

HCCA Compliance Institute Internal Audit's Role in Enhancing Your Risk Program

Lorrie Oelkers Ghose
Vice-President, CAE
Fairview Health Services

1

Agenda:

Enhance your Risk Program: Risk Assessment, Risk Tolerance and Enterprise Risk Management

- Risk Assessment: practical tools for conducting an Internal Audit and Compliance enterprise-wide risk assessment
- Enterprise Risk Management: the process for identification and ownership of enterprise risks risk assessment tools and Board reports.
- Risk Tolerance: guiding leadership to establish your organization's risk tolerance and principles
- Other Helpful Tools for Internal Audit Departments



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

2

Our Health System:



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

Fairview Health Services

- University of MN Academic Affiliation
- 34,000+ employees
- 5,000+ system providers
- 12 hospitals and medical centers
- 3,519 licensed beds
- 2,071 staffed beds
- 56 primary care clinics
- 100+ specialties
- 90+ senior housing facilities
- 36 retail pharmacies
- 360,000 health plan members

3

Why Perform a Risk Assessment?

An annual risk assessment:

- Provides insight as to the effectiveness of “tone at the top”; leadership’s commitment to openness, honesty and integrity.
- Is considered a best practice by the Institute of Internal Auditors – *The internal audit activity’s plan of engagements must be based on a documented risk assessment, undertaken at least annually* (IIA Standard 2010.A1).
- Assists in developing priorities and work plans based on risks and organizational needs.
- Identifies uncontrolled risks that may prevent the organization from achieving its goals and objectives.
- Considers the organization’s risk universe against industry risks, e.g. Protiviti’s, *Executive Perspectives on Top Risk for 2019 in Healthcare**:
 - Regulatory changes and scrutiny
 - Privacy/identity management and information security
 - Meeting performance expectations
 - Succession challenges/attracting and retaining top talent
 - Cyber threats
 - Disruptive innovations and new technologies
 - Opportunities for organic growth
 - Inability to utilize analytics and big data
 - Resistance to change operations
 - Sustaining customer loyalty and retention

* <https://www.protiviti.com/US-en/insights/top-risks-2019-healthcare>



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

4

Who do we include and why?

- Interview Executives and Board Members
 - Their responses indicate “high-level” strategic risks that form the basis of the ERM Risk Inventory
- Interview Functional Leaders and groups that support high-risk programs
 - Revenue Cycle
 - Pharmacy
 - Lab
- Survey all Non-Executive Leaders and a statistically relevant sample of employees
 - Differences in how these groups respond to questions may indicate “tone at the top” and culture problems
 - Provides ideas for audit and compliance work plans
 - Limit free text
 - Challenging to review
 - Document actions taken to address risk to protect the organization

5

Risk Assessment Process

Interview senior leaders across the organization – may inform the ERM process and audit and compliance work plans.

- What three things does the organization need to do well to succeed and achieve its goals and strategic priorities?
- What could significantly hinder (risks) the organization’s ability to achieve these goals and strategic priorities?
- How would you characterize the organization’s culture of compliance and integrity? What behaviors are promoted, what behaviors are discouraged?
- Review any enterprise risks the executive owns. Discuss mitigation plans and how Audit/Compliance may be able to assist or ensure plans continue to work as designed once completed.
- Ask if the executive if he/she has any specific work plan suggestions for the coming year.

6

Risk Assessment Process

Survey or interview key department and functional leaders (IT, HR, Finance, Revenue Cycle, Regulatory, Legal, Supply Chain, Service Line Leaders, Pharmacy).

- What are the 3-5 most important initiatives for your department/ function in the next 12 months?
- What systems/processes, including technology and tools, does your department/function plan to redesign, upgrade or replace?
- What activities or processes require significant oversight and management?
- What is the biggest compliance/operational/financial/reputational risk to your department/function?
- What concerns do you have with any regulatory changes?
- Do you have any concerns related to a potential compliance issue?
- What would be the operational impact if the confidentiality, integrity or availability of data, systems or processes were compromised?
- What is the greatest risk to our cyber security? Remote work?
- Solicit work plan ideas.



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

7

Risk Assessment Process

Survey management and a sample of non-management staff.

- Does Management demonstrate integrity and ethical behavior?
- Are you aware that the organization has an anonymous reporting tool (hotline)?
- Do system/department policies and procedures assist you in doing your job effectively?
- Do you believe the information in your department is reported with a high degree of integrity and accuracy?
- Do you believe you can freely report ethics and compliance issues without fear of retaliation?
- Would Management take appropriate corrective action if regulatory, ethical, policy, procedure or other violations were detected/reported?
- What has changed with remote work?
- Solicit work plan ideas.



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

8

Risk Assessment Process

Reviewing the Results

- Identify themes from each exercise (executive interviews, department/function survey, and management/employee survey) and share with applicable leaders and determine what, if any, immediate action should be taken. There may be system initiatives already underway to address some of the themes.
- Investigate specific concerns. We allow respondents to remain anonymous, so follow up can be challenging. Determine best way to address concerns – turned over to a leader, special investigation, consulting project and/or audit.
- Where possible, trend data year to year to identify problems or gaps, i.e. fear of retaliation – trending up or down?
- Document actions taken to demonstrate responsiveness.



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

9

9

Presentation to the Audit Committee - Example

- Interviewed 24 executives and senior leaders across the organization.
- Surveyed 250 department and functional leaders, including IT (40% responded) and non-IT (22% responded).
- Surveyed management (3,154) and a random sample of non-management staff (6,736). 28% of management and 33% of staff responded.
- All surveys and interviews solicited ideas for the Work Plan. Over 1000 ideas, areas of focus and comments were shared. Themes include:



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

10

Presentation to the Audit Co. - Example

Executive/Senior Leadership Interviews

What 3 things does the organization need to do well to succeed and achieve its goals and strategic priorities?

Realize the value of our strategic partnerships
Execute patient quality, safety, and experience goals.
Realize the value of the Service Line Model.
Achieve clarity/focus. Reduce the number of initiatives. Narrow strategy. Prioritize.
Build trust as a leadership team. What does it mean to "own" something? What does it mean to "align" something?
Develop leaders and managers beyond the Executive Team.
Create an exceptional customer experience that differentiates us.

What could significantly hinder (risks) the organization's ability to achieve its goals and strategic priorities?

Inadequate capital.
Too many competing priorities.
Failure to integrate legacy systems.
Inability to drive accountability.
Unable to make decisions quickly.
Unreliable data.
Non-compliance is weaponized, rather than escalated.
Tolerating behaviors that should be unacceptable and are contrary to stated priorities and goals.
Execution risk.

How would you characterize the organization's culture of compliance and integrity? What behaviors are promoted, what behaviors are

Everyone comes to work wanting to do the right thing, but may lack the compliance knowledge to know when non-compliance occurs.
High integrity.
Tend to normalize deviance. Non-compliance is tolerated.
Need to model "see something, say something".



A collaboration among the University of Minnesota, University of Minnesota Physicians and Fairview Health Services

11

Presentation to the Audit Committee - Example

Department/Functional Interviews

What are the 3 to 5 most important initiatives for your department in the next 12 months?

- Integration of legacy systems, policies and procedures
- Partnerships
- Point of Service Collections, Prior Authorization Process
- Standardized Equipment Mgmt Strategy
- Meeting Financial Targets
- IT Projects

What systems/processes does your department plan to redesign, upgrade or replace?

- Technology Upgrades across 2 platforms
- Standardized billing
- Access Controls
- Kiosks, Signature Pads, Palm Readers
- Primary Care Delivery Transformation
- Data Governance
- Phishing Campaigns
- Email Threat Remediation

What activities or processes require significant oversight and management?

- Behavioral Patient Care
- Consent forms
- Guardian status
- Provider documentation
- Claims edits
- Contracts
- System implementation
- Supply levels
- Research data request process
- Data integration/management
- Software & hardware assessments for new contracts

What would be the operational impact if the confidentiality, integrity or availability of data, systems or processes were compromised?

- Clinical operations would be impacted
- Data submissions
- Patient Safety Concerns
- Inability to perform core services (e.g. payroll)
- Reputational harm if patients do not trust us to keep their data safe

What do you believe is the biggest compliance/operational/financial/reputational risk to your department/?

- Training & Data security
- Compliance with licensure
- Accuracy and completeness of agreements
- Denials

What concerns do you have with regulatory changes?

- Assisted Living licensure changes
- Patient-Driven Groupings Model
- ED Boarding

Do you have any concerns related to a potential compliance issue?

- HIPAA Compliance
- Cyber security
- Need coding and billing reviews
- Data management

What is the greatest risk to our cyber security? (IT only)

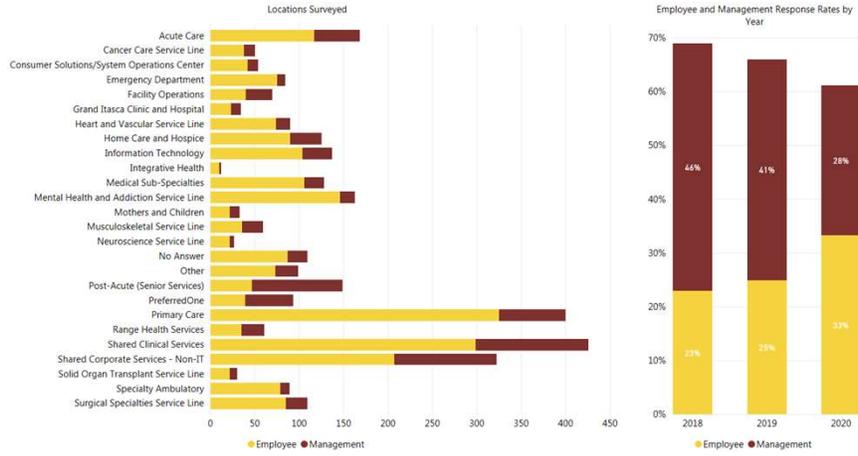
- Security awareness and training across the organization
- Access to and use of PHI, PII, HR, PCI data
- Clinical/IOT
- BYOD (bring your own device) & IoT devices



A collaboration among the University of Minnesota, University of Minnesota Physicians and Fairview Health Services

12

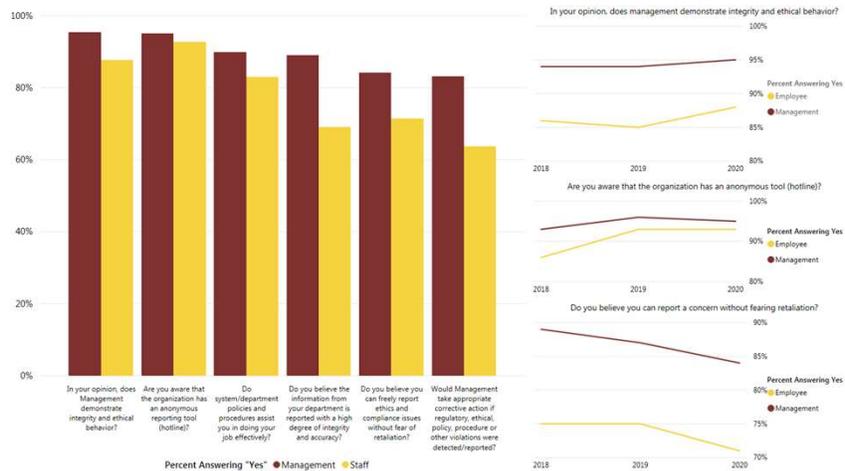
Presentation to the Audit Committee - Example



HEALTH FAIRVIEW
A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

13

Presentation to the Audit Committee - Example



HEALTH FAIRVIEW
A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

14

Presentation to the Audit Committee - Example

Key Take Aways

- Financial Performance/Pressures
- Realizing the Value of Partnership
- Competing Priorities
- Unclear Decision Making Model
- Integration Challenges
- Accountability



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

15

Presentation to the Audit Committee - Example

Leadership's Response

Leadership has already begun work to address the key risks identified in this assessment:

- An Enterprise Risk Management exercise was completed on January 10th. Owners are assigned responsibility for developing and executing mitigation strategies, with regular reporting to Leadership and the Audit and Compliance Committee.
- Enterprise Project Management Office is being created to support the execution of key system initiatives with focused project management support. The Executive Leadership Team is complete.
- Decision making model and expectations across the organization are being clarified.



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

16



17

Enterprise Risk Management

Identifies Strategic Risks

- Provides method to cascade Strategic Risk Management throughout the Organization

Engages Executives and Board Members

- Board participates in the ERM discussion
- Audit Committee receives quarterly updates on ERM mitigation

Addresses Gaps in Audit Risk Universe

- Internal Audit is a tactical function

HEALTH FAIRVIEW
A collaboration among the University of Minnesota, University of Minnesota Physicians and Fairview Health Services

18

Enterprise Risk Management

Impact: The financial or business impact if the adverse event were to occur.

5: Catastrophic	<ul style="list-style-type: none"> Event with a financial impact greater than \$100 Million. Significant downgrade in debt. Major enforcement action. Disqualification from participation in government reimbursement program.
4: Major	<ul style="list-style-type: none"> Event with a financial impact between \$50 and \$100 Million. Major adverse events with negative publicity (e.g. infant abduction, Accretive, Ebola in-patients)
3: Significant	<ul style="list-style-type: none"> Event with a financial impact between \$25 and \$50 Million. Adverse events with high reputational impact (e.g. workplace violence)
2: Minor	<ul style="list-style-type: none"> Event with a financial impact between \$2 and \$25 Million. Published malpractice claim.
1: Insignificant	<ul style="list-style-type: none"> Event with a financial impact less than \$2 Million.

Likelihood: The probability of occurrence given controls in place.

5: Almost Certain	Event will occur in most circumstances; 90% or more of the time (e.g. snow in MN in January)
4: Likely	Event should occur; more than 50% probability and up to 90% certainty (e.g. snow in MN in December)
3: Moderate	Event will probably occur; more than 25% and up to 50% probability (e.g. snow in MN in November)
2: Unlikely	Event could occur; more than 5% up to 25% probability (e.g. snow in MN in October)
1: Rare	Event would occur only in exceptional circumstances; <5% probability (e.g. snow in MN in September)

Velocity: The speed of onset of the event, should it occur.

5: Immediate	Very Rapid onset; little or no warning, instantaneous
4: Fast	Quick onset; several weeks or months to occur
3: Moderate	Moderate onset; between 6-12 months to occur
2: Slow	Slow onset; between 13 and 18 months to occur
1: Prolonged	Very slow; >18 months to occur



Risk Assessment Heat Map

LIKELIHOOD	almost certain	Moderate	Major	Critical	Critical	Critical
	likely	Moderate	Major	Major	Critical	Critical
	possible	Moderate	Moderate	Major	Major	Critical
	unlikely	Minor	Moderate	Moderate	Major	Critical
	rare	Minor	Minor	Moderate	Moderate	Major
		insignificant	minor	moderate	major	critical
		CONSEQUENCE				



ERM - A Simple Approach

- Obtain Top Three Risks from each Executive
 - Four weeks prior to the exercise
 - Pre-populate Risk Inventory Boards with Submitted Risks and Prior Year's "Red Risks"
- Schedule Meeting with Executives and Board Members
 - Executives and Board Members divide into Groups
 - Each Group works with the same Risk Inventory Boards
- Each Group generates a Top Ten List
 - Facilitate Group Discussion for a "Final List"
- Report Risk Inventory and RED/GREEN Status at each Audit Committee
 - Deep Dive on one RED Risk at each Meeting

Enterprise Risk Management

Risk	Accountable Owner
Talent –	
Consumerism –	
Clinical Learner Environment-	
Financial Execution –	
Digital Transformation-	
Analytics –	
Revenue Cycle Optimization-	
Ability to Execute Strategic Initiatives-	
Managing Risk Tolerance –	
Patient Safety and Quality Risks-	

Risk Dashboard

Risk Dashboard						
Consumerism: Financial Risk associated with Consumer-Driven Healthcare and Disrupters						
Process/risk owner:		Board governance: Audit Committee		Management governance: Enterprise Risk Steering Committee		
Risk Category	Root Causes / Risk Drivers	Mitigation action plans	Target Date	Project Status	% Complete	Key accomplishments/ challenges
					◐	
					●	
					◐	
					◐	
					●	
					◐	

Risk Appetite/Risk Tolerance

Risk Appetite (Risk Tolerance) is the amount of risk the organization is willing to accept in pursuit of value.



Risk Tolerance Guiding Principles

Define and state the Organization's Overall Risk Appetite:

ABC Organization operates within a moderate overall risk range. The organization's lowest risk appetite relates to patient care, quality, and safety with a higher risk appetite towards its strategic and operating objectives.

The Value is in creating risk tolerance principles and using them as part of the decision-making process.

The Value is in the Discussion, not the process!



25

Risk Appetite/Risk Tolerance

Principle	Examples	Tolerance
Risk in the pursuit of innovative, breakthrough research that improves the health of our patients		High Medium Low
		High Medium Low
Risk taking that enhances our health care delivery and/or promotes care model changes		High Medium Low
Risk taking that promotes productivity, creativity and reputation		High Medium Low
Risk for rewarded financial gain with an adequate due diligence process and appropriate oversight		High Medium Low
Risk arising from inappropriate discharge of management responsibilities		High Medium Low
Risk that undermine actual safety (patient and employee) or the perception of safety, at our hospitals, clinics, etc.		High Medium Low
Risk for behavior that puts our patients and others at harm		High Medium Low
Risk resulting from unwarranted variation in process		High Medium Low
Risk that inhibit care system integration		High Medium Low
Risk resulting from non-compliance with laws or regulations with appropriate due diligence		High Medium Low
Risk resulting from HR related actions or processes		High Medium Low

26

Other Helpful Tools for Internal Audit Departments



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

27

Internal Audit Balanced Score Card

Internal Audit adds Value to the Organization		
Goals	Measures	Frequency
Adds value by focusing on reviews that align with the organization's mission, vision, values, performance dimensions and strategic objectives.	Customer Survey Responses: How did the work add value to the organization and/or your department, i.e. reduce risk, improve the efficiency/effectiveness of operations?	After every audit
Adds value by focusing on reviews that align with the organization's mission, vision, values, performance dimensions and strategic objectives.	30% of the Audit Plan devoted to projects that advance Patient Quality and Safety	Annually
Audit Plan provides coverage of high risk areas for health care provider organizations.	75% of top health care risks	Annually
Adds value by focusing on reviews that align with the organization's mission, vision, values and strategic objectives.	Annual Survey of IA Customers to assess value (conducted by Chief Compliance Officer)	Annually
Internal Audit is a Business Partner		
Goals	Measures	Frequency
Builds business partnerships with leaders	Number of requests for audits/agreed upon procedures/investigations	Annually
Builds business partnerships with leaders; understands leaders challenges; identifies opportunities to support leaders	A speaker from outside the department is brought in to discuss areas of interest to the group one time per quarter. Each member of the staff shadow one leader per year.	Annually
Provides the highest quality service	Customer Survey Responses: In your interactions with the auditor, what did they do well? How could they be more effective?	After every audit or project
Internal Audit Process		
Goals	Measures	Frequency
Annual Review of the Standards and Code of Ethics; Discussion of Balanced Scorecard Results; Development of New Scorecard	Completed/Not Completed	Annually
AIDET	AIDET used at every meeting/AIDET part of Agenda	Ongoing
Employee Development		
Goals	Measures	Frequency
To have state of the art knowledge in internal audit and related healthcare information.	Minimum of 10 hours per year of relevant training and education for each member of staff. 100% of staff certified within 2 years of hire.	Annually

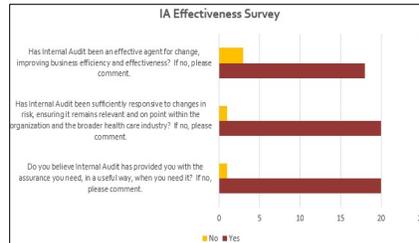


A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

28

Internal Audit Balance Score Card Reporting to the Audit Co. Example

The Chief Compliance Officer surveyed 74 members of the Executive and Senior Leadership Team and other members of management on the effectiveness of the Internal Audit Function. The survey received 21 responses (28% response rate) and identified the following:



Include examples of favorable (and unfavorable) comments.

Additional department goals included in our Balanced Score Card consist of the following:

- Sending customer satisfaction surveys to auditees after every project
- Bringing in leaders to speak to the department about their function and key initiatives
- Training requirements (a minimum of 10 hours/year)
- Certification requirements (100% of staff certified within 2 years of hire). Currently, 4 of 7 staff members have at least one certification, including Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Professional Accountant (CPA), Certified Fraud Examiner (CFE), and Certified Healthcare Internal Audit Professional (CHIAP).



29

Ethical Climate Survey

- Adapted from an employee survey developed by the University of MN's Audit Department.
- The survey assists in evaluating soft controls and tone at the top.
- The use of the survey depends on the area being audited, i.e. are there enough employees to allow for anonymity, do employees have a centralized reporting structure.
- Employees may remain anonymous.
- Each question is followed by a comment box to provide the employee to elaborate.
- Answers range from strongly agree, agree, disagree, strongly disagree and N/A.
- A summary of results are shared with management.
- Concerning themes may require a formal response from management and/or assistance from Human Resources (i.e. significant number of respondents have a fear of retaliation so are not comfortable reporting concerns).



30

Ethical Climate Survey (continued)

Survey Questions:

- Management demonstrates the importance of integrity and ethical behavior to patients and employees.
- Management is open to employee suggestions to improve productivity and quality.
- Management does not override the organization's policies, procedures or work place rules.
- Management has the right knowledge, skills and training to effectively perform their duties.
- Non-management staff has the right knowledge, skills and training to effectively perform their duties.
- Management effectively monitors and provides oversight and direction for the activities in my department.
- Management is concerned with and responsive to feedback or suggestions.
- I understand workplace policies and rules, and have an effective resource for obtaining clarification of policies when needed.
- Management has effectively communicated my job duties and responsibilities to me.
- Management would take appropriate corrective action if regulatory, ethical, policy, procedure or other violations were detected/reported.
- I believe I would be protected from retaliation if I report a suspected violation, e.g. policy, procedure or other regulatory violation, ethical or other concern.
- I am familiar with how to report violations of law or policy and other ethical concerns.
- Would you like to tell us anything else about the operations of your department?



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

31

Questions?

Lorrie Oelkers Ghose
lghose1@fairview.org
952.270.4069



A collaboration among the University of Minnesota,
University of Minnesota Physicians and Fairview Health Services

32