Deloitte.

Health Care Compliance Association (HCCA) Audit & Compliance Committee Conference

Communicating with The Audit & Compliance Committee of the Board

Leading Practices

February 25, 2013

Discussion Topics

1. Tactics for facilitating effective communication between internal audit, compliance, and the audit and compliance committee

2. Type and frequency of information audit committee members should ask for and receive

3. Emerging risks in the audit and compliance arenas and what board members should consider

4. Leading practices employed in industry to speak a common "risk" language, monitor risk, and identify priorities

1

Health Care Organizational Risks

The health care industry is experiencing significant change. Understanding (and managing) the risks specific to your organization will be critical.

- **Reductions in payments** – Both the states and the Federal government are continuing to reduce payments to hospitals and share risk as part of ACOs or other arrangements.
- **ICD-10 –** Though many organizations are challenged by its overall impact on finance, operations, and technology, there are benefits and opportunities associated with ICD-10 including enhanced quality measurement and better public health reporting. However, the risks of increased accounts receivable or denied payments will require further monitoring.
- **Technology –** Hospitals continue to have significant technology investments including CPOE and electronic medical records, and hospitals will likely continue to look to technology to provide more efficient health care.
- **Fraud, waste, and abuse (FWA)** – Reviews conducted by the OIG have historically focused on identifying areas that are at risk for noncompliance with Medicare billing requirements. Now, based on computer matching and data mining techniques, the OIG will select hospitals for focused reviews of claims that may be at risk for overpayments.
- **Consumerism –** Capitalizing on growth and service opportunities requires an in-depth understanding of patients and their needs and will become an important driver of success.
- **Reputation** – With security and privacy top of mind, combined with requirements as transparency of treatment metrics etc., the risks associated with reputation become more challenging.

2

What We Hear From Audit & Compliance Committees

Overwhelmed by heightened scrutiny from stakeholders, regulators, etc.

Concerned with the effects of Health Care Reform and new delivery models

Dissatisfied with process to identify risks

Unsure of their role in the oversight of enterprise risk management (ERM)

Uneasy with changes in digital information storage, usage, and security

A Common Theme:

The Audit Committee does not have a clear picture of the entirety of risks associated with the organization's operations, nor in some cases what its responsibilities are vis-à-vis the Board and other Board Committees for oversight of risk areas

3

The Changing Role of the A&C Committee

Key challenges of the past

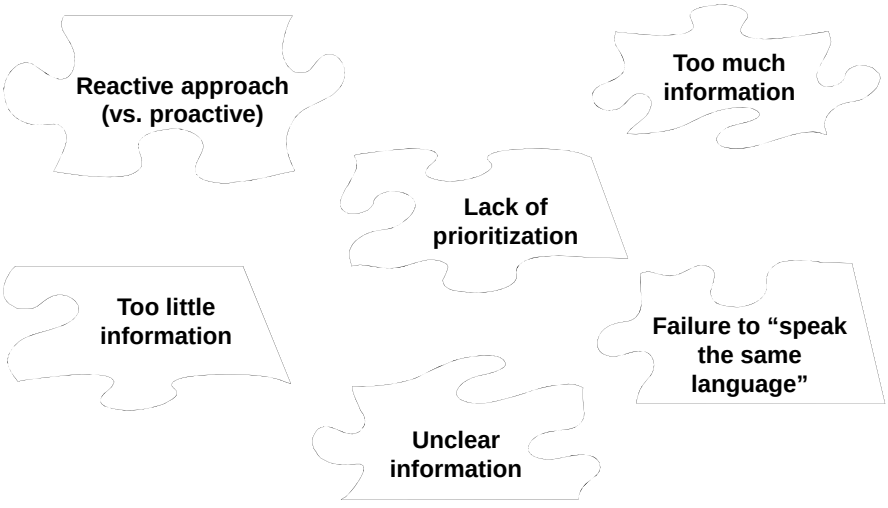
- The integrity of the company's financial statements
- The company's compliance with legal and regulatory requirements
- The independent auditor's qualifications and independence
- The performance of the company's independent auditor and internal-audit function

Current / New Key Challenges

- Oversight of enterprise risk management (and risk awareness in general)
- Heightened scrutiny from shareholders, regulators, media, etc.
- Concern about appropriate levels of resources and skill sets in compliance and internal audit
- Unease regarding digital information security

4

Communicating with A&C Committees: Common Pitfalls



5

So…How do you define risk?

"Risk" can mean different things to different people:

Formal definition:

Risk is "any event that can adversely affect the achievement of your objectives."

Risk intelligent definition:

Risk is the potential for loss or harm — *or the diminished opportunity for gain* — that can adversely affect the achievement of an organization's objectives.

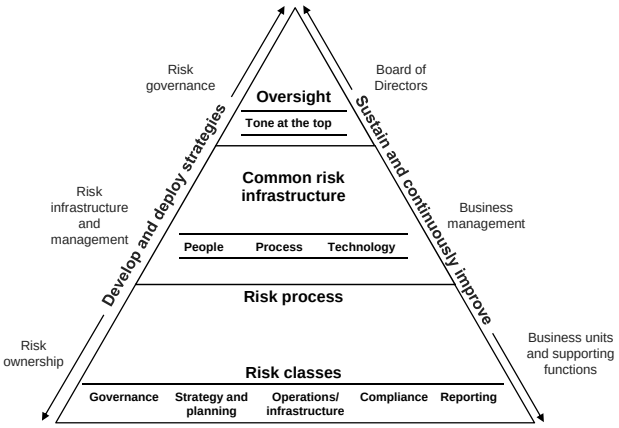
Simple definition:

Risk is the possibility of something bad happening or something good not happening.

In a risk intelligent enterprise, a common definition of risk — one that addresses both value preservation and value creation, is used consistently between management, the Board and throughout the organization.

6

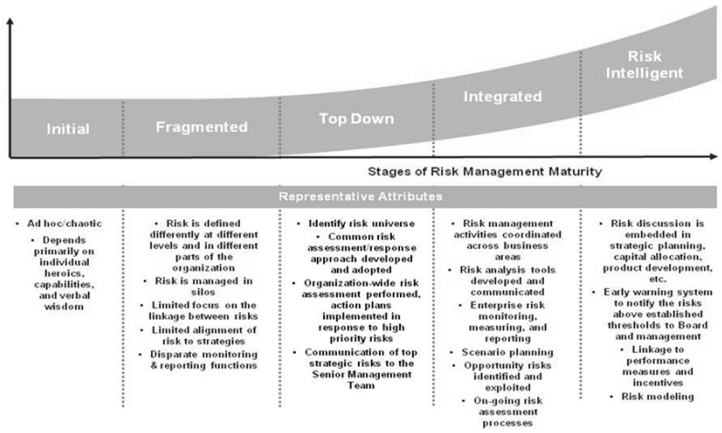
The Risk Intelligent Enterprise™



7

Assessing Your Organization's Risk Maturity

- ✓ How capable is the organization today to manage its risk profile?
- ✓ How capable does it need to be?
- ✓ How can it get to its desired state? By when?
- ✓ How can we leverage existing risk management practices?



Leading Trends in Board-Level Risk Oversight

- Increased focus on risk "intelligence" and risk assessment
- Periodic reassessment of the list of top risks, and determining who in management and which committee of the Board is responsible for each
- Avoiding becoming overly dependant on forms or tools for monitoring risks
- Acknowledging the importance of information technology (IT) and reviewing key IT milestone reporting, especially for significant IT implications
- Being aware of, and reviewing when applicable, acquisition and major initiatives, including risks, relevant integration milestones, and ROI analysis
- Considering the role of internal audit and compliance in major IT initiatives, other major organizational changes, and where these items fall on the IA/Compliance work plans

Questions the A&C Committee May Want to Consider…

…and questions management may want to answer.

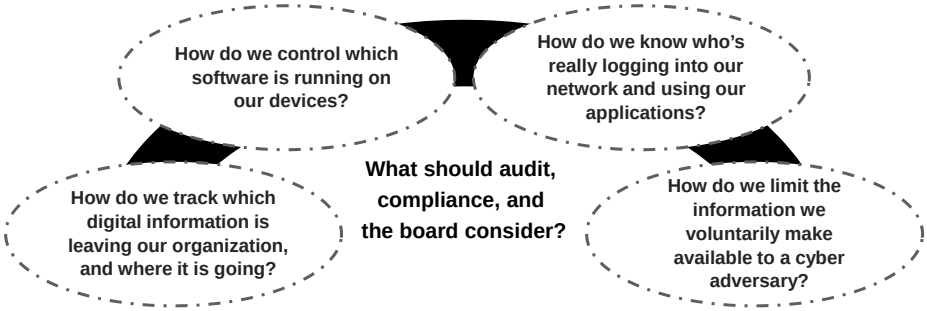
- ✓ What regulations, guidelines, and laws changed in 2012…..and what new processes have been put in place to address the changing requirements?
- ✓ What is the likely impact of regulatory activity on the organization?
- ✓ How prepared is the organization for the enactment of new rules and laws?
  - – How will the health care reform legislation affect the business (e.g., ACOs, quality of care, etc.)?
- ✓ How effective is our process for monitoring emerging risks?
- ✓ How do we know our internal audit and compliance functions are working effectively and staffed at the right levels?
- ✓ Have we engaged any outside advisors to assist in our efforts?
- ✓ What further impact do we expect in 2012, and has management begun assessing and planning for that impact?

10

Example Emerging Risk: Digital Information Security

The total economic burden created by data breaches in the health care industry is nearly $6 billion annually, while the impact of a data breach over a two-year period is approximately $2 million per organization.

The Department of Health and Human Services through its enforcement arm, the Office of Civil Rights, initiated the first-ever "proactive" auditing of the HIPAA privacy and security rules starting in January 2012.



11

Example: Enterprise Risk Framework

Illustrative

NOTE: The following risk framework should be customized for your organization. This is an example for discussion purposes.

Healthcare Provider Risk Framework: SNAP SHOT

Governance	Strategic Risk		Infrastructure Risk			Operational Risk		Ethics and Compliance Risk	
Corporate Governance	External Factors	Strategy	**Treasury**	**Finance**	**Managed Care**	**Care and Delivery**	**Patient Services**	**Regulatory Compliance**	**Contract Compliance**
Board Structure & Leadership	Competition	Alliances	Debt Management	Planning/ Budgeting	**Payer Contracting**	Diagnostic and Treatment Services	Introduction of Services	Medical Care	Vendors
Culture	Credit Rating	Business Concentration	Capital Management and Forecasting	Cost Accounting	Capitation Revenue	Outpatient Care	Delivery of Patient Services	Medicade/Medicare	Payers
Ethics	Customer Demands	Customers	Cash Management	Taxation	Claims Processing	Speciality Care	Delivery of Patient Support	HIPAA	Medical Staff
Performance Incentives	Economic Conditions/Industry Trends	Growth	Investment Management	Credit	Utilization Management	Long Term Care	Comprehensive Care Management	Antitrust	Other Business Partners
Risk Oversight	Environmental	Mergers / Acquisitions / Divestitures	Pension Management	Financial Accounting		Acute Care	Discontinuance of Services	Tax Exempt / Tax Status	Medical Research

Sample Risks:

RISK CATEGORY	RISK SUB-CATEGORY	RISKS	POTENTIAL RISK DESCRIPTION	SOURCE
Infrastructure	Managed Care	Payer Contracting	Inappropriate provisions for contract Ambiguity in contract terms Complex reimbursement terms Inaccurate contract pricing	

Example: Universe of Activities

Illustrative

1. Culture / Governance
Executive Sponsor: _____
Project Manager: TBD
- ✓ Culture / Tone at the Top
- ✓ Roles and Responsibilities
- ✓ Internal Controls
- ✓ Board Structure/Education
- ✓ Discipline of 'Speaking Up'
- ✓ Executive Compensation

2. Strategy/Deployment
Executive Sponsor: _____
Project Manager: TBD
- ✓ Quality
- ✓ Growth
- ✓ Integration
- ✓ Financial Sustainability
- ✓ Marketplace Assessment

3. Delivery of Patient Services – Support
Executive Sponsor: _____
Project Manager: TBD
- ✓ Case Management
- ✓ Utilization Review
- ✓ Social Work
- ✓ Patient Satisfaction
- ✓ Teaching/Students
- ✓ Volunteers

4. Delivery of Patient Services – Inpatient
Executive Sponsor: _____
Project Manager: TBD
- ✓ Access/Throughput
- ✓ Length of Stay
- ✓ Centers of Excellence
- ✓ ICU/CCU

5. Delivery of Patient Services – Outpatient
Executive Sponsor: _____
Project Manager: TBD
- ✓ Access/Throughput
- ✓ Emergency Department
- ✓ Primary Care
- ✓ Physician Practices
- ✓ Behavioral Health
- ✓ Laboratory

6. Delivery of Patient Services – Post Acute
Executive Sponsor: _____
Project Manager: TBD
- ✓ Hospice
- ✓ Home Care
- ✓ Long Term Care

7. Capital Management
Executive Sponsor: _____
Project Manager: TBD
- ✓ Capital Allocation / Budgeting
- ✓ Return on Investment Analysis
- ✓ Project/Construction Management
- ✓ Facilities Management
- ✓ Leased Property
- ✓ Asset Disposal

8. Revenue Cycle
Executive Sponsor: _____
Project Manager: TBD
- ✓ Scheduling/Verifications
- ✓ Registration/Admitting
- ✓ Charge Master/Charge Capture
- ✓ Health Information Management
- ✓ Clinical Documentation & Coding
- ✓ Pricing Transparency
- ✓ Patient Billing/Collections
- ✓ Credit & Collections Policies
- ✓ A/R, Denials, Bad Debts
- ✓ Credit Balances & Refunds

9. Human Resources
Executive Sponsor: _____
Project Manager: TBD
- ✓ Succession Planning
- ✓ Benefits Administration
- ✓ Leadership Development
- ✓ Performance Management
- ✓ Recruitment/Hiring/Retention
- ✓ Payroll – Time Reporting
- ✓ Expense Reimbursement
- ✓ Diversity
- ✓ Labor Strategy

10. Compliance Program
Executive Sponsor: _____
Project Manager: TBD
- ✓ Code of Conduct
- ✓ Training and Education
- ✓ Communication
- ✓ Enforcement and Discipline
- ✓ Policies and Procedures
- ✓ Auditing and Monitoring
- ✓ Response and Prevention
- ✓ Conflicts of Interest
- ✓ Privacy& Security

11. Clinical Risk Management
Executive Sponsor: _____
Project Manager: TBD
- ✓ FDA Recalls
- ✓ Medical Errors
- ✓ Occurrence/Incident Reporting
- ✓ Root Cause Analysis
- ✓ Serious Reportable Events (SREs)

12. Risk Financing
Executive Sponsor: _____
Project Manager: TBD
- ✓ Professional & General Liability Insurance / Self Insurance Program
- ✓ Workers Compensation
- ✓ Excess & Reinsurance
- ✓ Commercial Insurance Program
- ✓ Claims Reporting and Handling

13. Quality / Performance Improvement
Executive Sponsor: _____
Project Manager: TBD
- ✓ Patient Safety
- ✓ Value-based Care
- ✓ Quality Indicator Monitoring and Reporting
- ✓ Joint Commission/Other Accreditation
- ✓ Process re-design

14. Information Technology
Executive Sponsor: _____
Project Manager: TBD
- ✓ IT Ops., Infrastructure & Processes
- ✓ IT Governance, Compliance & Reporting
- ✓ IT Strategy & Planning
- ✓ Privacy & Security

15. Patient Care Information Systems
Executive Sponsor: _____
Project Manager: TBD
- ✓ Implementation
- ✓ Project Management
- ✓ System Acceptance

16. Legal/Regulatory
Executive Sponsor: _____
Project Manager: TBD
- ✓ Physician Arrangements
- ✓ Corporate Contracting
- ✓ Records Retention
- ✓ Regulatory Reporting
- ✓ Non-Profit Tax Status/ Community Benefit

17. Finance / Accounting / Reimbursement/Managed Care
Executive Sponsor: _____
Project Manager: TBD
- ✓ Financial Reporting & Closing
- ✓ Financial Audit Quality
- ✓ Accounting for Mgmt. Estimates
- ✓ Budgeting / Forecasting
- ✓ Cost of Consumerism
- ✓ Transactions w/ Medical School
- ✓ External Reimbursement & Funding
- ✓ Managed Care Contracting & Reimbursement
- ✓ Regulatory Filing Requirements

18. Treasury & Debt Management/Pension
Executive Sponsor: _____
Project Manager: TBD
- ✓ Credit Rating
- ✓ Debt Covenants
- ✓ Debt Portfolio
- ✓ Treasury Processes / Controls
- ✓ Pension Liability
- ✓ Exposure to Market Conditions
- ✓ Pension Administration
- ✓ Investment Management

19. Supply Chain / Procurement
Executive Sponsor: _____
Project Manager: TBD
- ✓ Supply Chain Leadership
- ✓ Ordering/Purchasing/Receiving
- ✓ Credit Cards
- ✓ Accounts Payable

20. Medical Staff
Executive Sponsor: _____
Project Manager: TBD
- ✓ Privileging and Credentialing
- ✓ Disciplinary Actions
- ✓ Hospital/Physician Relations
- ✓ Recruitment and Retention
- ✓ Succession Planning

Example: Risk Assessment Criteria

Illustrative

Impact Criteria	Financial	Reputation	Customers	Operations	Employees	Legal/ Regulatory
HIGH (4-5 Rating)	5 rating: Greater than $XX million impact on earnings before taxes 4 rating: Greater than $XX million and less than $XX million	International/ national media attention Significant negative impact on reputation and brand, likely to have long-lasting impact	Wide-spread impact on customer satisfaction Serious threat to future growth. Inability to sell	Significant interruptions of business operations of 2 or more divisions or countries Potential losses may be considered	Unplanned loss of several key and senior employees Serious injury to employees and/or dangerous near miss Significant impact	Major federal or state scrutiny Investigations subject to substantial fines and penalties including criminal charges and/or cease-and-desist
MEDIUM (3 Rating)						
LOW (1-2 Rating)						

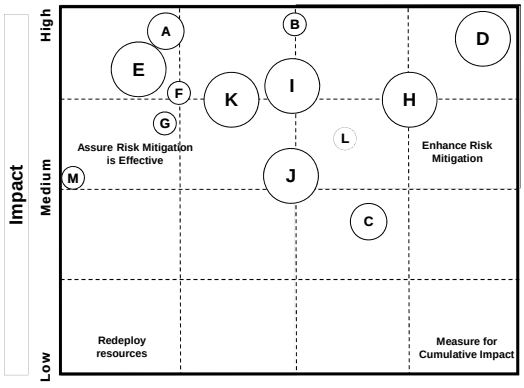
Vulnerability Criteria	Mitigation/ Monitoring	Complexity	Risk Management Capability		
			People	Process	Technology (if technology enabled process)
HIGH (4-5 Rating)	5 rating: No mitigation/monitoring plans exist 4 rating: Mitigation/monitoring plans exist but are not consistently applied	Risk affects a high # of transactions or a high # of processes Transactions are highly subject to judgment and estimation	Limited level of internal staff capable of managing risk potential Limited access to resources Significant level of change experienced by resources as a result of risk event	5 rating: No effective process in place to manage the risk 4 rating: Process in place but not consistently followed and/or no monitoring, testing or reporting of process	Major system performance, reliability and validity issues Significant security exposures Outdated and ineffective technology Significant changes
MEDIUM (3 Rating)					
LOW (1-2 Rating)					

Speed of Onset Criteria	`Definition
HIGH (4-5 Rating)	Very rapid onset; little or no warning, instantaneous.
MEDIUM (3 Rating)	Moderate onset; several days or weeks to occur.
LOW (1-2 Rating)	Very slow onset; several months or years to occur.

Example: Enterprise Risk – Heat Map

Illustrative

Sample heat map to show potential top risks

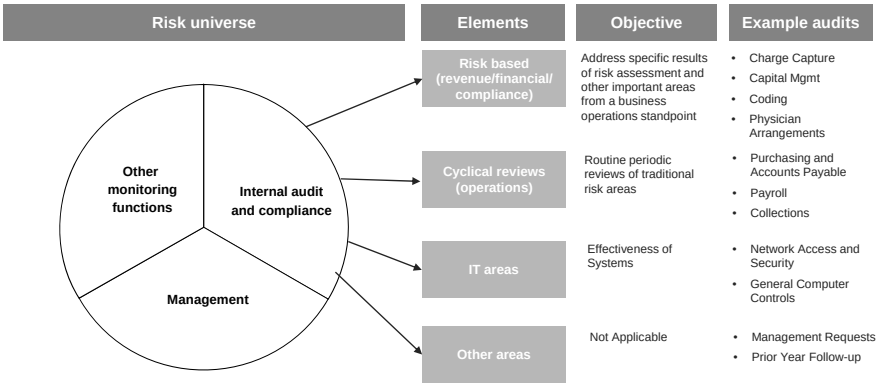


ID	Potential Risks
A	Risk A
B	Risk B
C	Risk C
D	Risk D
E	Risk E
F	Risk F
G	Risk G
H	Risk H
I	Risk I
J	Risk J
K	Risk K
L	Risk L

Dot size reflects Speed of Onset: Low ○ Medium ○ High ○

Translating Risk Assessment Results into an Integrated Audit and Compliance Work Plan

Enterprise wide risk assessments identify a broad range of risks applicable to the organization. Not all the risks, however, will be appropriate for either compliance or internal audit focus. Conversely, there will be areas of compliance and internal audit focus which are not identified during the risk assessment process. In addition, not all "auditable" risks can be addressed in one year.

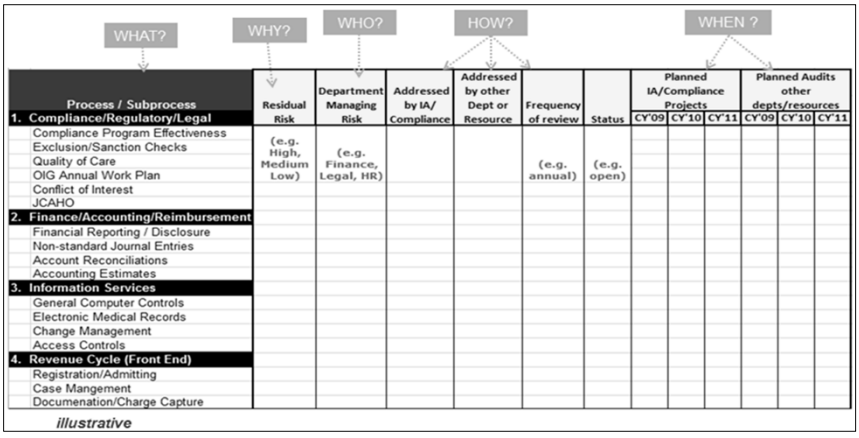


Example: Risk and Audit Universe

Illustrative

Responding to Risks

The risk and audit universe is an efficient tool 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 CY'09	CY'10	CY'11	Planned Audits other depts/resources CY'09	CY'10	CY'11
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												
Non-standard Journal Entries												
Account Reconciliations												
Accounting Estimates												
3. Information Services												
General Computer Controls												
Electronic Medical Records												
Change Management												
Access Controls												
4. Revenue Cycle (Front End)												
Registration/Admitting												
Case Mangement												
Documenation/Charge Capture												

illustrative

The Changing Risk Profile

Risks are fluid and can often change over time. So too can the risk profile of an organization change, as reflected in the example below.

Prior Year "Red" Risks	2012 "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

The "How and What" Examples: Reporting to the A&C Committee

Internal Audit Plan

Audit	Description	Source	Estimated hours	Resource
HIPAA privacy	Review of instituted HIPAA compliance policies, procedures, forms and initiatives and assessment organizational compliance with HIPAA statute with regulations.	Risk assessment	120	**Co-sourced compliance**
Physician arrangements	Review, documentation and analysis of the design of controls over physician arrangement management including review of arrangements sample for compliance and control operating effectiveness.	Risk assessment	180	**Co-sourced compliance**
Anti-kick back/stark laws	Review, documentation and analysis of the design of controls including policies and procedures to validate compliance with anti-kick back/stark law compliance with selected control testing for operating effectiveness.	Industry	160	**Co-sourced compliance**
Supply chain: Materials and services procurement	Review, documentation and analysis of the controls over materials and services procurement with selected control testing for operating effectiveness.	Risk assessment	250	**Internal**
Medical supplies inventory management	Review, documentation and analysis of the controls over medical supplies inventory management with selected control testing for operating effectiveness.	Industry	140	**Internal**
Payroll processing	Review, documentation and analysis of the controls over payroll processing with selected control testing for operating effectiveness.	Industry	120	**Internal**
Construction	Review, documentation and analysis of the design of controls over construction management with selected control testing for operating effectiveness (e.g. change orders, applications for payment, bids).	Risk assessment	200	**Internal**
Asset management	Review, documentation and analysis of the controls over asset management with selected control testing for operating effectiveness.	Risk assessment	200	**Internal**

The "How and What" Examples: Reporting to the A&C Committee

Dashboards 1

Internal Audit or Compliance Reports Completed

Audits	Quarter	Total # Obs.	# of Red	# of Yellow	# of Green
HIPAA privacy	Q1	10	3	4	3
Physician arrangements	Q1	11	7	3	1
Anti-kick back/stark laws	Q2	6	1	2	3
Supply chain: Materials and services procurement	Q2	3	0	2	1
Medical supplies inventory management	Q3	4	2	0	2
Payroll processing	Q3	7	2	2	3
Construction	Q3	3	0	0	3
Asset management	Q4	5	1	1	3

Compliance Reporting & Hotline Activity

Issue	Complaints Received
Employee Misconduct	6
Patient Care	5
Theft	3
Billing/Coding Issues	2
HIPAA	1
Conflict of Interest	1
Other	1

Compliance Training

Compliance Training	% Complete
New Hire Training (within 30 days)	94%
General Online Compliance Training	92%
Specialized Compliance Training	85%
Code of Conduct - Acknowledgement Signed	95%

The "How and What" Examples: Reporting to the A&C Committee

Dashboards 2

Management Action Item Status Dashboard Summary

			COSO Category				Business Importance Code			Completion Status					
Location	Audit	IA / Reg	Operational Findings	Financial Findings	Compliance Findings	Total Findings	A	B	C	Items Completed	Items Not Yet Due	Items Overdue	Contact	Overdue Test # & Action Item Notes	Auditor
Hospital A	Controls Self-Assessment	IA	3	1	0	4	2	1	1	2	2	0	Name, Title		
	Security Policies and Procedures	IA	3	2	1	6	2	2	2	3	3	0	Name, Title		
	HIPAA Compliance	REG	0	0	2	2	1	0	1	0	1	1	Name, Title		
			6	3	3	12	5	3	4	5	6	1			
Hospital B	Billing & Collections	IA	3	0	0	3	1	1	1	1	0	2	Name, Title		
	Internal Control Documentation	IA	2	1	0	3	0	0	3	2	0	1	Name, Title		
			5	1	0	6	1	1	4	3	0	3			
Hospital C	Denial Processing	IA	9	0	0	9	3	3	3	0	9	0	Name, Title		
	Charge Capture	IA	0	4	2	6	1	4	1	4	2	0	Name, Title		
			9	4	2	15	4	7	4	4	11	0			
Hospital D	Development Office	IA	10	0	0	10	3	6	1	0	7	3	Name, Title		
	Employee Benefits	IA	1	0	0	1	0	1	0	0	1	0	Name, Title		
	Pharmacy - Drug Diversion	REG	3	0	0	3	2	1	0	3	0	0	Name, Title		
	Physician - EMTALA	REG	1	0	1	2	1	1	0	0	0	2	Name, Title		
			15	0	1	16	6	9	1	3	8	5			
Hospital E	Physician Master Database	REG	1	2	3	6	1	2	3	2	3	1	Name, Title		
	Contract Management	REG	0	0	1	1	0	1	0	0	1	0	Name, Title		
	Grant Compliance	REG	0	2	3	5	1	2	2	3	1	1	Name, Title		
	Charge Capture - Emergency	IA	0	4	1	5	1	2	2	3	2	0	Name, Title		
			1	8	8	17	3	7	7	8	7	2			
TOTAL			36	16	14	66	19	27	20	23	32	11			

Completed or Not Overdue
1–14 Days Overdue
15–29 Days Overdue
30+ Days Overdue

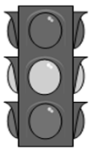
The "How and What" Examples: Reporting to the A&C Committee

Internal Audit Reports

Leading Practices

Executive summary — should include relevant background information, overall summary of findings, audit history and should answer the question, "Why did we conduct this audit?"

Observation rating system — Assigning a rating to each of the observations in an internal audit report assists management and the audit committee with gaining a better understanding of "what is really important". An effective scale often takes the form of "high, medium, low".



Red Light - A significant weakness in internal controls or business processes that requires immediate correction

Yellow Light - A weakness in internal controls or business process that requires correction

Green Light - An opportunity for business process or control improvement

Management responses should include:

- Detailed action plans to address observation/mitigate risk
- Action plan owners/responsible parties
- Due dates to allow more effective follow-up/facilitate discussion with the Audit Committee on progress to date.

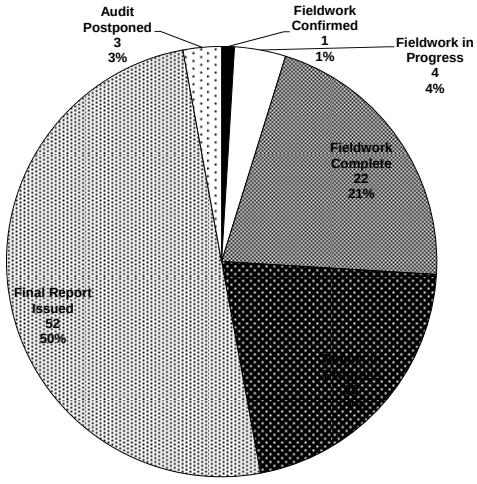
22

The "How and What" Examples: Reporting to the A&C Committee

Dashboards 3

Internal Audit Fieldwork Status

Audits by Fieldwork Status	# of Audits	% of Audits	% of Audits (2009)
Fieldwork Confirmed	3	6%	12%
Fieldwork in Progress	1	12%	6%
Fieldwork Complete	10	20%	15%
Report in Progress	10	10%	23%
Final Report Issued	25	50%	42%
Audit Postponed	1	2%	2%
Total	50	100%	100%



23

Leading Governance Practices for the Board

Benchmarking and evaluating the governance process allows organizations to track the progress of their governance program along a risk maturity model. Consider the following:

- ✓ *Use internal monitoring and feedback*
- ✓ *Participate in continuing education and updates*
- ✓ *Solicit independent viewpoints*
- ✓ *Include risk as a topic in the annual board self-assessment*

An assessment of the Audit & Compliance Committee by both committee members and selected members of senior management may reveal areas where the Committee is perceived to function well and areas where the Committee could improve:

Category	Avg. Score
Composition and Quality	4.1
Understanding the Business, including Risks	3.2
Process and Procedures	4.2
Communications and Information	3.5
Oversight of the Financial Reporting Process, including Internal Controls	3.6
Oversight of the Audit Function	4.4
Overall Ethics and Compliance Culture	3.3
Monitoring Activities	2.9
Overall Assessment	3.65

***Note*: score is based on a scale of 1 (low) to 5 (high).**

24

Board-Level Interaction with Compliance and Internal Audit: Leading Practices

- Be involved with the internal audit and compliance risk assessment and resulting plans (whether separate or combined plans)
- Conduct annual evaluations of the internal audit and compliance functions
- Understand internal audit and compliance staffing, skill sets and succession planning
- Assess whether the internal audit and compliance functions have a direct reporting line to the audit/compliance committee and an indirect line to management
- Follow meetings with executive sessions as warranted (but no less than annually with the Internal Auditors, Compliance Officer and Counsel)
- Understand the response and resolution for each issue raised at meetings

25

Board Expectations from Compliance and Internal Audit

- Objectively monitoring and reporting on the health of financial, operational and compliance controls
- Providing insight into the effectiveness of enterprise-wide risk management
- Becoming a catalyst for positive changes in processes and controls
- Delivering value to the audit & compliance committee, executives, and management in the areas of controls, risk management, and governance
- Coordinating activities and sharing perspectives with the independent auditor, where appropriate

26

Facilitating Effective Relationships with Compliance and Internal Audit

- Review work plans, process against work plans and reports resulting from work plans on a regular basis
- Be available when contacted by compliance or internal audit
- Engage in discussions regularly; make the reporting relationship a substantial and communicative one (not just “check the box”)
- Actively participate with management in discussing goals and evaluating performance of the compliance and internal audit functions
- Challenge the compliance and internal audit departments by setting high expectations, communicating those expectations clearly and holding the department(s) accountable for meeting them
- See that the compliance and internal audit functions have appropriate resources, stature and respect and are visibly supported by senior management throughout the organization

27

Contact Information

Kelly J. Sauders
Partner
Deloitte & Touche LLP
Office: (212) 436-3180
Cell: (518) 469-0890
Email: ksauders@deloitte.com

Deloitte.