Integrated Risk Functions

Industry changes call for an alliance between risk and compliance

By Lisa Adinolfi-Tejera, CPA, CHC, Michael Visconti, CIA, Adam Bruhnke, MBA, and Jason Wallace, JD, MPH

The Office of Inspector General's (OIG) Practical Guidance for Healthcare Governing Boards on Compliance Oversight has recently laid out guidance on the interrelationships between traditionally siloed risk and governance functions, including compliance, internal audit, legal and human resources.

Lisa Adinolfi-Tejera is a Partner leading PwC's New York Metro Risk Assurance Healthcare Practice. Lisa also manages internal audit co-sourcing and outsourcing arrangements. She can be reached at Lisa.Adinolfi-Tejera@pwc.com and (646) 471-3646.

Mike Visconti is a Director in PwC's Risk Assurance Internal Audit Services practice. Mike has managed numerous internal audit engagements and provided consulting services. Mike can be reached at Michael.J.Visconti@pwc.com and (646) 471-0475.

Adam Bruhnke is a Manager in PwC's Risk Assurance Internal Audit Services practice providing advisory services related to internal audit, risk management and compliance. You can reach Adam at Adam.M.Bruhnke@pwc.com and (646) 471-8167.

Jason Wallace served as National Compliance Director and Regulatory Counsel for the largest emergency medical services provider in the world and has provided compliance and in-house legal counsel services to leading regional healthcare organizations. Jason can be reached at Jason.P.Wallace@pwc.com and (917) 825-3976.

In responding to unprecedented market disruption in the industry, healthcare leaders are taking a step back and reevaluating their risk management programs to address an ever-evolving risk landscape and help ensure they are protecting the value of these programs and capitalizing on them.

To do this, some healthcare organizations are integrating risk management efforts with coordinated IA and compliance functions.

Risk management structure

Organizations' risk profiles are constantly changing, causing senior management to rethink how they are addressing risk. Organizations are adapting to the new risk landscape by increasing their use of data analytics and subject matter specialists, and also rethinking risk management organizational structure.

Traditionally, organizations have been structured with the Chief Audit Executive (CAE) and Chief Compliance Officer (CCO) reporting to the Chief Financial Officer (CFO) or Chief Executive Officer (CEO), for administrative purposes. Functionally these individuals reported to the organization's governing boards or committees (e.g., audit committee, compliance committee).

The healthcare sector is seeing a growing trend where organizations are designating a Chief Risk Officer (CRO) to oversee risk management functions, including internal audit (IA), compliance, and enterprise risk management (ERM). In this role, the CRO supports holistic reporting to executive leadership and the board, with a balanced focus of resources on both IA and compliance.

In addition, the CRO is responsible for coordinating overall risk management activities among these functions (which provides a consistent perspective on risk across the organization), while the CAE and CCO maintain independence by reporting functionally to the audit and compliance committees.

Five pillars of successful coordination

It is important to clarify that organizations are not being urged to combine their IA and compliance functions, but

> We hear consistently from the C Suite how much value they see when Internal Audit and Compliance work together.
>
> – Terry Puchley, Partner, PwC Risk Assurance National Health Industries Leader

rather to coordinate key activities and collaborate on risk to better serve their organizations.

IA and compliance should be viewed as separate lines of defense for the organization, each of which supports the appropriate level of oversight and independence expected by the organization. They should, however, align efforts, leverage each other's work where possible, and develop and leverage a common risk framework and risk language. See the sidebar for a discussion of the benefits that can be found in the intersection of roles when compliance and IA find coordinated ways to work together.

Your organization can facilitate integrated risk management by implementing coordination on key IA and compliance activities within five pillars. A few initial steps can be taken within each pillar to enhance coordination across IA and compliance to maximize value and efficiency.

Meeting in the middle—coordinating roles

Compliance continues to provide support and independent challenge on establishing and enforcing policies and procedures and assessing changes to laws and regulations.

Internal audit continues to provide independent assurance on management and second level of defense risk management functions, appropriateness and effectiveness of internal controls, and whether policy is being implemented effectively.

Coordinated benefits can include:

- Knowledge sharing and developing a common risk language
- Efficiencies in testing and coverage
- Cost savings
- Stronger control environment
- Improvements to processes and root cause analysis efforts

Pillar 1 – Business partners

IA and compliance should be strategic partners in mitigating enterprise risks. Initiate coordination between IA and compliance to jointly identify and assess group-level risks and coordinate/initiate the use of combined risk management plans.

Pillar 2 – Risk assessment

Coordinate or combine compliance risk assessment processes with IA risk assessment where possible (e.g., review and triage identified risks to determine whether each is in the compliance or IA scope).

IA and compliance should work together to leverage what ERM has done to facilitate a common risk framework.

Pillar 3 – Continuous monitoring

IA and compliance need to coordinate during annual work and audit plan development to identify areas that are more appropriate for continuous compliance monitoring, and work together to build the monitoring process such that compliance can efficiently monitor the risk and, once validated, IA can place reliance upon this risk mitigating activity.

Compliance, IA and relevant business areas should coordinate to develop key performance indicators (KPIs) and metrics that can facilitate monitoring and reporting of deficiencies identified during audits or reviews.

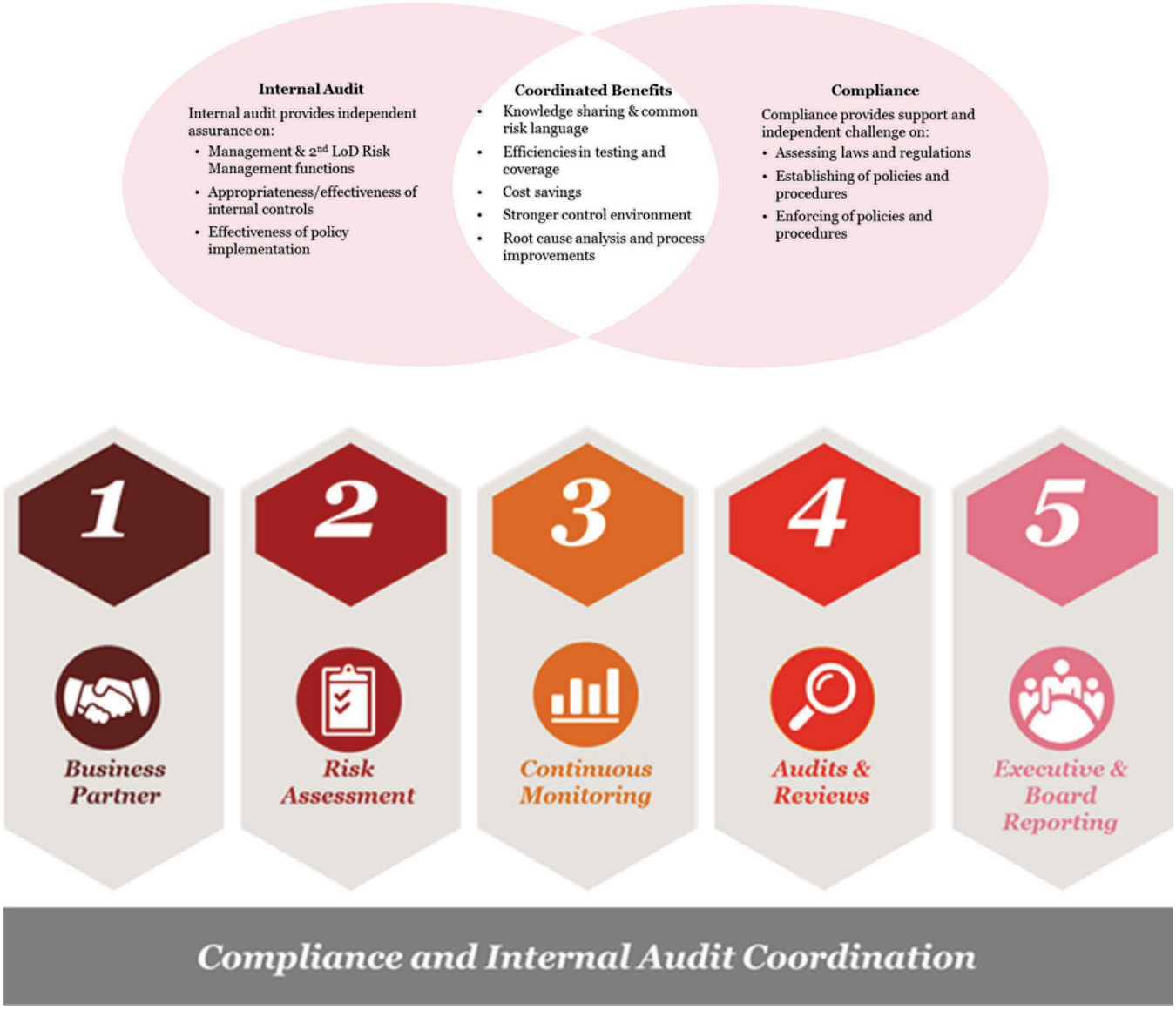
Formalize a process for information sharing between IA and compliance when related deficiencies are identified during audits and reviews, which will allow coordination in root cause analysis and development of a corrective action plan.

Pillar 4 – Audits and reviews

Identify additional opportunities to perform integrated assessments or audits between IA and compliance, and leverage the knowledge of staff members in other departments to increase efficiency during the planning process to develop a more holistic view of risk and increase efficiency.

IA and compliance should collaborate in development of annual work plans. The objective is to identify coordinated projects, minimize business area friction, and identify areas where IA can rely on compliance activities and divert those resources to address other risk areas.

Integrated Risk Functions: Coordinated Internal Audit and Compliance



Establish regular, formal meetings between IA and compliance to share the work that has been performed, discuss upcoming areas of focus and plan increased coordination.

Pillar 5 – Executive and board reporting

A close alliance between IA and compliance should help drive adoption of a common definition of risks, improve the organization's overall risk management effectiveness and allow presentation of common risk language to leadership.

Formalize a process for compliance and IA to hold pre-board and audit committee coordination meetings to assign roles and responsibilities regarding risk- and compliance-related reporting and minimize potential overlap in presentations.

Provide a risk coverage map to executive leadership and the board that depicts which risk management functions are responsible for providing assurance over each risk or risk area.

Facilitate routine coordination and communication between the three lines of defense. For example, legal, IA, compliance, ERM and business representatives should meet on a regular basis to discuss emerging risks and effectiveness of mitigation efforts, to share areas of concern or desired focus, and to define a common risk language.

> Organizations' business models and risk landscapes are evolving rapidly, and risk can no longer be managed in silos.
>
> – Jason Pett, Partner, US Internal Audit Leader at PwC

Benefits of coordination

Organizations that adopt a more integrated approach to managing risk and compliance issues may reap a number of benefits, including:

- Common risk language provided to the board and audit committee and leveraged by the business improves the ease of reporting to stakeholders (e.g. regulators), and the ability to track and respond to risk trends.
- Defines risk management needs and presents a clear understanding of roles and responsibilities of risk management functions (limits opportunity for things to fall through the cracks).
- Reduces the duplication of efforts across the organization (reduces effort and costs while improving risk function relationships with the organization).
- Reduces the risk of fines and sanctions due to noncompliance through more effective risk management.
- Facilitates greater investment in risk management by developing KPIs and Key Risk Indicators. **NP**

We Have Confirmed Diversion: Now What? – continued from page 19

agencies will allow them to investigate the incident and prosecute those responsible for the diversion."[8]

One individual had been caught diverting at several facilities in several states yet was still able to gain employment at another facility and go on to cause several patients to be infected with hepatitis C.

In that case, the New Hampshire Department of Health noted: "Drug diversion is a criminal activity and as such should be reported to law enforcement. Maintaining close working relationships between the dedicated drug diversion staff and local law enforcement can assist in coordinating activities to investigate drug diversion suspicions even prior to confirmation."[9]

Public health

With the possibility of bloodborne pathogen transmission in many diversion cases, it is advisable to reach out to public health officials, exchange contact information and discuss how these cases should be handled. In some states, the department of health gets involved early and has a substantial role, while in others the role of public health is less well established.

When diversion is suspected, facilities should discuss whether patient harm is possible or likely. If there is a risk of bloodborne pathogen transmission, as there always is in tampering cases, Infection Prevention should be consulted and a detail risk analysis should ensue. Depending on the risk, the local department of health may need to be contacted. Because time is of the essence in addressing bloodborne pathogen transmission, facilities should err on the side of reporting to the department of health.

Conclusion

Comprehensive reporting can mitigate potential civil and regulatory liability and protect patients. Having a robust reporting program is a credit to a hospital, since it demonstrates a commitment to patient safety. **NP**

Kim New, JD, BSN, RN, is the principal at Diversion Specialists. She is an expert in controlled substance security and DEA regulatory compliance, and a consultant to healthcare facilities across the country. She works with facilities to set up and expand their drug diversion programs. You can reach her at Kim_New@zoho.com or (865) 456-1813.

[8] DEA Pharmacist's Manual Section V(A)
[9] State of New Hampshire Hepatitis C Outbreak Investigation Report