Adding Value: Effective Risk Communication with the Audit and Compliance Committee

Challenges and roles of the key players as the risk playing field continues to evolve

By Kelly J. Sauders, CPA, MBA; Heather Hagan, CIA; and Ryan J. Pollock , CIA, CPA, CRMA

Kelly Sauders is a partner with Deloitte & Touche LLP with over 17 years experience providing services to healthcare providers. She specializes in providing risk assessments, internal controls and regulatory compliance services to healthcare providers. You can reach Kelly at KSauders@deloitte.com or (212) 436 3180.

Heather Hagan is a manager in Deloitte's Enterprise Risk Services practice. She assists healthcare providers with risk management, strategy and internal audit services as well as governance and regulatory compliance services for multi-institutional healthcare systems. You can reach Heather at HHagan@deloitte.com or (215) 439-1278.

Ryan Pollock is a Senior Consultant with Deloitte. He provides internal audit, risk management and strategy services to healthcare providers, and has participated in the development and execution of financial, operational, regulatory compliance and leading practice reviews. You can reach Ryan at RPollock@deloitte.com or (215) 446-5947.

In today's increasingly challenging and competitive marketplace, the importance of a healthcare provider's internal audit and compliance programs continues to reach new heights. The traditional perception of these programs acting as the organization's police or, alternatively, sitting on the sidelines, is outdated.

With new and complex payer requirements, increased scrutiny of regulatory agencies, limited capital resources and an ever-changing legislative platform, healthcare organizations are turning to their internal audit and compliance professionals to help them understand and meet the many expectations of the industry today. Further, today's internal audit and compliance professionals serve as advisors to help address and mitigate current and emerging risks facing their organizations.

To maintain an effective, value-adding role within the organization, internal audit and compliance professionals should be able to communicate risks in an intelligent, consistent manner. Moreover, they have a role to identify, prioritize and help the organization respond to risks that threaten the organization the most.

Additionally, internal audit and compliance leaders should clearly communicate various risk information—the results of an enterprise risk assessment and the opportunities identified during audits, including concerns raised through the compliance hotline—via meaningful dialogue with management and the audit and compliance committee(s).

Roles and challenges of the audit and compliance committee(s)

Healthcare organizations and their stakeholders rely on the judgment and skill of the audit and compliance committee of the board to actively govern areas such

as risk, mission, compliance and financial reporting. The changing industry dynamics, increased regulatory focus and expanding risk profiles in today's environment place an even brighter spotlight on the importance of effective board-level oversight.

Exhibit 1 – Common pitfalls in communicating with audit and compliance committees

1. Too much information
2. Too little information
3. Unclear information
4. Lack of prioritization
5. Reactive approach (vs. proactive)
6. Failure to speak the same language

As the healthcare landscape broadens and healthcare reform unfolds, the pace of change can be overwhelming for board members and can lead to a lack of confidence in an organization's ability to adapt and respond to these new demands. Today's environment can result in the board-level committee(s) not being aware of current risks associated with the organizations' operations, and in some cases, uncertainty regarding their role in the oversight of enterprise risk management.

Roles of the internal audit, compliance and risk management functions

In risk management, certain groups hold a unique role—namely, the groups that handle internal audit, compliance, and risk management functions.

Exhibit 2 – Risk management topics to consider

When a board committee is assessing the organization's risk management options, there are certain topics that should be considered and discussed, including:

1. The company's policies and processes for assessing and managing major risk exposures on an integrated, enterprise-wide basis
2. Key risks, vulnerabilities and plans to address them
3. The board's input and approval of the company's risk appetite
4. The capability of the company in preparing for, responding to and recovering from major financial risk exposures
5. The relationship between strategy and risk
6. The organization's ability to obtain the information required to make decisions
7. Individual and aggregate risk views of scenario planning
8. Mechanisms used by management to monitor emerging risks, including the efficacy of early warning indicators and how often they are reviewed.

Exhibit 3a – What are our risks?
Communicating an organization's risk profile may include a heat map that prioritizes risks based on their impact and vulnerability, and a risk list that provides both risk prioritization and categorization.

Risk Glossary		
Risk Title	**Risk Ranking**	**Ref**
Strategic		
Physician alignment		F
Continuing care model		Q
Point ventures		R
Strategic planning		U
Culture of accountability		CC
Implementing change		GG
Marketing		JJ
Compliance/Regulatory/Legal		
Quality of care/patient safety		G
Compliance – joint commission		O
Compliance program effectiveness		P
Physician arrangements		S
RAC readiness/preparedness		T
HIPAA privacy		Z
HIPAA security		FF
Physician credentialing		LL
Contract management		BB
Delivering Patient Care		
Behavioral health		K
ED patient throughput		H
Performance improvement		KK

The ninth principle of Deloitte's[1] Nine Principles for Building the Risk Intelligent Enterprise describes "comfort" as one major responsibility of these groups: to provide reasonable assurance to management and board members that the internal control and risk structure operates effectively.

These "comfort groups," by design, have no responsibility for the direction of the organization and its operations. Instead, they exist to monitor and enhance the effectiveness of the organization's risk management activities and to provide some objective level of assurance.

Internal audit and compliance functions are taking a leadership role in the process of identifying and prioritizing the key risks facing an organization by asking the right questions of the right people, gathering and analyzing relevant data, and identifying opportunities. Effectively communicating the results of these efforts to management and board members demonstrates the long-term value internal audit and compliance programs provide.

[1] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Exhibit 3b – Enterprise-wide Risk Assessment - Sample Heat Map

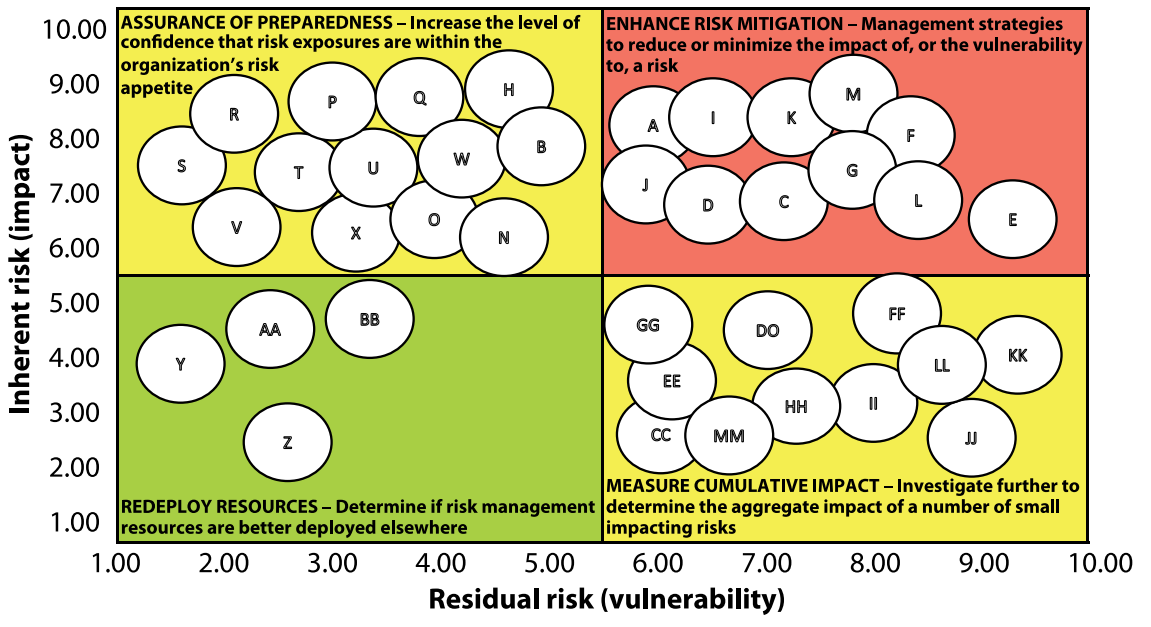

Exhibit 4 – How has our risk profile changed?
Illustrating the change in risks year by year may help facilitate an insightful discussion between internal audit, compliance and the board committee.

Prior year "red" risks	This year "red" risks
Physician financial relationships	Health care reform NEW
Revenue cycle: front end	Aging plant & equipment
Revenue cycle: back end	Alliances – physician and other partnerships
Medicare/Medicaid funding	Medicare/Medicaid funding ↑
Joint ventures/mergers ↓	Quality metrics reporting NEW
Physician billing ↑	Physician billing ↑
Credit balances	Talent management
Quality of care ↓	Financial margins ↓
RAC readiness/preparedness ↓	Clinical documentation and coding ↑

Legend		
NEW	=	New risk this year
↑	=	Risk ranked higher this year
↓	=	Risk ranked lower this year

Relationship between the board committee, internal audit and compliance

An effective relationship between the board committee, charged with oversight, and the internal audit and compliance programs is fundamental to the success of an organization. The relationship contributes to the board committee members' understanding of key risks and ability to play a meaningful role in overseeing the management of those risks that affect the organization. Internal audit and compliance programs that effectively identify, prioritize and communicate risks in a meaningful way help the board committee to confidently exercise its oversight role.

Once the board committee has established an effective relationship, the work does not stop there. It has become increasingly important for the board committee to not only understand the organization's risk profile, but also to assess whether the organization, including internal auditors and compliance professionals, is monitoring critical controls and addressing the right risks.

Risk intelligent communication

Historically, risk has been viewed as any event that can adversely affect the achievement of an organization's objectives. According to Deloitte's first principle for building the risk intelligent enterprise, today's risk intelligent organizations define risk by considering not only the potential for loss or harm, but also diminished or lost opportunities for gain that can adversely affect the achievement of their objectives.

In a risk intelligent enterprise, a common definition of risk—one that addresses both value preservation and value creation—is universally understood and used consistently throughout the organization. Establishing a common definition of risk enables the board committee, internal audit and compliance to speak the same language when discussing enterprise risks, including the results of the annual enterprise-wide risk assessment.

Translating risk assessment results into the internal audit and compliance work plans

Enterprise-wide risk assessments identify a broad range of risks applicable to the organization. Not all risks will be appropriate for internal audit and compliance focus. For example, certain strategic risks, such as physician alignment, and organizational risks, such as culture, may best be addressed through a management initiative. Conversely, there may be areas of focus for internal audit and compliance that are not identified during the risk assessment process. In addition, not all auditable risks can be addressed in one year.

It is important for internal audit and compliance to communicate the rationale behind the proposed annual work plans, including reasons why certain risk areas will not be reviewed within a given year.

Communicating audit results – the internal audit report

The benefits of and the need for risk intelligent communication is evident during the risk assessment process and development of work plans. However, this type of communication should be embedded within discussions and deliverables, including the results of executed audits, via the internal audit or compliance audit report. Several key questions should be answered for the board committee in the audit and compliance report.

Why? – The executive summary

To effectively communicate the results of audits, an audit report should be written with the board committee audience in mind. It is important for the report to begin with an executive summary to provide the reader with context, outline the issues identified and convey the reason for conducting the audit.

Exhibit 5 – How do we respond to risks?
Risk assessment and audit functions are efficient tools to communicate how the organization responds to prioritized risks, including those risks that will be included on the internal audit and compliance work plans, as well as those that are addressed through another function or management initiative.

	Process/Subprocess	Residual risk	Department managing risk	Addressed by IA/ Compliance	Addressed by other dept. or resource	Frequency of review	Status	Planned IA/ compliance projects			Planned audits other dept.s/resources		
								CY'10	CY'11	CY'12	CY'10	CY'11	CY'12
1.	**Compliance/Regulatory/Legal**												
	Compliance program effectiveness	(e.g High, Medium, Low)	(e.g. Finance, Legal, HR)			(e.g. annual)	(e.g. open)						
	Exclusion/sanction checks												
	Quality of care												
	OIG Annual Work Plan												
	Conflict of interest												
	JCAHO												
2.	**Finance/Accounting/Reimbursement**												
	Financial reporting/disclosure												
	Nonstandard journal entries												
	Account reconciliations												
	Accouting estimates												
3.	**Information Services**												
	General computer controls												
	Electronic medial records												
	Change management												
	Access controls												
4.	**Revenue Cycle (Front End)**												
	Registration/admitting												
	Case management												
	Documentation/charge capture												

In addition to including a general synopsis of the audit observations, the summary should highlight relevant background information about the business processes reviewed and details regarding previous audits performed. Setting this stage will help the committee understand the structure and scope of the review area and how the related processes affect the organization as a whole.

The executive summary should provide an overall snapshot of the audit's purpose and outcome with the focus on what the committee wants and needs to know.

What's really important? – The observation rating system

Not all audit findings are equal. Some findings, for example, highlight a best-practice opportunity and do not necessarily indicate a weakness in internal controls. Each observation requires a specific action plan that demands its own timeframe and level of resources.

When communicating observations, it is essential for the report to illustrate the priority and severity of each risk identified, using an observation rating system. Assigning a rating to each observation assists management and the board committee to gain a better understanding of what is important and how and when to deploy resources to address the risk. A common rating system often takes the form of high, medium or low.

Now what? – Facilitating effective management action plans

As important as it is to identify the challenges and risks facing an organization, it is just as vital to make sure they are

Exhibit 6 – Annual audit work plan
The annual internal audit work plan provides additional detail regarding the risk areas that internal audit will focus on, including audit descriptions and estimated level of effort.

Audit area	Audit description	Estimated hours
Evaluation of compliance program effectiveness	To understand and assess the effectiveness of the entity's compliance program as compared to the guidance provided by the Office of the Inspector General (OIG) and the US Federal Sentencing Guidelines.	300
Charge capture review	To understand and assess the procedures and controls as related to the charge capture, charge entry, and charge reconciliation practices of the identified hospital department.	200
Physician arrangements	To understand and assess the procedures and controls in place as related to financial relationships with physicians, including contract development, contract review and approval.	250
Risk assessment process	To perform procedures associated with the risk assessment process, including facilitated interviews, surveys and presentation of results.	100
Follow-up and audit committee participation	To perform follow-up on previously identified internal audit observations and management action plans; to prepare for and to participate in audit and compliance committee meetings	50
Total		**900**

Exhibit 7 – Compliance work plan example
An effective and efficient snapshot of the compliance work plan often includes risk sources and ratings, engagement descriptions, key dates and status.

Source	Entity	Engagement	Date of initial reporting	Risk	Status
Internal	JKL	Self-administered drug billing	2/10/2010	Moderate	1
Internal	DEF	Crediting of laboratory testing	1/9/2011	**High**	1
Internal	ABC	Interventional cardiology coding	4/29/2012	**High**	1
Internal	ABC	Dialysis charge capture	5/30/2012	Moderate	1
Internal	GHI	Vendor purchasing/conflicts disclosure process	5/30/2012	**High**	3
External	DEF	Short stay discharges	10/12/2012	**High**	4
External	JKL	Hemophilia clotting factors billing	11/19/2012	**High**	4
Internal	DEF	PQRI reporting for orthopedics	1/19/2013	Low	3
External	ABC	Partial hospitalization program documentation and billing	1/21/2013	Moderate	2

KEY

1. Corrective actions implemented
2. Corrective actions implementation in process—on track
3. Corrective actions implementation in process—overall on track, one or more moderate/low-risk items behind schedule
4. Corrective actions implementation in process—one or more high-risk items behind schedule
5. Corrective actions implementation in process—not started

Exhibit 8 – Management action-plan dashboard
The management action-plan dashboard provides board committees with an overview of management's progress toward implementing actions to mitigate risks identified through completed audits.

		Completion Status			Contact (name, title)	Overdue test # & action items notes	Auditor
Location	**Audit**	**Items completed**	**Items not yet due**	**Items overdue**			
Hospital A	Controls self-assessment	2	2	0			
	Security policies and procedures	3	3	0			
	HIPPA compliance	0	1	1			
		5	**6**	**1**			
Hospital B	Billing & collections	1	0	2			
	Internal control documentation	2	0	1			
		3	**0**	**3**			
Hospital C	Denial processing	0	9	0			
	Charge capture	4	2	0			
		4	**11**	**0**			
Hospital D	Development office	0	7	3			
	Employee benefits	0	1	0			
	Pharmacy – drug diversion	3	0	0			
	Physician – EMTALA	0	0	2			
		3	**8**	**5**			
Hospital E	Physician master database	2	3	1			
	Contract management	0	1	0			
	Grant compliance	3	1	1			
	Charge capture – emergency	3	2	0			
		8	**7**	**2**			
TOTAL		**23**	**32**	**11**			

addressed. After receiving an internal audit or compliance report, board committees are primarily concerned with what actions management is taking to remediate identified deficiencies.

Facilitating effective action plans is a critical component of an audit. Management responses should include key elements that outline planned actions and effective tracking and follow-up of the organization's progress to date. These elements include the detailed action plans to address observations and mitigate risk, identifying action plan owners and responsible parties, and the timeframe for completing the action plan.

Communicating progress, results and status updates

As a work plan is executed throughout the year, internal audit and compliance should continuously provide a snapshot of their progress and results to the Board committee. Providing

Nine fundamental principles of a risk intelligence program

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.
2. In a Risk Intelligent Enterprise, a common risk framework that is supported by appropriate standards is used throughout the organization to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities and authority relating to risk management are clearly defined and delineated within the organization.
4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. In a Risk Intelligent Enterprise, governing bodies (boards, audit committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with the primary responsibility for designing, implementing and maintaining an effective risk program.
7. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. In a Risk Intelligent Enterprise, certain functions (finance, legal, IT, HR, etc.) have a pervasive impact on the business, and provide support to the business units as the support relates to the organization's risk program.
9. In a Risk Intelligent Enterprise, certain functions (internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

From Deloitte's risk intelligence white papers available at www.deloitte.com, "Putting Risk in the Comfort Zone: Nine Principles for Building the Risk Intelligent Enterprise™"

too much information may cloud the board committee's view of where everything stands. Conversely, too little information can hinder the committee's ability to exercise effective oversight and ask the right questions.

As mentioned, the work of internal audit and compliance is not finished once a review is completed and results are delivered. It is important for board committees to understand progress made toward management's completion of action plans that resulted from audit observations.

The timely completion of agreed-upon action plans often serves as a gauge to measure the overall effectiveness of the internal audit and compliance programs. A leading practice is for compliance and internal audit to report on the completion status of management corrective actions approximately twice per year.

Board committees should periodically evaluate the status of internal audit and compliance work plans against the original plans and any significant changes made to those plans. Board committees and the internal audit and compliance programs should engage in discussions regularly and make the reporting relationship a substantial and communicative one.

Conclusion

Effective communication between internal audit, compliance, and the audit and compliance committee positions healthcare organizations to identify and understand the obstacles that may be impeding the achievement of their goals, and to become more proficient in developing solutions to overcome them. Ultimately, these groups need to work together to not only preserve the organization's position in the marketplace, but also to compete more effectively and sustain a competitive advantage. **NP**

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.