EVIDENTIARY RESILIENCE

The Continuity Condition of Institutional Reconstructibility

JM García-Maceiras

President of the Spanish BPO Banking Association

Abstract

As decision pathways come to depend on distributed technologies, cloud environments, evolving data architectures and third-party services, evidence can no longer be treated as a stock of records. This paper introduces *evidentiary resilience* as a distinct dimension of institutional resilience. It argues that accountability rests on an *evidence infrastructure*: the organisational, technological and governance arrangements through which evidence is generated, validated, preserved, connected and recovered over time.

Evidentiary resilience is the capacity of that infrastructure to remain sufficiently robust through technological change, organisational evolution and growing complexity. The paper identifies recurring modes of degradation (*reconstructibility drift*, *validation drift*, *fragmentation*, *contextual decay*, *attribution degradation*, *accountability dependency*) and argues that the possibility of *irreversible loss* is the common feature that gives them their preventive significance.

Building on prior work on explainability, opacity and institutional reconstructibility, the paper addresses the continuity conditions that allow accountability to remain effective through time. Its central proposition is simple: accountability cannot be more resilient than the evidentiary infrastructure that sustains it. *Evidentiary resilience* is therefore a necessary, though not sufficient, condition of durable accountability.

The Evidentiary Problem in AI-Driven Banking

Artificial intelligence is changing banking not only by altering the technologies through which decisions are produced, but by changing the conditions under which those decisions can later be understood and accounted for. A consequential decision may emerge from an interaction among data, models, cloud infrastructures, external services, human interventions and governance processes distributed across several

environments. The immediate output may belong to one system; the evidentiary history of the decision may not.

Consider a retail credit decision contested three years after it was taken. The model version has been archived. But the model has since been retrained, the feature store migrated to another cloud provider, the decision threshold adjusted by an analyst who has left the institution, and the validation report refers to assumptions nobody can now locate. Each element exists; none of them is missing in the documentary sense. Yet the bank cannot give a reliable account of how those elements interacted in *that* decision. The problem is not absence of information, but the erosion of the relationships that make information usable as evidence. The central unit of preservation is therefore not the artefact itself but the evidentiary relationship among artefacts.

This is why the problem cannot be reduced to record-keeping, and why existing regulatory requirements address it only in part. Instruments such as the EU AI Act (Regulation (EU) 2024/1689), DORA (Regulation (EU) 2022/2554) and BCBS 239 establish, in different ways, requirements concerning logging, documentation, ICT third-party arrangements, exit strategies and risk-data traceability. These obligations provide essential elements of evidentiary governance. They do not, however, necessarily establish whether the relationships among retained artefacts will remain recoverable and defensible through successive retraining, migration or organisational change. Retention and traceability are necessary; they do not by themselves secure evidentiary continuity.

Accountability is exercised retrospectively. Institutions are often required to establish the basis of an action after the technological and organisational circumstances surrounding it have changed. What is obvious contemporaneously may become obscure historically. Evidentiary governance must therefore anticipate temporal distance rather than assume that later scrutiny will encounter the environment in which the decision was made.

This paper is accordingly concerned not with any particular reconstruction, but with the institutional conditions that make reconstruction possible. Those conditions are inherently temporal: models are retrained, infrastructures migrated, providers replaced, responsibilities reorganised. Institutions may continue operating normally while the evidentiary foundations of past action become progressively weaker. The problem is one of *evidentiary continuity*: preserving not only records, but the conditions under which those records remain meaningful, recoverable and defensible. Hence the paper's starting proposition: accountability cannot be more resilient than the evidentiary infrastructure that sustains it.

The proposition states a necessary condition of effective accountability, not a sufficient one. The availability of a recoverable and defensible evidentiary pathway cannot by itself secure accountability, which also depends on applicable legal standards, supervisory capacity and institutional willingness to act on what the evidence shows. Nor does resilience eliminate the need for judgement about what should be preserved, for how long and at what cost. Its narrower claim is that, where the evidentiary

infrastructure fails, accountability will, to that extent, become ineffective regardless of the formal standards or institutional commitments in place.

Evidence Infrastructure

Evidence infrastructure refers to the conditions under which evidence acquires and retains meaning. It is not the document, database, model or log considered in isolation, but the evidentiary chain through which each becomes intelligible. Its purpose is not merely to preserve information but to preserve the possibility of institutional understanding.

A note on the sense of *evidence* is in order. It is used here in an institutional sense: material that an institution must be able to produce, connect and defend when its action is questioned, whether by a supervisor, a court, an internal control function or a customer. It is not limited to what is admissible in judicial proceedings, though it should be capable of meeting that standard where required. The sense is close to the archival notions of authenticity, reliability, integrity and usability of records.

Evidence is not merely retained; it is produced. Decision records, validation artefacts, model histories, audit trails, explanations, attribution mechanisms exist because organisational, technological and governance arrangements make their production possible.

Evidence infrastructure denotes those arrangements and the relationships among them. It has three mutually dependent dimensions: *technological* (data architectures, system configurations, model histories, logging arrangements, relevant external services); *organisational* (responsibility, attribution, continuity across functions, access to institutional knowledge); and *governance* (decisions on preservation, validation, materiality, responsibility, the use of evidence when scrutiny arises). *Evidence infrastructure* exists in the interaction of these dimensions, not in any one of them.

The decisive shift is therefore *from objects to connections*. In terms of reconstructibility, no object has an intrinsic quality to constitute a *because*. A model version matters because it can be linked to the decisions in which it operated; a validation record because it can be associated with the assumptions to which it applied; a governance decision because it can be connected to the authority through which it was exercised. An archive may be complete in a documentary sense while remaining incomplete in an institutional one.

This suggests a practical test of what must be preserved. Historical recoverability does not require indefinite conservation of every technical detail. It requires preservation of those relationships whose loss would materially impair future accountability. For a given class of decision, these *critical relationships* will typically include the links between the decision, the model version and configuration in force, the data on which it operated, the validation assumptions applicable to it and the authority under which it was taken or overridden. Identifying them is the first act of evidentiary governance.

Cloud services, third-party models and outsourced processing reinforce the point. They are not in themselves evidence of weak governance. The crucial issue is whether the

institution can preserve sufficient continuity across those dependencies to remain capable of explaining consequential action. Distributed accountability can otherwise become invisible accountability. Responsibility may be distributed in operation; it cannot simply be distributed away in accountability.

Evidence infrastructure sustains two related capacities. *Recoverability* is the ability to regenerate an evidentiary, causal and governance pathway, including where authority and judgement were exercised; *evidentiary assurance* is the ability to establish the integrity, relevance and limits of the pathway recovered, and to justify the confidence placed in it. Recoverability is thus the evidentiary condition of institutional reconstructibility. Accountability depends on both: reconstruction without adequate assurance may reproduce a pathway without establishing its reliability, while assurance cannot compensate for a pathway that can no longer be recovered.

Evidentiary Resilience

While *operational resilience* concerns continuity of service, *evidentiary resilience*, addressing continuity of accountability, may be defined as the continuing institutional capacity to generate, preserve, validate, connect, recover and defend the evidentiary foundations of accountability despite technological change, organisational evolution and increasing complexity.

The challenge is inherently temporal. A point-in-time assessment may show adequate evidentiary arrangements; resilience concerns whether that capacity survives successive transformations. A bank may replace a model, migrate infrastructure or reorganise functions without becoming less accountable. Conversely, a technically successful transformation may weaken accountability if it severs the relationships necessary to explain, validate, attribute or reconstruct consequential action. A sequence of individually acceptable changes may create a condition invisible to any individual control review.

Proportionality and the accountability horizon—A resilient infrastructure is not one in which everything is retained indefinitely, but one in which material evidence, with the relationships that give it meaning, remains available for as long as accountability reasonably requires. That duration is not uniform. This paper proposes the notion of an *accountability horizon*: the period during which a given class of decision may foreseeably be questioned, determined by the product lifecycle, applicable limitation periods and supervisory waves, and by the consequence and contestability of the decision. Materiality, in turn, can be graduated by the criticality of the decision class, in the same prudential spirit as the thresholds proposed in earlier work on *Tolerance for Opacity*.

Preservation and data protection—Preservation duties may appear to conflict with the data-minimisation and storage-limitation principles of the GDPR (Regulation (EU) 2016/679). The relationship must be assessed in the context of the decision class and the accountability horizon. Evidentiary resilience does not require indefinite retention of all personal data involved in a decision. It requires preserving the records and relationships necessary for future scrutiny, which may include lineage, versions, configurations,

metadata and integrity proofs, and, where necessary, access to underlying data. Data minimisation, controlled access, appropriate separation and proportionate retention periods should therefore form part of the design of an *evidence infrastructure*. The ability to preserve a defensible pathway while limiting unnecessary retention is itself a dimension of *evidentiary resilience*.

Irreversibility—The strongest justification for preventive preservation lies in an asymmetry. Operational disruption may often be remedied by repairing systems or redesigning controls; the loss of historical evidence may be harder, or impossible, to reverse. A missing model state, a deleted configuration, a lost validation artefact or a vanished contextual relationship does not necessarily make reconstruction impossible, since alternative sources may remain. But where the missing element was indispensable to recovering or defending the decision pathway, its loss may be irreversible. *Evidentiary resilience* therefore protects a capability that may otherwise disappear: the future possibility of accountability. This is a prudential argument, and it explains why the forms of degradation described next matter even before any visible failure occurs.

Reconstructibility is best understood as a principal capability sustained by resilient *evidence infrastructure*, not as a synonym for it. Where the infrastructure deteriorates, reconstructibility is progressively placed at risk. Evidentiary assurance occupies a complementary position: reconstructibilty concerns the recovery of a pathway; assurance concerns the integrity, relevance and limits of what has been recovered, and the grounds for relying on it.

Evidentiary Degradation

The forms described below are not a closed taxonomy. They identify recurring modes through which *evidentiary resilience* may weaken, and their value is primarily diagnostic. They make visible mechanisms of deterioration that conventional operational metrics miss. Their common feature is that they are cumulative rather than event-driven.

Institutions respond effectively to discrete failures; the harder governance problem is a succession of acceptable changes whose combined effect erodes future accountability. This is a familiar pattern in the study of organisational failure, where systems drift towards the boundary of safe operation through locally reasonable adaptations (Rasmussen 1997; Dekker 2011). The present analysis applies that insight to the evidentiary foundations of accountability.

Reconstructibility drift is the progressive weakening of an institution's ability to regenerate evidentiary, causal and governance pathways without any visible operational failure. It accumulates through retraining, migration, provider change, organisational reallocation, personnel turnover and contextual loss. The institution retains its records while losing the ability to connect them into a coherent account.

Validation drift concerns confidence rather than recoverability: it is the erosion of evidentiary assurance. A pathway may remain reconstructible while the assumptions,

controls or validation arrangements supporting confidence in it become increasingly difficult to justify.

Fragmentation occurs when evidentiary components remain distributed across functions and systems while the relationships connecting them weaken. Each function may perform correctly and yet the institution fails collectively to preserve a coherent account. The challenge is not necessarily centralisation but cross-functional intelligibility.

Contextual decay arises when evidence survives but loses the context required for interpretation: a log without its configuration, a model archive without its operating environment, a governance record without the assumptions that rendered it meaningful. Closely related is *obsolescence*, where records remain stored but the tools, interfaces or institutional knowledge needed to interpret them disappear.

Attribution degradation is the weakening of the pathway through which responsibility may be established. Accountability depends not only on showing what happened but on preserving where authority and judgement were exercised. Institutions may retain records about systems, users and decisions while losing clarity about their respective contributions.

Accountability dependency emerges when the ability to explain, validate or reconstruct consequential action becomes materially dependent on evidentiary resources outside the institution's direct control (cloud providers, data suppliers, AI services, outsourced processors). The issue is not outsourcing itself but the extent to which future accountability depends on information that may later become unavailable. This is the evidentiary face of what has elsewhere been described as an *algorithmic supply chain* (Cobbe, Veale and Singh 2023).

Behind all these forms lies the possibility of *irreversible loss*: the point at which deterioration can no longer be corrected through the available evidentiary resources. It is less a separate form than the threshold that gives the others their preventive urgency.

These forms rarely operate in isolation. Fragmentation may accelerate reconstructibility drift; accountability dependency may amplify contextual decay; technological transition may intensify both. Transitions deserve particular attention because they amplify several forms at once: a migration may preserve tomorrow's operations at the expense of yesterday's accountability. *Evidentiary degradation* is better understood as a network of vulnerabilities than as a set of independent failures.

A resilient *evidence infrastructure* cannot guarantee the absence of every gap. Its requirement is more modest: change should not silently accumulate into a condition in which accountability can no longer be exercised reliably. Resilience means the capacity to detect, absorb and correct deterioration before it becomes materially irreversible.

Governing Evidentiary Resilience

A capacity that may deteriorate silently cannot be governed by assumption. Some losses are irreversible once historical relationships, validation artefacts or contextual information disappear. The governance problem is therefore not only preservation but visibility, and it has some implications: observation should be longitudinal, rest on recovery exercises and be modest.

First, a single satisfactory review may conceal drift; repeated observation reveals direction. The object of governance is not the current inventory of evidence but the trajectory of the conditions supporting accountability. Second, documentation creates an assumption of reconstructibility; attempted recovery tests it. Such exercises need not investigate actual disputes. They are close in spirit to end-to-end internal auditing (Raji et al. 2020) and to the reviewability of automated decisions (Cobbe, Lee and Singh 2021). Their purpose is to determine whether the institution can still regenerate meaningful pathways, for representative classes of decision, before accountability is tested in practice. Finally, *evidentiary resilience* is a relational and contextual condition. Indicators, trends and testing may support institutional judgement, yet they cannot replace it. The risk is not only illusory reassurance but false precision, and a measure that becomes a target ceases to measure.

The *Reconstruction Readiness Report* (RRR) is one possible response. It is a mechanism for observing whether the *evidence infrastructure* supporting future accountability remains viable. It is neither a substitute for reconstruction nor a certification of accountability. Its development belongs to a companion paper, to follow shortly in this series, but the present analysis imposes four design constraints on it: it must be longitudinal, test-based rather than merely documentary, proportionate to the accountability horizon and criticality of each decision class, and candid about what cannot be recovered, including a declared register of known gaps. Its purpose is to make the condition of the institution's evidentiary foundations visible while deterioration remains remediable.

The proposition advanced here remains to be tested empirically. Repeated recovery exercises across time and representative classes of decision offer a means of examining whether the capacities described are preserved through technological and organisational change. The RRR is conceived to support that inquiry, not as evidence that the proposition has already been validated. The governance of *evidentiary resilience* therefore requires more than the preservation of records. It compels the continuing observation of whether an institution can recover and defend the pathways through which consequential decisions were made.

To Sum Up

The contribution of this paper is not another plea for transparency. It focuses on a different object: the infrastructure that allows an institution to remain intelligible to itself across time. Once that object is recognised, concerns that often appear separate (records, validation, attribution, dependency, recoverability) can be understood as aspects of a single institutional condition.

Innovation may legitimately increase complexity, distribute functions and introduce opacity. The institutional challenge is to ensure that these changes do not progressively erode the capacity to account for the exercise of consequential power and its effects. Decisions belong to the past, governance acts in the present and scrutiny may arise in the future. A resilient *evidence infrastructure* connects those moments.

The distinctive insight, therefore, is temporal. Between the instant of decision and the moment of scrutiny, technological change, organisational evolution, dependency, fragmentation and contextual loss may silently weaken the capacity to account. *Reconstructibility drift* concerns the capacity to recover; *validation drift*, the capacity to trust what is recovered; *irreversibility* gives the problem its preventive force.

The argument requires neither complete transparency, nor technological stasis, nor a universal metric. Institutions may remain operationally resilient while silently losing the ability to account for their own actions. Accountability cannot be more resilient than the evidentiary infrastructure that sustains it.

Madrid, November 3, 2026

References

External

Basel Committee on Banking Supervision (2013). *Principles for effective risk data aggregation and risk reporting* (BCBS 239).

Cobbe, J, Lee, MSA and Singh, J (2021). "Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems". *Proceedings of ACM FAccT 2021*.

Cobbe, J, Veale, M and Singh, J (2023). "Understanding Accountability in Algorithmic Supply Chains". *Proceedings of ACM FAccT 2023*.

Dekker, S (2011). *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*. Ashgate.

ISO 14721:2012 (OAIS) and ISO 15489-1:2016 (Records management).

Raji, ID et al. (2020). "Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing". *Proceedings of ACM FAccT 2020*.

Rasmussen, J (1997). "Risk management in a dynamic society: a modelling problem". *Safety Science* 27(2–3).

Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2022/2554 (DORA); Regulation (EU) 2024/1689 (AI Act).

García-Maceiras, JM (2024). *El Estadista*. Herakleitos Club.

García-Maceiras, JM (2026a). *The Banking Risk of AI Explanation*. *ADR Notebooks*, núm. 1.

García-Maceiras, JM (2026b). "The Five Beacons Model: A Prudential Architecture for AI Explainability and Legal Liability in Banking". *ADR Notebooks*, núm. 2. https://zenodo.org/records/18647318

García-Maceiras, JM (2026c). "Tolerance for Opacity: A Threshold Framework for AI-Driven Banking". *ADR Notebooks*, núm. 3. https://zenodo.org/records/19144304

García-Maceiras, JM (2026d). "Systemic Opacity Risk: Macroprudential Dimension of AI Governance in Banking". *ADR Notebooks*, núm. 4. https://zenodo.org/records/20109302

García-Maceiras, JM (2026e). "The Upstream Migration of Power: Toward a Theory of Infrastructural Constitutionalism". *ADR Notebooks*, núm. 5. https://zenodo.org/records/19441767

García-Maceiras, JM (2026f). "The HRAIS Chamber: Notes on Operationalizing Institutional Reconstructibility". *ADR Notebooks*, núm. 6. https://zenodo.org/records/19787461

García-Maceiras, JM (2026g). "La Migración Infraestructural del Poder". *Revista de Derecho Digital e Innovación* (29). Aranzadi La Ley.

García-Maceiras, JM (2026h). *Normatividad sin Autor: La Democracia ante la Máquina Inteligente*. *ADR Notebooks*, núm. 7.

García-Maceiras, JM (2026i). "Institutional Reconstructibility in AI-Driven Banking". *ADR Notebooks*, núm. 8. https://doi.org/10.5281/zenodo.22696151