Use	Evidence interpretation and readiness
Prospective live trace	The event is followed from signal through decision, implementation and closure.	Can create contemporaneous organisational evidence. Completion of a real application does not by itself validate the method.
Hybrid reconstruction plus prospective follow-up	Earlier stages are reconstructed while decision, action or closure are followed live.	Reconstructed elements remain labelled; prospective elements can be contemporaneous.
Retrospective reconstruction	A completed or partly completed event is traced after the fact.	Useful for diagnosis and method improvement; never described as contemporaneous field evidence.
Simulation / tabletop	A fictional or hypothetical event tests roles, thresholds and usability.	Learning use only. Set mode to **Simulation / tabletop**; no field claim.
Standing embedded process	The organisation maintains the Authority Map, Event Sheet and Register over multiple real events.	Portfolio evidence becomes meaningful only through actual events and traceable decisions.

Mode-readiness control. The field test was conducted in facilitated mode. Before organisation-run use is represented as operational, complete the Readiness self-check.

A single completed and documented application changes only the factual record of use; it does not, by itself, establish that the method is effective or transferable.

4.2 Two operating formats

Facilitated

An external facilitator structures the process, tests clarity, supports consistent application and makes interventions and deviations visible. The organisation retains every substantive decision.

A facilitator must:

- demonstrate competence in the method and in evidence discipline;
- disclose financial, professional, personal or outcome-related conflicts;
- never become the organisation's formal authority, actual authority or closure authority;
- document substantive prompts, interpretations, interventions, adaptations and method deviations;
- escalate when the organisation cannot identify valid authority, when a critical gate rests only on A evidence, or when self-use no longer preserves the method's minimum disciplines;
- distinguish facilitation from specialist legal, technical, security, privacy, human-factors or sectoral advice.

The label **independent facilitator** may be used only where the facilitator has no financial or outcome interest in the organisational decision being made. Payment for facilitation alone does not establish independence; any other relevant interest must be disclosed and assessed.

Organisation-run

The organisation uses the guide and templates without an external facilitator. The same evidence, authority and record-integrity rules apply. The named process owner is responsible for readiness, fidelity, escalation and the separation of operational ownership from any internal assurance or challenge role.

4.3 Step 0 - Organisation Authority Map

Start with one named operating scope. Complete the parts of Appendix A needed to receive the signal, assign an event owner, confirm the route, identify actual authority and a substitute, set permitted operation, and retain the record. Reference existing mandates and response procedures. Do not postpone intake or protective action while an organisation-wide map is being assembled.

Before an event reaches a decision or closure, the authority and evidence needed for that step must be confirmed. Record gaps as holds with owners and deadlines. Extend the map to other scopes when they enter the process; review it when roles, forums, systems, providers or emergency arrangements change.

The map should identify:

- signal channels and signal recipients;
- classification and triage owner;
- system, product and business owners;
- consequence owner and event owner;
- specialist-input functions and escalation contacts;
- formal authorities and actual authorities for **Continue**, **Continue with conditions**, **Restrict**, **Pause**, **Suspend**, **Transition** and **Exit**;
- routing authority;
- emergency authority, substitute authority and fail-safe containment role;
- implementation owner and closure verifier;
- escalation forum;
- register-and-learning owner;
- cumulation review cadence and aggregation review responsibility;
- authority-succession route and substitutes by decision type;
- last review date and next review date.

A move to self-hosting or open-source components requires a documented redesign of signal channels. The map must identify who receives maintainer notices, lineage changes, security advisories, dependency changes, patch information and internal configuration signals when there is no external provider notice.

Three diagnostic questions

1. Who can actually stop this system or use today - by name or decision forum?

2. Who believes they can stop it, but in practice cannot allocate resources or compel action?

3. Whose approval has been assumed, but was never actually given?

A committee name, RACI entry or job title is not enough if the person or forum lacks authority for the specific system, workflow, population, geography or consequence.

Readiness self-check

For the selected scope, answer **yes** or record a gap, remediation owner and date in A4. Intake and urgent protection may proceed; an unresolved prerequisite blocks only the step that depends on it.

1. Is a named process owner responsible for operating the method?

2. Is the Organisation Authority Map current for the intended operating scope?

3. Can the organisation identify formal authority and actual authority separately?

4. Is a routing authority or escalation forum named for disputed routes?
5. Are qualified legal, technical, privacy, security, human-factors and sectoral inputs accessible where relevant?
6. Is a system of record selected, with append-only transition history or a demonstrated functional equivalent?
7. Are evidence references, access limits and record ownership defined without unnecessary copying of sensitive material?
8. Is the Record Ownership & Data Schedule (G) complete before case information is shared in a facilitated use?
9. Are emergency authority, fail-safe containment and ratification rules documented?
10. Is the cumulation review cadence defined, including ownership of R0 aggregation review?

Organisation-run readiness. Organisation-run use remains untested until the organisation documents the prerequisites above and demonstrates operation of the method without facilitator substitution for ownership, authority or evidence discipline.

Quick Start - first event in ten steps

Step	What to do	Working record
1	Open an Event ID, record the signal and activate any parallel response immediately.	B1, B2, B9
2	Name the operating scope, legal entity, event owner and relevant authority.	A1-A3; B1; C2
3	Record the baseline status and evidence. Actual use reconstructed later is not an approval.	B3; B10
4	Verify the proposed or observed delta and label the timing and evidence.	B4; B5; B10
5	Screen all materiality lenses and hard triggers; document the touched lenses and any boundary invocation.	B6; B7; F
6	Propose and confirm the minimum route using §6.4.4.	B7; C12
7	Record permitted operation while review is open, including expiry and lapse consequences where temporary.	C3; C7

Step	What to do	Working record
8	Obtain required specialist inputs and record the authorised outcome, rationale and closure criteria.	B8; C2; C4; C5; C8
9	Assign actions and preserve implementation evidence.	C6; B10; workbook Actions
10	Apply the route-specific closure rule, record ten trace statuses and arrange learning or reopening.	C8-C13; C16; workbook Events and History

For R0, use the short record instead of duplicating Parts 1 and 2. Its fields map to the same identifiers. The editable templates contain a Record Ownership & Data Schedule (G) and an External Handoff Record (H) for applicable cases. The worked examples show an R3 case and an R0 case in these records.

5. Intake, taxonomy and descriptors

5.1 The five distinctions at intake

Term	Meaning
Signal	Information suggesting that something may have changed or that risk may require attention.
Verified change	A confirmed difference from the approved or reconstructed baseline. A delta is verified only under the rule in the glossary and this section.
Incident	An event that caused or could have caused harm, failure, disruption or loss.
Risk interpretation	A qualified or organisational conclusion about consequence, uncertainty or control relevance.
Governance trigger	The reason a defined review route or decision must now occur.

A provider notice is not automatically a material change. A complaint can enter intake before the underlying cause is known. An unannounced actual-use or supplier-side divergence can become a governance trigger once verified.

A delta is verified when the event owner or triage owner confirms the specific proposition with evidence of quality D Direct and contemporaneous or C Corroborated; on A Asserted or R Reconstructed alone it remains a candidate signal. For a planned change, this verifies what is proposed, not that it is operating. Deployment or changed practice requires its own later evidence. Record source date, observation date and effective date separately where they differ.

5.2 Establish the baseline before judging the delta

Select and record one baseline status:

- **approved**;
- **conditionally approved**;
- **reconstructed from an evidenced approval**;
- **no prior approval identified**;
- **approval contested**;
- **unable to determine**.

Reconstructed actual use is not an approval.

The baseline should cover, as relevant:

- approved purpose and actual operating use;
- model, provider, platform, hosting and key dependencies;
- data basis and relevant processing assumptions;
- affected people, language, market, geography and scale;
- autonomy, permissions and action boundaries;
- human role, review arrangement, competence, intervention and override;
- prior conditions, monitoring thresholds and review dates;
- formal authority, actual authority and decision forum;
- relevant legal, contractual or specialist assumptions.

Where the baseline, the prior approval or the prior authority rests only on R, A or U evidence at a critical point, R0 and unconditioned continuation are not available. The event proceeds with a time-bounded interim operating status and a new, explicit authorisation of the current state by the actual authority.

5.2.1 No prior approval identified

Where the baseline status is **no prior approval identified**, the organisation must not use reconstruction to manufacture legitimacy. The event proceeds to one of two branches:

1. **first authorisation** - the relevant actual authority considers whether and under which conditions the use may begin or continue for the first time; or
2. **containment decision** - the relevant actual authority decides what minimum restrictions, pause, suspension or other containment are required while first authorisation is prepared.

Both branches require an actual authority, an explicit interim operating status and the necessary specialist inputs. They are not reauthorisation because no demonstrated prior organisational authorisation exists.

Where baseline status is **approval contested** or **unable to determine**, record the competing accounts or evidence limits, set an interim operating status and route the question to actual authority.

5.3 Multi-label change-event taxonomy

Apply every class that meaningfully describes the verified event or signal. One label must not conceal the event's cross-functional or cross-boundary character.

Code	Change class	Typical examples	Evidence to seek
C1	Model, version or capability change	Model swap, update, fine-tuning, safety setting, tool use, context or modality change, model routing.	Provider notice, release note, model card, change request, evaluation summary; for self-hosted components, commit, lineage, maintainer, dependency or internal release record.
C2	Provider, platform, hosting or service change	New provider, replaced provider, self-hosting, cloud move, new subprocessor, service-boundary or SLA change.	Contract or notice, dependency map, architecture record, provider communication; for self-hosted components, deployment, lineage, maintainer, infrastructure or service-ownership record.
C3	Data-basis change	New RAG source, training or reference data, provenance, retention, sensitivity, synthetic data or processing location.	Data-flow update, source inventory, data-owner record, privacy or security input.
C4	Intended-use or actual-use change	New purpose, task or scenario; actual use departing from approval; outputs treated as decisions rather than advice.	Use-case record, usage data, workflow observation, support or incident signal.
C5	Affected population, volume or geography change	New or more sensitive group, new market, expansion to a new language, larger scale, materially higher volume.	Rollout plan, statistics, geography and language list, impact or domain input.

Code	Change class	Typical examples	Evidence to seek
C6	Autonomy, permissions or transaction-boundary change	New tool access, delegated action, automated execution, financial authority, external communication or reduced confirmation.	Permission map, access record, action limits, configuration or workflow record.
C7	Human-role, review-capacity or intervention change	Reviewer role, competence, staffing, workload, reviewer language or domain capacity, override, stop authority, escalation or appeal change.	Role description, workflow map, capacity data, competence or training record, language/domain coverage, escalation, appeal or redress record.
C8	Integration-channel or external-system change	API, connector, assistant, upstream or downstream system, partner channel, identity or orchestration change.	Architecture or data-flow update, interface specification, access or integration record.
C9	Performance, incident or provider signal	Drift, quality drop, complaint, near miss, threshold breach, failure, provider alert or recurring exception.	Monitoring alert, incident record, complaint trend, QA summary, provider notice.
C10	Regulatory, contractual or organisational-context change	New requirement, contract, customer condition, reorganisation, risk appetite, legal-role question, provider notification failure or governance-forum change.	Confirmed specialist input, contract summary, organisational record or decision mandate.

5.4 Cross-cutting descriptors

Dimension	Descriptors
Reality	actual / planned / simulated
Timing	prospective / retrospective / hybrid
Reversibility	reversible / partly reversible / difficult to reverse
Observability	observable / partly observable / weakly observable
Boundary	contained / cross-functional / cross-organisational
Relationship	single / cumulative / coupled
Operating condition	routine / exception / emergency / externally forced
Knowledge	known / uncertain / contested

Use **externally forced** where the feasible choice set or decision deadline is materially constrained by an external event, such as a provider sunset, market withdrawal, insolvency, contractual deadline, infrastructure

withdrawal or multi-tenant change. The descriptor does not remove the need to record actual options and constraints.

5.5 Actual-use and supplier-side override

Where actual practice differs from formally documented intended use, actual use takes precedence for materiality review. Actual use governs the factual risk and consequence assessment; the intended purpose, the approved scope and reasonably foreseeable misuse remain separately recorded and separately assessed. The divergence itself is recorded as a change and governance trigger.

The same rule applies where the supplied or self-hosted system, model, configuration, routing or integration differs from the state the organisation believed it had approved. A supplier-side or maintainer-side divergence is recorded even when user behaviour did not change.

5.6 Linked and cumulative events

Link related event IDs. A cumulative review is required when the combined effect of linked changes may alter the approved baseline, consequence, actual use, autonomy, human capacity, dependency, observability, reversibility or authority.

The register-and-learning owner is the aggregation owner. The organisation must:

- set and record a cadence for reviewing the Event Register for linked, repeated and cumulative effects;
- define an organisation-specific aggregation prompt or threshold for reviewing accumulated R0 events, without adopting a universal number;
- record the review window used;
- create a parent event where bundling is necessary to represent the combined decision basis without erasing the child-event history;
- record why events were bundled or kept separate.

There is no universal numerical threshold. Two coupled changes may be more material than several routine changes.

5.7 Unauthorised or unassessed operation period

Where a silent or retrospectively discovered change operated before review, record:

- the earliest supported start date and latest possible start date;
- the end date or current open status;
- the operating scope, population, outputs and decisions potentially affected;
- the evidence-quality limits on the period;
- whether outputs or decisions produced during the period require lookback review;
- the owner, scope and result of any lookback;
- any affected-person notification, correction, appeal or remediation question;
- the continuing interim operating status.

A failure by a provider, supplier or maintainer to give an expected change notification opens its own linked C10 event. The linked event records the notice obligation or expectation, what was missed, who owns the relationship and what standing change-notification arrangement must be corrected.

5.8 Experiments and parallel variants

A planned experiment or A/B variant is recorded against an **experiment boundary** that states:

- allocation logic;
- duration;
- exposed population, workflow or transaction scope;

- permitted data and permissions;
- success, stop and harm thresholds;
- monitoring and evidence sources;
- owner and actual authority;
- the decision point at experiment end.

Continue temporarily with conditions is the standard interim framework for an active experiment unless a stricter interim status is required. At the decision point, the actual authority records O0 **Continue** for the selected continuing arrangement or O5 **Transition** where the operating arrangement changes. Other outcomes remain available where the evidence requires them.

A standing experimental programme may be governed through a Pre-authorised Change Boundary only where the Boundary Record defines the permitted classes and magnitude of experimental change, exposure limits, excluded hard triggers, evidence requirements and expiry or review date.

6. Materiality and hard-escalation logic

6.1 Principle

Materiality is not the size of the technical change. It is whether the event changes the basis on which the organisation previously decided that the use, system, workflow or dependency was acceptable and governable.

Throughout this method, 'material' and 'materially' carry the meaning defined here: whether the change affects the basis on which the organisation previously decided that the use was acceptable and governable.

The method uses structured judgement, not a weighted score.

For every materiality lens touched by the event, record:

1. the approved or reconstructed baseline and its baseline status;
2. the verified delta;
3. evidence and its D/C/R/A/U quality (see §11.1);
4. uncertainty or disagreement;
5. the specialist input required;
6. whether the previous approval remains applicable and why;
7. any dissent that should remain visible.

6.2 Twelve materiality lenses

Code	Materiality lens	Questions to ask
M1	Functional capability and behaviour	Can the system do something different, behave differently, route differently or produce materially different outputs?
M2	Intended use, actual use and operating context	Has the purpose, actual task, workflow position, market, channel or operating reality changed?
M3	Consequence and action	Does the system now influence or execute decisions involving money, access, rights, safety, communications or other material consequences?
M4	Affected people, scale and geography	Are more people, different groups, a more sensitive population, a new jurisdiction, a new language or materially higher volume affected?
M5	Data, privacy and security	Has data provenance, sensitivity, processing location, access, retention, purpose, quality or security exposure changed?
M6	Autonomy, permissions and transaction boundary	Has the system gained new access, delegated authority, tool use, external-action capability or reduced human confirmation?

Code	Materiality lens	Questions to ask
M7	Human oversight, intervention and capacity	Can people still understand, challenge, disregard, override, reverse, stop and escalate in practice, with suitable competence and training, under real workload and time constraints?
M8	Provider, dependency and cross-boundary impact	Has a model, provider, platform, integration, subprocessor or external actor changed the organisation's visibility, influence, contractual leverage or continuity?
M9	Reversibility, substitution and exit	How quickly and reliably can the change be stopped, rolled back, substituted or exited, and at what operational cost?
M10	Observability and evidence availability	Can the organisation see the change, behaviour, outcome and implementation well enough to decide and verify closure?
M11	Regulatory, contractual, role and specialist uncertainty	Could the event change a legal role, obligation, contract, customer condition or specialist conclusion? The method records the question; qualified specialists provide the conclusion.
M12	Cumulative, coupled and recurring effect	Do linked changes, repeat incidents, complaints or recurring exceptions invalidate the earlier baseline or prior closure?

6.3 Hard-escalation triggers

A hard trigger prevents an event from being routed as routine documentation without explicit consideration. A hard trigger affects the minimum review route, not the final outcome.

The hard triggers are:

1. change of intended use or verified material divergence in actual use;
2. a new or materially wider consequential decision or action function;
3. increased autonomy, permissions, tool access or financial/external transaction authority;
4. a new, materially larger or more sensitive population, scale or geography;
5. weakening of human review, intervention, override, stop authority, capacity or appeal route;
6. provider, model, platform, hosting or integration change with behavioural, data, continuity or control implications;
7. material change to provider terms, retention, service boundary, subprocessing or change-notification arrangements;
8. new or changed data basis with material privacy, security, provenance, quality or access implications;
9. incident, near miss, recurring complaint, threshold breach or recurring exception with a reasonably possible serious consequence;
10. inability to monitor, evidence, reverse or roll back the change with sufficient reliability;
11. a credible legal, contractual or role-change question requiring qualified input;

12. unresolved specialist disagreement that is material to the decision;
13. linked or cumulative changes that make the earlier baseline unreliable;
14. emergency change;
15. change of the person or forum that actually holds decision authority.

For trigger 9, **reasonably possible** means supported by a credible causal pathway, relevant evidence or a recurring pattern. It excludes a purely remote or abstract worst case, but it does not require the consequence to be more likely than not.

6.4 How hard triggers affect routing

6.4.1 Pre-authorised Change Boundary

Every hard trigger normally requires at least R2 **Specialist reassessment** unless the event is demonstrably within a valid Pre-authorised Change Boundary.

A Boundary Record must contain:

- operating scope;
- permitted change classes and permitted magnitude of delta;
- excluded hard triggers;
- actual authority that established the boundary;
- evidence basis and assumptions;
- expiry or review date;
- owner;
- record version;
- reference ID.

The following triggers are non-delegable and may never be placed within a Pre-authorised Change Boundary:

- change of intended use or material divergence in actual use;
- new or materially wider transaction authority;
- material weakening of human oversight;
- change of the person or forum that actually holds decision authority.

Appendix F provides the Boundary Record. Every invocation is recorded on the Event Sheet as **Exemption invoked: yes/no**, with the Boundary Record ID, evidence that the event is within scope and the person who confirmed applicability. An invocation is not a method deviation; it is part of the method's controlled routing logic.

6.4.2 Route proposal, confirmation and history

The event owner or triage owner proposes the minimum review route. The actual authority or a pre-named routing authority confirms it. A disputed route goes to the escalation forum.

The route must be raised when new facts, crossed thresholds, specialist disagreement or consequences indicate a higher route. A route may be lowered after new facts only where the current method logic no longer indicates the higher route. That change is a recorded **re-route**, not a method deviation.

The append-only route history records:

- date and time;
- route proposed or changed from and to;
- proposer;
- confirmer;
- reason;
- evidence or new fact;

- any dissent or limitation.

The route record may also carry component flags for legal, technical, privacy, security, human-factors, cross-boundary, emergency and affected-person work. Component flags supplement but never replace the minimum review route.

6.4.3 Route floor and deviation

Changes to intended or actual use, consequential action, autonomy or transaction authority, material human-oversight arrangements, or actual authority itself normally require R3 **Formal reauthorisation**.

A hard trigger never requires a predetermined final outcome such as O5 **Transition** or O6 **Exit**. The actual authority decides the outcome after the necessary inputs are available.

A lower route than the one indicated by this logic must be recorded as a method deviation, with the authority, reason, evidence, limitations, temporary measures, expiry and reopen trigger. A method deviation cannot waive legal escalation, actual-authority confirmation, evidence labelling, emergency retrospective review or closure evidence.

6.4.4 One routing rule

Apply this table from top to bottom and record the highest applicable route. Record each trigger before considering an exemption. A valid boundary changes the route required for an in-scope trigger; it does not delete the trigger. Section 6.4.3 governs any declared method deviation.

Condition	Minimum review	Who confirms	Boundary or exception
No evidenced approval, contested approval, or critical baseline or authority evidence limited to R, A or U	R3 for first authorisation or a renewed decision on the current state; protective action may occur first	Valid actual authority; route may be confirmed by the named routing authority	R0 and unconditional continuation unavailable; no retrospective invention of approval
Intended or material actual-use change, wider consequential action, increased autonomy or transaction authority, material oversight change, or actual-authority change	Normally R3	Actual authority or named routing authority; succession confirmed by appointing or superior authority	The non-delegable exclusions in §6.4.1 cannot be put within a boundary
Any other hard trigger, including a credible legal question, material specialist disagreement or emergency	At least R2; raise to R3 where the preceding row applies	Actual authority or named routing authority	A boundary cannot waive legal escalation, unresolved material disagreement or emergency review
A delegable trigger demonstrably within a current boundary	Route specified by that boundary, subject to current facts; R0 only when the earlier decision basis remains applicable	Person expressly authorised to confirm applicability, within the recorded delegation	Boundary ID, trigger number, permitted class and magnitude, evidence, exclusions, date and confirmer required

Condition	Minimum review	Who confirms	Boundary or exception
No trigger and no new specialist question, but observation is needed before closure	R1	Actual authority or named routing authority	Define question, owner, threshold, source and review date
Verified delta leaves the earlier decision basis applicable, and no unresolved issue requires monitoring or specialist review	R0	Actual authority or an expressly authorised delegate	No interim change required; final O0 only; §10.4 short record applies

If a boundary expires or the change exceeds it, stop using its exemption and apply the normal rule. Keep the earlier applicability decision in the history and record the new fact, route and operating status.

7. Three-part decision architecture

The method separates three questions that are often confused.

7.1 A. Review route - how deeply the event must be reviewed

Code	Review route	Meaning	Minimum record
R0	Documentation only	The verified delta does not alter the basis of the earlier decision. R0 and O0 confirm that the earlier decision basis remains applicable. They do not discharge separate documentation, transparency, contractual, notification or record-keeping obligations; where such obligations may apply, they are checked through legal triage in §8.3 and the parallel-response record.	Delta, rationale, owner, route confirmation and date.
R1	Enhanced monitoring	Additional observation is required before closure or a later decision point; the interim operating status is recorded separately.	Monitoring question or metric, owner, threshold, evidence source, route confirmation and review date.
R2	Specialist reassessment	New qualified legal, technical, privacy, cyber, human-factors, sectoral or other input is required.	Questions, specialist owner, qualification assessment, status, conclusion, limitations and use in decision.
R3	Formal reauthorisation	The earlier authority is no longer sufficient or the event requires a renewed formal decision.	Formal and actual authority, options, rationale, conditions, closure criteria and review date.

The review route can be raised at any point when new facts, disagreement or consequences become visible.

7.1.1 Recommended practice - route × interim compatibility rules

Review route	Normally compatible interim operating status	Guard rule
R0	**No interim change required** only	R0 ends only with O0 **Continue**. Any need for a protective change requires a route review. R0 is also unavailable where the critical-evidence rule in §5.2 applies.
R1	**No interim change required**; **Continue temporarily**; **Continue temporarily with conditions**	**Restrict**, **Pause** or **Suspend** may be imposed only as an immediate protective measure while the route is raised or re-confirmed. They are not a stable R1 endpoint.

Review route	Normally compatible interim operating status	Guard rule
R2	Any of the six interim operating statuses	The selected status must match the unresolved specialist question, current evidence and authority.
R3	Any of the six interim operating statuses	The selected status must preserve control while a renewed formal decision is prepared.

Additional outcome guards:

- R0 ends exclusively with O0 **Continue**.
- R1 ends at the review date with O0 **Continue**, O1 **Continue with conditions**, or a raised route. It does not remain open by silent extension.
- R2 and R3 may end with O0-O6.
- O5 **Transition** and O6 **Exit** open a linked candidate event for the incoming or replacement arrangement where one exists.
- workflow_phase becomes **Closed** only when the applicable closure floor in §10.4 is met.

7.2 B. Interim operating status - what is permitted while review remains open

An open review must not leave the status of use implicit. The actual authority, or an expressly authorised delegate acting within a recorded mandate, records one of the following:

- **No interim change required** - the existing approved baseline continues while routine documentation or monitoring is completed.
- **Continue temporarily** - temporary continuation is explicitly authorised while defined facts are obtained.
- **Continue temporarily with conditions** - temporary continuation is limited by time, scope, human confirmation, monitoring or another protective condition.
- **Restrict** - scope, population, data, functionality, permissions or action is narrowed during review.
- **Pause** - rollout or use waits for evidence or a defined decision condition.
- **Suspend** - use stops until a new decision authorises return.

Before actual authority is confirmed, the triage owner may impose **Restrict**, **Pause** or **Suspend** as a temporary protective interim status where delay would materially increase exposure. The record must state that the status is pending ratification. The relevant actual authority must ratify, replace or end it within the period defined in the Authority Map.

For **No interim change required**, reference the applicable approval, name the confirmer and set the next documentation or monitoring checkpoint; no temporary permission is created. For R0 that checkpoint may be the recorded closure date. All temporary, restrictive, paused or suspended arrangements require:

- named authority or triage owner;
- reason;
- expiry or review date;
- owner of missing facts;
- consequence if the expiry or review date passes;
- trigger for escalation or reopen;
- ratification status where imposed before authority confirmation.

A lapsed interim expiry never becomes silent continuation; it escalates to the actual authority as an open governance finding.

7.3 C. Final governance outcome - what the actual authority decides

Code	Governance outcome	Meaning
O0	Continue	Use continues without changed conditions.
O1	Continue with conditions	Use continues subject to defined restrictions, evidence requirements, thresholds or time limits.
O2	Restrict	Scope, population, data, permissions, functionality or action is narrowed.
O3	Pause	Use or rollout waits for evidence, remediation or a decision condition.
O4	Suspend	Use is stopped until a new decision authorises return.
O5	Transition	The organisation changes model, provider, platform, workflow or operating arrangement.
O6	Exit	The use or dependency is decommissioned or terminated.

Enhanced monitoring, additional evidence and temporary human review can be conditions attached to any relevant outcome. They are not automatically final outcomes in their own right.

Reopen is governed as a transition action in §10.5. It does not appear in the outcome field.

An O5 **Transition** or O6 **Exit** decision opens a linked candidate event for any incoming provider, model, platform, workflow or replacement arrangement. The outgoing event does not confer approval on the incoming arrangement.

7.4 Decision example

A provider change may produce:

- Review route: R3 **Formal reauthorisation**;
- Interim operating status: **Continue temporarily with conditions**;
- Interim conditions: universal human review, defined scope and expiry date;
- Final governance outcome: O5 **Transition**;
- Final conditions: quality threshold, cutover criteria, rollback readiness and 30-day stabilisation review.

This is clearer than treating monitoring, reauthorisation, restriction and transition as points on one severity ladder.

8. Uncertainty, emergency change and legal escalation

8.1 Uncertainty rule

Missing evidence is not neutral, but it does not create an automatic numerical escalation.

Where uncertainty is material, the actual authority must explicitly decide whether to:

- obtain further specialist input;
- continue temporarily under named conditions;
- restrict scope or permissions;
- intensify monitoring with an owner, threshold and deadline;
- delay rollout;
- pause or suspend use;
- select an alternative, transition or exit;
- accept the uncertainty through named authorisation and a documented rationale.

Uncertainty about whether a legal prohibition, a mandatory transparency, reporting, notification or assessment obligation, or a required formal procedure applies is never accepted under this rule. It is resolved through legal triage and qualified legal input under §8.3, and use is restricted, paused or suspended where required until it is resolved.

The record must state:

- which fact is missing, uncertain or contested;
- who owns obtaining or resolving it;
- the deadline;
- the interim operating status;
- the consequence if the deadline or threshold is missed;
- the reopen trigger.

Material uncertainty must never be recorded as absence of risk.

8.2 Emergency path

An emergency exists where immediate or rapidly developing harm, material service interruption or loss of control does not permit the normal sequence to be completed before protective action. The emergency authority named in the Authority Map declares the emergency and records the basis. Where that authority is unavailable, the documented fail-safe applies.

If neither the emergency authority nor its substitute is available, the highest available person with relevant operational control may take the minimum containment action necessary to prevent or limit immediate harm or interruption. That action is not approval, reauthorisation or a final outcome. It must be ratified, replaced or ended by a valid actual authority within the period defined in the Authority Map. Failure to obtain ratification is a governance finding and activates the pre-defined **Pause** or **Suspend** fallback; it never becomes silent continuation.

Emergency action may shorten:

- full baseline reconstruction;
- complete materiality analysis;
- non-immediately available specialist input;
- the normal meeting or forum sequence;
- full option development before containment.

Emergency action may not omit:

- Event ID and reason for urgency;
- who activated the emergency path and evidence of authority or fail-safe basis;
- immediately available facts and evidence-quality labels;
- the interim operating status using the canonical §7.2 vocabulary;
- parallel response processes, owners and deadlines;
- action owner and implementation evidence;
- ratification deadline;
- retrospective review deadline;
- evidence-preservation and legal-hold question;
- formal decision record after the immediate event;
- learning question about the emergency procedure itself.

The minimum emergency record is therefore:

1. reason for urgency and declaration criterion;
2. who activated the emergency path;
3. emergency authority, substitute or fail-safe basis;
4. immediately available specialist inputs;
5. interim operating status and restrictions;
6. parallel response processes activated, with owners and deadlines;
7. expiry or review date and ratification deadline;
8. implementation evidence;
9. evidence-preservation or legal-hold decision;
10. deadline for full retrospective framing and reassessment;
11. formal decision record after the immediate event;
12. learning question about the emergency procedure itself.

The organisation must monitor the proportion and pattern of events using the emergency path. A rising or unexplained rate is a governance signal and may require a C10 organisational-context event.

The emergency path is not a method deviation and does not create a duplicate deviation record. Any departure from the emergency-path rules themselves remains a method deviation.

An emergency restriction or suspension must not be rewritten later as if a full reauthorisation had occurred at the time.

8.3 Legal triage and legal input

Legal triage identifies whether a question needs qualified legal input. It is not a legal opinion. The event or triage owner records one triage result in B8:

Triage result	Record and next step
No legal signal identified	Named screener, date, scope, sources considered and short reason. No legal owner is required solely to record this result. It is not confirmation of legality or absence of duties.
Legal input required	Identify the credible question, assign a qualified legal owner and due date, and record the interim operating status. Apply trigger 11 and at least R2, or R3 where required.
Triage unresolved	State what is unclear, assign an owner and deadline, and seek qualified help. A credible unresolved legal question cannot be routed R0.

Screen changes to purpose, people or jurisdictions, data handling, role or classification, contractual commitments, and potential transparency, notification, reporting or assessment duties. Existing scoped advice or an approved screening checklist may be referenced; record whether its assumptions still apply. Doubt about a decision-critical legal question goes to the legal owner.

For **Legal input required**, keep the original triage result and separately record the input status: **pending**, **preliminary**, **received**, **contested** or **unavailable**. Record the question, qualified owner and qualification basis, date, version, scope, conclusion, limitations and how the decision uses it. **Not required** is the input status only when no legal signal was identified. A forum decision does not turn a pending input into a received one.

Only the qualified legal owner resolves the substantive legal question. Receiving advice does not itself establish that the resulting action is lawful or authorised. A material outstanding legal question remains a hold until resolved; the uncertainty rule cannot be used to accept a possible prohibition or mandatory procedure. Re-screen when facts or scope change.

9. Actual authority and specialist inputs

9.1 Actual authority is a critical gate

The method asks not only which committee is responsible, but who can make and enforce the decision in practice.

The named person or forum should be able, within the relevant scope, to:

- approve continuation and conditions;
- allocate resources and require implementation;
- restrict, pause or suspend use;
- require transition or exit;
- decide whether a closed event should be reopened;
- act in an emergency or activate a valid substitute authority.

Actual-authority test

1. Is the authority valid for this system, workflow, population, geography and consequence?
2. Can it allocate the resources needed to implement the decision?
3. Can it compel action across the functions involved?
4. Can it impose conditions and verify that they are maintained?
5. Can it stop use or rollout, not only advise that it should stop?
6. Where is the decision made in practice if that differs from the policy, RACI or committee charter?
7. Who acts if the primary authority is unavailable?

Actual capacity without a lawful mandate is an authority gap, not decision authority. A final decision requires confirmation at a validly mandated level, or the gap is recorded and escalated.

Where formal authority and actual authority differ, record both in separate fields. The gap itself may require corrective action.

9.1.1 Authority succession and vacancy

Where the person or forum holding actual authority changes, ceases to exist or becomes unable to act, record:

- the reason the prior mandate ended or became unavailable;
- the last valid decision and its continuing conditions;
- all open events, interim statuses, actions and verification duties held by the prior authority;
- the appointing authority, superior authority or escalation forum responsible for confirming the successor;
- the evidence supporting the successor's mandate;
- any temporary custodian and the limits of that custodianship;
- quorum, veto, recusal and conflict rules for a successor forum;
- the deadlock route;
- the date by which every open event receives a new owner and verifier.

A successor never confirms their own authority. An A-labelled assertion alone is insufficient for succession. The appointing authority, superior authority or escalation forum must use D or C evidence, or record the mandate as unresolved with an interim custodian and bounded powers.

A temporary custodian may preserve the record, maintain an existing protective interim status and route urgent questions. Unless expressly authorised, the custodian may not grant permanent continuation, materially expand use, waive a hard trigger or close the event.

Every open event transfers through an append-only record naming the prior owner or authority, successor, date, evidence, interim status and pending actions. An event left without a valid owner, verifier or authority after the transfer deadline is an open governance finding.

9.2 Specialist-input record

Field	Required content
Question	The precise legal, technical, cyber, privacy, human-factors, sectoral or other question.
Qualified owner	Named internal or external specialist with the relevant authority and depth, assessed against the test below.
Input	Conclusion, assumptions, uncertainty, dissent and limitations.
Status and date	Confirmed, preliminary, unavailable or contested; date and version.
Use in decision	How the actual authority incorporated, rejected or conditioned the input.

Qualification test

For each specialist input, record whether the person or function has:

1. a relevant qualification or demonstrated expertise for the precise question;
2. sufficient independence from the desired outcome, or a disclosed interest that the authority can evaluate;
3. awareness of the boundaries of their domain and of questions requiring another specialist;
4. the ability to date, scope and limit the conclusion.

A **qualified** specialist is not defined by job title alone.

For human-oversight questions, the specialist record should address, as applicable:

- reviewer competence and training;
- automation-bias risk;
- the person's ability to interpret the output and its limits;
- the person's ability to disregard, override, reverse, pause or stop;
- the sufficiency of provider information for meaningful review;
- reviewer language and domain capacity;
- whether the oversight design remains feasible under real workload, volume and time pressure;
- the accessibility of challenge, appeal and redress for affected people.

The method does not resolve a specialist disagreement by vote or by facilitator judgement. It records the disagreement, tests whether it is decision-relevant and routes it to the authority with appropriate qualified support.

10. Decision, action, closure, reopen and learning

10.1 Reauthorisation decision test

Before the decision is signed or recorded, the actual authority should answer:

1. What exactly changed against the baseline, and what is the baseline status?
2. Which facts are direct or corroborated, and which are reconstructed, asserted, unavailable or contested?
3. Which taxonomy classes, materiality lenses and hard triggers are engaged?
4. Which specialist inputs are required, and have they been received within their stated scope?
5. Does a demonstrated previous approval still apply? If so, why? If no prior approval is identified, which first-authorisation or containment branch applies?
6. What is the confirmed review route and what interim operating status applies?
7. Which options were considered, including non-AI alternatives where relevant? Where the feasible set is externally constrained, what constraint limits the options, and by when must the external decision be made?
8. Which final governance outcome best addresses the actual problem?
9. What conditions, restrictions, thresholds, stop criteria and review dates apply?
10. Who owns implementation, and what evidence will prove that each action occurred?
11. Who verifies each closure type, what transition action reopens the event, and what learning must return to the standing governance process?

Where an external provider, authority, market event or multi-tenant arrangement limits the feasible options, record the limitation and evidence. Do not invent alternatives the organisation cannot in fact choose.

10.2 Required decision record

For R2/R3, the decision record contains the following applicable elements. R0/R1 use the proportionate rule in §10.4:

- event and baseline status;
- linked-event IDs and cross-boundary tier;
- review-route proposal, confirmation and route history;
- interim operating status, history and consequence of lapse;
- options considered and any externally constrained choice set;
- external decision deadline where applicable;
- final governance outcome;
- rationale;
- conditions and restrictions;
- unresolved uncertainty;
- dissent or unresolved specialist disagreement;
- temporary measures;
- formal authority, actual authority and date;
- action owners, dependencies, due dates and per-action verifiers;
- closure criteria and closure types set at decision time;
- affected-person questions and owners;
- review, recurrence and reopen conditions.

Dissent is preserved. It is not deleted because the decision has been made.

10.3 Corrective-action record

Field	Required discipline
Action	State the concrete change to practice, use, workflow, permissions, system, provider arrangement, documentation, communication or affected-person remediation.
Owner and due date	Name one accountable owner, dependencies and a realistic date.
Dependencies	Record each internal or external dependency, its owner and its effect on timing or completion.
Implementation evidence	Identify what will prove that the action occurred in practice.
Per-action verifier	Where proportionate, use a verifier different from the action owner. Any exception follows the proportionality note.
Status	Do not treat assigned, communicated or ticket closed as implementation.

10.4 Closure types and route-specific requirements

This section is the controlling rule for documentation and closure. General lists elsewhere identify available fields; they do not add unconditional requirements to R0 or R1. References to current standing records are acceptable. Complete additional modules only when the event requires them.

Every closure statement names one or more types:

Closure type	What the evidence must show
implementation	The required action or configuration occurred.
condition	A continuing condition, monitoring duty or review is operating and has an owner.
outcome-confirmation	The required operating state or decision outcome was observed or otherwise evidenced.
remediation	Relevant consequences for people, records or downstream decisions were addressed.
residual-risk acceptance	Actual authority accepted a defined residual uncertainty or consequence, with a scope, rationale, owner and review date.

Mandatory records by route

Route	Required record and closure evidence	Confirmation and continuing review
R0 Documentation only	Event identity and scope; owner; evidenced baseline or boundary; verified delta; trigger and exemption result; concise rationale that the earlier decision basis remains applicable; legal and parallel-process screen; No interim change required; authorised O0 Continue; closure type, evidence and date; ten trace statuses; source and history references. Use the R0 short record.	Actual authority or expressly authorised delegate confirms O0 and the evidence. No separate legal opinion, full affected-person assessment or event-specific recurrence window is required when screening identifies no relevant issue. Record the people-screen rationale and reference the standing cumulation owner/cadence. If an action was performed, evidence its completion and apply the verifier separation or documented exception.
R1 Enhanced monitoring	Core identity, baseline, delta and route fields; monitoring question/metric, source, owner, threshold and review date; interim record; observed result; O0 or O1 decision; applicable action or condition evidence; closure type, people-screen result, ten trace statuses and history.	Named authorised confirmer and evidence reviewer; may be the same person where there is no self-verification of an action. Record review and learning owner/date. A threshold breach or unresolved specialist question raises the route. No silent extension.
R2 Specialist reassessment	Core record plus the specialist question, qualified owner, dated input and its use in the decision; authority, outcome, action/condition records, applicable closure types, evidence review, affected-person assessment, ten trace statuses and history.	Named actual authority or valid delegate within scope; closure verifier and limitations; event-specific learning owner and recurrence/review date. Complete each conditional module that applies.
R3 Formal reauthorisation	Full Parts 1 and 2 relevant to the event: authority and options; specialist inputs; interim and final decision; actions, conditions, closure criteria set at decision time; evidence and verification; affected-person assessment; recurrence and reopen; ten trace statuses and histories.	Valid actual authority for the renewed or first decision; named closure verifier; continuing conditions and residual uncertainty explicitly owned and dated. A facilitator cannot supply organisational authority or closure approval.

For all routes, closure requires the applicable decision and actions to be implemented or superseded by a new authorised decision, evidence supporting the named closure type, and no unresolved hold that prevents closure. Material uncertainty may become an explicitly authorised continuing condition or permitted residual-

risk acceptance with an owner and date; it is not deleted. Legal questions excluded by §8.1 cannot be accepted this way. Retain the transfer reference when a hold becomes a continuing condition.

When additional records apply

Condition	Additional record
Possible impact on people, incident, unassessed operating period, or downstream decisions	C9 affected-person assessment and C18 lookback where applicable; actions and evidence for notification, correction, appeal or remediation. Revisit the route.
A proposed or observed change requires action	C6 action owner, dependencies, due date, evidence and verifier. Assignment or ticket closure alone is insufficient.
Multiple unresolved facts or decisions	One C7 or workbook Holds entry per issue, each with owner, due date and lapse consequence.
Emergency or protective action before authority confirmation	C14 and C3 ratification and retrospective review; the emergency record may precede full intake.
Cross-entity dependency or limited external visibility	H External Handoff Record; no inference of another entity's approval.
Authority succession, experiment, or method deviation	C15, C19 or C17 respectively.
External disclosure of a case	Optional publication-clearance record under the organisation's disclosure process.

The full affected-person assessment states who was or may have been affected; notification, explanation, correction, appeal, redress or remediation questions; language and accessibility needs; owners and dates; and evidence or a named, reasoned not-applicable conclusion. R0/R1 screening is sufficient only when it identifies no such issue. A favourable technical result alone cannot close an affected-period question.

What does not establish closure

An email, meeting, assigned action, updated policy or closed ticket is a record of activity. Closure requires evidence that the relevant decision, action or condition is operating. If no implementation action is needed, the closure record explains that fact and confirms the continuing approved state.

10.5 Reopen as a transition action

Reopen is an append-only transition action initiated when a trigger suggests that a closed event no longer has a reliable closure basis.

The register-and-learning owner submits the trigger to the relevant actual authority within the organisation-defined period. While the authority's decision is pending, create a linked current review record with a **reopen decision pending** hold and an explicit interim operating status. Preserve the closed historical version. Use the named substitute if the authority is unavailable; urgent protection follows §8.2. A vacancy never allows silent continuation or self-confirmed succession.

The reopen record contains:

- trigger and reason;
- person or forum submitting it;

- actual authority;
- date;
- interim operating status at reopen;
- new decision point and due date;
- relationship between the earlier and continuing record;
- record version or linked-event ID;
- affected actions, conditions and evidence.

The earlier record remains unchanged. Continuation occurs through a new record version or linked record, with **supersedes** and the relationship stated explicitly.

Submit a reopen trigger when:

- closure evidence is disputed, withdrawn, inaccurate or no longer applicable;
- a condition or restriction is not maintained;
- a monitoring threshold or stop criterion is crossed;
- the event recurs or a related complaint, incident or provider signal appears;
- a linked or cumulative change alters the earlier basis;
- new specialist input materially changes the decision;
- actual use diverges from the closed scope;
- the earlier decision authority or ownership is no longer valid;
- the review date passes without the required evidence.

A trigger does not by itself reopen the record. The transition action and authority decision do.

10.6 Recurrence and learning

The review window must fit the event. Thirty or ninety days can be examples, not universal rules. A critical cutover may require checks after 24 hours, seven days and thirty days; slower drift may require 30-, 90- or 180-day review.

For R0, the standing cumulation review may supply the learning and recurrence record; link its owner and cadence. For other routes, set an event-specific review. At least one learning question should return to the standing process:

- Did the signal reach the right channel early enough?
- Was the authority clear, valid and available?
- Did specialist input arrive in time and within scope?
- Was the review route proportionate?
- Were the interim and final conditions practical?
- Did the expiry or review date return the event to a decider?
- Was closure evidence sufficient for each named closure type?
- Were affected-person consequences identified and addressed?
- Should the Authority Map, taxonomy, trigger, Boundary Record, template or standing process change?

11. Evidence quality, transition ledger and six-axis status model

11.1 Evidence-quality labels

Code	Evidence quality	Meaning	Use at critical gates
D	Direct and contemporaneous	Created at the time of the event by a primary system, signed decision or operational record.	Preferred for actual authority, decision and closure.
C	Corroborated	Supported by two or more independent records, systems or participants.	Can support a critical gate where direct evidence is unavailable and limitations are clear.
R	Reconstructed	Rebuilt after the event from available records and testimony.	Must remain visibly labelled; never presented as contemporaneous.
A	Asserted	A participant statement without sufficient corroboration.	Actual authority, decision and closure must not be presented as firmly confirmed on assertion alone.
U	Unavailable or contested	Missing, inaccessible, inconsistent or disputed.	Requires an explicit uncertainty decision, interim status, owner and closure plan.

Records, systems or participants are independent when they originate from different sources and do not share a common interest or a single upstream source in the matter recorded. Concordant accounts from participants who share context or interest are convergent, not independent.

The labels record provenance and the support available at critical gates. They are not a qualitative ranking of whether the underlying proposition is true. A D record can be authentic and still contain an error; a lower-provenance record can contain an accurate statement that remains insufficiently supported for a critical gate.

Source and reconstruction example

A signed approval created on 3 June and inspected on 10 September is D Direct and contemporaneous evidence of that approval: the source remains contemporaneous even though it was inspected later. Record both dates and its scope. A September participant account of what happened in June is A Asserted unless sufficiently supported. A chronology combining the approval and the later account is R Reconstructed for its retrospective links. Preserve each source label separately. The original approval may support a critical gate within its scope; unsupported links in the chronology may not.

Record **statement type** using full labels: Fact, Specialist conclusion, Assumption, Risk interpretation or Decision. Record **evidence quality** separately: D Direct and contemporaneous, C Corroborated, R Reconstructed, A Asserted or U Unavailable or contested. A decision record establishes that a decision was recorded, not that every premise was correct. A provider notice and a summary copied from it are one source, not two independent supports.

11.2 Evidence discipline

- Record source, owner, date, version and limitation.
- Do not turn testimony into documentary evidence merely by paraphrasing it into the Event Sheet.
- Keep reconstructed and simulated evidence visibly distinct from live evidence.

- Evidence of implementation is not evidence that the underlying technical or legal assessment was correct.
- A trace with many completed fields can still be materially incomplete if actual authority or closure evidence is missing.
- No completeness percentage becomes a maturity or effectiveness score. Critical gates outweigh a count of fields.
- Use full statement-type and evidence-quality labels in the working records. Legacy statement tags F / SC / A / RI / D may be retained in imported records only with an explicit key; do not confuse Decision with D evidence or Assumption with A evidence.

11.3 Record-integrity and transition-ledger rules

1. Records are not overwritten retrospectively. Corrections are new, dated versions linked to the earlier record.
2. Facts, specialist conclusions, assumptions, risk interpretations and organisational decisions are labelled separately.
3. Every change to route, interim status, workflow phase, operating state, hold reason, record disposition or outcome records the date, actor and reason.
4. Dissent and material disagreement remain in the record.
5. The facilitator never becomes the organisation's decision authority or closure authority.
6. The current method version and any method deviation are recorded.
7. Source evidence remains in the organisation's systems where possible; the trace keeps references rather than unnecessary copies.
8. A simulated or retrospective record cannot be used to imply a live field application.
9. Every record carries **record version**, **supersedes**, **created by-at**, **changed by-at** and **change reason**.
10. Every transition is entered in an append-only transition table with **from → to**, date, actor and reason.

An organisation may use its own GRC, ITSM, ticketing, change-management, records or workflow system instead of the supplied templates only where it can demonstrate a functional equivalent for the controlled fields, append-only history, evidence references, route and interim histories, authority records, closure types and transition log.

Transition-log minimum

Field	Requirement
transition ID	Unique identifier.
field or axis	The field or axis that changed.
from → to	Earlier and new controlled value.
date and time	When the transition was recorded and, where different, when it took effect.
actor	Person or forum making or recording the change.
authority basis	Decision, route, rule or evidence supporting the transition.
reason	Plain-language reason, including new facts or thresholds.
record version	Version created by the transition.

11.4 Data boundary

Sensitive source evidence should remain in the organisation's own systems. The trace should hold references rather than copies wherever possible.

For each referenced item, record:

- source system or repository;
- document or record identifier;
- owner;
- date and version;
- access limitation;
- evidence-quality label;
- the part of the decision or closure it supports;
- statement-type tag for the proposition recorded from it.

Do not copy personal data, security-sensitive material, trade secrets or confidential technical content into the Event Sheet unless it is necessary, proportionate and covered by an agreed handling basis.

11.4.1 Record Ownership & Data Schedule

Before the first facilitated event, the organisation and facilitator record:

- the participating legal entities and operating scopes;
- each class of record created, referenced or retained;
- the system of record and access rights;
- retention and deletion rules;
- breach and incident routes;
- the boundary between organisational source evidence and the facilitator's working record;
- what, if anything, remains with the facilitator or other external party after the engagement;
- the case-specific channel for evidence, incidents or personal data.

The method-feedback address in §14.4 is not a case-evidence, incident or personal-data channel.

The editable templates include G, the Record Ownership & Data Schedule. For organisation-run use, reference equivalent internal records; external access, retention and return/deletion terms must be completed before external sharing.

11.5 Six-axis status model

A single status field must not combine workflow progress, operational state, evidence hold, record disposition, outcome and mode. Record the six axes separately. The hold axis is a set of active issues, not a single-choice field. Each issue has a Hold ID, Event ID, reason, question, owner, due date, interim reference, lapse consequence and resolution evidence. Closing one hold does not remove another. The workbook displays active hold counts and links to the Holds sheet; any primary reason used in a summary is only a display aid.

Controlled values

Axis	Controlled values
workflow_phase	Open / Triage / Assessment / Decision pending / Action in progress / Closure review / Closed
operating_state	Operating under approved baseline / Operating temporarily / Operating under conditions or restrictions / Paused / Suspended / In transition / Exited

Axis	Controlled values
hold_reason	Zero or more active reasons from evidence pending / specialist input pending / authority pending / reopen decision pending. Use none only when no active hold exists.
record_disposition	active / cancelled
outcome	O0 / O1 / O2 / O3 / O4 / O5 / O6 - populated after a decision
mode	Prospective live trace / Hybrid reconstruction plus prospective follow-up / Retrospective reconstruction / Simulation / tabletop / Standing embedded process

A status value becomes valid when…

Axis	Value	Minimum record required
workflow_phase	Open	Event ID, candidate signal, date opened and event owner.
workflow_phase	Triage	Intake distinction, operating scope, initial ownership, parallel-process check and proposed route or triage plan.
workflow_phase	Assessment	Baseline status, candidate or verified delta, applicable taxonomy and active evidence or specialist work.
workflow_phase	Decision pending	Confirmed or disputed route, actual-authority status, explicit interim operating status and outstanding decision inputs.
workflow_phase	Action in progress	Recorded outcome, action owners, dependencies, due dates and implementation-evidence plan.
workflow_phase	Closure review	Named closure types, closure criteria, evidence references and closure verifier.
workflow_phase	Closed	The applicable §10.4 route requirements are met. Record closure type, supporting evidence and authorised confirmation. Full affected-person assessment, separate verifier and event-specific recurrence apply only as §10.4 requires; the R0 standing-review reference is sufficient where permitted.
operating_state	Operating under approved baseline	Baseline status **approved**, **conditionally approved** or **reconstructed from an evidenced approval**, with evidence and no contrary interim or outcome.

Axis	Value	Minimum record required
operating_state	Operating temporarily	**Continue temporarily** interim record with authority, reason, expiry/review date, owner of missing facts and lapse consequence.
operating_state	Operating under conditions or restrictions	**Continue temporarily with conditions**, **Restrict**, O1 **Continue with conditions** or O2 **Restrict**, with conditions, owner and evidence.
operating_state	Paused	**Pause** or O3 **Pause**, scope of non-operation, authority, criteria for return and expiry/review date.
operating_state	Suspended	**Suspend** or O4 **Suspend**, authority, implementation evidence, return conditions and review date.
operating_state	In transition	O5 **Transition**, target arrangement, incoming linked event, action owner, continuity and exit controls.
operating_state	Exited	O6 **Exit** and evidence that the use or dependency has been decommissioned or terminated within the defined scope.
hold_reason	none	No unresolved hold condition prevents the current workflow phase from progressing.
hold_reason	evidence pending	Named missing evidence, owner, deadline, interim operating status and lapse consequence.
hold_reason	specialist input pending	Named specialist question, qualified owner, status, deadline, interim operating status and lapse consequence.
hold_reason	authority pending	Formal and actual authority question, escalation route, interim custodian or protective interim status, and deadline.
hold_reason	reopen decision pending	Reopen trigger submitted, actual authority, interim operating status and decision deadline.
record_disposition	active	The record remains the current trace for the event or linked event.
record_disposition	cancelled	Named owner, rationale, second-person confirmation, relationship to any duplicate or non-occurring event, and preserved transition history.
outcome	O0	Actual-authority decision to **Continue**, with rationale and applicable closure floor.

Axis	Value	Minimum record required
outcome	O1	Actual-authority decision to **Continue with conditions**, with conditions, owners, evidence and review dates.
outcome	O2	Actual-authority decision to **Restrict**, with defined scope and implementation evidence.
outcome	O3	Actual-authority decision to **Pause**, with return criteria and review date.
outcome	O4	Actual-authority decision to **Suspend**, with implementation evidence and return-authorisation rule.
outcome	O5	Actual-authority decision to **Transition**, with incoming linked event and continuity or exit actions.
outcome	O6	Actual-authority decision to **Exit**, with decommissioning or termination evidence.
mode	Prospective live trace	Event followed from signal through one or more later stages as they occur; contemporaneous and reconstructed elements labelled separately.
mode	Hybrid reconstruction plus prospective follow-up	Earlier stages reconstructed and at least one later stage designated for live follow-up; each element labelled by evidence timing.
mode	Retrospective reconstruction	Event traced after the relevant stages; no claim of contemporaneous application.
mode	Simulation / tabletop	Fictional or hypothetical event, visibly marked; no field claim.
mode	Standing embedded process	Organisation maintains the Authority Map, Event Sheet and Register across real events, with a named process owner and functional record system.

The six axes do not replace evidence. Each value becomes valid only when its minimum record is present.

12. Using the toolkit

12.1 Recommended sequence

1. Activate applicable parallel response processes and record their owners and deadlines.
2. Confirm the Organisation Authority Map, readiness and operating scope.
3. Create an Event ID and record the signal without pre-judging materiality.
4. Select the baseline status, confirm or reconstruct the baseline and label evidence quality.
5. Verify the delta, apply the multi-label taxonomy and descriptors, link related events and record any Pre-authorised Change Boundary invocation.
6. Review the materiality lenses and hard triggers; the event owner or triage owner proposes the minimum route and the routing authority confirms it.
7. Where necessary, record a protective interim operating status before authority confirmation and obtain mandatory ratification.
8. Obtain the required specialist inputs, apply the cross-boundary tier and confirm formal and actual authority.
9. Record the final decision, outcome, rationale, conditions, dissent, external constraints and closure criteria.
10. Track corrective actions and implementation evidence; verify closure by type, set recurrence review and update standing governance where needed.

This method never delays or replaces any applicable incident, security, privacy, safety, employment, customer-remediation or regulatory response process. Record which parallel processes are activated, their owners and deadlines; this trace runs alongside them, never before them.

12.2 Organisation Authority Map

Use once for the organisation or a defined operating scope, then review it after changes in systems, roles, forums, providers, self-hosting arrangements or emergency arrangements.

Minimum rule: name actual authorities, not only advisory committees. Name substitutes by decision type, not only one generic substitute.

12.3 AI Change Event Sheet - Part 1

Open when a candidate event or signal enters intake. Record:

- event ID, date and mode;
- operating scope and legal entity;
- system owner, consequence owner and event owner;
- signal source, date, statement tag and evidence quality;
- baseline status and baseline evidence reference;
- verified delta or candidate-signal status;
- taxonomy classes and descriptors;
- linked event IDs and parent-event ID where applicable;
- affected people and consequence;
- materiality-lens records;
- hard-escalation triggers;
- required specialist inputs;
- legal triage result, screener, date and reason; separate legal-input status and qualified owner where required;
- Exemption invoked: yes/no, Boundary Record ID and evidence;

- external entity and external decision deadline where applicable;
- route proposed by and route confirmed by;
- minimum review route;
- interim operating status if already required;
- parallel response processes activated;
- method deviation or limitation.

Do not call the event material before review. Record unknown, contested and reconstructed inputs. Link events on the Event Sheet, not only in the Register.

12.4 AI Change Event Sheet - Part 2

Complete the applicable fields through authority, decision, action, closure and learning. Part 2 carries its own Event ID. R0 uses the mapped short record and §10.4 controls required content. Record:

- formal authority and evidence;
- actual authority and evidence;
- authority succession or vacancy record where applicable;
- options considered and external constraints;
- review route and route history;
- interim operating status, interim history and lapse consequence;
- final governance outcome O0-O6;
- rationale, conditions, uncertainty and dissent;
- emergency record where applicable;
- specialist-input records;
- corrective actions, owners, dependencies, dates and per-action verifiers;
- implementation evidence;
- closure types, closure criteria and closure verifier;
- affected-person assessment;
- six-axis current state;
- recurrence window and reopen trigger;
- learning and standing-process update;
- Event ID, record version, supersedes, created by-at, changed by-at and change reason;
- transition log;
- reopen transition block;
- method deviation or limitation.

Define closure criteria when the decision is made, not after implementation.

12.5 Event Register

Use the Register to maintain a portfolio view and link cumulative or coupled events. Minimum fields:

- event ID and short name;
- operating scope and legal entity;
- baseline status;
- primary and secondary taxonomy classes;
- linked event IDs and parent-event ID;
- mode;
- workflow_phase;
- operating_state;
- hold_reason;
- record_disposition;
- event owner, formal authority and actual authority;

- review route and route-history reference;
- interim operating status and interim-history reference;
- outcome O0-O6;
- legal triage result and separate legal-input status; B8/C4 reference for owner, question, date and reason;
- action due date;
- closure type;
- closure evidence status and quality;
- recurrence or reopen status;
- record version and supersedes;
- current method designation;
- optional publication clearance only when a case is proposed for external disclosure.

Recommended practice - primary-class rule. Where the Register requires one primary taxonomy class, the event owner records the class that most changes the basis of the earlier decision. The judgment and rationale are recorded. Every other applicable class remains secondary. This does not reduce or replace multi-label classification.

Do not add a risk score, maturity score or completion percentage.

12.6 Closure & Learning Supplement

Use when the Event Sheet cannot hold multiple actions, evidence items, unresolved conditions, affected-person remediation or recurrence reviews. Keep it linked to the same Event ID. It supplements rather than replaces the two-part core record.

Editable forms corresponding to Appendices A-D and F, with the G data schedule and H external handoff module, are supplied in the Working Templates document. Appendix E defines the workbook and its references.

12.7 Working with existing systems

The method does not replace IT service change enablement, deployment, release or configuration management. It addresses the organisational decision and accountability questions that remain when a technically managed change alters actual use, human authority, external dependency, legal assumptions or the basis of an earlier AI decision.

The method should connect to, rather than duplicate, existing organisational systems.

Signals that may open an event

A signal may come from:

- IT or product change management;
- incident, security, privacy, safety or customer-remediation processes;
- model or provider monitoring;
- procurement, third-party risk or contract management;
- release, deployment, lineage or maintainer records;
- risk, compliance, audit or legal issue logs;
- complaint, appeal, redress, quality or workforce channels;
- ticketing, service-management or operational-resilience systems.

Existing specialist inputs

Where an existing process has already produced qualified legal, technical, privacy, security, human-factors, sectoral or other input, reference it rather than re-performing or copying it. Record its owner, date, version, scope, limitations and use in the decision.

System of record

Before use, designate one system of record for the event trace. Existing ITIL, GRC, ITSM, ticketing, records-management or workflow systems may be used where they provide the functional equivalent required by §11.3. References should replace copies wherever possible.

A tool, ticket or control record is not functionally equivalent merely because it contains a status field. It must preserve the method's separate route, interim, outcome, authority, evidence, closure and transition disciplines.

Example of mapping into an existing change record

Existing record	ACAR content and reference
Change ticket CHG-1042	Event ID ACAR-1042 in the ticket; B1/B2 signal and scope; link to the AI inventory
Approved configuration and release request	B3/B4 baseline, proposed delta and dated source references
Governance decision attachment	B7 route; C2 authority mandate; C3 interim status; C5 final outcome and conditions as distinct fields
Existing action subtasks	C6 owners, dependencies, dates, implementation evidence and verifiers
Issue list and approval history	C7 all active holds; C12 dated changes, actors and authority references
Governance closure entry	C8 evidence by closure type and §10.4 confirmation; C10 review/reopen criteria; C16 trace statuses

The ticket's technical completion does not close the governance record automatically. The organisation designates the authoritative record and preserves its history. Do not maintain two independently editable sources for the same decision.

12.8 Cross-boundary events

Use one of three evidence tiers.

Tier	Minimum record	What may be concluded	What may not be concluded
full linked external trace	Linked event ID for each participating entity; external authority; decision and evidence references; notice; contractual leverage; handoff; external decision deadline.	Bounded conclusions about the linked organisational chain within the accessible records and named scopes.	Legal compliance, technical adequacy or facts outside the inspected and evidenced linked traces.
internal boundary evidence only	Internal event trace plus external entity, known authority, notice, contractual leverage, handoff, unavailable fields and limitation.	What the organisation knew, requested, decided and could influence at its boundary.	The quality, completeness or implementation of the external party's decision.

Tier	Minimum record	What may be concluded	What may not be concluded
external decision or evidence unavailable	Unavailability record, attempts or constraints, internal interim status, authority and decision deadline.	That the external decision or evidence was unavailable and how the organisation responded.	Any inferred external decision, approval, control effectiveness or closure.

Use H External Handoff Record for these tiers. It is distinct from F, the Pre-authorised Change Boundary. For every tier, record:

- external entity;
- external authority, if known;
- notice and notice threshold;
- contractual leverage and practical leverage;
- handoff owner and handoff evidence;
- external decision deadline;
- subprocessor or downstream dependency depth known to the organisation;
- limitations on visibility.

In multi-tenant one-to-many arrangements, the organisation may not be able to negotiate or inspect the same controls as in a bespoke relationship. Record that constraint rather than assuming equal leverage. Visibility into deeper subprocessor chains is limited by contractual flow-down and available evidence; the limitation itself is recorded.

13. Synthetic examples - not field evidence

Both examples are fictional. They are not case studies, pilot results or field evidence. Their mode is Simulation / tabletop. The separate Worked Examples document completes the same fields as the editable templates. The Example Register contains their corresponding portfolio records, actions, holds and dated transitions. All scenario evidence, dates, names and numerical thresholds are invented for instruction.

13.1 Customer-service assistant and proposed refund authority

Northbank Retail's approved assistant drafts customer-service replies, with human approval of every reply and refund. A provider model update arrives alongside a proposal for automatic refunds, a payment connector, a second market and sampled human review. The event engages C1, C4, C5, C6, C7 and C8, all twelve materiality lenses, and hard triggers 1, 2, 3, 4, 5, 6, 8, 10, 11 and 13. It is NBR-SIM-001.

The forum confirms R3 Formal reauthorisation. The proposed expanded workflow is Paused; the existing drafting service remains within its evidenced approved baseline. Two holds coexist: scoped legal input and evidence of reversal/logging. Legal input arriving does not resolve the technical-evidence hold. Each is assigned, dated and resolved separately.

The qualified inputs support a narrower authorisation: Market A, EUR 30 cap, human confirmation of every refund, full logging, daily exception review, trained reviewers and a customer challenge/correction route. The forum records O1 Continue with conditions before rollout, with prelaunch evidence and four weeks of observed records as closure criteria. The original legal triage remains Legal input required; its separate input status becomes received when the scoped advice arrives.

Named owners implement the configuration, reviewer arrangements, logs and customer route. A verifier outside those action owners checks the evidence. The fictional four-week record supports implementation, condition and outcome-confirmation closure. The workflow remains Operating under conditions or restrictions. Universal human confirmation does not expire merely because four weeks have passed; removing it requires a new decision. The next review remains owned and dated after the event closes.

13.2 Routine model patch within an approved boundary

NBR-SIM-002 concerns an internal knowledge assistant with a conditionally approved baseline and a current Pre-authorised Change Boundary. The boundary covers specified patch-level updates in the same family, subject to staged checks, unchanged scope and exclusions.

On 2 October, a provider notice verifies what is proposed and a separate internal staged record verifies the scoped test and configuration findings. These are D source records for different propositions. Neither proves that production has changed. Trigger 6 remains recorded; the boundary exemption is invoked and confirmed because its class, magnitude, evidence, authority and expiry conditions are met. The route is R0 Documentation only, the interim status is No interim change required, and actual authority confirms O0 Continue within the earlier approval.

The patch is deployed on 3 October. Only then do the production deployment record and smoke-test support implementation. A named confirmer who did not perform the deployment verifies closure. The short R0 record links the evidence, people-screen rationale, ten trace statuses and standing cumulation review without requiring a legal opinion or a full R3 record. The final six axes are Closed; Operating under approved baseline; no active holds; active; O0 Continue; Simulation / tabletop.

If a later patch adds external messaging, it exceeds the boundary. The linked variant NBR-SIM-002B preserves the earlier valid record, records the new permission/action triggers and follows the normal R3 rule. The new capability remains Paused pending a valid decision. A patch label does not override the boundary's scope.

14. Assumptions, limitations, status, licence and citation

14.1 Assumptions and limitations

Limitation	Consequence
Signal visibility	The method governs events that reach intake. Detection, provider feeds and technical-source reconciliation remain organisational responsibilities.
Event granularity	Linked and parent events handle related changes. This guide does not supply a complete model for continuous high-frequency or mass provider change.
Access	Decisions depend on access to actual authority, records and proportionate evidence.
Specialist and decision quality	A completed trace does not prove the substantive correctness of a specialist input or an organisational decision.
Organisational specificity	Authority, conditions and evidence are scope-specific. Adaptation must retain the applicable gates.
Administrative burden	Use §10.4 and the short R0 record; additional modules require an event-specific reason.
Transferability	One context does not establish effectiveness across contexts or independent organisation-run usability.
Organisation-run readiness	Complete and operate the stated prerequisites before representing self-use as operational.
External visibility	Conclusions stop at the boundary of accessible evidence, authority and contractual leverage.

14.2 Relationship to established frameworks

The following mapping is the author's interpretation of where the method can support organisational implementation. It identifies specific functions and records; it is not a finding that a whole principle, framework provision or legal requirement has been fulfilled. The sources remain authoritative for their own scope.

Relevant source function	ACAR activity and record	Limit of the contribution
OECD accountability and the ability to act; NIST GOVERN 2.1, 2.3 and 3.2	A/C2 distinguish formal authority, practical decision powers and oversight roles; C5/C12 preserve decisions and changes.	Records an event-level authority path. It does not establish satisfaction of the principles or all governance provisions.

Relevant source function	ACAR activity and record	Limit of the contribution
OECD human agency and oversight	B6/C4 identify changed review, intervention and capacity; C3/C5 record permitted operation and conditions.	Specialist assessment of meaningful oversight remains necessary.
OECD traceability and responsible-AI due diligence on tracking implementation/results	B10/C6/C8 connect a source, decision, action and closure evidence.	Supports a bounded organisational record; not full value-chain due diligence or model explainability.
NIST GOVERN 1.5/1.7 and MANAGE 4.1-4.3	Signal intake, changed approval basis, actions, recurrence and closure in B/C.	Supports the organisational change-response component. Technical monitoring, incident handling, recovery and decommissioning need their own processes. NIST AI 800-4 supplies monitoring context, not validation of ACAR.
NIST GOVERN 6 / MANAGE 3 and OECD business-relationship due diligence	H records notices, internal leverage, handoff and evidence limits.	Does not replace supplier assessment, contracting, cybersecurity or upstream technical evaluation.
EU AI Act actor roles, human oversight and relevant lifecycle duties	B8/C4 route questions to qualified owners; C2/C5 record the organisational response.	Legal applicability, classification and substantive compliance remain external determinations.
GDPR and other applicable data requirements	B6/B8 and G reference specialist input and record handling.	Does not determine lawfulness, privacy or security compliance.
Technical evaluation, assurance and certification	Existing scoped results may be referenced in C4/B10.	These activities are outside the method.

Selected primary sources:

1. OECD (2024), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
2. OECD (2026), OECD Due Diligence Guidance for Responsible AI, OECD Publishing. https://doi.org/10.1787/41671712-en
3. NIST (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1
4. Rao, A. K. et al. (2026), Challenges to the Monitoring of Deployed AI Systems, NIST AI 800-4. https://doi.org/10.6028/NIST.AI.800-4
5. European Union, Regulation (EU) 2024/1689, consolidated text of 27 July 2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng
6. European Union, Regulation (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Sources checked for this edition on 23 September 2026. Apply the law and framework version relevant to the organisation and decision at the time of use.

14.3 Method provenance and responsibility

The method was developed from practitioner experience in complex, cross-functional and governance-sensitive technology environments. It was not developed, mandated or tested at any former employer.

Maja Kurek developed the organisational problem framing, event-level architecture, taxonomy, materiality and escalation logic, and the focus on authority, interim operation and evidenced closure. Adjacent governance, change-management and due-diligence disciplines inform the method; the selected frameworks are mapped in §14.2.

OpenAI ChatGPT and Anthropic Claude assisted with drafting, structural implementation, cross-references and consistency checks in the earlier edition. OpenAI ChatGPT assisted with the author-directed revisions, editable records, fictional examples and document preparation in this edition. Authorial and publication responsibility remains with Maja Kurek; those tools do not provide organisational decision authority, specialist approval or independent assurance.

14.4 Status, licence and citation

Status and field application

The method comes from practice, drawn from a decade of practitioner experience in large, regulated technology organisations, where obligations had to become decisions someone owned and evidence that survived scrutiny.

In one organisational field study, the author applied the method with two senior participants holding final business authority in practice and the principal technical and implementation levers. The facilitated work reconstructed related AI change pathways, distinguished authority from implementation powers, made three open operating states explicit and elicited the criteria participants identified for resolving them. Interviews, limited direct screen views, later factual confirmation and analytical inference remained separately identified.

The study documented real operating arrangements and decisions. The organisation did not independently operate the method's records, and no new complete decision-to-implementation-to-evidenced-closure cycle arose during the fieldwork. The study does not establish that the method caused the articulation of the findings or that later changes to this edition have been tested in organisational use.

The accompanying paper reports the study: Kurek, M. (2026), Governing AI After Deployment: Field Evidence on Model Changes, Platform Configuration and Organisational Authority, working paper, revision dated 30 August 2026, SSRN. https://doi.org/10.2139/ssrn.7329378

Licence

© 2026 Maja Kurek · RuleBridge Advisory.

The original guide, templates, register and fictional worked examples in this edition are licensed under Creative Commons Attribution 4.0 International (CC BY 4.0): https://creativecommons.org/licenses/by/4.0/. You may share and adapt the materials, including commercially, under that licence. Give appropriate credit, link the licence and indicate changes. Do not imply that the author endorses your use or adaptation. No additional licence restrictions are imposed here.

The licence does not require users to publish completed records, confidential information or source evidence. Third-party materials and rights remain with their respective holders; citations do not relicense those sources. Rights in trade marks, privacy and other interests are not supplied by this copyright licence.

Suggested citation

Kurek, M. (2026), AI Change Accountability & Reauthorisation: A practitioner-derived method for tracing AI change from signal to decision, implementation and closure, RuleBridge Advisory, revised edition 23 September 2026. https://rulebridge.eu/instrument/

Edition and maintenance

This edition revises the public guide dated 22 August 2026. The accompanying change log identifies the changes; earlier editions retain their own dates and licensing notices. Use the method edition and record version in every event. Do not relabel older organisational evidence as use of the new rules or examples.

Method corrections and new editions are maintained at https://rulebridge.eu/instrument/. Report issues to office@rulebridge.eu with the method date, field or section, generic issue and mode of use. The method is maintained through dated revisions and correction notices; this statement does not claim a fixed external review or certification cycle.

Do not send case evidence, incidents, security-sensitive material or personal data to the feedback mailbox. Use the case-specific channel in the Record Ownership & Data Schedule for those matters.

Glossary and controlled vocabulary

This glossary collects the controlled terms for reference. Short definitions appear beside the relevant first use in the guide. Detailed rules remain in the cited sections. A controlled label must be reproduced exactly wherever it appears in the guide, examples, templates or Register.

Document hierarchy

Term	Meaning
package	The public guide, editable templates, register and worked examples.
method	The decision logic that takes one candidate event from signal through authority, decision, action, closure evidence and learning.
guide	This document.
templates	The working artefacts used to record and operate the method.

Core roles and scope

Term	Meaning
operating scope	One named AI system or workflow within one legal entity. Where more than one legal entity is involved, apply the cross-boundary rules in §12.8.
system owner	The person accountable for the system or technical service as defined by the organisation.
consequence owner	The person accountable for the business or human consequence affected by the use. This role may differ from the system owner.
event owner	The person accountable for the completeness, currency and routing of the event trace. The event owner is not automatically the system owner, consequence owner or decision authority.
triage owner	The person authorised to open an event, preserve the initial record, propose a route and impose a temporary protective interim status subject to ratification under §7.2.
formal authority	The person or forum named in a policy, charter, RACI, delegation or other formal record.
actual authority	The person or forum that can make and enforce the relevant decision in practice, including allocating resources, compelling action and stopping or conditioning use.
routing authority	The actual authority or pre-named person or forum authorised to confirm the proposed minimum review route.
event-level learning owner	The owner of the learning and recurrence review for one event.

Term	Meaning
register-and-learning owner	The standing owner of the Event Register, cumulation review cadence and cross-event learning.
closure verifier	The person who reviews closure evidence and records what it confirms and what remains limited.
containment	A minimum protective action taken to reduce immediate exposure or preserve control. Containment is not approval or reauthorisation.

Reauthorisation and change terms

Term	Meaning
reauthorisation	A renewed organisational decision by the relevant actual authority on whether, and under which conditions, an AI use, system, workflow or dependency may continue. It is not a regulatory approval, a legal qualification, a certification, or a technical revalidation.
verified change / verified delta	A delta is verified when the event owner or triage owner confirms it with evidence of quality D or C; on A or R alone it remains a candidate signal.
material / materially	Whether the change affects the basis on which the organisation previously decided that the use was acceptable and governable.
reasonably possible serious consequence	A serious consequence supported by a credible causal pathway, relevant evidence or a recurring pattern; it is not remote, purely speculative or based only on an abstract worst case.
unauthorised or unassessed operation period	A bounded period during which a material change, divergence or configuration operated without a demonstrated applicable approval or assessment.
method deviation	A recorded departure from a method rule. A legitimate re-route caused by new facts is not a method deviation when the current logic no longer indicates the earlier route.
Pre-authorised Change Boundary	A documented, versioned and time-bounded decision boundary within which specified change classes and magnitudes may be handled without invoking the normal hard-trigger route, subject to the exclusions and record requirements in §6.4.
Boundary Record	The record that defines and evidences a Pre-authorised Change Boundary.

Modes of use

The five canonical mode labels are:

1. **Prospective live trace**
2. **Hybrid reconstruction plus prospective follow-up**
3. **Retrospective reconstruction**

4. **Simulation / tabletop**
5. **Standing embedded process**

Operating formats

- **Facilitated**
- **Organisation-run**

Intake distinctions

Term	Meaning
Signal	Information suggesting that something may have changed or that risk may require attention.
Verified change	A confirmed difference from the approved or reconstructed baseline, subject to the verification rule above.
Incident	An event that caused or could have caused harm, failure, disruption or loss.
Risk interpretation	A qualified or organisational conclusion about consequence, uncertainty or control relevance.
Governance trigger	The reason a defined review route or decision must now occur.

Baseline status

Use exactly one:

- **approved**
- **conditionally approved**
- **reconstructed from an evidenced approval**
- **no prior approval identified**
- **approval contested**
- **unable to determine**

Change-event taxonomy

Code	Canonical class
C1	Model, version or capability change
C2	Provider, platform, hosting or service change
C3	Data-basis change
C4	Intended-use or actual-use change
C5	Affected population, volume or geography change
C6	Autonomy, permissions or transaction-boundary change
C7	Human-role, review-capacity or intervention change

Code	Canonical class
C8	Integration-channel or external-system change
C9	Performance, incident or provider signal
C10	Regulatory, contractual or organisational-context change

Cross-cutting descriptors

Dimension	Controlled values
Reality	actual / planned / simulated
Timing	prospective / retrospective / hybrid
Reversibility	reversible / partly reversible / difficult to reverse
Observability	observable / partly observable / weakly observable
Boundary	contained / cross-functional / cross-organisational
Relationship	single / cumulative / coupled
Operating condition	routine / exception / emergency / externally forced
Knowledge	known / uncertain / contested

Materiality lenses

Code	Canonical lens
M1	Functional capability and behaviour
M2	Intended use, actual use and operating context
M3	Consequence and action
M4	Affected people, scale and geography
M5	Data, privacy and security
M6	Autonomy, permissions and transaction boundary
M7	Human oversight, intervention and capacity
M8	Provider, dependency and cross-boundary impact
M9	Reversibility, substitution and exit
M10	Observability and evidence availability

Code	Canonical lens
M11	Regulatory, contractual, role and specialist uncertainty
M12	Cumulative, coupled and recurring effect

Hard-escalation triggers

The canonical hard triggers are numbered 1-15 and stated in full in §6.3. Trigger 14 is **emergency change**. Trigger 15 is **change of the person or forum that actually holds decision authority**.

Review routes

Code	Canonical route
R0	Documentation only
R1	Enhanced monitoring
R2	Specialist reassessment
R3	Formal reauthorisation

Interim operating status

Use exactly one:

- **No interim change required**
- **Continue temporarily**
- **Continue temporarily with conditions**
- **Restrict**
- **Pause**
- **Suspend**

Final governance outcome

Code	Canonical outcome
O0	Continue
O1	Continue with conditions
O2	Restrict
O3	Pause
O4	Suspend
O5	Transition
O6	Exit

Reopen is a transition action, not a final governance outcome.

Legal triage and input

Triage: No legal signal identified / Legal input required / Triage unresolved.

Input status: Not required / pending / preliminary / received / contested / unavailable. See §8.3. A received input does not erase the reason it was needed.

Evidence-quality labels

Code	Canonical label
D	Direct and contemporaneous
C	Corroborated
R	Reconstructed
A	Asserted
U	Unavailable or contested

Statement types

Use full labels: Fact / Specialist conclusion / Assumption / Risk interpretation / Decision. Keep this field separate from evidence quality. Legacy tags F / SC / A / RI / D require an explicit key.

Trace-element status

Use one for each Governance Outcome Trace element:

- **completed**
- **pending**
- **not required with rationale**
- **unavailable**
- **contested**
- **not within this trace**

Closure type

Use one or more:

- **implementation**
- **condition**
- **outcome-confirmation**
- **remediation**
- **residual-risk acceptance**

Six-axis status model

The six axes and their controlled values are defined in §11.5. They are:

- **workflow_phase**

- **operating_state**
- **hold_reason** - all active issues, each with owner and deadline
- **record_disposition**
- **outcome**
- **mode**

Publication clearance

Optional, only when external disclosure is planned; use one in the separate disclosure record:

- **publication not assessed**
- **review required**
- **blocked**
- **cleared for defined output**
- **cleared with conditions**

Any clearance value is held in the separate disclosure record and may be referenced from the Event Register. The method does not create clearance.

Other record values

Field	Values
Closure evidence status	not defined / defined / partial / complete / contested
Affected-person assessment	complete / pending / not applicable with rationale / unavailable / contested
Recurrence or reopen	none / scheduled review / linked trigger / reopen decision pending / reopened by transition action
External evidence tier	full linked external trace / internal boundary evidence only / external decision or evidence unavailable

Appendix A. Organisation Authority Map

The editable Working Templates contain writing space for every field below. Use one scoped map and reference it from events. Repeat A3 where decision powers differ.

A1 Scope and record control

Standing record for the selected operating scope.

Field	Requirement
Scope	Named system/workflow, legal entity/business unit, map reference and version
Record control	Owner; last and next review dates; authoritative record system; G data-schedule reference
Signal channels	Source, recipient and substitute; include provider and internal configuration notices; for self-hosting include maintainer, lineage, patch and dependency channels

A2 People and functions

Name the people or forums and reference their mandates.

Field	Requirement
Owners	Process; triage; event; system/product; consequence; implementation; closure verification; register-and-learning
Specialist contacts	Legal; technical/model; privacy/data; security; human factors/domain; other required expertise. Contacts do not imply universal review
Escalation	Routing authority; escalation forum; authority-succession owner; conflicts, quorum, recusal, veto and deadlock arrangements

A3 Decision authority

Repeat this block for distinct decision scopes.

Field	Requirement
Decision scope	Continue/condition; restrict/pause; suspend; transition; exit; reopen; emergency ratification. Specify the permitted system, population, geography and limits
Formal and actual authority	Record separately; mandate reference; evidence quality; practical ability to allocate resources and compel action; any split budget or implementation powers

Field	Requirement
Delegates and substitutes	Name each delegate/substitute by decision type, mandate, scope, limits and expiry; identify who confirms succession. No self-confirmation
Authority gaps	What is missing; custodian and bounded powers; owner and deadline; applicable hold; who can actually stop this use today

A4 Timing and readiness

Rules rather than role names.

Field	Requirement
Response times	Ratification period for emergency action; ratification of protective interim status; period for submitting reopen triggers; fallback and escalation if a deadline is missed
Cumulation	Register owner, cadence, review window and organisation-specific aggregation prompt; no universal numeric threshold
Readiness and access	For each readiness question in §4 record yes, or gap/owner/date. Complete G before external sharing. Confirm access to specialists, source references and version history

Appendix B. AI Change Event Sheet - Part 1

R0 uses the mapped short record rather than duplicating all blocks. Part 1 establishes the signal, baseline, proposed or observed delta and route.

B1 Event identity

Core record for every event.

Field	Requirement
Event	Event ID; short name; opened date; current record version; method edition; mode; operating format
Scope and ownership	Legal entity; named workflow/system; event owner; system owner; consequence owner; Authority Map reference
System identifiers	Inventory ID; provider/model version or alias; environment/cohort/market; configuration/prompt/policy reference; technical change/release ID
Links and boundary	Related Event IDs; parent ID or none; external tier/H reference where applicable

B2 Signal and intake

Record what became visible before judging significance.

Field	Requirement
Signal	What became visible; source/channel; date received; intake distinction: Signal, Verified change, Incident, Risk interpretation or Governance trigger
Evidence	Reference; source/effective/inspection dates where different; statement type; evidence quality; limits
Intake disposition	New event, linked event, duplicate or cancelled candidate; reason and related record. Cancellation needs owner and second-person confirmation

B3 Baseline

An observed historic practice is not evidence of approval.

Field	Requirement
Status	approved / conditionally approved / reconstructed from an evidenced approval / no prior approval identified / approval contested / unable to determine
Approved state	Purpose/use; model/provider/platform; data; people/scale/geography; permissions; human review; conditions and review dates

Field	Requirement
Approval evidence	Decision and authority references; dates/versions; evidence quality; unresolved limits. Where no approval is identified, state first-authorisation or containment branch

B4 Delta and timing

Separate a verified proposal from implemented change.

Field	Requirement
Change	What differs from the baseline; proposed or observed; effective date or planned date; candidate/verified status and who checked it
Support	Specific proposition supported; evidence references, qualities and limitations; later implementation evidence belongs in C6/C8
Earlier period	Did it operate before assessment? If yes, complete C18; otherwise state the basis

B5 Classification

Screen the taxonomy without forcing a single label.

Field	Requirement
Classes	All relevant C1-C10 classes; primary class and rationale if used in the register
Descriptors	Reality; timing; reversibility; observability; contained/cross-functional/cross-organisational; single/cumulative/coupled; routine/exception/emergency/externally forced; known/uncertain/contested

B6 Materiality review

Screen M1-M12 and repeat for each touched lens.

Field	Requirement
Lens and comparison	Lens; baseline/status; verified delta; evidence and quality
Judgement	Uncertainty/disagreement; specialist question or none; does earlier approval apply and why; dissent
Other lenses	Record why remaining lenses do not change the route. R0 may use one concise scoped screening record

B7 Triggers boundary and route

Trigger first, exemption second, route third.

Field	Requirement
Triggers	Numbers 1-15 identified; rationale/evidence; exclusions or none. Do not delete an identified trigger after an exemption
Boundary invocation	Exemption invoked yes/no; F Boundary ID/version/expiry; within-scope evidence; excluded triggers checked; applicability confirmer, mandate and date
Route	Proposed route with full label; proposer/date; confirmed route; confirmer/mandate/date; basis under §6.4.4; dissent; C12 history reference

B8 Legal triage

Core screening with conditional specialist input.

Field	Requirement
Triage	No legal signal identified / Legal input required / Triage unresolved; screener/date; scope, sources considered and reason
Legal input	Not required / pending / preliminary / received / contested / unavailable; question, qualified owner, due date and C4 reference when required
Use and change	How advice affects the decision; limitations; re-screen trigger. Preserve original escalation reason after input arrives

B9 Parallel responses

These processes must not wait for ACAR.

Field	Requirement
Response check	Applicable incident, security, privacy, safety, employment, customer-remediation or regulatory processes; or reason none is activated
Active processes	For each: process/record ID, owner, deadline, required action and status; cross-reference existing record

B10 Evidence record

Repeat for each substantive proposition or reference.

Field	Requirement
Identity and access	Evidence ID; repository; source document/record ID; owner; source date/version; inspection date; access limits

Field	Requirement
Proposition	Exactly what the item supports; statement type: Fact / Specialist conclusion / Assumption / Risk interpretation / Decision
Provenance	D Direct and contemporaneous / C Corroborated / R Reconstructed / A Asserted / U Unavailable or contested; independent supports if C; limitations; simulation marker where applicable

Appendix C. AI Change Event Sheet - Part 2

Part 2 carries the same Event ID and records authority, decision, action and closure. Section 10.4 controls applicability. C13-C15 and C17-C19 are conditional; C16 is completed for every route.

C1 Part 2 record control

Part 2 always carries its own Event ID.

Field	Requirement
Identity	Event ID; short name; link to Part 1; current version; method edition
History	Supersedes; created by/at; changed by/at; reason; authoritative record location; preserve previous versions

C2 Authority for this event

Evidence authority for the actual scope.

Field	Requirement
Formal authority	Name/forum; mandate and evidence; scope, powers and limits
Actual authority	Name/forum; ability to require action/resources/stop use; evidence and limits; split powers and commitments
Delegate or succession	Delegate basis or none; substitute by decision type; C15 if authority changed or is vacant; conflicts/recusals

C3 Interim operating status

Separate from the review route and final outcome.

Field	Requirement
Permission and scope	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend; affected scope; approved baseline reference
Authority and timing	Decider or protective-action actor; mandate; reason; date/effective time; expiry/review date; ratification status if needed
Open work	Owner of missing facts; conditions; lapse consequence; escalation/reopen trigger; C7 and C12 references

C4 Specialist input

Repeat only for identified specialist questions.

Field	Requirement
Question and owner	Precise question; specialist name/function; qualification or demonstrated expertise; independence or disclosed interest; domain limits
Input and status	Dated/versioned conclusion; assumptions, uncertainty, dissent and limitations; confirmed/preliminary/unavailable/contested; evidence reference and quality
Decision use	How authority incorporated, rejected or conditioned the input; unresolved issue/hold; for legal questions keep the separate B8 input status

C5 Final decision

Set closure criteria at decision time.

Field	Requirement
Options	Feasible options including non-AI alternative where relevant; evidence of external constraints and deadlines; reason options were excluded
Outcome and authority	O0 Continue / O1 Continue with conditions / O2 Restrict / O3 Pause / O4 Suspend / O5 Transition / O6 Exit; actual authority or authorised delegate; decision/effective date; mandate/reference
Rationale and limits	Reason; conditions; restrictions; uncertainty; dissent; temporary measures; no silent widening of scope
Completion plan	Closure types and criteria; action/condition owners; review dates; incoming linked Event ID for O5/O6 replacement; C8 reference

C6 Actions and dependencies

Repeat one record per action or use workbook Actions.

Field	Requirement
Action	Action ID and Event ID; concrete action; one accountable owner; dependencies with their owners; due date
Evidence and verification	Planned evidence; actual evidence ID/quality and completion date; verifier; confirmation and limitations; self-verification exception and compensating check if used
Status	Not started / In progress / Ready for verification / Verified / Superseded; replacement decision reference if superseded

C7 Open issues and holds

Repeat one record per unresolved issue or use workbook Holds.

Field	Requirement
Issue	Hold ID and Event ID; evidence pending / specialist input pending / authority pending / reopen decision pending; precise issue
Response	Owner; due date; interim reference; lapse consequence; escalation route
Resolution	Open / Resolved / Transferred to condition; resolution or condition reference; who confirmed it and when. Preserve other active holds

C8 Closure

Apply §10.4 for the confirmed route.

Field	Requirement
Criteria	Closure type(s); criteria set at decision time and reference; route-specific floor applied
Evidence	Evidence IDs and qualities; what each confirms; evidence status: not defined / defined / partial / complete / contested; missing or contested support
Verification	Named reviewer/authorised confirmer; date; authority basis; action-owner separation or documented exception; limitations
Remaining conditions	Holds resolved or explicitly transferred; ongoing conditions, owners and dates; C9 people assessment/screen; C10 learning and standing or event-specific review reference

C9 People and downstream consequences

R0/R1 may use the short screen where no relevant issue is identified.

Field	Requirement
People screen	Who was or may have been affected; basis for no further assessment if applicable; screener and date
Assessment	Notification/explanation; correction/appeal/redress/remediation; language/accessibility needs; owner/date; completion evidence; or named not-applicable rationale
Status	complete / pending / not applicable with rationale / unavailable / contested; related C18 or parallel-process reference

C10 Review recurrence and learning

R0 may reference standing cumulation review.

Field	Requirement
Review	Event-level or standing review; named owner; date/cadence; evidence source and question; recurrence window
Reopen	Thresholds/triggers; submission route and timing; substitute if authority unavailable
Learning	Finding retained; standing-process/Authority Map/boundary/template change; action owner and reference

C11 Current state

Six distinct axes; holds are a set.

Field	Requirement
Workflow and operation	workflow_phase; operating_state; explicit references supporting each
Holds and disposition	All active Hold IDs and reasons, or none; active/cancelled and reason/reference
Outcome and mode	Final outcome code and full label or not yet decided; canonical mode; next action owner and due date

C12 Transition history

Append one entry per change or use workbook History.

Field	Requirement
Transition	Transition ID; Event ID; field/axis; from value; to value; recorded date/time and effective time if different
Decision trail	Actor/proposer; confirmer where required; mandate/evidence reference; reason; dissent/limitation; resulting record version

C13 Reopen review

Conditional on a new challenge to earlier closure.

Field	Requirement
Trigger	Reason and evidence; submitter/date; earlier closed Event ID/version; new review record/version and link

Field	Requirement
Current protection	Interim status; valid authority or substitute; new decision point/due date; pending hold; affected actions/conditions/evidence
Decision	Reopen or retain closure and why; authority and dated reference; new version; preserved historical record

C14 Emergency action

Conditional; act before full framing where necessary.

Field	Requirement
Activation	Urgency and declaration criterion; actor; emergency/substitute authority or fail-safe basis; available facts and specialist inputs
Protection	Canonical interim status and restrictions; parallel processes/owners/deadlines; action owner and implementation evidence
Return to authority	Expiry/review; ratification deadline/status/fallback; evidence-preservation/legal-hold question; full retrospective review deadline; later formal decision and learning

C15 Authority succession or vacancy

Conditional; successor cannot confirm their own mandate.

Field	Requirement
Prior state	Why mandate ended/unavailable; last valid decision/conditions; affected events/actions/verification duties
New authority	Appointing/superior authority; successor mandate and D/C evidence; custodian and bounded powers; quorum/veto/recusal/deadlock
Transfer	Owner/verifier transfer date; new assignments and acknowledgement; overdue-gap hold; dated append-only transition

C16 Ten trace statuses

Complete for every route; use references instead of duplicate narratives.

Field	Requirement
Trace status record	For each of the ten elements: completed / pending / not required with rationale / unavailable / contested / not within this trace; reference or rationale; owner/date for open work

Trace element	Required record
1 Candidate signal	Record status and source, or rationale for not required; owner/date for outstanding work.
2 Intake and classification	Record status and source, or rationale for not required; owner/date for outstanding work.
3 Ownership	Record status and source, or rationale for not required; owner/date for outstanding work.
4 Specialist inputs	Record status and source, or rationale for not required; owner/date for outstanding work.
5 Actual decision authority	Record status and source, or rationale for not required; owner/date for outstanding work.
6 Decision	Record status and source, or rationale for not required; owner/date for outstanding work.
7 Changed practice or system	Record status and source, or rationale for not required; owner/date for outstanding work.
8 Corrective-action ownership	Record status and source, or rationale for not required; owner/date for outstanding work.
9 Evidence of completion	Record status and source, or rationale for not required; owner/date for outstanding work.
10 Recurrence and learning	Record status and source, or rationale for not required; owner/date for outstanding work.

C17 Method deviation

Conditional; a valid boundary invocation is not a deviation.

Field	Requirement
Departure	Rule departed from; authority; reason; evidence; scope and limitations; do not waive protected gates
Control	Temporary measures; expiry; reopen trigger; method edition; facilitator intervention and conflict record where relevant

C18 Earlier unassessed operation

Conditional on a change operating before assessment.

Field	Requirement
Period	Earliest supported start; latest possible start; end or open; evidence quality and limits

Field	Requirement
Lookback	Affected scope/population/outputs/decisions; review needed and why; owner; scope; result; notification/correction/remediation questions
Current position	Interim operation; evidence; linked C10 notification-failure event if needed; ongoing owner and date

C19 Experiment or parallel variant

Conditional on experimentation.

Field	Requirement
Boundary	Allocation logic; duration; exposed population/workflow/transactions; permitted data and permissions
Conditions	Success/stop/harm thresholds; monitoring sources; owner; actual authority; interim status; end decision point; F reference if within standing experiment boundary

Appendix D. Closure & Learning Supplement

Use D where more space is needed. The companion templates also supply G and H for the data-handling and external-handoff rules already required by the guide.

D Closure and learning supplement

Optional extra space; same Event ID and field identifiers.

Field	Requirement
Control	Event ID; supplement date; version; supersedes; C6/C8/C9/C10 references
Additional records	Repeat the applicable action, condition, evidence, remediation or learning blocks; retain IDs and owners. Do not create a second independent decision record

G Record Ownership and Data Schedule

Complete before facilitated information sharing.

Field	Requirement
Parties and records	Participating legal entities; scopes; organisational source evidence, event records and facilitator working records; owner for each class
Access and location	System of record; access permissions; evidence-reference practice; external working-copy boundary; approved case-specific transfer channel
Retention and return	Retention/deletion rule for each class; legal-hold exception; what remains with each external party; return/deletion confirmation and owner/date
Incidents	Case-specific breach/incident/security route, contacts and deadlines under applicable organisational arrangements; feedback mailbox is not a case-evidence channel

H External Handoff Record

Conditional on a cross-entity event; distinct from F.

Field	Requirement
Scope and tier	Event ID; external entity; full linked external trace / internal boundary evidence only / external decision or evidence unavailable; external event ID where accessible
Authority and notice	External authority if known; notice/threshold; evidence; external decision deadline

Field	Requirement
Leverage and handoff	Contractual and practical leverage; handoff owner/evidence; subprocessor/downstream depth known; constraints including multi-tenant limits
Visibility	Unavailable fields, attempts to obtain them, access limits and supported conclusion; internal interim decision/owner/date

Appendix E. Event Register field specification

The workbook is a portfolio index and working log. Detailed questions and rationales remain in the linked event record. The table below defines the storage location so users can preserve complete coverage without repeating every narrative in a very wide spreadsheet.

Content	Location	Rule
Event ID and short name	Events	Unique ID and plain-language description.
Scope, entity and inventory ID	Events; B1	Named workflow and internal entity. B1 holds model, environment, configuration and release identifiers.
Event, system and consequence owners	Events for event owner; B1/A for other roles	Named people; reference the current authority map.
Baseline status	Events; B3	Use canonical baseline labels with approval/source reference in B3.
Taxonomy, linked and parent events	Events; B5/B1	Primary class C1-C10; all other applicable classes retained as secondary. No scoring.
Route and route confirmation	Events; B7/C12	Full R0-R3 labels. Proposer, confirmer, authority and dates in B7/history.
Interim operating status	Events; C3	Canonical status; conditions, ratification, expiry, lapse and history remain in C3/C12.
Workflow, operating state, outcome, mode and disposition	Events; C11	Separate axes. Outcome empty until decided. Full names accompany codes.
Active holds	Holds; Events count; C7	One row per concurrent issue with stable Hold ID; reason, owner, due date, consequence and resolution reference. Zero only means no recorded active hold.
Formal and actual authority	Events for actual authority; C2 for both	Mandate/evidence, role separation, delegation and successor limits remain visible in C2.
Legal triage and input status	Events; B8/C4	Screener/date/reason required. Qualified legal owner only when input is required; original trigger retained.
Boundary invocation	B7/F; Field Guide	Yes/no, Boundary ID/version, trigger, evidence and authorised applicability confirmer/date.
External entity/tier/deadline	B1/H; Field Guide	Use the distinct External Handoff Record; no external approval inferred.
Parallel responses	B9; Field Guide	Activated process, owner, deadline and record reference, or scoped reason none is activated.

Content	Location	Rule
Actions and due dates	Actions; Events next action; C6	Owner, dependencies, evidence and verifier; closure does not follow automatically from a status choice.
Closure types and evidence	Events; C8/B10	Type, evidence status/quality/reference; scope and limitations; authorised confirmation and date.
Affected-person screen/assessment	C9; Field Guide	Complete/pending/not applicable with rationale/unavailable/contested. Full assessment conditional under §10.4.
Review, recurrence and reopen	Events next review; C10/C13	Standing cadence for eligible R0; event-specific owner/date for other routes; preserve historical closure.
Record control	Events; C1/History	Current version, supersedes, actor/timestamps, reason and method edition.
Transition history	History; C12	Append-only discipline: field, from/to, time, actor, authority, reason and resulting version.
Publication clearance	Separate optional disclosure record	Only when external disclosure is planned; applicable authority/process supplies clearance. Not an event-completion requirement.

The blank Event Register is ready for organisational records. The Example Register is separately labelled Simulation / tabletop and must not be represented as operational use. Both have controlled lists, filters and editable record areas. Formulas show missing evidence, due work or incompatible entries; they do not judge evidence quality or authorise closure. A neutral or blank formula result is not proof that all method requirements are met.

Workbook history is a user-maintained record, not a tamper-proof audit log. Keep the workbook in the designated version-controlled system, preserve earlier versions and record transitions. The prepared capacity is 200 events, 500 holds, 500 actions and 1,000 history rows. Extension instructions are in the workbook; the count ranges and validations must be extended together.

Appendix F. Boundary Record

A controlled record for the Pre-authorised Change Boundary under §6.4.1 and each invocation. It must not be confused with H, the External Handoff Record.

F1 Pre-authorised Change Boundary

Standing authorisation with an expiry or review date.

Field	Requirement
Identity and scope	Boundary ID/version; owner; operating scope; underlying approved baseline; creation/review/expiry dates
Permission	Permitted C classes and magnitude; triggers expressly covered; required checks/evidence; permitted minimum route
Exclusions	Non-delegable triggers and other excluded changes; no waiver of credible legal questions, material disagreement or emergency review
Authority	Actual authority establishing it; decision/mandate evidence; authorised applicability confirmer and limits; conditions for R0 O0 confirmation

F2 Boundary invocation

Repeat for every event relying on the boundary.

Field	Requirement
Event and check	Event ID/date; Boundary ID/version; trigger identified; evidence within permitted class and magnitude; checks for exclusions/expiry
Confirmation	Applicability confirmer and delegation; date; permitted route and rationale; implementation verification; overrun/re-route record if applicable