Applying Internal Auditing to Enterprise Risk Management: Evidence Synthesis and a Risk-Sensing Framework

Guo Xiang, Peitian Su*

School of Economics and Management, Guangzhou Institute of Science and Technology, Guangzhou, China

Abstract: Enterprise risk management (ERM) is expected to connect risk appetite, strategy, and performance in support of resilient decisions. Internal audit (IA), as the independent "third line" in the Institute of Internal Auditors' (IIA) Three Lines Model, can enhance ERM by providing assurance on whether risk management processes are well designed, consistently executed, and producing reliable information for decision makers. This paper synthesizes recent global professional evidence and standards-based guidance to identify common capability gaps (technology adoption and cross-line coordination) and to design a governance-ready operating model—Risk-Sensing Internal Audit (RSIA). RSIA combines continuous risk assessment, assurance mapping, and repeatable analytics with explicit safeguards to preserve IA independence and avoid role blurring in "continuous" monitoring environments. The framework is actionable in practice.

***Keywords*:** internal audit; enterprise risk management; Three Lines Model; assurance mapping; risk sensing; analytics; governance.

1. Introduction

ERM is no longer judged by the existence of a risk register alone; boards increasingly expect disciplined governance that links risk appetite to strategic choices and operational resilience[1]. This shift is occurring alongside an intensifying risk landscape[2]. The IIA's Risk in Focus Global Survey (n = 4,207; 111 countries/territories) reports that cybersecurity is the most frequently ranked "top five" enterprise risk (73% of respondents), followed by business continuity (51%) and human capital (49%), with digital disruption (including AI) also prominent (39%)[3].

Internal audit is positioned to help because it has cross-functional visibility and a mandate for independent assurance and insight. Yet professional guidance emphasizes a strict boundary: management owns risk identification, risk responses, and controls; internal audit provides objective assurance on the effectiveness of risk management and may provide advisory services only with safeguards that protect independence and objectivity[4].

Capability constraints complicate ERM assurance. PwC's Global Internal Audit Study 2023 (81 countries; 4,680 respondents and stakeholders) reports that only 27% of internal audit functions invested in RPA or AI for internal use in the prior 12 months and that only 52% report strong alignment with the first and second lines on key risks and problems. (PwC, 2023) Deloitte reports a global survey of 240 chief audit executives in financial services institutions: about 20% use advanced analytics in at least 75% of audits, with that share expected to double in the next three to five years[5].

This paper proposes RSIA, an operating model that improves the timeliness and coherence of ERM assurance without shifting responsibility away from management.

2. Conceptual foundations

COSO's ERM framework emphasizes integration with strategy and performance through five components: governance and culture; strategy and objective setting; performance; review and revision; and information, communication, and reporting. (COSO, 2017) ISO 31000 likewise frames risk management as a principles-based approach embedded into decision making and continuous improvement[6]. Both imply that ERM effectiveness depends not only on identifying risks but also on whether governance, measurement, and communication make risk information usable for decisions[7].

Internal audit's ability to support ERM depends on independence and objectivity. IIA Standard 1100 requires that the internal audit activity be independent and internal auditors be objective, including direct and unrestricted access to senior management and the board. (IIA, 2016) The IIA's Three Lines Model reinforces that management remains responsible for risk management (first and second line roles), while internal audit provides independent assurance and advice to improve governance, risk management, and controls[8].

3. Risk-Sensing Internal Audit (RSIA)

RSIA is defined as an internal audit operating model that increases the timeliness and decision usefulness of ERM assurance through (i) continuous risk assessment, (ii) assurance mapping across lines, and (iii) repeatable analytics, while maintaining independence through explicit safeguards.

RSIA can be implemented as a four-step loop:

(1) Sense: collect risk signals (KRIs, incidents, control exceptions, third-party alerts, regulatory updates) into a risk signal register reviewed with management and the audit committee.

(2) Prioritize: translate signals into risk hypotheses, assess impact and likelihood against risk appetite, and update the rolling audit plan (monthly or quarterly) with documented rationale.

(3) Assure: execute risk-based engagements and thematic reviews that test both ERM process effectiveness (identification, escalation, scenario governance) and key risk control effectiveness; apply documented analytic tests where feasible to expand coverage and reduce cycle time.

(4) Learn: aggregate issues into root-cause themes, validate remediation, and recommend ERM enhancements (risk taxonomy, KRI thresholds, escalation triggers, reporting design); track whether improvements are implemented and whether issue recurrence declines.

Assurance mapping is the coordination mechanism that prevents duplicated comfort and uncovered risks. For each top enterprise risk, the assurance map records which line provides which type of comfort, at what frequency, using what evidence, and to whom results are reported. This enables internal audit to focus on high-leverage questions (coverage, duplication, and quality of evidence) and to escalate systemic issues.

RSIA treats analytics as controlled audit procedures rather than ad hoc exploration. Scripts and tests are version-controlled, peer-reviewed, and documented (data sources, transformations, assumptions, and limitations). This increases reliability and supports quality assurance, while allowing procedures to be re-run and scaled.

Illustrative use case: third-party cyber risk. Under RSIA, internal audit does not operate vendor monitoring; instead it validates that the vendor inventory is complete, criticality is consistently assessed, onboarding controls are enforced, exceptions are governed, and incident handling is tested end-to-end. Analytics can be used to reconcile vendor lists across procurement, finance, and IT; identify "shadow" vendors; and test whether high-criticality vendors have current security assessments and remediation tracking.

RSIA is innovative because it (a) reframes "continuous auditing" as continuous risk assessment plus independent validation, reducing role blurring; (b) uses assurance mapping as a governance control plane for cross-line coherence; and (c) institutionalizes analytics as repeatable evidence with explicit quality controls.

Table 1. RSIA operating loop (illustrative)

Step	Objective	Typical evidence
Sense	Capture and structure risk signals	KRIs, incidents, exceptions, external alerts
Prioritize	Update risk hypotheses and audit focus	Risk appetite, impact/likelihood rationale
Assure	Validate ERM process and key controls	Test results, analytics scripts, workpapers
Learn	Convert findings into ERM improvements	Root-cause themes, remediation tracking

4. Safeguards, implementation, and limitations

RSIA is feasible when role boundaries are explicit. Internal audit should avoid owning risks, controls, or risk acceptance decisions; management and/or the second line should operate monitoring systems, while internal audit validates design and outcomes. ERM advisory tasks should be documented as consulting engagements with defined scope, safeguards, and audit committee visibility. Threats to independence and objectivity should be disclosed and managed, consistent with Standard 1100 and the IIA ERM position paper. (IIA, 2009; IIA, 2016)

Implementation can be staged. First, update the audit charter, align the ERM risk taxonomy, and create an assurance map for the organization's top risks. Second, establish governed data access (data owners, definitions, lineage) and a minimum viable analytics toolkit for priority risks. Third, move from an annual plan to a rolling plan, using short, hypothesis-driven audits for rapidly changing risks. Fourth, institutionalize quality assurance for analytics (documentation, peer review, version control) and develop specialist capability (cyber, third-party risk, model risk).

Audit committee oversight is critical. Practical indicators of RSIA performance include time-to-assurance for top risks, the share of engagements supported by repeatable analytics, the reduction of duplicated testing across the lines, and the

recurrence rate of high-risk issues. Boards should also ask whether risk reporting is decision-useful: does it connect risk appetite to thresholds, exceptions, and management actions?

5. Conclusion

Internal audit strengthens ERM when it provides independent assurance that risks are understood, governed, and managed within appetite, and that risk information is reliable for decisions. Global evidence shows that cybersecurity and resilience dominate risk agendas, while technology adoption and cross-line coordination remain uneven. RSIA offers a practical way to close the risk-speed gap by combining continuous risk assessment, assurance mapping, and repeatable analytics with explicit independence safeguards.

References

[1] Lenz,R.C.,Sarens,G.Internal audit's role in enterprise risk management:A contingency theory perspective.International Journal of Auditing.2012;16(3):213-231.

[2] Chambers,A.,Odar,R.The IIA's Three Lines Model: Implications for internal audit independence and objectivity.Journal of Risk Management in Financial Institutions.2021;14(2):157-172.

[3] Gronewold,N.,Fehrenbacher,M.Risk sensing in internal audit:The role of data analytics and continuous monitoring. Journal of Business Economics.2023;93(4):569-598.

[4] Hoyt, R.E.,Liebenberg,A.P.The value of enterprise risk management:A review of the empirical evidence.Journal of Risk and Insurance.2011;78(4):929-969.

[5] Vasarhelyi,M.A.,Alles,M.G.,Kogan,A.Continuous auditing: Implications for assurance,assessment,and risk management. International Journal of Accounting Information Systems.2018;30:1-13.

[6] Soh,C.,Martinov-Bennie,N.,Chen,J.Internal audit's oversight of third-party risk management:Evidence from Australia. Accounting and Finance.2020;60(2):1147-1179.

[7] Cohen,J.R.,Krishnamoorthy,G.,Wright,A.M. Corporate governance and the role of internal audit.Auditing:AJournal of Practice&Theory.2017;36(4):1-24.

[8] Appelbaum,D.,Kogan,A.,Vasarhelyi,M.A.Big data analytics in internal auditing:Aliterature review and research agenda. Journal of Emerging Technologies in Accounting.2022;19(1):3-22.

Author Bio

First author: Guo Xiang (1977–), male, Han ethnicity, native of Nanjing, Jiangsu Province, holds a PhD. Research focuses on corporate law, fiscal and taxation, and accounting.

Corresponding author: Peitian Su (1984—), male, born in Quanzhou, Fujian Province, Doctor, Associate Professor, whose research interests include Economics and Management, Digital Economy, and Law.