
# Integrated = Risk + Audit Talking – Forward Looking Approach.

## Disclaimer:

Views are personal and does not reflect the views of the organization I am employed.

Author: Roshan Neville Sequeira
Date: 1st October, 2025
Place – Abu Dhabi, United Arab Emirates

The idea for this article is rooted in several conversations I've had with Internal Audit and Risk Management teams across diverse industries — BFSI, Manufacturing, Education, Healthcare, and Leisure. While each sector faces unique risks, a common theme emerged: the relationship between risk and audit is evolving rapidly, and integration between the two has become essential for effective governance.

## Part 1: The Paradigm Shift

Over the last decade, industry has undergone a paradigm shift — **from compliance-driven, backward-looking assurance to risk-based, forward-looking assurance** — in how it addresses uncertainty and its impact on strategic objectives. Risk, defined as *the **effect of uncertainty on objectives*** (ISO 31000), is now a universally accepted construct. Yet in many organizations, risk was not consistently central to how objectives were pursued. It was acknowledged within governance structures, while audit and compliance — **the other key pillars of effective governance** — often operated in silos, without fully integrating risk as a guiding principle.

### The Evolution of Assurance

The **traditional Three Lines of Defense (3LoD)** model, formalized by the Institute of Internal Auditors (IIA) in 2013, became the global reference point for governance, risk, and assurance practices. For more than a decade, it provided organizations with a structured framework to allocate responsibilities and deliver independent assurance to boards and senior management. However, many practitioners, particularly in cybersecurity, financial services, and organizational resilience, have argued that the 3LoD is too narrow to capture today's broader landscape of accountability and assurance.

**Traditional Three Lines of Defense (IIA, 2013)**

1. **First Line** – **Management / Operational Owners**: Own and manage risks day-to-day.
2. **Second Line** – **Risk & Compliance Functions**: Monitor, guide, and facilitate risk frameworks.
3. **Third Line** – **Internal Audit**: Provides independent assurance to the board and senior leadership.

Many organizations now embrace the **Expanded Five Lines of Defense**, which add:

4. **External Assurance / Regulators**: Regulators and external auditors validating compliance and resilience.
5. **Stakeholders / Society / Ecosystem**: Shareholders, customers, rating agencies, and public trust demanding accountability, resilience, and ESG maturity.

This reflects a wider assurance ecosystem that organizations must navigate.

# Part 2: Why Integration Matters

## Risk and Audit in Conversation

**Risk teams** → Spot what could go wrong (emerging threats, regulatory shifts, strategic risks).
**Audit teams** → Verify whether controls truly work (assurance, effectiveness, evidence).
**Integrated conversations** → Create a closed loop: Risk informs Audit → Audit validates Risk → Together they guide strategy.

Figure 1 below shows the forward-looking approach in action

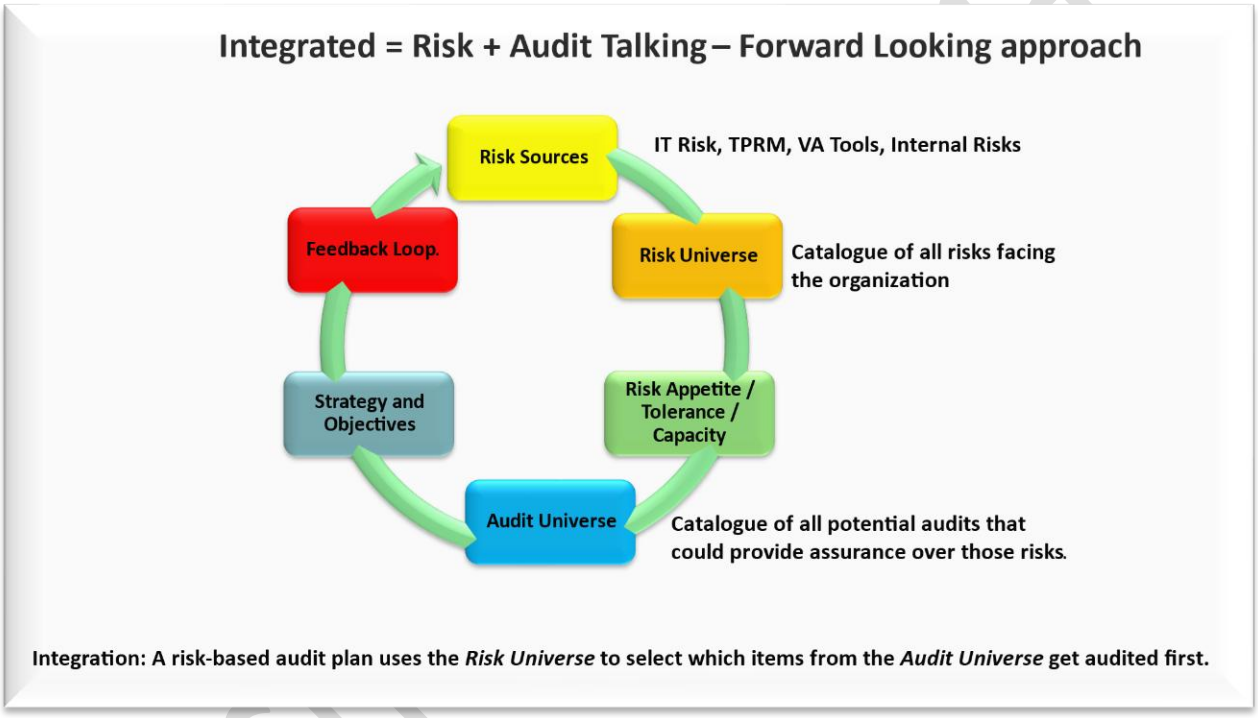


**Figure 1**

## Forward vs Backward Assurance

## Backward-Looking (Traditional Compliance Audit):

Checks if rules were followed last year.
Focuses on evidence of past conformity.
Misses creeping risks.

## Forward-Looking (Integrated Risk + Audit):

Anticipates emerging risks and validates controls dynamically.
Aligns audit scope with enterprise risk priorities.
Builds resilience by addressing tomorrow's threats today.

### Analogy:

Risk Alone = Weather forecast.
Audit Alone = Inspecting yesterday's umbrella.
Integrated (Risk + Audit Talking) = Checking if tomorrow's umbrella can withstand the coming storm.

## Part 3: The Impact

### Organizational Benefits of Integration

**Improves Risk Posture** → More strategic view of vulnerabilities.
**Strengthens Security Posture** → Defenses aligned with current and future threats.
**Reduces Risk Exposure** → Focus on material risks, not just compliance.
**Boosts Trust** → Executives and boards see one integrated story, not fragmented signals.

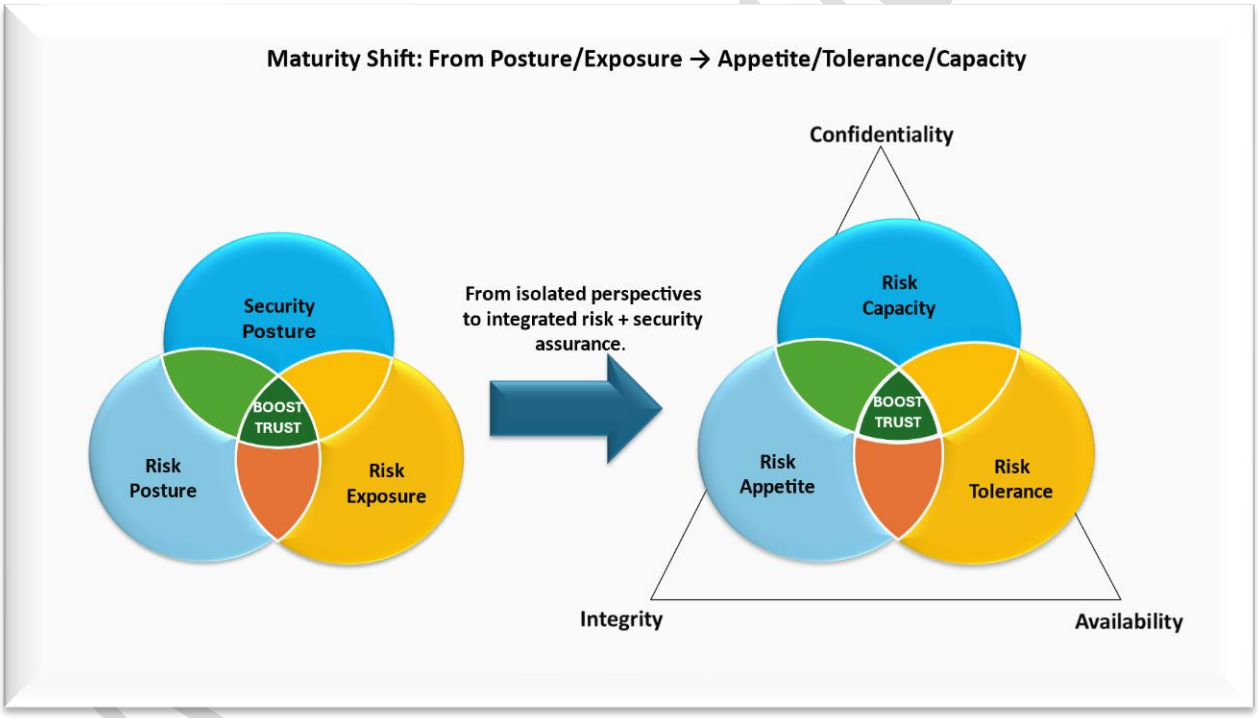


**Figure 2**
**Maturity Shift: From Posture/Exposure → Appetite/Tolerance/Capacity**

Figure 2 illustrates the maturity shift in assurance thinking. On the left, organizations focus on Risk Posture, Security Posture, and Risk Exposure as separate views, which when integrated, build trust. On the right, maturity deepens by aligning these dimensions with Risk Appetite, Risk Tolerance, and Risk Capacity, directly linked to the Confidentiality, Integrity, and Availability (CIA) principles. Together, they move assurance from isolated perspectives to a fully integrated model that both protects objectives and boosts trust.

## Boosting Trust Through Integration

**Risk Posture** highlights where the organization is most vulnerable.
**Security Posture** measures how strong defenses are against current and future threats.
**Risk Exposure** shows the vulnerabilities the organization continues to carry forward.

When combined, they deliver a single narrative that executives and boards can rely on. This integration moves beyond compliance checklists and directly aligns with **Confidentiality, Integrity, and Availability (CIA),** the foundations of security.

## Avoiding the "Boiling Frog" Effect.

Organizations must also guard against the danger of **normalizing creeping risks** — the classic boiling frog effect, where slow but dangerous changes go unnoticed until it's too late. Traditional audits, tied to fixed checklists and annual cycles, are especially vulnerable.

A dynamic risk-based audit, by contrast, keeps the organization alert through:

**Continuous Risk Sensing** → Detects **"slow boil"** changes using ERM data and threat intelligence.
**Adaptive Audit Planning** → Updates scope regularly instead of waiting for annual cycles.
**Scenario Testing** → Explores **"what if"** outcomes for emerging risks.
**Feedback Loops** → Lessons from each audit flow back into risk management.

***Like a thermometer in the water, it alerts leadership before the frog boils.***

## Creating a Closed Loop

Integration also ensures that risk and audit work from the same picture. Risk teams identify what could go wrong. Audit teams test whether controls actually work. Together, they strengthen the closed loop introduced earlier, ensuring that both functions work from the same risk picture and guide strategy in unison

## Key Takeaways

**Audit and Risk functions both play vital roles in governance, and** organizations depend on them for assurance and trust.
**But** when they operate in silos, assurance becomes backward-looking, creeping risks are normalized (the "boiling frog" effect), and boards receive fragmented messages.
**Therefore**, integration is essential — Risk informs Audit, Audit validates Risk, and together they sustain a forward-looking loop that strengthens posture, reduces exposure, and builds trust.

## Conclusion

Integration is not about coexistence; it is about sustaining the closed loop between risk and audit. When that loop is active, organizations strengthen posture, reduce exposure, and build trust with boards, regulators, and stakeholders.

Integration is not just the fusion of synergies — it is a harmonized march toward sustained success.

After all, it takes two to tango. Integration builds trust. Passion sustains it. Passion is our strength. In the end, it is passion — not process alone — that defines our true strength.