Exploring the Internal Audit Domain -Beyond the Rear-View Mirror: Engineering the "LiDAR" Internal Audit for India's Financial Resiliency

In my years navigating the high-stakes corridors of India's regulated entities—from the rapid-fire lending of NBFC-MFIs to the intricate plumbing of Payment Aggregators—I have often encountered a dangerous comfort. Boards and Senior Management frequently lean on "clean" audit reports like a security blanket, unaware that their Third Line of Defense is operating as a **passive security camera**. It records that a door was opened; it confirms a document exists. But a camera is a historian. It cannot tell you if the person entering has the right fingerprint or if they are carrying a concealed, systemic risk.

2. Internal Audit - A Reality Check

Internal Audit in most NBFCs, banks, NBFC-MFIs and PA/PGs still behaves like a **passive camera**. It records. It verifies. It ticks.

From a regulatory standpoint, that is not comfort. That is a warning sign. RBI does not look at Internal Audit as a standalone function. It reads IA as a mirror of governance quality and management maturity. When risks are first identified by supervisors—and not by Internal Audit—the conclusion is immediate: The institution is not sensing its own risks early enough. That single failure quietly impacts everything.

- It affects the Supervisory risk assessment,
- Management of quality perception,
- Composite risk ratings and
- Eventually, Escalation.

Here is what many still miss: **Superficial Internal Audit attracts more scrutiny, not less.** Because ticking boxes proves compliance, not control. A checklist can confirm that a policy exists. It cannot tell you whether the policy is being bypassed/or gamed/or overridden systematically. RBI today is not asking, *"Was it done?"* It is asking, *"Will this system hold when conditions turn adverse?"* That is where the difference lies—**between a camera and a motion sensor**. A motion-sensor Internal Audit does not stop at outputs. It watches behaviour.

-It notices credit concentration quietly building through sourcing channels.
-It sees override patterns inside proprietary scoring models.
-It questions assumptions that no longer match economic reality.
-It picks up ethical drift in recoveries that paperwork carefully hides.
-It flags outsourcing arrangements that look efficient but create single-point failures.
-It tests escrow and merchant flows that comply on paper but leak risk in practice.

These are not documentation gaps. These are **process fingerprints**.

In digital institutions, this becomes even sharper. Today, **the algorithm is the policy**. Verifying approvals or vendor certificates is meaningless if Internal Audit cannot test data integrity, model bias, override controls, back-testing discipline, and governance independence. I have personally seen models pass internal audits and fail RBI inspections—because no one audited the logic, only the paperwork. Boards and Audit Committees are central to this failure.

When Boards focus on audit coverage, closure percentages, or cost minimization, Internal Audit retreats into safety mode. When IA is outsourced without ownership, depth disappears. When Audit Committees lack diversity in risk, technology, and business understanding, challenge evaporates.

Today's volatile regulatory environment, marked by intense RBI scrutiny, demands we trade the camera for a **moving sensor**. The Board of REs must empower Internal Audit to act as a "Motion Sensor". This is not a cost-center exercise; it is a strategic necessity. It requires investing in auditors who understand the statistical nuances of credit scoring and the technical complexities of IT security. We must move beyond the "box-ticking" culture and engineer a **high-tech LiDAR** framework for Internal Audit (IA). LiDAR doesn't just see what is behind us; it pulses into the fog of the future, sensing obstacles before the vehicle even reaches them.

3. Cracking the "Black Box": Auditing the Logic of the Machine

I've seen many audits that stop at verifying a KYC document. In a digital-first world, that is like checking the paint on a car while ignoring a failing engine. If your entity is driven by **proprietary scoring technology**, the audit must look under the hood.

- **Mathematical Integrity:** We should no longer just ask if a credit model exists. We must verify the **mathematical and statistical principles** behind it and ensure the assumptions are soundly documented.

- **The "Sensor" Approach:** I look for independent oversight—does the team validating the model report to the same person who built it?. Without independence, the audit is a mirage.
- **Stress and Back-Testing:** If a model isn't being back-tested against actual defaults and subjected to sensitivity tests, it isn't a tool; it’s a liability waiting to explode during a market shift.

4. Sectoral Depth: Why "One Size" Fits None

It is now evident that the generic audit checklist is the enemy of foresight. Financing a hospital in a rural district is a different universe from financing a digital travel portal.

- **Dynamic Due Diligence:** For Healthcare or Education, an active audit doesn't just glance at a license. It verifies the institution's current standing and sectoral due diligence to ensure they aren't under regulatory sanction.
- **The Early Warning "Tripwire":** Monitoring a single borrower is easy; monitoring **Sectoral and Group concentration** is where the LiDAR pays off.
- **Time-to-Action:** An active audit tests the **Time-to-Action** once an Early Warning System (EWS) alert is raised. If the Travel sector hits a slump, does your entity have a tripwire that triggers *before* the NPA classification kicks in?

5. Sensing the "Ghost in the Machine": Operations & IT Resilience

In our digital world, fraud rarely leaves a paper trail; it leaves a digital "fingerprint" error.

- **Access Control Integrity:** I look for system bypasses. Can one person onboard a customer, approve the loan, and trigger the disbursement ? A passive camera misses this; a motion sensor flags the lack of "Maker-Checker" integrity.
- **The Outsourcing Weak Link:** We must audit the financial and operational health of our vendors. If your KYC or collection vendor has a data breach, it is *your* entity that carries the regulatory and reputational scars.
- **Beyond Backups:** Standard audits review "backup procedures". A LiDAR-based audit evaluates the **actual effectiveness of disaster recovery plans**. Data is our primary asset; its access must be restrictive and monitored, not just stored.

6. The Ethical Radius: Auditing the "Spirit" of Recovery

This is where the "Passive Camera" fails most spectacularly. A checklist says "Recovery action documented: Yes". An analytical auditor asks: **"Is the recovery action ethical?"**.

- **Spirit vs. Letter:** We must audit the **Fair Practices Code (FPC)** in spirit, not just in letter.

- **Tone Compliance:** I believe in randomly sampling communication logs. Is the tone used with our customers compliant with RBI guidelines?. If our collections are effective but unethical, we are trading short-term liquidity for a long-term regulatory disaster.

7. Board's Role

Boards that want Internal Audit to function as a strategic defense must stop asking how many audits were completed and start asking:

- What risks did IA identify before the regulator did?
- Where did management disagree with IA—and why?
- What assumptions in our business model worry IA the most?

The transition from camera to motion sensor does not require perfection or massive budgets. It requires intent:

- sharper risk-based audit planning,
- selective use of data analytics,
- auditors who understand systems, behaviour, and incentives—not just files,
- and reports that speak about **what could break next**, not just what complied with last quarter.

LiDAR (Light Detection and Ranging) Analogy at a Glance

LiDAR Concept	"Engineering the LiDAR Internal Audit" Explanation	Audit Function Equivalent
High Resolution 3D Scanning	Deep, Detailed and Continuous scan	Moving beyond sample-based testing to 100% population analysis of transactional data
Real Time/Continuous data capture	'Continuous scan' of a **highly dynamic environment**	Continuous Auditing & Monitoring (CA/CM), not just Annual or Quarterly reviews.
Precision and Accuracy	"Highly Precise Audit function"	Data-driven analytics reducing subjective judgement, identifying exact anomalies and patterns
Penetrating Obstacles for full Visibility	"Ensuring Complete Visibility"	Using technology to see through complex digital layers(APIs, Cloud services, encrypted data and interconnected systems.

Proactive Mapping and Modelling	“Proactively identifying all potential Risks “	Predictive Analytics and Risk Modelling to foresee issues before they materialize, rather than post facto detection.
Digital Twin	“Designing an Internal Audit system”	Building a living, digital audit landscape that mirrors the organization's financial ecosystem for constant assessment

Conclusion: The Strategic Mandate

Internal Audit must be enabled to function as a **risk-sensing mechanism**, not a ceremonial control. This is not about cost allocation or compliance optics. It is a strategic choice that demands auditors with the ability to interrogate credit models, data behaviour, and technology architecture with depth and independence. By moving to a motion-sensor framework, we ensure that our entities don't just grow fast—they grow **resiliently**.

****