May 20, 2026

The Institute of Internal Auditors
1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746

Via email: Standards-Guidance@theiia.org (Role of IA in ERM)

Re: Society for Corporate Governance Comment Letter on IIA Stakeholder Review Draft – Statement of Position: The Role of the Internal Audit Function in Enterprise Risk Management (ERM)

Dear Ladies and Gentlemen:

On behalf of the Society for Corporate Governance (the "Society"), we appreciate the opportunity to review and comment on the Institute of Internal Auditors' (IIA) stakeholder review draft of its Statement of Position, *The Role of the Internal Audit Function in Enterprise Risk Management (ERM)* (the "ERM Draft").

The Society is a professional membership association of corporate secretaries, general counsel, and other governance professionals serving public companies and other organizations. Our members work closely with boards of directors and senior management on matters relating to governance, board oversight, risk management, compliance, and disclosure. As a result, frameworks addressing the interaction among the board, management, risk management functions, and internal audit are of significant interest to our membership.

The Society recently submitted a comment letter on the IIA's stakeholder review draft of its updated *Three Lines Model*.[1] Consistent with the themes expressed in that letter, our comments below are offered with the objective of supporting the continued usefulness of the ERM framework while encouraging the IIA to preserve its principles-based, flexible, and non-prescriptive nature. In providing these comments, the Society understands that the ERM Draft is intended to provide conceptual, principles-based guidance regarding governance and organizational practices, rather than to prescribe legal requirements or standards of conduct.

Support for a Principles-Based Framework

The Society supports the ERM Draft's positioning as a principles-based framework designed to provide high-level guidance regarding the role of the internal audit function in enterprise risk management within a modern governance environment.

We believe such frameworks are most effective when they describe functional roles and relationships at a conceptual level, rather than prescribing specific organizational structures, governance arrangements, or operational practices. Organizations vary widely in their size, complexity, regulatory environment, and

[1] Society: Comment Letter on IIA Stakeholder Review Draft - Three Lines Model, March 2026

business and risk profiles, and a principles-based approach allows for appropriate flexibility in implementation.

Importance of Maintaining Flexibility

We encourage the IIA to continue emphasizing that the ERM framework is intended to be adaptable and should not be interpreted as favoring particular governance structures or approaches.

The ERM Draft includes helpful discussion of coordination, reliance, and, in certain contexts, more structured approaches to aligning assurance and advisory activities.

As noted in our prior comment letter, however, frameworks intended as conceptual guidance are sometimes used as benchmarks for evaluating governance practices. Clarifying that organizations may achieve effective enterprise risk management through a variety of approaches and processes—and that differing structures do not necessarily indicate heightened risk or weaker governance—would help preserve the framework's intended flexibility. For example, while integrated assurance approaches may create efficiencies in some organizations, the costs and complexity associated with coordination, shared methodologies, and aligned processes may outweigh the benefits in others. As a result, the appropriate degree of integration and coordination may vary across organizations and over time.

Clarity and Precision of Language

The Society encourages the IIA to review the ERM Draft for clarity and precision, particularly where terminology may be interpreted differently across organizations or where concepts are not clearly defined. We believe it is important to be as clear as possible in articulating the principles in the framework. This helps avoid confusion in *interpreting* the principles while allowing flexibility in their *application* and *implementation*.

Several phrases used in the draft would benefit from clarification to promote consistent understanding. For example:

- References to "significant" risks in the context of escalation to the board may be interpreted differently across organizations depending on risk appetite, governance structures, and escalation thresholds and processes;[2]
- The statement that risks are "reported with integrity" may benefit from further explanation to clarify the intended meaning in this context;[3]
- The draft indicates that the board is responsible for approving the organization's risk appetite and accountable for "ensuring that risk-related information supports effective oversight and decision-making." While "risk appetite" is a commonly used governance and ERM concept, the ERM Draft would benefit from additional clarity regarding both the intended meaning of "risk-related information" and the scope of the board's oversight role in relation to such information. In particular, terminology such as "ensure" may imply a level of operational responsibility that differs from the board's oversight role and its practical reliance on management and reporting structures for risk-related information. Terminology such as 'review' or 'oversee' may more accurately reflect the board's oversight function in this context;[4]
- References to safeguards being "visible to the board" should be clarified to indicate how such visibility could be achieved in practice. Moreover, it should not be assumed that "formal board approval" of internal audit's assumption of additional ERM-related responsibilities and

[2] ERM Draft page 3 ("Internal Audit Assurance in Relation to ERM").
[3] ERM Draft page 3 ("Internal Audit Assurance in Relation to ERM").
[4] ERM Draft page 3 ("ERM Within the Governance System").

acknowledgment of associated risks and mitigation measures is required to support the board's visibility;[5]

- The use of terms such as "governance" in certain contexts may benefit from additional specificity; [6]and
- Certain provisions—such as references to the framework being "used with" boards, regulators, or other stakeholders—particularly in the context of statements lacking in clarity or precision such as those noted above—may invite counterproductive misuse of the proposed framework by third parties.[7]

Clarifying these and similar terms would help support consistent application of the framework across organizations.

Avoiding Overstatement and Generalization

The Society encourages the IIA to review the ERM Draft to avoid statements that may be interpreted as overbroad or not universally applicable across organizations.

For example, statements describing the ERM framework, together with the Three Lines Model, as providing a "holistic" framework for organizational governance may be read as extending beyond their intended scope as conceptual guidance. The use of "organizational governance" in this context is unclear and implies a breadth of scope that may extend beyond the intended role of the framework.[8]

Similarly, certain statements regarding internal audit capabilities or stakeholder expectations may not apply uniformly across organizations. For example:

- Not all organizations maintain an internal audit function, and those that do may differ significantly in structure, reporting, scope, and capabilities;[9]
- The ERM Draft suggests that internal audit's advisory services "should enhance governance and management…"[10]. While this may be true in a general sense, in this context, we recommend that it be adjusted to specifically reference risk management. For example, the draft could read: "Advisory services may support an organization's risk management practices and risk governance framework"; and
- Assertions regarding the expectations of boards or stakeholders with respect to internal audit's role in ERM may vary depending on organizational context.[11]

---

[5] ERM Draft pages 5 – 6 ("Standards to Preserve Independence and Objectivity").

[6] For example, the draft provides: "ERM provides the governance context and integration mechanism that elevates..." (page 3, "Defining Enterprise Risk Management") See also, "The internal audit function may also provide advisory services that improve governance and…" (page 4, "Internal Audit Advice in Relation to ERM") and "The IIA provides a holistic, flexible framework of organizational governance…" (page 2, "Purpose and Context") discussed further below.

[7] ERM Draft page 2 ("Audience").

[8] ERM Draft page 2 ("Purpose and Context").

[9] In practice, where the internal audit function reports functionally to a board body (which is a leading but not universal practice), it typically reports to the audit committee or another board committee rather than the full board. According to the Internal Audit Foundation's "2026 North American Pulse of Internal Audit" report based on its late 2025 survey of 373 internal audit leaders across organization types and industries (84% US-based companies), 85% of chief audit executives report functionally to the audit committee, board, or similar body, while the balance report functionally to a member of management.

[10] ERM Draft page 4 ("Internal Audit Advice in Relation to ERM")

[11] For example, the statement on page 4 ("Internal Audit Assurance in Relation to ERM") of the ERM Draft: "Because the internal audit function is positioned to take an enterprise-wide view…" assumes a certain organizational structure that may not exist in a particular organization.

We encourage the IIA to calibrate such statements to reflect that practices, structures, and expectations differ across organizations.

Role Clarity and Distinction Among Functions

The Society appreciates the ERM Draft's recognition that, in practice, responsibilities relating to enterprise risk management may overlap across management, second-line functions, and the internal audit function. At the same time, descriptions of internal audit involvement in activities such as designing ERM frameworks, coordinating enterprise risk activities, monitoring risk indicators, or preparing enterprise risk reports underscore the importance of maintaining clear distinctions among operational, advisory, and assurance roles and preserving independence and objectivity through appropriate safeguards and organizational flexibility.

Independence and the Balance Between Assurance and Advisory Activities

The ERM Draft includes a detailed discussion of safeguards designed to preserve independence and objectivity in situations involving overlapping responsibilities between advisory and assurance activities. While these safeguards are helpful, the level of specificity in certain areas could be interpreted as establishing expected practices or minimum conditions.

As noted above, assumptions or expectations that the board formally approve arrangements where internal auditors assume additional ERM-related responsibilities and acknowledge associated risks and mitigation measures, or that actual or perceived threats to objectivity be communicated directly to the board, may not reflect the range of governance structures across organizations. Similarly, references to internal audit involvement in the design, coordination, or operation of ERM processes reinforce the importance of preserving organizational flexibility and maintaining clear distinctions between operational, advisory, and assurance responsibilities. Clarification that safeguards may be implemented in different ways depending on organizational context would further support the framework's principles-based approach.

Board Oversight Considerations

The ERM Draft appropriately recognizes the board's role in overseeing governance, risk management, and control processes. At the same time, the board's role may differ across these areas in practice, including where boards commonly exercise more direct decision-making authority with respect to governance matters and a broader oversight role with respect to risk management and controls.

We encourage the IIA to clarify that the framework is not intended to create, prescribe, or expand governance or other obligations of boards of directors, nor to specify the manner in which such responsibilities should be carried out.

In particular, certain provisions would benefit from clarification to reflect the practical realities of board oversight. For example:

- As noted above, statements suggesting that boards "ensure" that risk-related information supports effective oversight and decision-making may be read as implying a level of direct responsibility that, in practice, depends on information provided by management and other functions;[12]

[12] The draft indicates that board is accountable for "ensuring that risk-related information supports effective oversight and decision-making." It is unclear what "risk-related information" means in this context or how the board could "ensure" this given its reliance on management to share or provide visibility of risk-related information.

- The ERM Draft asserts board “expectations” regarding certain models and frameworks, in addition to noting the expectations of unenumerated ‘stakeholders’, without providing any citation or point of reference. This may create the impression that certain standards or approaches reflect broadly accepted governance expectations without identifying a supporting reference point or organizational context; and
- References to board approval of specific arrangements or visibility into detailed reliance decisions may be more appropriately understood as matters typically addressed at the committee level, or through broader oversight mechanisms, as discussed above.

Clarifying these points would help avoid unintended interpretations regarding the scope of board responsibilities.

Coordination, Reliance, and Integrated Approaches

The Society appreciates the ERM Draft’s emphasis on coordination and appropriate reliance among assurance and advisory providers. At the same time, as noted in our prior comment letter, references to coordinated or integrated approaches may be interpreted as favoring particular governance models. We encourage the IIA to reiterate that organizations may achieve effective coordination through a variety of approaches depending on organizational structure, complexity, and governance needs.

Conclusion

The Society appreciates the IIA’s ongoing efforts to develop guidance addressing the role of the internal audit function in enterprise risk management.

Consistent with our prior comments on the Three Lines Model, we encourage the IIA to maintain the ERM framework’s principles-based, flexible, and conceptual nature, and to avoid language that could be interpreted as prescribing specific governance structures, expanding board responsibilities, or establishing de facto benchmarks for evaluating organizational practices.

Thank you for considering the Society’s comments. We would be pleased to discuss our views further or provide additional input as the IIA continues to develop this important framework.

Respectfully submitted,

Randi Val Morrison
General Counsel & Chief Knowledge Officer
Society for Corporate Governance

Paul F. Washington
President & Chief Executive Officer
Society for Corporate Governance