INSTITUTIONAL RECONSTRUCTIBILITY IN AI-DRIVEN BANKING

[A Contribution to CPMI-IOSCO's Consultations on Cyber Resilience]

JM García-Maceiras

President of the Spanish BPO Banking Association

Abstract

Contemporary discussions on cyber resilience, operational resilience and third-party dependencies recognise the challenges posed by ecosystem complexity, concentration, outsourcing arrangements and technological opacity.

This paper argues that these developments reveal a broader governance challenge. As financial market infrastructures (FMIs) become dependent upon complex technological ecosystems, the central question is no longer limited to operational continuity: institutions must also preserve the capacity to generate, validate, supervise and defend the evidence upon which decisions, accountability and oversight ultimately depend.

To address this challenge, this contribution introduces, among other concepts, the construct of *Evidence Infrastructure***:** the set of organisational, technological and governance arrangements through which evidence is produced, preserved, validated and made available for scrutiny. From this perspective, operational disruptions and *validation failures* may represent different manifestations of a common problem: deterioration of the infrastructures that sustain institutional governability.

Rather than proposing an alternative to existing resilience frameworks, this contribution seeks to complement ongoing CPMI-IOSCO, Basel and DORA-related discussions by examining how institutions may preserve governability when critical infrastructures remain operational but become progressively more difficult to validate, supervise or reconstruct.

Beyond Operational Resilience

The CPMI-IOSCO discussion on third-party dependencies highlights concerns that are becoming relevant for FMIs: ecosystem complexity, concentration, dependency chains, supply-chain opacity, cyber resilience.

These concerns are usually examined through the lens of operational continuity—whether critical services can withstand disruption, recover from incidents and continue supporting financial stability under adverse conditions. These objectives remain essential.

However, the evolution of contemporary infrastructures suggests that a complementary issue deserves attention. An institution may continue operating successfully while progressively losing the ability to establish how critical outputs were produced; which dependencies supported them; how their validity was assessed; how responsibilities were allocated; how decisions could be justified under supervisory or external scrutiny.

In such circumstances, the challenge is no longer one of operational continuity alone; it concerns governability. Traditional resilience frameworks generally focus on events that interrupt operations; for instance, cyber incidents, service failures, outages, corruption of data or infrastructure disruption.

Institutions may also face situations where systems remain operational while the evidentiary foundations required to supervise, validate or defend their outputs gradually deteriorate. Such situations do not necessarily produce immediate operational consequences, yet they may affect the institution's ability to assert its ownership of the decisions it makes and the outcomes it produces.

What institutional capabilities must remain intact for governance itself to remain possible? This contribution suggests that the answer lies not only in the resilience of systems, providers or technologies, but also in the resilience of the infrastructures through which evidence is produced, preserved, validated and made available for scrutiny.

Evidence Infrastructure

Resilience challenges affecting FMIs cannot be fully understood through operational dependencies alone. At the centre of every governance process lies a more fundamental requirement: the availability of evidence capable of supporting decisions, accountability, supervision and institutional trust.

In contemporary technological ecosystems, evidence is not simply produced by institutions: it is generated *through* infrastructures—data flows, validation procedures, model outputs, operational records, dependency mappings, controls and records of human intervention are generated, stored and maintained through complex arrangements involving technological systems, third-party providers and organisational processes. Evidence therefore ceases to function merely as documentation of activity; it becomes an output of what may be described as *Evidence Infrastructure.*

For the purposes of this contribution, an *evidence infrastructure* is the set of technological, organisational and governance arrangements through which institutions generate, preserve, validate and reconstruct the evidence required to support their activities under conditions of scrutiny. It encompasses information sources, validation processes,

governance controls, dependency relationships, decision records, attribution mechanisms and reconstruction capabilities. Its purpose is not merely to preserve information, but to underpin institutional intelligibility.

Traditional resilience frameworks focus primarily on operational failure: a system becomes unavailable; a service is interrupted; data are corrupted; a provider experiences disruption. These events remain critically important. However, convoluted infrastructures may also experience a different category of failure: *validation failures*.

Unlike operational disruptions, *validation failures* do not interrupt services directly; rather, they weaken the institution's capacity to justify confidence in outcomes. In this sense, operational failures and *validation failures* may be understood as disruptions affecting different dimensions of the same underlying *evidence infrastructure*.

The CPMI-IOSCO discussion highlights several resilience concerns. Each may also affect *Evidence Infrastructure*. Concentration can reduce the diversity of evidentiary sources; dependency chains may obscure validation processes; supply-chain opacity may weaken attribution.

Once evidence is understood as the product of infrastructure, a further question naturally emerges. The key issue is not technological complexity in itself, but the degree to which institutions remain capable of governing infrastructures whose internal operation becomes progressively less visible.

Institutional Opacity

Discussions concerning complex technological systems frequently focus on technological opacity. Cloud infrastructures, advanced analytics, AI systems, outsourced services, and layered dependency chains may all reduce direct visibility into the processes through which outcomes are generated.

However, technological opacity is not, in itself, the principal challenge. The overriding concern arises when the deficit of transparency becomes *institutional opacity*. Financial institutions are not required to understand every line of code, every technical configuration, every operational detail within highly complex infrastructures. They are nevertheless expected to remain accountable for the decisions, services and outcomes that those infrastructures support. The question is not whether technologies become difficult to understand, but whether institutions remain capable of governing them.

Institutional opacity emerges when an organisation can no longer establish, under conditions of scrutiny, how relevant outcomes were produced, which dependencies contributed to them, how validity was assessed, how responsibility was allocated or how decisions may be defended. Opacity should therefore be understood not merely as a property of technology, but as a condition affecting governability. An institution cannot effectively govern what it cannot adequately understand.

Structural Explanation and Responsibility Governance

Debates concerning advanced technologies frequently revolve around *explainability.* Institutions must be capable of knowing, assessing and challenging the outputs generated by the systems upon which they rely. However, *explainability* alone does not fully fix the governance challenges described in the preceding sections.

The emergence of complex *evidence infrastructures* means that institutions face a broader problem than understanding individual outputs. They must also preserve clear attribution of responsibility across the organisational, technological and governance structures through which those outputs are produced. The key governance question is therefore not simply why a system produced a particular result, but who remains responsible for that result throughout the governance chain.

As *institutional opacity* increases, a formal explanation may remain fully available while responsibility morphs into muddled fragmentation. An organisation may display technical statements of how a particular outcome was generated and still face uncertainty regarding its ownership of the resulting decisions, because of the blurring of its core operational and oversight dependencies.

In highly distributed infrastructures, the principal challenge therefore concerns responsibility management as much as explanation itself. This suggests the need for structural approaches capable of preserving intelligibility across the governance chain.

The *Five Beacons* (5B) framework was developed as one such approach. Rather than treating explanation as an exclusively technical exercise, the framework distributes intelligibility and accountability across multiple institutional layers. Its purpose is not primarily to maximise disclosure but to ensure that responsibility remains identifiable, reviewable and governable despite increasing technological complexity.

From this perspective, 5B may be understood as a model of responsibility governance. By linking explanation to responsibility allocation, the framework supports institutional self-governance under conditions of opacity. Yet even where responsibility structures are preserved, a further question arises: how much opacity can institutions safely govern?

Tolerance for Opacity and Systemic Opacity Risk

Some degree of opacity is unavoidable. Financial institutions cannot possess complete visibility into every technological component, every provider relationship, every dependency chain, every evidentiary process upon which their activities depend. The question is therefore how to establish the conditions under which opacity remains governable. This contribution approaches it through two complementary concepts previously developed in related work: *Tolerance for Opacity* (TfO) and *Systemic Opacity Risk* (SOR).

Tolerance for Opacity (TfO) concerns the degree of opacity an institution can sustain while preserving effective governance. In the context of *evidence infrastructure*, this depends upon the continuing ability to validate critical outputs, reconstruct significant decisions, attribute responsibility and support supervisory scrutiny. As infrastructure complexity increases, these capabilities may become progressively more difficult to maintain. Resilience therefore relies not only on operational performance, but also on keeping opacity within governable limits.

Systemic Opacity Risk (SOR) focuses on the accumulation of opacity across interconnected ecosystems. Concentration, common providers, shared validation infrastructures and layered dependency structures may generate opacity that no individual institution fully controls, even when each institution remains operationally resilient. Under such conditions, opacity ceases to be merely an organisational characteristic and becomes an ecosystem-level concern.

Viewed through the lens of *evidence infrastructure*, TfO/SOR extend concerns already identified by CPMI-IOSCO. Third-party concentration is not only an operational issue but a clustering of evidentiary dependencies. The blurring of supply-chain boundaries is not only a visibility issue; it may also affect the capacity to validate, attribute and reconstruct critical activities.

Institutional Reconstructibility

Even where opacity remains within governable limits, institutions face a further challenge: maintaining the ability to explain, justify and defend significant decisions after they have been made. This requirement is particularly important in environments characterised by third-party dependencies, cloud concentration, AI-enabled processes, outsourcing arrangements and complex evidentiary chains.

Accountability cannot depend exclusively upon real-time supervision. Institutions must also remain capable of reconstructing how governance was exercised when decisions, incidents or disputes become subject to subsequent scrutiny. *Institutional reconstructibility* refers to the capacity of an organisation to regenerate the evidentiary, validation and governance chains required to support accountability under conditions of challenge.

The concept extends beyond *traceability*. Institutions may retain extensive records, audit logs and documentation while remaining unable to establish how relevant evidence was produced, how its validity was assessed, which dependencies influenced outcomes or how responsibility was exercised. *Institutional reconstructibility* therefore concerns not merely the preservation of information, but the continuing intelligibility of governance.

The relationship with *evidence infrastructure* is straightforward. *Evidence infrastructure* concerns the conditions through which evidence is produced and preserved; *institutional reconstructibility* refers to the capacity to regenerate and examine those conditions retrospectively.

The concept also highlights a category of events distinct from traditional operational failures. An institution may remain operationally functional while becoming unable to regenerate the evidentiary chains required to support accountability. Critical services may continue operating, relevant records may continue to exist, yet *reconstructibility* may nevertheless deteriorate. These situations may be described as *reconstructibility failures*.

Unlike operational incidents, *reconstructibility failures* affect the institution's ability to demonstrate governability rather than its ability to provide services. Their significance becomes visible when decisions, incidents or outcomes must be examined under external scrutiny. They matter not because they interrupt operations, but because they weaken confidence in the institution's capacity to justify its actions.

Institutional reconstructibility cannot therefore remain merely an evidentiary capability; it becomes an object of governance in its own right. Institutions must consider not only whether decisions remain valid, but whether their capacity to reconstruct and defend those decisions is being preserved over time.

Validation Scenarios and Evidentiary Resilience

If *institutional reconstructibility* is necessary to sustain accountability and supervisory confidence, it cannot be treated as a quiescent attribute of systems, records or documentation: it becomes a hallmark of governance. Operational resilience frameworks recognise that resilience cannot be assumed; it must be monitored, tested and governed—the same logic may apply to *institutional reconstructibility.*

FMIs operate in highly complex environments in which reconstructive capability may gradually deteriorate even where operational performance remains satisfactory. Dependencies evolve, providers and models change, governance arrangements adapt. As a result, institutions may lose the ability to regenerate evidentiary and accountability chains without experiencing any immediate operational disruption.

That phenomenon may be described as *reconstructibility drift*: the gradual deterioration of an institution's capacity to reconstruct the evidentiary foundations upon which accountability depends. Unlike operational incidents, such deterioration may remain largely invisible until decisions, incidents or outcomes become subject to external scrutiny. Its significance lies not in service interruption but in the erosion of the institution's ability to demonstrate governability when challenged.

Reconstructibility, however, addresses only part of the governance problem. Institutions may remain capable of rearticulating significant decisions while progressively losing confidence in the evidentiary foundations supporting those decisions. This shifts attention from reconstruction to *validation*, which extends beyond technical verification.

Validation encompasses the institutional processes through which organisations determine whether evidence remains reliable, outputs remain trustworthy, dependencies remain acceptable and the governance assumptions underlying them remain sound. *Validation* is therefore a governance function as much as a technical one.

As FMIs evolve, institutions may continue relying upon an evidentiary corpus whose original assumptions are no longer fully visible, documented or independently reviewable; this may give rise to *validation drift*: the gradual deterioration of an institution's capacity to justify confidence in evidence despite continued operational performance.

Like many latent technical fragilities, *validation drift* may remain largely imperceptible until challenged by supervisors, auditors, courts or significant external events. Resilience frameworks may therefore benefit from mechanisms capable of identifying a decay in validation capacity alongside deterioration in operational performance.

The CPMI-IOSCO Cyber Resilience Toolkit places considerable emphasis on testing, exercises and scenario analysis. A complementary approach may involve *validation scenarios*: situations in which critical dependencies remain operational but become insufficiently observable; evidentiary chains become fragmented across multiple providers; validation assumptions can no longer be independently verified; responsibility attribution becomes uncertain; supervisory confidence deteriorates despite continued operational performance. Such scenarios do not necessarily involve operational failure; their significance lies in the likelihood that institutions may gradually lose the capacity to establish why outcomes should continue to be trusted.

The concepts developed throughout this paper converge in what may be described as *evidentiary resilience*: the capacity of an institution to preserve, regenerate and govern the evidence required to sustain accountability, supervisory confidence and effective oversight over time. From this perspective, the concerns identified by CPMI-IOSCO affect not only operational continuity but also the evidentiary foundations upon which governance depends.

Operational resilience remains indispensable. However, institutions may confront situations in which critical services remain available while confidence in the evidentiary structures supporting those services weakens. Future resilience frameworks may therefore benefit from considering not only operational disruption, recovery scenarios and service continuity, but also *validation scenarios* and *evidentiary resilience*.

Concluding Remarks

The CPMI-IOSCO discussion highlights a set of challenges that are likely to become increasingly important for FMIs: ecosystem complexity, concentration of service providers, third-party dependencies, supply-chain opacity and cyber resilience. These issues are usually approached within the framework of operational continuity. This paper suggests that an additional perspective may be useful.

As FMIs become inextricably intertwined with complex technological ecosystems, resilience may depend not only upon the continuity of operations but also upon the steadfastness of governability. The paper approaches this challenge through several

concepts to protect governability under conditions of opacity. Future resilience frameworks may benefit from considering not only operational disruption and recovery, but also deterioration in *institutional reconstructibility*, *validation scenarios* and *evidentiary resilience*. This strategy does not intend to replace existing approaches reflected in CPMI-IOSCO, Basel or DORA-related work—far from it. Rather, it strives to extend their scope from operational continuity to the institutional conditions that make continuity governable.

Institutional reconstructibility is not merely an evidentiary capability: it is the prerequisite for responsibility, supervision and accountability to survive under conditions of limited transparency. As technological ecosystems grow more complex, fostering this capability becomes just as critical as preserving operational continuity itself. Institutions may continue to function despite disruption, but they cannot govern legitimately unless they remain capable of validating and defending the evidentiary foundations upon which confidence ultimately depends.

Madrid, October 3rd, 2026

Internal References

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

García-Maceiras, JM (2026a). *The Banking Risk of AI Explanation*. *ADR Notebooks*, No. 1.

García-Maceiras, JM (2026b). "The Five Beacons Model: A Prudential Architecture for AI Explainability and Legal Liability in Banking". *ADR Notebooks*, No. 2. [Working Paper] DOI 10.5281/zenodo.18647318.

García-Maceiras, JM (2026c). "Tolerance for Opacity: A Threshold Framework for AI-Driven Banking". *ADR Notebooks*, No. 3. [Working Paper] DOI 10.5281/zenodo.19144304.

García-Maceiras, JM (2026d). "Systemic Opacity Risk: Macroprudential Dimension of AI Governance in Banking". *ADR Notebooks*, No. 4. [Working Paper] DOI 10.5281/zenodo.20109302.

García-Maceiras, JM (2026e). "The Upstream Migration of Power: Toward a Theory of Infrastructural Constitutionalism". *ADR Notebooks*, No. 5. [Working Paper] DOI 10.5281/zenodo.19441767.

García-Maceiras, JM (2026f). "The HRAIS Chamber: Notes on Operationalizing Institutional Reconstructibility". *ADR Notebooks*, No. 6. [Working Paper] DOI 10.5281/zenodo.19787461.

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

García-Maceiras, JM (2026i). *Normatividad sin Autor: La Democracia ante la Máquina Inteligente*. *ADR Notebooks*, No. 7.

10.5281/zenodo.22696151