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

22 August 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.

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.

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

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

Complete the Authority Map before the first event and review it when roles, governance forums, systems, providers, operating scopes 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.

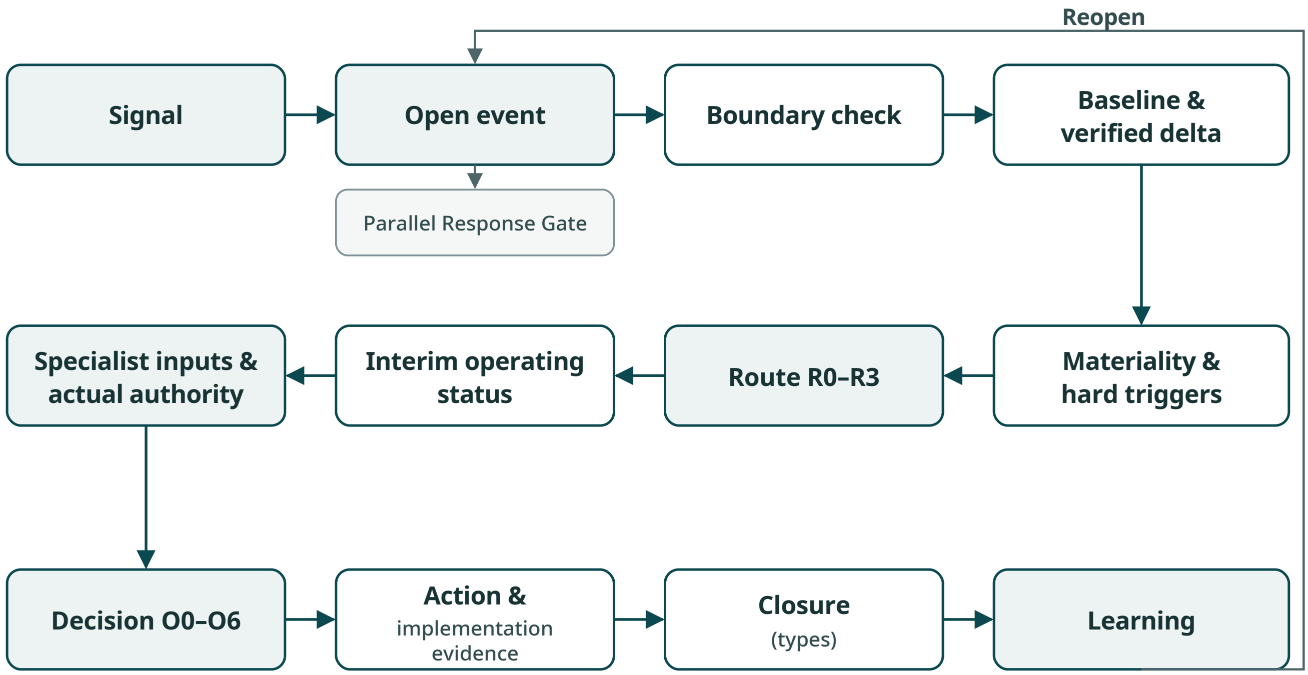
Readiness self-check

Before the first event, answer **yes** or record a remediation owner and date.

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 (§11.4.1) complete for 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



1. **Open the trace.** Create an Event ID, record the candidate signal without pre-judging materiality, assign the event owner and activate any parallel incident, security, privacy, safety, employment, customer-remediation or regulatory processes.
2. **Set the boundary.** Name the operating scope, legal entity or cross-boundary tier, system owner, consequence owner and event owner.
3. **Establish the baseline.** Select one baseline status and record the evidence. Reconstructed actual use is not an approval.
4. **Verify the delta.** Confirm the change with D or C evidence, or keep it as a candidate signal. Apply all applicable taxonomy classes and descriptors; link related events.
5. **Review materiality and triggers.** Record each touched lens, the verified delta, evidence, uncertainty, specialist input, applicability of earlier approval and dissent.
6. **Propose and confirm the route.** The event owner or triage owner proposes the minimum route. The actual authority or routing authority confirms it; a disputed route goes to the escalation forum.
7. **Make the interim explicit.** Where the actual authority is not yet confirmed, the triage owner may impose a protective interim status, subject to mandatory ratification. Record the expiry or review date and the consequence of lapse.
8. **Obtain inputs and decide.** Record qualified specialist inputs, actual authority, constrained options, final outcome, rationale, conditions, dissent, external deadlines and closure criteria.
9. **Assign and evidence action.** Name one owner per action, dependencies, due date, implementation evidence and per-action verifier.
10. **Close, reopen or keep open consciously.** Name the closure type, affected-person assessment, verifier and recurrence window. Reopen by transition action when a trigger arises; preserve the earlier record.

Two worked illustrations of these steps, both fictional, are set out in §13.

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 it with evidence of quality D or C; on A or R alone it remains a candidate signal.

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.
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?
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.

Appendix F provides the Boundary Record template.

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.

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.

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 the Legal Escalation Flag 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.
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 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.

Every interim record requires:

- 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.

Code	Governance outcome	Meaning
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 the Legal Escalation Flag, 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 Escalation Flag

Record one of:

- **legal escalation required**;
- **legal escalation not required**;
- **legal escalation unresolved**.

Use the flag where the event may affect substantial modification, legal role, regulatory classification, rights, sectoral obligations, contract or another legal question.

The trace records:

- the legal question;
- the qualified legal owner;
- the input, date, scope and limitations;
- how the input affected the governance decision.

Only a qualified legal owner may set the flag to 'legal escalation not required'. Until then, a credible question keeps the flag 'unresolved'. 'Not required' records the owner, date and a brief rationale.

The method does not convert a legal input into its own legal conclusion. Organisational materiality and legal qualification remain separate.

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

The decision record contains:

- 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.

Field	Required discipline
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, requirements and proportional floors

Every closure statement names one or more closure types:

Closure type	What must be shown
implementation	The required action or configuration was carried out in practice.
condition	A continuing condition, restriction, threshold, monitoring duty or review date is operating and owned.
outcome-confirmation	The required operational state or decision outcome was observed or otherwise evidenced.
remediation	Consequences for affected people, users, customers, staff, records or downstream decisions were identified and addressed.
residual-risk acceptance	The actual authority consciously accepted a defined residual uncertainty or consequence within a named scope, with rationale, owner and review date.

An event can close only when:

- the decision has been implemented, or formally replaced by a new decision;
- required actions meet the closure criteria defined at decision time;
- evidence is labelled and reviewed;
- the closure verifier records confirmation and limitations;
- open uncertainty is closed or converted into an explicit continuing condition or residual-risk acceptance with an owner and date;
- the affected-person assessment is completed;
- an event-specific recurrence window and learning owner are recorded.

Affected-person assessment

Record:

- whether any person, group, customer, worker or user was or may have been affected;
- whether notification, explanation, correction, appeal, redress or remediation is required;
- the owner and date for each action;
- language and accessibility needs where relevant;
- evidence of completion;
- **not applicable** only with a named owner and rationale.

Proportional closure floor by route

Route	Minimum closure floor
R0	Verified delta, documented rationale that the earlier decision basis remains applicable, named owner and O0 **Continue**.
R1	Monitoring result, threshold or review-date assessment, named owner and an O0 **Continue** or O1 **Continue with conditions** decision. Otherwise the route is raised.
R2	Full decision and action record for the specialist question, implementation evidence, applicable closure types, affected-person assessment and verifier.
R3	Full §10.4 closure record, including authority, decision implementation, conditions, affected-person assessment, closure evidence, verifier and recurrence review.

An incident, unauthorised or unassessed operation period, or event with possible downstream consequences may require **remediation** and **outcome-confirmation** even where the immediate technical cause was fixed.

Closure is not

Administrative signal	Why it is insufficient
Email sent	Does not show that practice or system behaviour changed.
Ticket closed	May show workflow completion, not that the governance condition was satisfied.
Action assigned	Shows ownership, not implementation.
Policy updated	Does not show that the update reached the affected workflow or was applied.
Meeting held	Does not show that the decision was authorised, implemented or verified.

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, hold_reason is **reopen decision pending** and an explicit interim operating status is recorded.

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.

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.

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.
- Apply the statement-type tag F / SC / A / RI / D separately from the evidence-quality label D / C / R / A / U.

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 method text date 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.

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.

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
hold_reason	none / evidence pending / specialist input pending / authority pending / reopen decision pending
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	Applicable route floor met, closure types named, evidence reviewed, affected-person assessment completed, verifier record and recurrence owner/date.
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.
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.
outcome	O1	Actual-authority decision to **Continue with conditions**, with conditions, owners, evidence and review dates.

Axis	Value	Minimum record required
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; where the baseline rests only on R, A or U evidence, apply the restriction in §5.2.
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 Escalation Flag;
- 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 through authority, decision, action, closure and learning. 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;
- record version, supersedes, 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 Escalation Flag, legal owner and rationale where applicable;
- action due date;
- closure type;
- closure evidence status and quality;
- recurrence or reopen status;
- record version and supersedes;
- method text date;
- publication clearance.

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.

Blank textual templates are included in Appendices A–D.

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.

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.
boundary record 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.
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.

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**.

Northbank Retail — customer-service assistant, provider update and proposed refund authority

Context and signal

Northbank Retail uses an AI assistant to draft customer-service replies. The baseline status is **approved**. The approved baseline requires a human agent to approve every reply and every refund.

The provider announces a model update. At the same time, the product team proposes allowing the assistant to issue refunds automatically, connecting it to the payment connector and customer-service platform, expanding the workflow into a second market and replacing universal review with sampled review.

The provider notice is recorded as a **Signal** with statement tag F and evidence quality D. The dated product change request, configuration proposal and interface specification verify the planned delta with statement tag F and evidence quality D.

Intake and classification

- Event ID: NBR-SIM-001.
- Mode: **Simulation / tabletop**.
- Reality: simulated.
- Timing: prospective.
- Relationship: coupled.
- Boundary: cross-functional.
- Reversibility: partly reversible.
- Observability: partly observable.
- Operating condition: routine.
- Knowledge: uncertain.
- Baseline status: **approved**.
- Taxonomy: C1 **Model, version or capability 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**; C8 **Integration-channel or external-system change**.
- C8 integration basis: the proposed payment connector and customer-service platform integration would enable the assistant to execute rather than merely draft a refund action.
- Linked event IDs: none at intake.
- External decision deadline: provider update date and planned second-market launch date, each recorded separately.

Materiality and hard triggers

The touched lenses are:

- M1 — the model and action capability may change;
- M2 — the assistant would move from drafting to executing a refund workflow;
- M3 — the system would execute a financial consequence;
- M4 — a second market and new language would be affected;
- M5 — payment data, customer data, processing, retention and access assumptions require review;
- M6 — the assistant would receive transaction authority and connector access;
- M7 — universal human approval would become sampled review, requiring competence, workload and override analysis;
- M8 — provider and connector dependencies would change;
- M9 — rollback and transaction reversal require evidence;
- M10 — logging must show the model, decision, refund action and human intervention;
- M11 — consumer, payment, data-protection and role questions require qualified input;
- M12 — the provider update, new integration, new market and human-review change are coupled.

Hard triggers engaged are 1, 2, 3, 4, 5, 6, 8, 10, 11 and 13. Triggers 14 and 15 are not engaged.

The event owner proposes R3 **Formal reauthorisation**. The COO-led product-risk forum, recorded as routing authority and actual authority, confirms the route. The route-history entry is D-labelled because it is represented by a dated forum decision record in the fictional scenario.

Interim operating status

The interim operating status is **Pause** for the proposed expanded workflow. The existing assistant continues under its approved baseline, with universal human approval, while technical, privacy, legal and operations inputs are completed.

The interim record states:

- authority: COO-led product-risk forum;
- reason: the proposed transaction authority and human-review change require R3;
- review date: four weeks before the planned launch date;
- owner of missing facts: product-risk lead;
- consequence of lapse: the proposed expanded workflow remains **Paused** and the missed date becomes an open governance finding;
- escalation trigger: inability to evidence logging, reviewer capacity or refund reversal.

Specialist inputs

Question	Qualified owner	Input	Status and date	Use in decision
Behaviour, logging, failure modes and rollback	Technical specialist	SC: scoped evaluation with assumptions and failure limits	confirmed; dated	Conditions the cap, logging, rollback and stabilisation review.
Data use, retention and second-market processing	Privacy specialist	SC: scoped data-protection assessment; no method-level legal conclusion	confirmed; dated	Conditions data fields, retention, access and second-market launch.
Consumer and payment requirements	Qualified legal owner	SC: scoped legal input with jurisdiction and product limits	confirmed; dated	Legal Escalation Flag remains **legal escalation required** until the forum records the decision.
Exception handling, reviewer competence, language capacity and workload	Operations and human-factors specialists	SC: capacity and oversight assessment	confirmed; dated	Conditions universal review period, reviewer training, override and appeal arrangements.

The qualification test is recorded for each specialist. The provider's documentation is treated as an input, not as independent proof that oversight will work under Northbank Retail's workload.

Actual authority and decision

The Organisation Authority Map records evidence that a COO-led product-risk forum has formal authority and actual authority to approve, condition, restrict, pause, suspend or require transition for this workflow. The authority evidence is D-labelled in the fictional scenario because it consists of a dated charter and a dated decision record.

The forum decides O1 **Continue with conditions** for the expanded workflow:

- automated refunds capped at EUR 30;
- one market only during the initial period;
- human confirmation for every refund for four weeks;
- full logging and daily exception review;
- defined complaint, reversal and error thresholds;
- reviewer competence, language coverage and workload limits;
- a customer challenge and correction route;
- formal review after four weeks;
- automatic reopen submission if the cap, logging, reviewer-capacity or complaint threshold is breached.

The options record includes O0–O6 and explains why O0 **Continue** without conditions is not selected. The second-market launch remains outside the authorised scope and, if pursued, opens a linked candidate event.

Action and closure

Product owns the configuration change. Operations owns the exception and reviewer process. Data engineering owns logging. Customer operations owns the affected-person correction and appeal route. A manager outside those action owners verifies closure.

Closure types are **implementation**, **condition** and **outcome-confirmation**. **Remediation** is held ready if any affected transaction requires correction. **Residual-risk acceptance** is not used.

Closure requires:

- configuration record — statement tag F, evidence quality D;
- technical test summary — statement tag SC, evidence quality D;
- staff operating instruction — statement tag F, evidence quality D;
- reviewer competence and language-coverage record — statement tag F, evidence quality D;
- four weeks of transaction, override, complaint and reversal evidence — statement tag F, evidence quality D;
- affected-person assessment and evidence of any correction or appeal action — statement tag F, evidence quality D;
- closure-verifier record — statement tag D, evidence quality D.

A C-labelled verifier proposition would require two genuinely independent supports. A manager's statement and the manager's own downstream summary would not be independent.

Six-axis state at closure

Axis	Value
workflow_phase	Closed
operating_state	Operating under conditions or restrictions
hold_reason	none
record_disposition	active
outcome	O1
mode	Simulation / tabletop

Learning

The Authority Map is updated to name the forum that controls transaction authority. Provider notices are routed to the governance owner in parallel with engineering. A future proposal to remove universal human confirmation becomes a linked event rather than an unrecorded implementation change.

Boundary. The method connects qualified inputs and organisational authority. It does not decide whether the model is technically adequate or whether the arrangement is legally sufficient.

Northbank Retail — routine model patch within a Pre-authorised Change Boundary

Context and signal

Northbank Retail operates an internal knowledge assistant that retrieves approved policy documents and drafts non-binding internal answers. Its baseline status is **conditionally approved**. A Boundary Record authorises routine provider model patches within the same model family where there is no change to intended use, data sources, permissions, human review, actual authority or external action.

The provider issues a routine patch notice. The event owner opens NBR-SIM-002 and records the notice as a **Signal**, statement tag F, evidence quality D.

Boundary test and verified delta

The event owner verifies the delta through the provider notice and a separate internal deployment record. The evidence is C because the two records originate from independent sources and do not share one upstream record for the deployment fact.

The Boundary Record is current and contains:

- operating scope: internal knowledge assistant;
- permitted class: C1 **Model, version or capability change** within the same family;
- permitted magnitude: patch-level change with no new tools, data, permissions, routing or modality;
- excluded triggers: intended or actual use, transaction authority, material weakening of human oversight and change of actual authority, plus any other hard trigger not expressly permitted;
- actual authority: Head of Internal Operations;
- evidence basis: provider notice plus internal deployment and smoke-test records;
- expiry: quarterly review date;
- owner, version and Boundary Record ID.

Exemption invoked: **yes**. Boundary Record ID and evidence are recorded on the Event Sheet.

Classification and route

- Taxonomy: C1 **Model, version or capability change**.
- Descriptors: simulated; prospective; reversible; observable; contained; single; routine; known.
- Materiality lenses: M1, M9 and M10.
- Hard triggers: none after the boundary test.
- Route proposed by: event owner.
- Route confirmed by: routing authority named in the Boundary Record.
- Review route: R0 **Documentation only**.
- Interim operating status: **No interim change required**.

The R0 record states why the verified delta does not alter the basis of the earlier decision. If any smoke test, user signal or internal deployment record suggested changed routing, data, permission, human review or actual use, the boundary would not apply and the route would be raised.

Decision, action and closure

The actual authority records O0 **Continue**.

The action is to deploy the patch within the approved maintenance window. The implementation owner records the deployment reference and smoke-test result. The closure type is **implementation**.

The R0 closure floor is met through:

- verified delta — evidence quality C;
- rationale that the earlier decision basis remains applicable — statement tag RI, recorded by the event owner and confirmed by the routing authority;
- named owner;
- deployment evidence — evidence quality D;
- O0 **Continue**.

Six-axis state at closure

Axis	Value
workflow_phase	Closed
operating_state	Operating under approved baseline
hold_reason	none
record_disposition	active
outcome	O0
mode	Simulation / tabletop

Learning

The event remains available for the register-and-learning owner's cumulation review. A pattern of repeated R0 patches, complaints or performance signals may create a parent event under M12 even though each patch was individually within the Boundary Record.

14. Assumptions, limitations, status, licence and citation

14.1 Assumptions and limitations

Limitation	Consequence
Signal visibility	The method governs events that reach intake. It does not, by itself, detect changes that are never reported or surfaced. Detection controls — reconciliation with technical change sources, provider feeds and coverage checks — are the organisation's responsibility; they lie outside the method.
Event granularity	The method processes discrete candidate events. Continuous, high-frequency or one-to-many provider changes are handled through linked and parent events; a fuller model for continuous and mass change is outside this guide.
Access	It depends on access to actual authority, decision records and proportionate evidence.
Specialist quality	It does not improve the substantive quality of legal, technical or other specialist conclusions.
Decision quality	A complete record does not prove that the decision was optimal, safe, fair or compliant.
Organisational specificity	Authority, conditions and closure evidence are organisation-specific; standardisation has limits.
Administrative burden	The trace must remain proportionate. Over-documentation can obscure the decision.
Transferability	Application in one context does not establish general effectiveness, self-use feasibility or transferability.
Organisation-run readiness	Organisation-run use remains untested until the organisation documents and operates the prerequisites in the Readiness self-check.
Cross-boundary visibility	Conclusions are limited by access, contractual flow-down, external authority and evidence tier.

14.2 Relationship to established frameworks

The method is designed as an event-level organisational process layer. It is intended to be mapped to established frameworks and legal requirements, as applicable from time to time, not to compete with or replace them.

The coverage label in each row means:

- **directly operationalised** — the method contains a concrete organisation-side process for the named function;
- **partially supported** — the method supports part of the function but does not contain every required substantive or technical element;
- **requires external input or process** — a qualified specialist or separate organisational process is necessary;
- **out of scope** — the function is expressly excluded from the method.

RuleBridge element	Relevant hook	Coverage	Relationship	Limitation
Actual authority, roles and organisational accountability	OECD AI Principles on accountability, role, context and ability to act; NIST AI RMF GOVERN 2.1, 2.3 and 3.2.	directly operationalised	Provides an organisation-side process for naming formal and actual authority, recording decisions and preserving succession.	Does not determine whether an OECD principle or legal requirement is satisfied.
Human oversight, intervention and affected-person routes	OECD AI Principles on human agency and oversight; Regulation (EU) 2024/1689, including relevant human-oversight provisions.	partially supported	Records competence, training, authority, interpretation, automation-bias questions, disregard/override/reverse powers, provider-information sufficiency, workload feasibility, appeal and redress.	Requires qualified legal, technical, human-factors and domain input; does not test compliance or substantive oversight effectiveness.
Traceability and evidence	OECD AI Principles on lifecycle traceability; OECD Due Diligence Guidance steps on tracking implementation and results.	partially supported	Structures event-level records from signal through closure and learning.	Not a technical traceability, model-documentation or assurance system.

RuleBridge element	Relevant hook	Coverage	Relationship	Limitation
Change, incident, monitoring and decommissioning	NIST AI RMF GOVERN 1.5 and 1.7; MANAGE 4.1–4.3; NIST AI 800-4. MANAGE 4.1 expressly includes change management alongside incident, recovery and decommissioning concerns.	directly operationalised	Connects a visible signal to organisational review, authority, action, evidence and closure.	Does not replace technical monitoring, incident response or validation of monitoring methods.
Third-party, provider and dependency change	NIST AI RMF GOVERN 6 and MANAGE 3; OECD Due Diligence Guidance on co-operation and action across the AI value chain.	partially supported	Provides a cross-boundary process for organisational ownership, notice, leverage, handoff and evidence tier.	Does not replace TPRM, contracting, cybersecurity, supplier assessment or technical due diligence.
Data-basis, privacy and security change	Regulation (EU) 2016/679; M5 and C3 in this method.	requires external input or process	Provides an organisational process layer for recording a data-basis change and routing it to qualified data-protection and security assessment.	Does not make a data-protection, security or compliance conclusion.
Legal role, regulatory classification and lifecycle context	Regulation (EU) 2024/1689, as applicable from time to time, including relevant actor-role, deployer-duty, human-oversight and post-market provisions.	requires external input or process	Provides a record relevant to implementation and escalation.	Qualified legal and technical assessment remains necessary; no legal qualification or compliance conclusion.
Technical model evaluation, cybersecurity testing, assurance and certification	Applicable technical, security, audit, assurance and certification methods.	out of scope	The method may reference their results as specialist inputs.	It does not perform or replace them.

Recommended relationship language: **mapped to**; **supports implementation of**; **provides an organisational process layer relevant to**; **should be used alongside qualified legal and technical assessment**.

Selected primary sources

1. OECD (2024), *Recommendation of the Council on Artificial Intelligence / OECD AI Principles*, OECD Legal Instruments, OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
2. OECD (2026), *OECD Due Diligence Guidance for Responsible AI*, OECD Publishing, Paris, DOI: 10.1787/41671712-en. 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. NIST (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 laying down harmonised rules on artificial intelligence, consolidated text at 27 July 2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng
6. European Union, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/eli/reg/2016/679/oj

14.3 Method provenance and responsibility

No-employer-provenance statement

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.

Instrument-level provenance record

Component or change layer	Practitioner contribution	External source or adjacent discipline	Design decision	Generative-AI contribution	Responsibility
Governance Outcome Trace and event-level unit	Practitioner-derived organisational problem framing and method architecture.	OECD, NIST and EU framework hooks mapped in §14.2.	One candidate event traced from signal to closure and learning.	Drafting and structural implementation assistance for this edition (OpenAI ChatGPT and Claude (Anthropic)).	Maja Kurek.
Taxonomy, materiality and hard triggers	Practitioner-derived classification and escalation logic.	Change management, governance, due diligence and lifecycle sources.	Multi-label classification; route separate from outcome; fifteen hard triggers.	Consistency checking and implementation of the author's revisions (OpenAI ChatGPT and Claude (Anthropic)).	Maja Kurek.
Actual authority, interim status and closure	Practitioner-derived focus on practical authority, operating status, implementation and closure evidence.	Organisational governance, incident/ change and due-diligence disciplines.	Formal/actual authority split; six interim labels; closure types; reopen as transition action.	Drafting and cross-reference assistance for this edition (OpenAI ChatGPT and Claude (Anthropic)).	Maja Kurek.

The table records contribution and provenance. It does not transfer authority to a model, facilitator or source.

14.4 Status, licence and citation

Status and claims

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.

It has been tested in the field. In one organisation, with the author facilitating, the method was applied to a real AI change event, reconstructed with the people who held the decision. Actual authority was engaged and mapped, the organisation's existing way of deciding was captured as a comparator, interim operating status was articulated while the decision remained open, and closure criteria were elicited.

The event was a live organisational decision with named owners and real consequences, not a tabletop exercise. The record the application produced set out formal authority and actual authority separately, reconstructed the chronology of the decision across two decision cycles, identified and recorded a linked exception event with its own trace, and left a closure state that was documented rather than assumed.

Organisation-run use and the full decision-to-implementation-to-evidenced-closure chain were not exercised.

The accompanying paper reports the scope, method and evidence: Kurek, M. (2026), Operational Change Is Not Governance Closure: Evidence from a First Field Pilot of AI Change Accountability & Reauthorisation, working paper, 21 August 2026, SSRN, DOI: 10.2139/ssrn.7329378.

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, 22 August 2026. https://rulebridge.eu/instrument

Any corrections to this document are published at the same address.

Contact

Method feedback: office@rulebridge.eu.

Send method feedback or notices of potential functional overlap. Identify:

- — the method text date;
- — the field, section or decision point involved;
- — a generic description of the issue;
- — the mode of use, if relevant.

Do not send case evidence, incidents, confidential information, security-sensitive information or personal data to this address.

Case enquiries

Use only the case-specific channel defined in the engagement's Record Ownership & Data Schedule. The method-feedback email is not a channel for case evidence, incidents, security notifications or personal data.

Glossary and controlled vocabulary

This glossary defines the controlled terms before their first coded use. 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
instrument	The public package consisting of this guide and its templates.
method	The decision logic that takes one candidate event from signal through authority, decision, action, closure evidence and learning.
guide	This guide.
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.
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.

Term	Meaning
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
C8	Integration-channel or external-system change

Code	Canonical class
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
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 Escalation Flag

Use exactly one:

- **legal escalation required**
- **legal escalation not required**
- **legal escalation unresolved**

Evidence-quality labels

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

Statement-type tags

Every substantive record line carries one tag:

Code	Canonical tag
F	fact
SC	specialist conclusion
A	assumption
RI	risk interpretation
D	decision

The statement-type tag and the evidence-quality label are separate fields. The repeated letters **A** and **D** have different meanings in each field and must never be inferred from context alone.

Trace-element status

Use exactly 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**

Term	Controlled values
Closure evidence status	not defined / defined / partial / complete / contested
Affected-person assessment	complete / pending / not applicable with rationale / unavailable / contested
Recurrence / reopen	none / scheduled review / linked trigger / reopen decision pending / reopened by transition action

Six-axis status model

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

- **workflow_phase**
- **operating_state**
- **hold_reason**
- **record_disposition**
- **outcome**
- **mode**

Publication clearance

Use exactly one in the Event Register:

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

The Register records a clearance state supplied by the applicable publication process. It does not create clearance.

Appendix A. Organisation Authority Map

Operating scope: ____
Legal entity / business unit: ______________________________
Last reviewed: _______________ **Next review:** _______________
Cumulation review cadence: _________________________________
Record system: ____

Function	Named person or standing forum	Evidence of mandate / authority	Substitute by decision type / escalation
Signal channels and recipients			
Classification and triage owner			
Event owner			
System owner			
Product owner			
Consequence owner			
Routing authority			
Escalation forum			
Legal input function			
Technical / model input function			
Privacy and data input function			
Cyber / security input function			
Human-factors / domain input function			
Formal authority to continue / condition			
Actual authority to continue / condition			
Formal authority to restrict / pause			
Actual authority to restrict / pause			
Formal authority to suspend			
Actual authority to suspend			
Formal authority to require transition			
Actual authority to require transition			
Formal authority to exit / decommission			
Actual authority to exit / decommission			
Emergency authority			
Fail-safe containment role			
Ratification period for emergency action			
Ratification period for interim status imposed before authority confirmation			
Period for submitting a reopen trigger to actual authority			

Function	Named person or standing forum	Evidence of mandate / authority	Substitute by decision type / escalation
Implementation owner			
Closure verifier			
Register-and-learning owner			
Authority-succession owner			

Substitute instruction. Name substitutes by decision type. A person who may approve routine continuation may not necessarily have authority to suspend, transition, exit or ratify emergency containment.

Authority diagnostic: Who can actually stop this use today?
____

Known authority gaps, vacancies, conflicts or assumptions:
____

Self-hosting signal-channel redesign completed, where applicable: yes / no / not applicable
Owner and evidence reference: ________________________________

Appendix B. AI Change Event Sheet — Part 1

Event, baseline, delta and route

Field	Record
Event ID / short name	
Date opened	
Mode	Prospective live trace / Hybrid reconstruction plus prospective follow-up / Retrospective reconstruction / Simulation / tabletop / Standing embedded process
Operating scope	
Legal entity / cross-boundary tier	
System and baseline identifiers	
Stable system or inventory ID	
Model and provider version, alias or release identifier	
Deployment environment and cohort or market scope	
Configuration, prompt or policy version reference	
Technical change, release or deployment record ID	
System owner	
Consequence owner	
Event owner	
Signal source and date	
Signal / Verified change / Incident / Risk interpretation / Governance trigger	
Statement-type tag	F / SC / A / RI / D
Signal evidence quality	D / C / R / A / U
Baseline status	approved / conditionally approved / reconstructed from an evidenced approval / no prior approval identified / approval contested / unable to determine
Baseline description	
Baseline evidence quality and reference	
Verified delta or candidate-signal status	
Taxonomy classes	C1–C10, multi-label
Recommended practice — primary taxonomy class and rationale	
Descriptors	
Linked event IDs	
Parent-event ID	
Affected people, language, scale, geography and consequence	
Hard-escalation triggers	1–15
Required specialist inputs and status	
Legal Escalation Flag	legal escalation required / legal escalation not required / legal escalation unresolved
Legal owner, date and rationale if not required	
Exemption invoked	yes / no
Boundary Record ID and evidence	
External entity	

Field	Record
External decision deadline	
Route proposed by	
Route confirmed by	
Minimum review route	R0 / R1 / R2 / R3
Interim operating status	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
Consequence if interim expiry or review date passes	
Parallel response processes activated	process / owner / deadline
Method deviation or limitation	

Evidence references

Reference ID	Source system or repository	Document or record identifier	Owner	Date and version	Access limitation	Evidence quality	Supports which decision or closure proposition

Materiality-lens record

Complete one row for every touched lens.

Lens	Baseline and status	Verified delta	Evidence and D/C/R/A/U quality	Uncertainty or disagreement	Specialist input required	Does earlier approval remain applicable, and why?	Dissent to preserve

Part 1 decision prompt: What changed against the baseline, which facts are verified, what remains a candidate signal, and why is this the minimum proportionate route?

Appendix C. AI Change Event Sheet — Part 2

Authority, decision, action, closure and learning

Record control

Field	Record
Record version	
Supersedes	
Created by-at	
Changed by-at	
Change reason	

Authority and decision

Field	Record
Formal authority and evidence	
Actual authority and evidence	
Authority succession / vacancy reference	
Options considered	
External constraints on options	
External decision deadline	
Review route	R0 / R1 / R2 / R3
Interim operating status	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
Final governance outcome	O0 / O1 / O2 / O3 / O4 / O5 / O6
Decision and rationale	
Conditions and restrictions	
Dissent / unresolved specialist disagreement	
Temporary measures	
Decision statement-type tag	D
Decision evidence quality	D / C / R / A / U

Uncertainty record

Element	Record
Missing, uncertain or contested fact	
Owner of obtaining or resolving it	

Element	Record
Deadline	
Interim operating status	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
Consequence if deadline or threshold is missed	
Reopen trigger	

Specialist-input records

Question	Qualified owner	Input	Status and date	Use in decision

Emergency record — complete only where applicable

Element	Record
Reason for urgency and declaration criterion	
Person activating emergency path	
Emergency authority, substitute or fail-safe basis	
Immediately available specialist inputs	
Interim operating status and restrictions	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
Parallel response processes, owners and deadlines	
Expiry or review date	
Ratification deadline and fallback	
Implementation evidence	
Evidence-preservation / legal-hold decision	
Full retrospective framing and reassessment deadline	
Formal decision record after immediate event	
Learning question about emergency procedure	

Corrective actions

Use Appendix D where more space is required.

Action	Owner	Dependencies	Due date	Implementation evidence	Per-action verifier	Status / limitation

Route history

Date and time	From → to	Proposed by	Confirmed by	Reason and evidence	Dissent / limitation

Interim history

Date and time	From → to	Authority or triage owner	Ratification status	Reason	Expiry / review date	Lapse consequence

Closure record

Field	Record
Closure type	implementation / condition / outcome-confirmation / remediation / residual-risk acceptance
Closure criteria set at decision time	
Implementation evidence and quality	
Closure verifier	
What the evidence confirms	
What remains open, uncertain or conditioned	
Recurrence / review window	
Event-level learning owner	

Affected-person assessment

Field	Record
Were people or groups affected or potentially affected?	
Notification / explanation required	
Correction / appeal / redress / remediation required	
Language or accessibility needs	
Owner and due date	
Evidence of completion	
Not applicable rationale and owner	

Six-axis current state

Axis	Controlled value
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
hold_reason	none / evidence pending / specialist input pending / authority pending / reopen decision pending
record_disposition	active / cancelled
outcome	O0 / O1 / O2 / O3 / O4 / O5 / O6
mode	Prospective live trace / Hybrid reconstruction plus prospective follow-up / Retrospective reconstruction / Simulation / tabletop / Standing embedded process

Transition log

Transition ID	Field or axis	From → to	Date and time	Actor	Authority basis	Reason	Record version

Reopen transition block

Field	Record
Trigger and reason	
Submitted by	
Actual authority	
Date	
Interim operating status at reopen	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
New decision point and due date	
Earlier record ID and version	
New record version or linked-event ID	
Affected actions, conditions and evidence	
hold_reason	reopen decision pending

Authority sign-off / record reference: ________________________ Date: _________

Closure verification / record reference: ______________________ Date: _________

Appendix D. Closure & Learning Supplement

Event ID: ________________________
Supplement date: __________________
Record version: ____________________
Supersedes: ________________________

Actions and implementation evidence

Action	Owner	Dependencies	Due date	Evidence reference and D/C/R/A/U quality	Per-action verifier	Status / limitation

Closure review

Closure type(s): implementation / condition / outcome-confirmation / remediation / residual-risk acceptance
Closure criteria tested: ____
Verifier and authority: ____
What the evidence confirms: ____
What remains open, uncertain or conditioned: ____________________________
Affected-person assessment reference: ___________________________________

Recurrence, reopen and learning

Review window: ________________________
Reopen trigger: ________________________
Did the event recur or link to another event? ____________________________
One learning retained: ____
Standing process, Authority Map, Boundary Record, trigger or template change:
____

Appendix E. Event Register field specification

Field	Controlled value or instruction
Event ID	Unique identifier.
Short name	Plain-language event description.
Operating scope	Named system or workflow within one legal entity; cross-boundary tier where applicable.
Legal entity	Named internal legal entity.
External entity	Named external entity where applicable.
System / inventory identifier	Stable identifier linking the event to the organisation's inventory and technical records.
Baseline status	approved / conditionally approved / reconstructed from an evidenced approval / no prior approval identified / approval contested / unable to determine
Primary taxonomy class	C1–C10 under the recommended-practice rule in §12.5.
Secondary taxonomy classes	Multi-label C1–C10.
Linked event IDs	Related cumulative, coupled, incoming, outgoing or reopen-linked events.
Parent-event ID	Parent record used for cumulative bundling, where applicable.
Mode	Prospective live trace / Hybrid reconstruction plus prospective follow-up / Retrospective reconstruction / Simulation / tabletop / Standing embedded process
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
hold_reason	none / evidence pending / specialist input pending / authority pending / reopen decision pending
record_disposition	active / cancelled
Event owner	Named person.
System owner	Named person or function.
Consequence owner	Named person or function.
Formal authority	Named person or forum and reference.
Actual authority	Named person or forum and reference.
Route proposed by	Named person and date.
Route confirmed by	Named person or forum and date.
Review route	R0 / R1 / R2 / R3
Route history reference	Reference to append-only route history.
Interim operating status	No interim change required / Continue temporarily / Continue temporarily with conditions / Restrict / Pause / Suspend
Interim history reference	Reference to append-only interim history.
Outcome	O0 / O1 / O2 / O3 / O4 / O5 / O6 — populated after decision.
Legal Escalation Flag	legal escalation required / legal escalation not required / legal escalation unresolved
Legal owner / rationale	Required for every flag; mandatory owner, date and rationale for **legal escalation not required**.
Exemption invoked	yes / no
Boundary Record ID	Required where exemption is invoked.
External decision deadline	Date or not applicable, with basis.
Parallel response processes	Reference to activated processes, owners and deadlines.
Action due date	Date.
Closure type	implementation / condition / outcome-confirmation / remediation / residual-risk acceptance
Closure evidence status	not defined / defined / partial / complete / contested
Closure evidence quality	D / C / R / A / U

Field	Controlled value or instruction
Affected-person assessment	complete / pending / not applicable with rationale / unavailable / contested
Recurrence / reopen	none / scheduled review / linked trigger / reopen decision pending / reopened by transition action
Record version	Current record version.
Supersedes	Earlier record version or none.
Transition-log reference	Reference to append-only transition log.
Method text date	Date of the method edition applied to this event.
Publication clearance	publication not assessed / review required / blocked / cleared for defined output / cleared with conditions
Publication-clearance authority	Reference to the separate applicable disclosure or publication process.

Register clearance rule. The Register records publication clearance supplied by the applicable process. It does not create, imply or replace clearance.

Register precision rule. Use filters and controlled values. Do not add a risk score, maturity score, decimal pilot score, completion percentage or hidden formula that creates false precision.

Appendix F. Boundary Record

A controlled record for a Pre-authorised Change Boundary under §6.4.1 and for every event that invokes it.

Field	Record
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	

Event ID	Date	Within-scope evidence reference	Applicability confirmed by