COSMOS
Navigate the Compliance Universe

Compliance Today - May 2023

Dhara Satija (dharasatija@paulhastings.com, linkedin.com/in/dharasatija/) is Healthcare Consulting Leader at Paul Hastings LLP, Andover, MA.

Destin Harcus (destin.harcus@adventhealth.com, linkedin.com/in/destinharcus/) is Executive Director of Internal Audit at AdventHealth, Altamonte Springs, FL.

One goal, two teams: Aligning on managing risk and audits

by Dhara Satija and Destin Harcus

In today's world, with unpredictable economic and geopolitical events that have contributed to relentless volatility, it is essential for risk and compliance professionals and their teams to extend their capabilities to help cut through the silos and develop risk-sensing and measurement capabilities. There is a business imperative for organizations to become proactive, data-driven, and risk-intelligent in how they manage risk.

The Institute of Internal Auditors Inc.'s (IIA) Three Lines Model provides a framework for organizations to align activities using communication, coordination, cooperation, and collaboration.[1] It highlights leading practices to strengthen and sustain collaboration across the three lines and offers practical considerations to elevate an organization's risk, compliance, and internal audit programs.

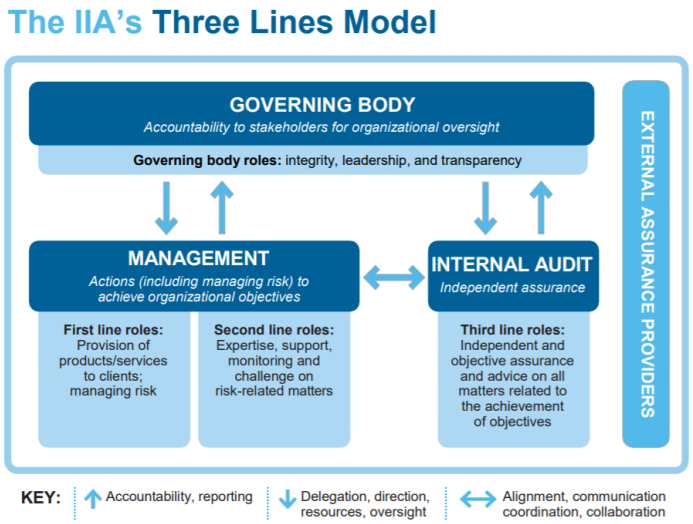
What is the Three Lines Model?

As the name suggests, the Three Lines Model comprises three "lines": a governing body, management, and internal audit. Each line offers unique perspectives to help ensure the organization's risks are appropriately managed across the enterprise.

The objectives of the Three Lines Model are:

- To provide clarity on roles overseeing risk and controls.
- To align risk management objectives to help achieve optimal assurance activities and a lower cost of compliance.
- To help prevent over-indexing on risk mitigation activities and enhance focus on value creation.

Figure 1[2]



The Three Lines Model is centered around the following two goals:

1. **Risk-based decision-making**: A considered process that includes analysis, planning, action-taking, monitoring, and review while considering the potential impacts of uncertainty on organizational objectives.

2. **Assurance**: Independent confirmation and confidence related to achieving objectives.

The Three Lines Model was formerly known as the "Three Lines of Defense Model" but was shortened in 2020 by the IIA to de-emphasize a defensive approach. This acknowledges that risk-based decision-making is as much about seizing opportunities as it is about defensive moves.

Additional 2020 updates to the Three Lines Model included:[3]

- Enhanced mechanisms to improve *interactions and responsibilities* of those charged with governance.
- A greater emphasis on the role of the governing body, management, and internal audit to *enhance the value of the organization, not just protect it.*
- Increased recognition of *emerging risks* in advance to prepare the organization to mitigate, address, or take advantage of them.
- Increased awareness of the importance of *communication and collaboration.*
- *Confirmation that the role of internal audit is relevant* and assists the organization both strategically and operationally.

Overview of roles and responsibilities within the Three Lines Model

First line: Management (e.g., operations)

- *Lead and direct actions (including managing risk) and the application of resources to help achieve the organization's objectives.*
- *Maintain a continuous dialogue with the governing body and report on planned, actual, and expected outcomes*

linked to the objectives of the organization.

- *Establish and maintain appropriate structures and processes for managing operations and risk (including internal control).*
- *Confirm alignment with legal, regulatory, and ethical expectations.*

Second line: Management (e.g., compliance, legal)

- *Provide complementary experience, support, monitoring, and challenges related to the management of risk, including:*
    - The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, system, and entity level.
    - The achievement of risk management objectives, such as compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.
- *Provide analysis and reports on adequacy and effectiveness of risk management (including internal control).*

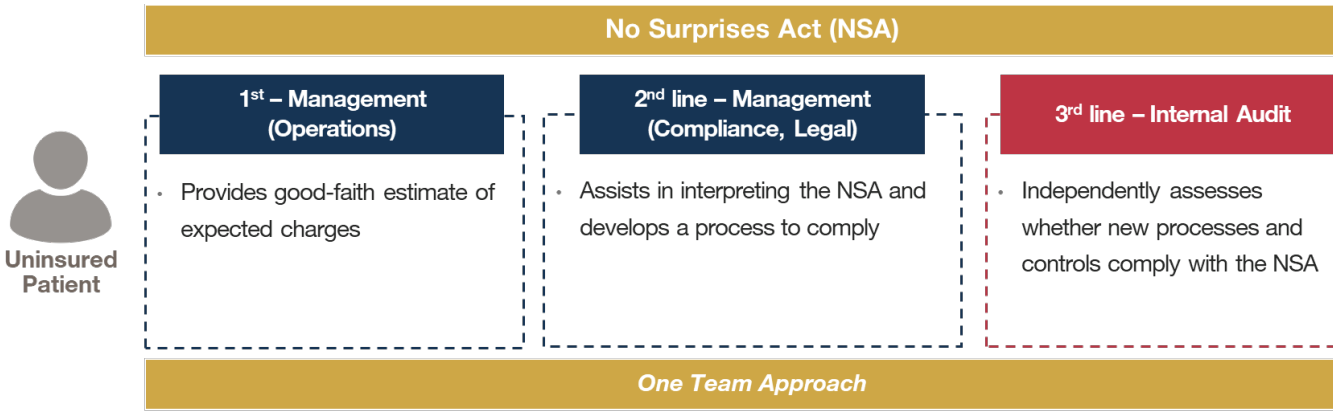
Third line: Internal audit

- *Maintain primary accountability to the governing body and independence from management responsibilities.*
- *Communicate independent and objective assurance and advise management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organizational objectives and to promote and facilitate continuous improvement.*
- *Report impairments to independence and objectivity to the governing body and implement safeguards as required.*

How does each line collaborate in practice?

The No Surprises Act (NSA) became effective in 2022 and provides federal protections against individuals receiving surprise medical bills for certain services.[4] One NSA requirement is that healthcare providers give uninsured (or self-pay) individuals good faith estimates of expected charges for scheduled healthcare services. This creates multiple layers of risk for the organization and requires all lines within the Three Lines Model to work together to develop processes and controls to comply with the new NSA requirements. Figure 2 is an illustrative example of how these lines work together in practice.

Figure 2



Collaboration in practice: Practical considerations for compliance and internal audit

Increased coordination between compliance and internal audit is critical in increasing overall efficiency and evolving the capabilities of both teams. You'll see in Figure 3 examples of areas where significant coordination/collaboration can be experienced, given traditional compliance, and internal audit roles and responsibilities.

Figure 3

Planning risk assessment/universe	Coordination of key stakeholders to be included in risk assessment discussions to incorporate perspective (e.g., previous audits/issues)
Conducting risk assessment	Collaborated identification of priority risks to include in yearly workplans based on external (trends) and internal (interviews) perspectives
Developing workplan(s)	Collaborated development in the scopes for audits / assessments for identified risks / focus areas; identifying possible "joint audits"
Conducting audit(s)	Ongoing collaboration and communication during audits to provide feedback and guidance to both teams; shared resourcing of selected audits
Monitoring & analytics	Coordination in monitoring and tracking status of management action plans until completion; Opportunity for teams to leverage data analytics for efficient monitoring

Harmonizing and operationalizing between compliance and internal audit

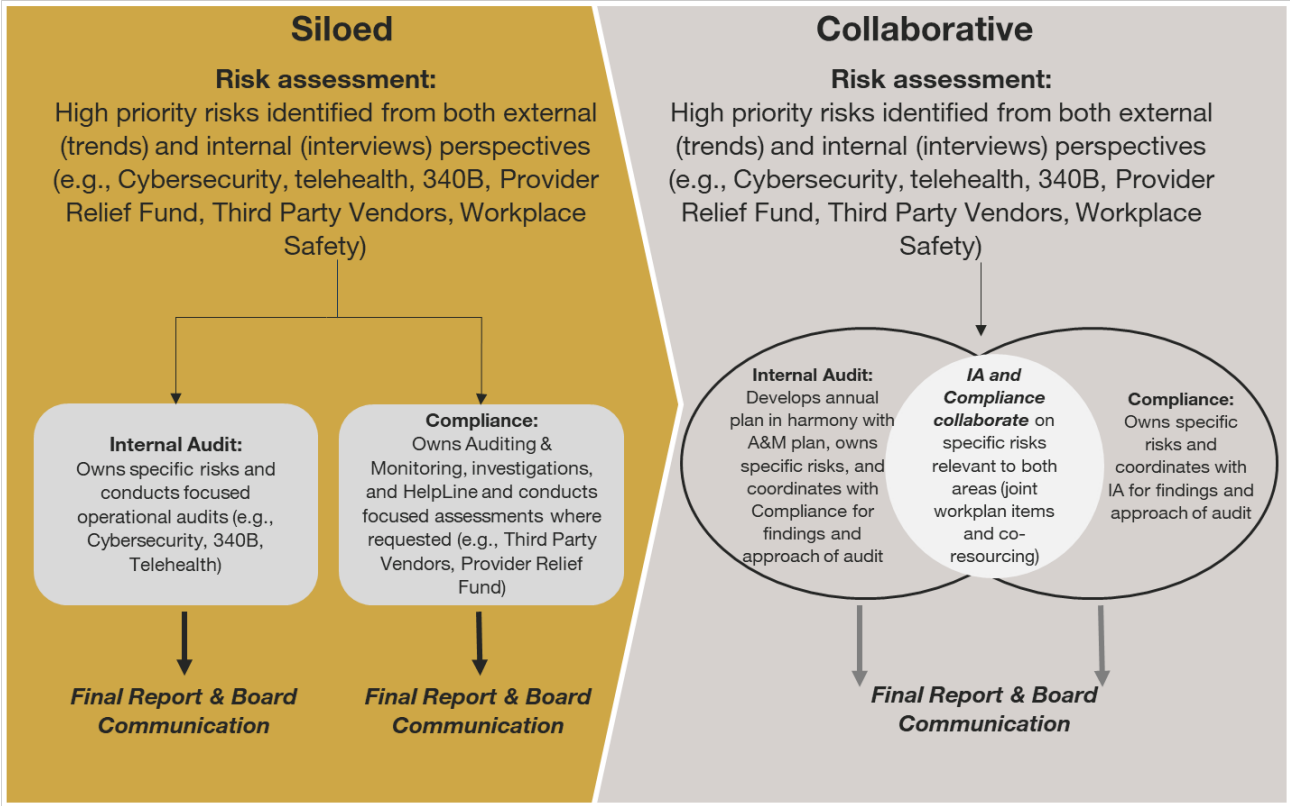
Effective collaboration requires intention and ongoing communication. Although each team has its own roles and responsibilities, their common focus on risk warrants collaboration across risk assessment, project execution, and reporting processes. A lack of collaboration can facilitate each team operating in a silo, naturally reducing enterprise-wide risk mitigation's effectiveness and/or efficiency. It is not uncommon for compliance

and internal audit to focus on the same risk but assess that risk independently, perform a project around that risk without input from the other team, and report results to the primary audience of the respective team. Successful collaboration moves away from this kind of siloed approach and harnesses the expertise of each team to provide deeper risk coverage and a broader perspective.

Collaboration may occur more naturally in organizations where compliance and internal audit report to the same leader. In these instances, it is important to keep roles and responsibilities clear, as it is imperative for internal audit to maintain its independence.

Healthcare organizations should pause to reflect on their current risk management programs and structure and take measures to facilitate and maintain consistent collaboration across the organization to eliminate operational silos and strengthen management of risks (see Figure 4).

Figure 4



Leading practices to help strengthen and sustain collaboration across the Three Lines Model

As organizations move to implement or advance the Three Lines Model, keeping in mind the leading practices and common pitfalls can help further assess the model's value. Although the listing below is not exhaustive, it does represent leading practices and common pitfalls that many of us have likely faced in our respective roles.

Common leading practices include:

- "One team" culture and common understanding of risk
- Dynamic, talented, and experienced with an innovative mindset
- Unified approach and guiding principles

- Effective stakeholder management, collaboration, and timely communication
- Tools, digital assets, analytics, and automation
- Knowledge sharing

Common pitfalls include:

- Silo mentality, leading to a lack of coordination and duplication of risk areas and gaps
- Misaligned or conflicting assurance opinions
- Duplication of assurance activities between three lines
- Duplicative testing results in less time to focus on the business at hand
- Overfitting or overstrengthening of the second line

Embracing the leading practices and intentionally avoiding common pitfalls can provide a natural harmony between three lines. An intentional review of the pitfalls can assist in proactive identification of opportunities to align more closely. Who can relate to the situation in which you receive feedback that another team has already requested a request made by your team? If so, this might be a symptom of many of the pitfalls listed above, as duplication amongst the three lines can be a common cause. Contrast this with a "one team" culture in which teams work together to understand and address risk holistically. Value can be unlocked as an organization strives toward continued alignment.

Conclusion

Harnessing the full potential of the Three Lines Model can bring alignment and value to your organization. It starts with the governing body, management, and internal audit aligning with the organization's objectives. Once aligned, sharing risk across functions promotes the identification of risks from different perspectives. Compliance and internal audit can further align and collaborate to increase overall efficiency and evolve the capabilities of both teams. When effective, organizations may find themselves more effective in risk-based decision-making and seizing opportunities that come with the dynamic environment we all operate in today.

Takeaways

- Raised expectations – Risk and compliance professionals need to be proactive, data-driven, and risk-intelligent in managing risk.
- One culture – Successful coherence across the three lines is based on regular and effective coordination, collaboration, and communication.
- Enhanced perspectives – Risk-sharing for cross-functional coverage promotes the identification and management of risks from different perspectives.
- Both proactive and defensive – Risk management is no longer just about protecting organizational reputation but also about seizing opportunities.
- Collaboration benefits – Increased coordination between compliance and internal audit is critical in increasing overall efficiency and evolving the capabilities of both teams.

1 The Institute of Internal Auditors, *The IIA's Three Lines Model: An update of the Three Lines of Defense*, July 2020, https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf.
2 The Institute of Internal Auditors.
3 The Institute of Internal Auditors.
4 Centers for Medicare & Medicaid Services, "Ending Surprise Medical Bills," last modified December 5, https://www.cms.gov/nosurprises.