Compliance Institute
Health Care Compliance Association's 2012 Conference

P7 - Risk Assessments: From a Compliance Audit and Internal Audit Perspective

Agenda:

- Introduction
- Evolution to Risk Assessment / Management
- Audit Risk Assessments
- Risk Frameworks
- ERM Approach
- Risk Assessment Resources
# Introductions

## Introductions: Presenters

<table>
<thead>
<tr>
<th>Yvonne Mazarredo</th>
<th>Florie Munroe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erlanger Health System</td>
<td>Saint Raphael Healthcare System</td>
</tr>
<tr>
<td>Director, Compliance Audit &amp; Monitoring</td>
<td>Director, Internal Audit &amp; Compliance</td>
</tr>
<tr>
<td>- CPA &amp; CIA</td>
<td>- CPA, CIA, CCSA, CHC</td>
</tr>
<tr>
<td>- 20+ Years in Accounting, Finance, Internal Audit &amp; Compliance Audit</td>
<td>- Public Accounting and Industry experience in multiple sectors including as CCO/CAE in Academic and community based health systems</td>
</tr>
<tr>
<td>- Transportation, Franchising, Restaurant &amp; Healthcare Industry Experience</td>
<td></td>
</tr>
</tbody>
</table>
Introductions: Erlanger Health System

- Licensed for 819 acute-care beds and 50 long-term care beds.
- Serving patients from 50 counties within a 150-mile radius.
- Level I Trauma Center for adults.
- Affiliated with the University of Tennessee College of Medicine Chattanooga:
  - 160 Residents and Fellows
  - 9 residency programs and 4 fellowship programs at the Chattanooga campus based at Erlanger.
- UT Erlanger Physicians Group, comprised of over 100 physicians and 25 practices.

Introductions: Saint Raphael Healthcare System

- Acute care 511 bed Academic Health Center in New Haven, CT
  - High Volume Emergency Department, Level II Trauma Center
  - Cardiology, Oncology and Orthopedic Centers of Excellence.
- 125 Bed Skilled Nursing Facility.
- Multi-specialty Physician Practice (108 FT/400 PT).
- Joint Ventures Radiology, Dialysis.
- Captive Insurance for Malpractice.
- Affiliated With Yale New Haven School of Medicine
  - 175 Residents and 70 Physician Assistants.
Evolution to Risk Assessment / Management

**Business risk is:**
Events, actions or opportunities which could impact an entity’s ability to meet its objectives and achieve their strategic goals.

**Risk assessment is:**
The identification and analysis of relevant risk to achievement of objectives.

**Risk Management is:**
The determination of how the risk should be managed. (Accept, reject, share, reduce).

**Key Risk Categories:**
(See Appendix I For Additional Risk Categories)

- **Strategic Risk** - Doing the wrong thing
- **Operating Risk** - Doing the right thing the wrong way.
- **Financial Risk** - Losing financial resources or incurring unacceptable liabilities.
- **Compliance Risk** - Non-compliance with Federal or State Legislation / Regulations.
Evolution to RA/RM: Why is it Important?

RA/RM supports value creation by enabling management to:

- Identify potential events that can erode or enhance value.
- Determine risk tolerance/appetite.
- Reduce the impact and likelihood of unexpected / negative outcomes.
- Improve alignment of resources to support achievement of objectives.
- Increase management's ability to achieve objectives.
- Provide consolidated reporting of entity-wide risks.

Evolution to RA/RM: What are the benefits to a formal process?

- Establishes a common business risk language.
- Develops a risk-sensitive culture.
- Provides reasonable assurance that key (strategic/other) risks are identified.
- Provides a structured, consistent, and continuous risk management process.
- Provides a flexible framework for evaluating risks designing mitigating action plans.
Evolution to RA/RM: Risk Effects & Limitations

- Risks **affect an entity’s ability to survive; successfully compete** within its industry; maintain its financial strength and positive public image; and maintain the overall quality of its products, services and resources.

- There is **no practical way to reduce risk to zero**.

- **Benefits should outweigh the costs** associated with a Risk Mitigation Plan.

- **Management and Board must determine how much risk** is to be accepted, and strive to maintain risk within these levels (Risk Appetite).

Evolution to RA/RM: Risk Effects & Limitations (cont.)

- RA/RM is **dependent on human judgment** and therefore susceptible to decision making errors.

- Human failures such as **simple errors or mistakes** can lead to inadequate responses to risk.

- **Controls can be circumvented** by collusion or overridden by management; Risk management decisions can also be overridden/ignored.
Evolution to RA/RM: Key Success Factors

- Board & management sponsorship.
- Determination of company’s overall risk appetite.
- Active participation of key personnel in risk assessment & response processes.
- Risk response roles & responsibilities defined.
- Ongoing monitoring & reporting of:
  - Risk results,
  - Risk action plans and,
  - Risk alignment.
- Timely resolution of critical risks.

Evolution to RA/RM: What is the scope? Who is responsible?

Scope:
- RA/M should be applied at each key business unit/division level and at a corporate level to arrive at entity and consolidated results.
- Consider performing under “Attorney-Client Privilege”.

Responsibility:
- RA/RM is the responsibility of the Board and Management, requiring their involvement in and/or sponsorship of the process.
- RA/RM can be facilitated by Compliance, Internal Audit, Legal Counsel, Risk Management or external consultants.
Evolution to RA/RM: Roles & Responsibility

Evolution to RA/RM: Internal Audit's Role in RM

Reprinted with permission of the Institute of Internal Auditors
Evolution to RA/RM: Who should participate?

Suggested Key Businesses & Participants

Organization Perspective:

CEO & Direct Reports:
[Minimum participants recommended are in Bold; Can be performed via questionnaire, live workshop or combination of both.]

- Joe Healthcare, Inc. (JHI) / Hospital
  - CEO
  - COO
  - CFO
  - General Counsel
  - CAE
  - CCO
  - CMO
  - CIO
  - SVP, Human Resources
  - SVP, Strategic Planning
  - SVP, Investor Relations
  - SVP, Corporate Development

Other:

- JHI Subsidiary I / Home Health
  - President
  - Controller
  - SVP, Global Ops & GM
  - CIO

- JHI Subsidiary II / SNF
  - President
  - Controller
  - SVP, Global Ops & GM
  - CIO

- JHI Subsidiary III / DME
  - President
  - Controller
  - SVP, Global Ops & GM
  - CIO

Compliance Perspective:

Minimum participants recommended are in Bold; Can be performed via questionnaire, live workshop or combination of both.

- Joe Healthcare, Inc. (JHI) / Hospital
  - CFO
  - General Counsel
  - CAE
  - CCO
  - Revenue Cycle Dept. Heads
  - CIO
  - Privacy & Security Officer
  - CMO
  - Risk Management
  - Other relevant staff based on risk topic.

Other:

- JHI Subsidiary I / Home Health
  - President
  - Controller
  - Other Revenue Cycle Staff

- JHI Subsidiary II / SNF
  - President
  - Controller
  - Other Revenue Cycle Staff

- JHI Subsidiary III / DME
  - President
  - Controller
  - Other Revenue Cycle Staff
**Evolution to RA/RM: Compliance Perspective**

**Governance, Risk, Compliance (GRC)**

- **Fiduciary Standards of Conduct**
  - Role of Governance vs. Role of Management
  - Financial management of assets-Prudent Business Judgment
  - Conflicts of Interest
  - Quality of Care
  - Executive Compensation Determinations

- **Regulatory Environment: Federal and State**
  - Not for Profit/Charity regulations
  - Sarbanes-Oxley
  - Dodd Frank

**Historic Approach:**

- Complex Compliance issues dealt with in an ad hoc manner.
- P&P created in silos; with no rationalization to existing CC or business framework.
- Fragmented compliance control environment.

**Historic Outcome:**

- Unnecessary and redundant infrastructures.
- Lack of effective plans of correction.
- Inefficient, incoherent communication.
- High untracked compliance and audit costs.
- Reduced organizational transparency.
Evolution to RA/RM: Compliance Perspective

Compliance Evolution to RA/RM:
- Boards and management revisiting compliance.
- CCO performing qualitative and quantitative analysis of Compliance Program.

Outcome Sought:
1) Compliance Program that is:
   - Comprehensive
   - Effective
   - Efficient
   - Measurable

2) Clear articulation of Compliance:
   - Objectives
   - Roles
   - Responsibilities
   - Accountability

Evolution to RA/RM: Compliance Perspective

Reactive
- Lack of Board or senior management emphasis on risk
- No common risk lingo
- Stove-pipe risk management
- Ad hoc approach
- Missing coverage of risk areas

Aware
- Some board and senior management support
- Risk leader identified
- Periodic risk profiling
- Key risks defined in common vocabulary
- Recognized need for ERM

Strategic
- Proactive board and senior management involvement
- Risk managed and assessed across entire organization
- Common language and approach used and understood
- Real-time analysis of risk portfolio

Courtesy of Anne Mc George, Grant Thornton
1. Shared Accountability

1. Provide Assurance to the Board
2. Independence, Objectivity, Integrity, Transparency
3. Operating Context:
   - Policy, Procedures, Controls and Regulations
   - Audit and Monitor
   - Educate and Train
   - Document, document, document
4. Risk identification (inherent, residual);
   Probability/Likelihood; Impact;
   Controls, etc.

2. Shared Operating Principles

3. Shared Methodology

4. Shared Language

Evolution to RA/RM: Internal Audit Vs. Compliance Audit

Core Differences

1. Shared Accountability

Scope of:

1) Responsibilities
2) RA/RM Focus
3) RA/RM Role / Responsibilities

2. Shared Operating Principles

3. Shared Methodology

4. Shared Language
Audit Risk Assessments

As defined by the Institute of Internal Auditors (IIA):

*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.* It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and *improve the effectiveness of risk management, control, and governance processes.*
Audit Risk Assessments: Approach

Things to Consider:

- **What is Objective?**
  - Base Line Control/Risk Assessment
  - SOX Materiality
  - Financial Statement Assurance
  - Operations Efficiency
  - Regulatory Compliance
  - Risk Management

- **What is Area of Focus?**
  - Organization Level (BU, Company, Affiliations, etc.)
  - Function (A/R, A/P, HIM, PFS, HIPAA, etc.)
  - Product / Service Lines

- **What is Audit’s Role / Responsibility?**
  - **Audit** can perform a detailed business risk assessment and obtain agreement from business process owners or have process owners perform assessment.
  - **Compliance** Audit can also participate in the facilitation of risk assessment as well as implementation of Compliance related action plans/risk management.
  - For Organization Strategic risk assessment and risk management, **Internal Audit’s** role is that of facilitator.

Audit Risk Assessments: Process Overview

1. **Develop Audit Risk Universe:**
   - Identify all auditable entities such as:
     - Company
     - Business Unit
     - Subsidiary
   - Identify all auditable Operation, Financial & IT key processes such as:
     - HIM
     - PFS
     - Purchasing
     - Accounts Payable
     - Charge Master
     - Software Development
     - Network & Application Security
2. Risk Rank Audit Universe:
   - Rank can be based on various metrics such as:
     - Inherent risk
     - Financial statement impact/materiality
     - Complexity of process
     - History of adjustments / Prior audit results
     - Propensity for Change
     - Management’s strategic risk assessment results
     - Managements control self assessment (CSA) results.
   - Identify ranking metric for each criteria and total such as:
     - High = 3; Med = 2; Low = 1
     - High = 4.0 – 5.0 ; Med = 2.5 – 3.9; Low = 1.0 – 2.4
   - Review Risk Ranking Results with Process Owner / Management.

3. Incorporate into Audit Plan
   - Prioritize audits based on risk ranking.
   - Develop audit plan based on High / Medium risk ranking & resources.
   - Consider periodic cycle for material key processes (i.e. Revenue Recognition).
   - Obtain Audit Committee approval.
### Audit Risk Assessments: Example 1 - Audit Risk Universe

<table>
<thead>
<tr>
<th>JHI - Sub1</th>
<th>Likelihood of Ineffective or Non-Effective 1=Low 2=Med 3=Hi</th>
<th>Impact of Ineffective Procedures or Controls 1=Low 2=Med 3=Hi</th>
<th>P&amp;L Impact 1=Low 2=Med 3=Hi</th>
<th>Age of Prior Audit 1=1-2 Years 2=3-4 Years 3=5+ Years</th>
<th>Total Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit &amp; Collections</td>
<td>Capital Planning (CPR Process)</td>
<td>A/R</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Capital Assets</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Consolidation Reporting/SEC</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>G&amp;A Control</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Risk Management (Insurance, WC)</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>A/P</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Planning &amp; Reporting</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Payroll</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Human Resources:</td>
<td>Compensation</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Recruiting, Hiring, Retention &amp; Termination</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Benefits (including TPA on-site audit)</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Training &amp; Development</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

### Audit Risk Assessment: Example 2 - Audit Risk Universe

<table>
<thead>
<tr>
<th>JHI - Sub1</th>
<th>Materiality of Amounts 1=Low 2=Med 3=High</th>
<th>Complexity of Process 1=Low 2=Med 3=High</th>
<th>History of Adjustments 1=Low 2=Med 3=High</th>
<th>Propensity for Change 1=Low 2=Med 3=High</th>
<th>Total Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit &amp; Collections</td>
<td>Capital Planning (CPR Process)</td>
<td>A/R</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Capital Assets</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Consolidation Reporting/SEC</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>G&amp;A Control</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Risk Management (Insurance, WC)</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>A/P</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Planning &amp; Reporting</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Payroll</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Human Resources:</td>
<td>Compensation</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Recruiting, Hiring, Retention &amp; Termination</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Benefits (including TPA on-site audit)</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Training &amp; Development</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
### Audit Risk Assessment: Example 3 – SOX B/S Materiality

(See Appendix II for Full Template)

### Audit Risk Assessment: Example 3.1 – SOX I/S Materiality

(See Appendix II.A for Full Template)
Audit Risk Assessment: Example 3.2 - Audit Risk Universe

(See Appendix II.I for Full Template)

Audit Risk Assessment: Example 4 - Audit Risk Universe

(See Appendix IV for Full Template)
### Audit Risk Assessment: Example 5 - Audit Risk Universe

(See Appendix IV for Full Template)

### Risk Frameworks
Risk Frameworks: Risk Process

- Risk Assessment
- Risk Management
- Performance Management

Risk Frameworks: Risk Management / Performance

**Methodologies**
- TQM
- Six Sigma
- Lean
- SCOR
- GRC
- COSO ERM

**Related Process**
- PDCA
- DMAIC
- PSMDR
Risk Frameworks: Total Quality Management (TQM)

Risk Frameworks: Six Sigma, Lean, SCOR
Enterprise Risk Management is:

“A process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Source: COSO Enterprise Risk Management Framework
**Risk Frameworks: COSO ERM Framework**

ERM Framework:
New COSO-ERM Framework, builds on the Original framework, with a focus on Risk Management.

- Risk philosophy & risk appetite is established.
- Objectives/goals are set & aligned to entity’s mission.
- Potential events/risks are identified.
- Identified risks are assessed.
- Risks are evaluated & action plans defined.
- Policies & procedures are established.
- Timely and effective communication of information.
- ERM process is monitored to ensure it remains aligned to the entity’s objectives.

---

**Risk Frameworks: Common Elements of All Methodologies**

**Phase 1: Understand the Business**
- Understand business objectives, strategies and goals.
- Understand control environment.
- Identify relevant healthcare industry, regulatory and economic trends / issues.

**Phase 2: Develop the Risk Model**
- Create risk framework.
- Define impact and vulnerability criteria.
- Validate risk framework and criteria with Management.
- Create preliminary list of risk for assessment.

**Phase 3: Assess and Prioritize**
- Define risk assessment approach (top-down or bottom-up).
- Identify key individuals to participate in interviews, surveys, workshops.
- Summarize assessment results and prioritize risks.
- Confirm risk prioritization results with Management.

**Phase 4: Develop Risk-Based Audit Plan**
- Identify risks for audit focus.
- Map key risks to the Audit Universe.
- Determine audit scope for IA risks.
- Develop risk-based audit plan.
ERM Approach

ERM Approach: How does it work?

ERM process is comprised of 5 key elements:

1. Objective Setting
2. Event / Risk Identification
3. Risk Assessment
4. Risk Response / Control Activities
5. Monitoring & Reporting
ERM Approach: How does it work?

1. Objective Setting

- Objectives are defined as part of the planning process and confirmed at the start of the ERM process.

- Management's risk strategy and appetite determined in the setting of objectives (i.e. How much risk is management and the board willing to accept).

Example 1 – Organization Strategic Perspective:

1. Objective Setting

- **Organization's Mission:**
  To offer highly valued, innovative and minimally invasive solutions to medical needs.

- **Organization’s Strategic Objective:**
  To reach $5B Gross Revenue by 2012.

- **Related Organization’s Strategic Initiative:**
  R&D Objective - To provide new or enhanced quality Products timely to meet industry needs and support company revenue growth
Example 3 - Corporate Compliance’s Perspective:

1. Objective Setting

- **Compliance Mission:**
  
  Joe Healthcare, Inc. (JHI) is committed to full compliance with all Federal and state healthcare program requirements, including a commitment to prepare and submit accurate claims.

- **Compliance Strategic Objective:**
  
  Provide reasonable assurance of Claims / Billing Accuracy through an effective Compliance Audit Plan.

- **Related Compliance Work Plan Initiatives:**
  
  Review billing policies, educate staff, perform periodic random and focused claims audits, develop corrective action plans if needed, report results to management and the Board.
ERM Approach: How does it work?

1. Objective Setting
2. Event / Risk Identification
3. Risk Assessment
4. Risk Response / Control Activities
5. Monitoring & Reporting

ERM Approach: Who Regulates Healthcare?

Federal

Any Provider USA

Regional Home Health Intermediaries
Local Government
Joint Commission

State

State Medicaid
State Survey & Survey Certificates

DOI's RAC's, PSOC's

CMS Center for Medicare Medicaid Services

Departmental Appeals
Congress
Federal Circuit Courts
Supreme Court

DME Regional Contractors
MACs
MICS
PRRB

Regional Offices

OIG / DOJ

Federal

IRS
OPO
OCR
FCC
DOJ
DOT
OHRP
OSHA
FTC
DOL
NRC
FDA
HHS
FBI
EPA
HRSA
NIOSH
SEC

Adapted from AHA News, May 29, 2000
December 2000 / NNG
ERM Approach: Sources for Risk Identification

Applicable From a Compliance Audit & Internal Audit:

External Sources:
- OIG Work plan
- HCCA
- AHLA
- AHIA
- HFMA
- IIA
- AICPA
- MCR/MCD Contract Auditor Targets
- PEPPER Report
- Industry / Professional Publications

Internal Sources:
- Internal Committees Meetings
- Key Personnel Interviews
- Control / Risk Assessment Questionnaires
- Live Group Sessions
- Internal/External Audit Findings
- Financial Statements
- Service/Product Lines
- Audit Universe
- Benchmarking Analysis

ERM Approach: Examples of Business Risk Categories

- Environmental Risk
- Reputation risk
- Economic Conditions Risk
- Succession Planning Risk
- Sovereign / Political risks
- Legal / Litigation Risk
- Business Interruption Risk
- Supply Chain

(See Appendix I.C for list of additional Risk Categories)
### ERM Approach: Examples of Healthcare Industry Risks

- Implications of Health Care reform
- Heightened regulatory environment
- Increased transparency in reporting quality and pricing
- Recessionary economy
- Increasing capital demands including HIT investment
- Quality and price transparency impact competition
- Physician relationships under increased scrutiny
- Talent shortage continue to intensify
- Community benefits practices threaten tax-exempt status

### ERM Approach: Examples of Hospital Compliance Risks

- HIPAA (PHI Breaches)
- Physician Supervision
- Upcoding
- Patient Status - Medical Necessity / CC44
- Physician Arrangement’s
- 3-Day Payment Window
- 60-Day Refund of Overpayments
- Reputational
- HCAPS
- Adverse Event & PSI Reporting
- OIG Audits and Enforcement Actions
ERM Approach: Examples of Hospital Internal Audit Risks (Financial, Operation & IT Risks)

- Cost Reporting
- Inventory Management
- Purchasing
- Bad Debt Recognition and Valuation
- Medical Device Warranty & Replacement
- Product Recall
- Charge Master
- Network & Application Access
- Disaster Recovery Planning
- Business Continuity Planning

ERM Approach: How does it work for Compliance?

Select Appropriate Tools to Facilitate Risk Identification:

- Policy Management Software
- Communication Plan (Hotline, internet, intranet)
- Training Platform, training modules
- Audit /Monitoring analytic tools
- Incident Management and Tracking System
- Risk Assessment Tool
ERM Approach: How does it work?

2. Event / Risk Identification

➢ Expand understanding of known risks and opportunities that have not been emphasized previously.
  ▪ Dialogue among participants is critical to achieving this objective. Each participant has different exposure levels to risks; Participants with more knowledge of a particular risk should be strongly encouraged to share their perspective with the group.
  ▪ Identify internal and external events that could affect strategy and achievement of objectives.

➢ Differentiate risks and opportunities.
  ▪ Events that may have a negative impact represents risks.
  ▪ Events that may have a positive impact represents opportunities for management's assessment and inclusion in strategy.

➢ Discuss the key activities in place to mitigate each of the highest priority risks and determine if management believes that more should be done to manage each of the highest priority risks.

➢ Recap and discuss the objectives for the next phases of ERM.

ERM Approach: Sample Memo #1

Joe Healthcare, Inc.

December XX, 2011

To All ERM Participants:

In order to effectively identify the Strategic Risks of the company, Enterprise Risk Management workshops have now been scheduled for key members of management.

To best prepare for the workshop it will be helpful if you would review the three attachments provided and give some preliminary thought to the risks. The first attachment provides you with an overview of the ERM methodology to be followed. In the workshops, we plan on covering steps one through four.

The second attachment is a brief questionnaire to be completed prior to the workshop. This will help you think about risks prior to attending the workshop.

The third attachment provides an extensive list of risk types. Please review this list and refer to it when completing the above questionnaire.

Your active involvement is needed and also greatly appreciated for the success of the ERM process. If you should have any questions, please do not hesitate contacting me.

Best Regards,

Jane Smith

(See Appendix I for Full Template)
ERM Approach: Sample Memo #2

Joe Healthcare, Inc.

December XX, 2011

To All ERM Participants:

An Enterprise Risk Management workshop has been scheduled to be held during the corporate offices on January 9, 2012 at 9:00 A.M.

To best prepare for the workshop and make the ERM process more efficient and effective, please review the materials attached and complete the Risk Questionnaire. All Risk Questionnaires will be required in advance of the live workshop. Please fax to my attention at (423) 999-9999 or forward to jane.smith@jhi.com no later than January 3, 2012.

ERM Materials Overview:

1. ERM Overview: The first attachment provides you with an overview of the ERM methodology to be followed. In the workshop, we plan on covering step three, “Risk Assessment”.
2. Risk Types: The second attachment provides an extensive list of risk types. Please review this list and refer to it when completing the Risk Questionnaire in the following step. You can also utilize the list as a quick check list of potential risks to the company, specifically risks that will keep us from achieving strategic objectives.
3. Risk Questionnaire: The third attachment is a brief questionnaire to be completed prior to the workshop. This will help you document key risks and your individual assessment of their importance prior to attending the workshop.

Your active participation will be needed and also greatly appreciated for the success of the workshop. If you should have any questions, please do not hesitate to contact me.

Best Regards,

Jane Smith

(See Appendix I.A for Full Template)

ERM Approach: Example of Risk Identification Template

Joe Healthcare, Inc.
ERM Risk Profile

Please complete and return this initial profile to Jane Smith by January 3rd. You can either mail it to Jane Smith’s address or fax it to (423) 999-9999.

The information provided will be summarized and used to further assess and prioritize enterprise risks during the workshop scheduled for January 9th.

Name: 

Business Unit: 

Enterprise Risks:

List your suggested risks and preliminary score using the following measurement criteria categories and descriptions. Consider the following questions and also refer to the list of “Risk Types” provided separately (See Appendix I.A).

- Where do you devote considerable internal effort in order to control?
- What areas receive considerable management reporting?
- What areas are least controlled?
- What have you devoted significant resources to?
- What are the analysts and rating agencies most interested in?
- What wouldn’t you want on the front page of the newspaper?
- What are key obstacles to taking advantage of opportunities or meeting strategic objectives?
- What is impeding growth?
- What are our competitors do better?
- What do our competitors do worse?
- What keeps you up at night?
- What do people complain about within the organization?

(See Appendix I.B for Full Template)
ERM Approach: Example of Risk Category List

JOE Healthcare, Inc.

**Risk Types & Definitions**

Below is a comprehensive list of risk types. Please review and refer to this list as part of the risk identification process for the Risk Questionnaire to be completed. Always note that this list is not all inclusive and there may be other risk types not noted.

You can also use this list as an initial exercise for identifying risks by completing the columns noted to the right of the risk type. Once completed, you can rank the list based on the criteria outlined in the Risk Questionnaire and document these risks you believe are to be the most critical ones to JHE on the Risk Questionnaire.

If you should have any questions, please contact Jane Smith at 423-999-9990 or at jane.smith@jhe.com.

### Risk Types & Definitions

<table>
<thead>
<tr>
<th>Risk Types &amp; Definitions</th>
<th>Applicable (Y/N)</th>
<th>Describe Area of Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Environmental Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic conditions / competitor pricing strategies / cost structures / market share / industry and/or market sector. These are external forces outside management’s ability to control.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory conditions / competitor Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual property rights and competitiveness / new entrants actions that threaten our ability to compete, survive and thrive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Consumer Trends / Social Trends Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The company is not aware of what customer needs, wants and feelings are. Understanding consumer needs and wants may apply to desired quality, willingness to pay and/or speed of execution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Shareholders / Investors Expectations Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The risk of failure to manage shareholder expectations, resulting in a decline in investor confidence that may lead to decline in share price, impact the company’s ability to efficiently raise capital, etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(See Appendix I.C for Full Template)

ERM Approach: How does it work?

**Example 1 – Organization’s Strategic Perspective:**

2. Event / Risk Identification (cont.)

- **Risk:**
  
  Product development projects are not prioritized and monitored to ensure timely rollout of products that will allow company to achieve established revenue.

- **Opportunity:**
  
  Product’s with early rollout capability are identified and implemented to achieve/enhance revenue goals.
Example 2 – Compliance Audit’s Strategic Perspective:

2. Event / Risk Identification (cont.)

- **Risk:**
  Claims financial error rate is trending significantly above 5.0% (i.e. averaging 32.0%). Overcoding and lack of supporting documentation may lead to FCA penalties

- **Opportunity:**
  Undercoding is identified which leads to lost revenue.

ERM Approach: How does it work?

1. Objective Setting
2. Event / Risk Identification
3. Risk Assessment
4. Risk Response / Control Activities
5. Monitoring & Reporting
3. Risk Assessment

- Understand the extent to which potential events might impact objectives.
- Assess risk on both an inherent (risk prior to any mitigating processes/controls) and a residual basis (risk remaining subsequent mitigating processes/controls).
- Assess / prioritize risks from two key perspectives:
  - **Likelihood** of occurrence – What is the probability that this risk would actually occur?
  - **Impact** - How big of an impact would this risk have if it were to occur? This could be in many areas including financial, reputation, human/capital resources, stock valuation, etc.

**ERM Approach: Assessing Identified Risks**

**ERM Approach: How does it work? Example 1**

Assess risk from the following two perspectives:

<table>
<thead>
<tr>
<th>Score</th>
<th>Category</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manageable</td>
<td>Small impact, able to recover from with minor effort</td>
<td>&lt; $25M Rev or, &lt; $12.5M NI</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Medium to serious impact, able to recover from with significant effort</td>
<td>Rev = $25M - $50M or, NI = 12.5M - $25M</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
<td>Very serious impact, very hard to recover from</td>
<td>&gt; $50M Rev or, &gt; $25M NI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score</th>
<th>Category</th>
<th>Description</th>
<th>Chance of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote</td>
<td>Possible but not expected to occur</td>
<td>&lt; 10%</td>
</tr>
<tr>
<td>2</td>
<td>Possible</td>
<td>Possible and could occur</td>
<td>10 - 50%</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>An event that is expected to occur</td>
<td>&gt; 50%</td>
</tr>
</tbody>
</table>
### ERM Approach: How are risks assessed? Example 2

Assess risks from the following two perspectives:

<table>
<thead>
<tr>
<th>Score</th>
<th>Category</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manageable</td>
<td>Small impact, able to recover from with minor effort</td>
<td>&lt; $25M Rev or, &lt; $12.5M NI</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Medium to serious impact, able to recover from with significant effort</td>
<td>Rev = $25M - $50M or, NI = 12.5M - $25M</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
<td>Very serious impact, very hard to recover from</td>
<td>&gt; $50M Rev or, &gt; $25M NI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score</th>
<th>Category</th>
<th>Description</th>
<th>Chance of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote</td>
<td>Possible but not expected to occur</td>
<td>&lt; 10%</td>
</tr>
<tr>
<td>2</td>
<td>Possible</td>
<td>Possible and could occur</td>
<td>10 - 50%</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>An event that is expected to occur</td>
<td>&gt; 50%</td>
</tr>
</tbody>
</table>

### ERM Approach: How are risks assessed? Example 3

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Almost Impossible</td>
<td>Less than 1% chance in 3 years</td>
</tr>
<tr>
<td>B</td>
<td>Remote</td>
<td>Greater than 1% but less than 3% chance in 3 years</td>
</tr>
<tr>
<td>C</td>
<td>Low</td>
<td>Greater than 3% but less than 10% chance in 3 years</td>
</tr>
<tr>
<td>D</td>
<td>Reasonably Possible</td>
<td>Greater than 10% but less than 25% chance in 3 years</td>
</tr>
<tr>
<td>E</td>
<td>Probable</td>
<td>Greater than 25% and less than 50% chance in 3 years</td>
</tr>
<tr>
<td>F</td>
<td>Very High</td>
<td>Greater than 50% chance in 3 years</td>
</tr>
</tbody>
</table>
ERM Approach: How does it work?

Evaluate & prioritize based on prior risk assessment in the following matrix:

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
<th>MED</th>
<th>HIGH</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Remote</td>
<td>2) Possible</td>
<td>3) Likely</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Manageable</td>
<td>LOW</td>
<td>LOW</td>
<td>MED</td>
<td></td>
</tr>
<tr>
<td>2) Major</td>
<td>LOW</td>
<td>MED</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>3) Critical</td>
<td>MED</td>
<td>HIGH</td>
<td>CRITICAL</td>
<td></td>
</tr>
</tbody>
</table>

Risk Profile Deliverables:
Joe Healthcare, Inc. Risk Profile
(Int'l Healthcare Public Company)

Mission:
To offer highly valued, innovative and minimally invasive solutions to medical needs.

Strategic objectives:
1) Reach $5B in Revenue by 2012; 2) XX; 3) XX; 4) XX; 5) XX; 6) XX.

Business Risks:
(ranked by net evaluation)
1. R&D Pipeline
2. Natural Disaster
3. Third Party Reimbursement
4. Supply Chain/Distribution Inefficiencies
5. Legislation
6. Regulatory Compliance (FDA, ISO, Medicare)
7. Product Risk/Liability
8. Economic Conditions/Key Marketa
9. Supply Chain Supplier Capacity, Stability & Decentralization
10. IT Infrastructure, Capacity & Capability
ERM Approach: How are risks assessed? Example 2

Risk Profile Deliverables:

Jane Health System
(Hospital Compliance)

Mission:
To provide compliance guidance and training for all Health System employees and affiliates for the prevention, detection and resolution of violations of laws and regulations.

Business Risks Samples:
(rank by net evaluation):
1. Privacy & Security Enforcement/Compliance
2. Coding / Billing Errors
3. Clinical Documentation
4. Physician Arrangements
5. Lack of sufficient & qualified internal resources to monitor, correct & report compliance issues timely.
6. Untimely responses to RAC Audits
7.
8.
9.
10.

LIKELIHOOD
1) Remote (< 10%)
2) Possible (10 -- 50%)
3) Likely (> 50%)

IMPACT
1) Manageable (< $5m)
2) Major ($25 - $49m)
3) Critical (> $50m)

Business Risk Profile

Objectives:
1) Maintain claims error rate below 5%; 2) XX; 3) XX; 4) XX; 5) XX; 6) XX.

75

ERM Approach: How are risks assessed? Example 3

Risk Analysis for Entity: Hospital 1 12/03/2010

- Safety
- Radiology
- Physician Services
- Pharmacy
- Patient Rights
- Patient Accounting
- Nursing Services
- Medical Records
- Marketing
- Laboratory
- Information Systems
- Human Resources
- HIPAA - Security
- Finance
- Emergency Preparedness
- Deficit Reduction Act
- Corporate Responsibility
- Compliance
- Ambulatory Surgery
- Ambulance Services
- Advanced Imaging Services

- Residual Risk
- Not Assessed
- Unmitigated on Initial Assessment
- Mitigation Underway
- Mitigated Risk After Assessment
- Mitigated on Initial Assessment

76
ERM Approach: How are risks assessed? Example 4

Risk Profile Example 3:
1. Governance Structure
2. Regulatory / Healthcare Reform
3. ABCMP Strategic Objective
4. AP / Purchasing
5. SYSTEM System Implementation
6. Research
7. Charge Capture, Billing, Coding
8. Community Reputation
9. Attracting, Retaining and Promoting Talent
10. Competition
11. Mass Patient Event
12. AP / Purchasing
13. HIPAA Compliance
14. Pace of Change / Competing Priorities
15. Patient Outcomes / Quality
16. Access to Information to Perform Job Functions
17. Physician Relations

ERM Approach: How are risks assessed? Example 5

Risk Profile Example 4 - Two Year Comparison:
1. Compliance Audits
2. P&P
3. Compliance Training
4. COI Process
5. Provider Documentation
6. Operations
7. Support
8. Stark Reviews
9. Business Continuity Management and Disaster Recovery
10. IT Infrastructure

ERM Approach: How are risks assessed? Example 5
**ERM Approach: How are risks assessed? Example 6**

Organizational Compliance Planning: Heat Map

To what extent can the failure to comply with a requirement result in loss, harm or the diminished opportunity for gain such that it could affect the sustainability of the organization.

- Employment Discrimination
- Physician Supervision
- Wage and Hour
- False Claims Act
- HIPAA Privacy
- Payment Recovery Audits
- Physician Compensation Stark/AKAs
- Tax - Billing and Collections
- EMTALA
- Tax - Financial Assistance Policy
- Vendor Relations Antitrust
- FTC Red Flags
- Excluded Providers
- Clinical Research
- Conflict of Interest
- Provider-Based Department
- Mandatory Reporting
- Joint Ventures

**ERM Approach: How does it work?**

1. Objective Setting
2. Event / Risk Identification
3. Risk Assessment
4. Risk Response / Control Activities
5. Monitoring & Reporting
ERM Approach: How does it work?

4. Risk Response / Control Activities

- Determine mitigation choices (see next slide)
- Identify and evaluate risk mitigation possibilities.
- Evaluate and select options in relation to entity’s risk appetite, cost vs. benefit, and degree to which a response will reduce impact and/or likelihood.
- Document risk response, action plan and metrics where applicable.
- Identify responsible individual(s) for action plan.

ERM Approach: Risk Mitigation Choices

Reduce
Avoid
Accept
Share

RISK
ERM Approach: How does it work?

Example 1 - Organization’s Strategic Perspective:

4. Risk Response / Control Activities
   - Risk:
     Product development projects are not prioritized and monitored to ensure timely rollout of products that will allow company to achieve established revenue.
   - Action Plan / Risk Response:
     Reduce - Implement a product development pipeline that prioritizes projects based on metrics such as planned launch date, estimated revenue stream, etc.
   - Responsible Party:
     R&D

ERM Approach: Example 2 – Risk Action Plan

Example 1 – Compliance Perspective:

4. Risk Response / Control Activities
   - Risk:
     Failure to properly credit Medicare for Medical Device warranty & replacement credits/no charge.
   - Action Plan / Risk Response
     - Medical Device tracking logs developed.
     - Quarterly audits of logs.
   - Responsible Party:
     Multi-disciplinary team formed (OR, Cath Lab, MM, Finance, CC, IA)
ERM Approach: Example 1 – Risk Action Plan Template

ERM Approach: Example 2 – Detailed Action Plan
ERM Approach: How does it work?

5. Monitoring & Reporting

- Dashboard of risks and related responses (visual status of where key risks stand relative to risk tolerances)
- Process for communicating and monitoring risks, action plans and responsibility to key personnel, Management and BOD.
- Obtain Concurrence of Key Risks (Management & BOD)
- Effectiveness of the ERM process.
- Frequency
  - Monitor action plans quarterly
  - Periodic updates to risk profile to reflect and realign:
    - Changes in objectives
    - Changes in systems
    - Changes in processes
    - Changes in risk environment
  - Triggers for full risk assessment
    - Significant/material changes in Organization, regulatory environment
ERM Approach: How does it work? Example 1 – Dashboard

<table>
<thead>
<tr>
<th>Risk Area ID</th>
<th>Risk Area</th>
<th>High Priority Risk Events</th>
<th>Medium Priority Risk Events</th>
<th>Low Priority Risk Events</th>
<th>Completed</th>
<th>In Process</th>
<th>Not Started</th>
<th>Summary Action Plan Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>121 Physician Arrangements</td>
<td></td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>3 - Med</td>
<td>1 – High</td>
<td>High-risk remains “In Process”. 2 out of 5 “Medium” risks have been completed.</td>
<td></td>
</tr>
<tr>
<td>119 3-Day Window</td>
<td></td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>72 Physicians at Teaching Hospitals (PATH)</td>
<td></td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td></td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>50 Graduate Medical Education Payments (GME)</td>
<td></td>
<td>0</td>
<td>3</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>For the 1 remaining Risk “In Process” - 1 out of the 4 detailed action plans has been completed.</td>
<td></td>
</tr>
<tr>
<td>120 Medical Necessity</td>
<td></td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td></td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>113 Provider-Based Status</td>
<td></td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td></td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>117 Affiliation Agreements</td>
<td></td>
<td>0</td>
<td>0</td>
<td>7</td>
<td></td>
<td>NA - Only addressing Medium &amp; High Risks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>67 Waiver of Copayments and Deductibles</td>
<td></td>
<td>0</td>
<td>0</td>
<td>5</td>
<td></td>
<td>NA - Only addressing Medium &amp; High Risks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall/Total</td>
<td></td>
<td>5</td>
<td>28</td>
<td>46</td>
<td>22</td>
<td>10</td>
<td>0</td>
<td>69.7% 30.3% 0.0%</td>
</tr>
</tbody>
</table>

Quarterly Change in Results

ERM Approach: How does it work? Example 2 – Dashboard

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Issues</th>
<th>Percent of Cases</th>
<th># Closed</th>
<th>Percent Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>28</td>
<td>53%</td>
<td>24</td>
<td>45%</td>
</tr>
<tr>
<td>Billing</td>
<td>5</td>
<td>9%</td>
<td>3</td>
<td>6%</td>
</tr>
<tr>
<td>HIPAA</td>
<td>8</td>
<td>15%</td>
<td>1</td>
<td>2%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>4</td>
<td>8%</td>
<td>4</td>
<td>8%</td>
</tr>
<tr>
<td>Operations</td>
<td>7</td>
<td>13%</td>
<td>8</td>
<td>15%</td>
</tr>
<tr>
<td>Quality</td>
<td>1</td>
<td>2%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Fraud &amp; Abuse</td>
<td>-</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>53</td>
<td>100%</td>
<td>40</td>
<td>75%</td>
</tr>
</tbody>
</table>
ERM Approach: How does it work? Example 3 – Dashboard

ERM Approach: How does it work? Example 4 – Dashboard
ERM Approach: How do you implement?

The following is the suggested approach for executing ERM:

- **ERM Step 1 – Objective Setting**
  - Obtain company/function’s strategic objectives if available from key businesses (via email/conf call).
  - Determine Management’s risk appetite – Thresholds to be approved by CEO & CFO (via email/conf call).

- **ERM Step 2 – Event / Risk Identification**
  - Determine individuals to be involved in ERM process (via email/conf call).
  - Provide participants with ERM materials in advance of live workshop (via interoffice mail, email or live meeting).
    - ERM process overview (See Appendix I & I.A)
    - Risk questionnaire (See Appendix I.B)
    - List of “Risk Types” (See Appendix I.C)
  - Summarize questionnaire responses in advance of workshop.

- **ERM Step 3 – Risk Assessment**
  - Discuss risks identified by participants in prior step and assess/prioritize risk (via live Sr. Management workshop).
  - Identify Risk Owners (via live Sr. Management workshop).

- **ERM Step 4 – Risk Response / Control Activities**
  - Summarize risk assessment results from workshop.
  - Obtain suggested mitigation/action plans from Risk Owner (via email/conference calls).
  - Provide Risk Profile and respective action plans to participants/key Management (i.e. CEO, CFO, GC) for final review/agreement (via email).
  - Present to the BOD.
  - Distribute to all participants.

- **ERM Step 5 – Monitoring & Reporting**
  - Obtain status update on action plans (via email/conf call).
  - Verify risks initially identified – Do risks still exist and/or has a new risk been identified (via email/conf call).
  - Summarize results and report to Sr. Management and BOD (via email/live at BOD meetings).

Note: ERM step 1-4 should be performed annually. Step 5 should occur quarterly.

---

**Project Timeline Example:**

<table>
<thead>
<tr>
<th>Jan’12</th>
<th>Feb’12</th>
<th>Mar’12</th>
<th>Apr’12</th>
<th>May’12</th>
<th>Jun’12</th>
<th>Jul’12</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERM Step 1 - Objective Setting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Currently in process for all 3 Subsidiaries.</td>
</tr>
<tr>
<td>ERM Step 2 - Event / Risk Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERM Step 3 - Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Should be completed prior to new fiscal year strategic planning and budgeting process.</td>
</tr>
<tr>
<td>ERM Step 4 - Risk Response / Control Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Will work towards delivering results at 1Q ’12 BOD meeting; other risks will be delivered by 3Q ’12 BOD meeting.</td>
</tr>
<tr>
<td>ERM Step 5 - Ongoing Monitoring &amp; Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Occurs Quarterly.</td>
</tr>
<tr>
<td>Present to BOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- **Planned**
- **In Process**
- **Completed**

---

47
Closing Summary

Closing Summary: Effective RA/RM

Risk Assessment

Risk Management

Performance Management
Effective RA/RM:

- Aligns resources to key objectives and risks.
- Embeds RA/RM in business processes.
- Provides a method for highlighting & communicating RA/RM key risks to Management & BOD.
- Assigns accountability.
- Measures performance.
- Increases ability to achieve objectives.

Closing Summary: Questions? Comments?

Presenters contact information:

Yvonne Mazarredo  
Director, Compliance Audit & Monitoring  
Erlanger Health System  
mazarrey@erlanger.org  
(423) 778-7908

Flore Munroe  
Director, Internal Audit and Corporate Compliance  
Saint Raphael Healthcare System  
fmunroe@srhs.org  
(203) 789-4228