Compliance Risk Management Strategies

Arlene F. Baril, MS, RHIA
Director, Facility Reimbursement Services
Sinaiko Healthcare Consulting
Agenda

• Objectives of Risk Management

• Understanding the Risk Management Process

• Risk Management Tools & Techniques

• Q&A
What is Risk Management?

The practice of identifying and analyzing risk or losses and taking those measures necessary to minimize the real or potential losses to levels acceptable to the organization.

The risk management function can be broken down into four steps:

- Identification and analysis of loss exposures
- Selection of the appropriate mechanism(s) to reduce or, if possible, eliminate the possibility of loss
- Implementation of the chosen technique(s)
- Monitoring and review of the results
Issues in Risk Management

- The legal setting
- Malpractice
- Avoiding malpractice
- The medical record
- Patient’s rights
Why is Risk a Priority?

- Many executives see an array of ever-increasing business risks
- Business risk management practices require improvement
- Substantial revisions in business risk management have either been made or will be made
- Key constituents want more confidence that all potentially significant risks are identified and managed
- Current economic conditions – paradigm shift for many
Why Do We Assess Risk?

- Improve strategic planning
- Increased regulatory exposure
- Better address uncertainty
- Seize opportunities
- Allocate resources to priorities
- Shrinking margins
Nature of Risk

- **R** = risk is **relative** because perception of downside and upside risk is individual, and that applies to people and organizations

- **I** = risk is **intuitive** because we learn with experience and time

- **S** = risk is **significant** because everything we do has positive and negative consequences

- **K** = risk is **kinetic** because it changes relative to situations, events, time and space
Nature of Risk (continued)

- Risk is universal
- Risk is not properly identified and managed by most organizations, including governments
- Risks are diverse and inherent to the business operations
Internal Risks

- Policies and procedures
  - Internal controls
- Contracting
  - Vendor relationships
  - Loan relationships
- Financial reporting
  - Financial statements
  - Tax returns
  - Investor reporting
  - Credit risk
  - Liquidity
Internal Risks (continued)

- Crisis management program
  - Business continuity plan
- Human resource management
  - Hiring and terminations
  - Employee relations
- Governance
  - Succession
  - Board knowledge
- Information technology
  - Security
  - Disruptions
- Document management
External Risks

- Accreditation agencies
- Office of the Inspector General
- OSHA
- EPA
- State Attorney General Office
- Public relations/reputation
- Competition
- Litigators
- Past employees
- HIPPA
- IRS
- Auditors
Internal Environment

- Foundation for all the other components
- Sets tone of institution
- Attention and direction provided by board and committee
- Integrity and ethic values of management
- Management philosophy and operating style
- The way management assigns authority and responsibility
Risk Domains

- Operational – core business including systems and processes. Example: admission process
- Financial – ability to earn, raise or access capital. Example: financial reporting
- Human – recruiting, retention and managing workforce. Example: worker’s compensation
- Strategic – ability to grow and expand. Example: program development
- Legal/regulatory – statutory, regulatory compliance, licensure, accreditation. Example: OSHA
- Technology – biomedical and information technologies. Example: desktop service
Risk Assessment Benefits

- Successful risk identification and mitigation become key elements of a strategic plan
  - Competitive advantage for those with ERM capability and discipline
  - Mitigate downside exposure and capitalize on upside opportunities
- Reduced financial losses
- Improve business performance
- Enhanced risk identification and assessment processes
- Improved awareness and collaboration
- Improved decision making and accountability
- Improved regulatory compliance
Risk of No Risk Assessment

- All risks are a threat if ignored
- Bankruptcies
- Fraud
- Restatement of earnings
- Decrease business valuation
- Loss of customers
- Careers destroyed
- Lack credibility in market
Steps to a Risk Management Program

- Set objectives and understand context
- Identify boundaries, risks and opportunities
- Assess risks and define management actions
- Prioritize risks and allocate resources
Risk Management Analysis Tools

- Root cause analysis
- External assessments
- Incident reports
- Complaints
- Claims
- Clinical audits
- Performance monitoring
Building a Risk Assessment

- Select a risk framework or combination of frameworks
- Develop a risk ranking model
- Identify the risk universe
- Conduct the risk assessment
Risk Frameworks to Consider
COSO Risk Frameworks

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) is a voluntary private sector organization that encompasses the five professions
  - American Accounting Association
  - American Institute of CPAs
  - Financial Executives International
  - Institute of Internal Auditors
  - Institute of Management Accountants
Internal Control Framework Components

1. **Control Environment**
   
   The organizational culture that influences ethical behavior, workplace integrity, risk and compliance consciousness of its personnel.

2. **Risk Assessment**
   
   The process of identifying risks that threaten the institution’s achievement of objectives.

3. **Information and Communication Systems**
   
   The process for providing the right information to the right people at the right time for them to effectively carry out their responsibilities.

4. **Monitoring**
   
   The management process in place to verify controls are working as intended and identify anomalies.

5. **Control Activities**
   
   The activities established to support compliance requirements and risk responses selected by management are carried out.
COSO Enterprise Risk Management Framework

- States “ERM 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.”
Expanded Risk Domains

- **Operational**
  - core business including systems and processes. Example: admission process

- **Financial**
  - ability to earn, raise or access capital. Example: financial reporting

- **Human**
  - recruiting, retention and managing workforce. Example: worker’s compensation

- **Strategic**
  - ability to grow and expand. Example: program development

- **Legal/regulatory**
  - statutory, regulatory compliance, licensure, accreditation. Example: OSHA

- **Technology**
  - biomedical and information technologies. Example: wireless access
New Components

- **Objective Setting**
  - Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

- **Event Identification**
  - Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.

- **Risk Response**
  - Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
Compliance Framework: Seven Essential Elements of a Compliance Plan

- Standards and Procedures
- Oversight
- Education and Training
- Monitoring and Auditing
- Reporting
- Enforcement and Discipline
- Response and Prevention
Identify the Risk Universe
Using OIG Guidance to Assess Risk Areas

- Hospitals
- Clinical Laboratories
- Home Health Agencies
- Third Party Billing
- Durable Medical Equipment
- Medicare + Choice
- Nursing Facilities
- Ambulance Suppliers
- Pharma Manufacturers
- Research
- Hospice
- Individual and Small Group Physicians
Hospital Risks

- Billing for services not rendered, duplicate claims, unbundling, billing for discharge in lieu of transfer
- Medically unnecessary services
- Upcoding or DRG creep
- Outpatient services rendered in connection with inpatient stay
- Teaching physician and resident requirements
- Credit balances
- Anti-kickback
- Stark physician referral
- Financial arrangements between hospitals and hospital-based physicians
- Patient dumping
Research Risks

- IRB processes
- Time & effort reporting
- Proper allocating charges to award projects
- Informed consent
- Human & animal subjects protection
- Sub-recipient monitoring
Clinical Laboratories Risks

- Anti-kickback
- Stark self-referral issues
- CLIA requirements
- Medical Necessity
  - Requisition design
  - Notice to physicians
  - Physician acknowledgement
  - Test utilization monitoring
- Billing practices
- Reliance on standing orders
- Marketing practices
- Profile pricing
Individual and Small Group Physician Risks

- Coding and billing: services not rendered or documented, double billing, misuse of provider numbers, unbundling, use of modifiers, upcoding
- Reasonable and necessary services
- Documentation quality
- Improper inducements, kickbacks or self-referrals
- Retention of records
Home Health Agency Risks

- Billing practices: services not rendered, medical necessity of services, duplicate billing, billing for patients that don’t meet homebound requirement, etc.
- Inadequate or substandard care
- Falsifying documentation: amendments, plans of care, forgery
- Cost reports
- Credit balances
- Incentives to potential referral sources
- Stark physician self-referral
Home Health Agency Risks (cont)

- Over and under utilization
- Marketing practices
- Oversight of sub-contracted services
- Discriminatory admissions and discharges
- Improper influence over referrals by hospitals that own home health agencies
- Patient abandonment
Hospice Risks

- Uniformed consent to elect the Medicare Hospice Benefit
- Admitting patients to hospice that are not terminally ill
- Arrangements with other health care providers
- Under-utilization
- Falsified medical records or plans of care
- Untimely and/or forged physician certifications of the plan of care
- Insufficient oversight of patients
- Inadequate or incomplete Interdisciplinary Group services
- Incentives to potential referral sources
- Overlap in services (nursing home and hospice)
Hospice Risks (cont)

- Improper relinquishment of services and responsibilities to nursing homes
- Providing hospice services in a nursing home prior to an agreement
- Billing for higher level of care or inadequate/substandard care
- Billing for unqualified personnel
- Pressure on patient to revoke the benefit
- And the list goes on…..
Durable Medical Equipment

- Billing for items or services not provided or ordered, duplicate billing, unbundling,
- Billing patients for denied charges without a signed written notice;
- Upcoding
- Billing for new equipment and providing used equipment
- Continuing to bill for rental items after they are no longer medically necessary
- Using a billing agent whose compensation arrangement violates the reassignment rule
- Resubmission of denied claims with different information in an attempt to be improperly reimbursed
- Refusing to submit a claim to Medicare for which payment is made on a reasonable charge or fee schedule basis
- Inadequate management and oversight of contracted services, which results in improper billing
- Charge limitations
Durable Medical Equipment (cont)

- Providing and/or billing for substantially excessive amounts of DMEPOS items or supplies
- Providing and/or billing for an item or service that does not meet the quality and standard of the DMEPOS item claimed
- Capped rentals
- Performing tests on a beneficiary to establish medical necessity
- Failure to monitor medical necessity on an on-going basis and maintaining documentation
- Delivering or billing for certain items or supplies prior to receiving a physician’s order and/or appropriate CMN
- Falsifying information on the claim form, CMN, accompanying documentation, or medical record
- Manipulating the patient’s diagnosis in an attempt to receive improper payment
- Inappropriate use of place of service codes or ZX modifier
- Cover letters that encourage physicians to order medically unnecessary items or services
- Routine waiver of deductibles and coinsurance
- Providing incentives to actual or potential referral sources that may violate the anti-kickback statute
Durable Medical Equipment (cont)

- Compensation programs that offer incentives for items or services ordered and revenue generated
- Joint ventures between parties, one of whom can refer Medicare or Medicaid business to the other
- Billing for items or services furnished pursuant to a prohibited referral under the Stark physician self-referral law
- Improper telemarketing practices, patient solicitation activities and high-pressure marketing of non-covered or unnecessary services
- Co-location of DMEPOS items and supplies with the referral source
- Non-compliance with the Federal, State and private payor supplier standards
- Providing false information on the Medicare DMEPOS supplier enrollment form
- Knowing misuse of a supplier number, which results in improper billing
- Failing to refund overpayments to a health care program or patients
Nursing Facility Risks

- Quality of care
- Resident’s rights
- Employee screening
- Vendor relationships
- Billing and cost reports
- Kickbacks, inducements and self-referral
- Creations and retention of records
Ambulance Supplier Risks

- Improper transport of individuals with other acceptable means of transportation
- Medically unnecessary trips
- Trips claimed but not rendered
- Misrepresentation of the transport destination to make it appear as if the transport was covered
- False documentation
- Billing for each patient transported in a group as if he/she was transported separately
- Upcoding from basic life support to advanced life support service
- Payment of kickbacks
Third Party Billing Risk

- Billing practices: services not documented, unbundling, upcoding, inappropriate balance billing, duplicate billing, use of modifiers, waiver of co-pays, etc.
- Coding practices: assumption coding, coding without documentation, coding from unqualified provider documentation, availability of all necessary documents
- Claims submission practices: billing only for documented services, financial incentives for billing staff, provider clarification processes
- Credit balances
- Integrity of data systems
Medicare+Choice Risks

- Election process
- Benefits and beneficiary protections
- Quality assessment and performance improvement
- Cost sharing
- Solvency, licensure and other State regulatory issues
- Claims processing
- Appeals and grievance procedures
- Marketing materials and personnel
- Selective marketing and enrollment
- Disenrollment
- Underutilization and quality of care
- Data collection and submission processes
- Anti-kickback statute and other inducements
- Emergency services
Pharma Manufacturer Risks

- Integrity of data used to develop government reimbursement
- Kickbacks and other illegal remuneration
- Relationship with purchasers: discounts, terms of sale and average wholesale price
- Relationship with physicians and other healthcare professionals
  - Switching arrangements
  - Consulting & advisory payments
  - Other remuneration (entertainment & gifts)
- Relationship with sales agents
- Drug samples
Other Compliance Risks

- RAC/MIC initiatives
- Wage and Hour initiatives
- Product Recalls
- Physician Contracts
- Physician Call Pay
- Medical Staff Dues
- Conflicts of Interest
- EMTALA
- CMS Conditions of Participation
Other Compliance Risks (cont.)

- Software User Access
- Disaster Planning
- Wireless Penetration
- Password Management
- Vendor Access Management
- Wireless Devices
HIPAA Security Rule

- Risk Management implementation specification
  - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Audit controls standard
  - Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI (e-PHI)
- Evaluation standard
  - Perform a periodic technical and non-technical evaluation to demonstrate and document compliance with the entity’s security policy and the requirements of the HIPAA security rule
- CMS Guidance
Develop a Risk Ranking Model
# Sample Risk Ranking Model

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Internal control actions - quality</th>
<th>Written Policies and Procedures - adequacy</th>
<th>Operations - changes</th>
<th>Elapsed time from previous audit</th>
<th>Consequences to Board, staff, phys., patients, or public</th>
<th>Priority of Senior Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation</strong></td>
<td><strong>Segregation of duties</strong></td>
<td><strong>Adequacy of written procedures</strong></td>
<td><strong>Changes in operations</strong></td>
<td><strong>Elapsed time from previous audit</strong></td>
<td><strong>Consequences to Board, staff, phys., patients, or public</strong></td>
<td><strong>Priority of Senior Management</strong></td>
</tr>
<tr>
<td></td>
<td>One person should not have total control of process without intervention, and this protects staff, financial resources and fixed assets. Authorizat...</td>
<td>Shows the degree to which procedures are documented. Policies should assure complete proper communication to staff, consistent performance of work, instructions for continuity of operation during staff turnover. Sufficient detail should exist.</td>
<td>Changes in operations can impact efficiency and effectiveness of the companies performance. Criteria include changes in staff size, processing changes (manual or computerized), systems (input and or output) as well as staff turnover.</td>
<td>This refers to previous audit results and the number of years since the date of the previous internal audit report affecting the unit.</td>
<td>Public perception concerns from adverse publicity, laws &amp; regulations, patient demands, political exposure, physician contracts, vendors &amp; major payors.</td>
<td>Areas on which Senior Management wants to focus</td>
</tr>
</tbody>
</table>

- **Segregation of duties**: One person should not have total control of process without intervention, and this protects staff, financial resources and fixed assets. 
- **Authorization procedures**: A system of using designated forms and authorizations are an important control in safeguarding resources, inclusive of an audit trail. Well trained staff to handle the job at hand.
## Sample Vulnerability Criteria

<table>
<thead>
<tr>
<th>CONTROL EFFECTIVENESS AND EFFICIENCY</th>
<th>SPEED OF RESPONSE</th>
<th>COMPLEXITY</th>
<th>PEOPLE</th>
<th>OPERATIONAL EFFICIENCY</th>
<th>SYSTEM CAPABILITY</th>
<th>RATE OF CHANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIGH 1.0</strong></td>
<td>No method for anticipating and assessing specific risk events exists, so issues are not escalated to the appropriate executives effectively.</td>
<td>Manual processes with many data transfer points and owners.</td>
<td>A limited number of staff or current staff has limited competency to manage risk events. Inadequate cross training exists.</td>
<td>High/unmeasured cost of operations, many quality concerns noted, and unacceptable or unmeasured cycle/process time.</td>
<td>Systems are not operating as Designed or design is flawed; very limited controls.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a HIGH rate of change over the last 6 months.</td>
</tr>
<tr>
<td><strong>MEDIUM .66</strong></td>
<td>A method for anticipating and assessing specific Risk events exists But issues are not effectively escalated to the appropriate executives.</td>
<td>Automated processes encompassing multiple systems and owners.</td>
<td>A limited number of staff and/or staff has moderate competency to manage risk events.</td>
<td>Above industry average cost of operation, some quality concerns noted, and below industry average cycle/process time.</td>
<td>Systems are operating as designed, but design can be improved; controls are bolted on top of the system.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a MODERATE rate of change over the last 6 months.</td>
</tr>
<tr>
<td><strong>LOW .33</strong></td>
<td>Controls are appropriately preventive and detective and there is effective reporting.</td>
<td>Automated processes with Integrated systems.</td>
<td>Most staff has high competency to manage risk events.</td>
<td>Low/average cost of operations, no quality concerns noted, and cycle/process times within specified standards.</td>
<td>Systems are designed, implemented and operating effectively; controls are embedded in the system.</td>
<td>Risk is managed by or directly impacts people, processes, systems or businesses that have experienced a LOW rate of change over the last 6 months.</td>
</tr>
<tr>
<td>Compliance Risk Areas</td>
<td>200X</td>
<td>200X</td>
<td>Risk Assessment Rating Current Year</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------</td>
<td>------</td>
<td>------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospital</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing Practices</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medically unnecessary services</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upcoding or DRG creep</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outpatient services rendered in connection with inpatient stay</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teaching physician and resident requirements</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit balances</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-kickback</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stark physician referral</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial arrangements: hospitals and hospital-based physicians</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient dumping</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRB processes</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time &amp; effort reporting</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proper allocating charges to award projects</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Informed consent</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human &amp; animal subjects protection</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-recipient monitoring</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical Laboratory</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-kickback</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stark self-referral issues</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIA requirements</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical Necessity</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing practices</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliance on standing orders</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing practices</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profile pricing</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conduct the Risk Assessment
Risk Assessment

- Process of identifying, analyzing and managing risks relevant to objectives
- Consideration of the risk’s significance, likelihood of occurrence and how they should be managed
- Management may initiate plans, programs or actions to address risks or accept the risk due to cost or other considerations

- Elements to consider:
  - Changes in operating environment
  - New personnel
  - New or revamped information systems
  - Rapid growth
  - New technology
  - New lines, products or activities
  - Corporate restructuring
  - Accounting pronouncements
Data Sources

- Survey front line managers
- Interview senior and middle management
- Review available reports:
  - CMS inquiries and results
  - OIG inquiries and results
  - RAC, MIC and ZPIC results
  - DHS inquiries and results
  - Hotline data
- OIG Workplan
Sample Process

- Interview senior leadership
- Survey front-line managers on risks related to their area of accountability
- Summarize interview and survey results by department
- Meet with senior management to assign risks to “heat map”
Suggested Questions for the Board

● How is the compliance program structured and who are the key employees responsible for its implementation and operation? How is the Board structured to oversee compliance issues?
  – A compliance committee or other subset to monitor compliance program operations that regularly reports to the Board can be instituted

● How does the organization’s compliance reporting system work? How frequently does the Board receive reports about compliance issues?
Suggested Questions for the Board

- What are the goals of the organization’s compliance program? What are the inherent limitations in the compliance program? How does the organization address these limitations?
  - A solid understanding of the rationale and objectives of a compliance program, as well as its goals and limitations. Evidence of mechanisms in place to ensure timely reporting of violations and to evaluate and implement remedial measures.
Suggested Questions for the Board

- Does the compliance program address the significant risks of the organization? How were those risks determined and how are new compliance risks identified and incorporated into the program?
  - It is vital to address all of the various standards, government participation COP’s, reimbursement guidelines and all other applicable standards.
  - There needs to be a comprehensive ongoing process of compliance risk assessment in place to educate the Board’s awareness of new challenges.
Surveys and Interviews: Questions to Ask

- Who is the accountable leader for the risk area?
- Are there policies and procedures that address the risk area?
- How is this area monitored?
- Have we had issues related to this area?
- Does this area related to a strategic initiative for our organization?
Questions to Ask (cont.)

- Are processes for the risk area “hard-wired” or fragmented?
- Has there been significant turn-over of key employees over the processes for this risk area?
- Has technology related to this area changed or are their new capital initiatives planned?

Focus Questions on Changes: Change = RISK
Risk Assessment Data Analysis
Art or Science?

- Analyzing the data is an Art and Science
  - Art: your experience and senior management’s knowledge and experience
  - Science: risk ranking model
# Sample Risk Assessment Results

<table>
<thead>
<tr>
<th>Risk Area/Project Name</th>
<th>Assign Risk Domain:</th>
<th>Total Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue Cycle</td>
<td>Financial</td>
<td>655</td>
</tr>
<tr>
<td>Billing Compliance</td>
<td>Regulatory</td>
<td>655</td>
</tr>
<tr>
<td>Privacy and Security</td>
<td>Regulatory</td>
<td>655</td>
</tr>
<tr>
<td>Grants and Research</td>
<td>Financial</td>
<td>625</td>
</tr>
<tr>
<td>Competition</td>
<td>Strategic</td>
<td>625</td>
</tr>
<tr>
<td>Investments</td>
<td>Financial</td>
<td>610</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td>Operational</td>
<td>560</td>
</tr>
<tr>
<td>Mental Health Access</td>
<td>Operational</td>
<td>560</td>
</tr>
<tr>
<td>Core Measures</td>
<td>Operational</td>
<td>525</td>
</tr>
<tr>
<td>Cash Controls</td>
<td>Financial</td>
<td>525</td>
</tr>
<tr>
<td>Human Resources Operations</td>
<td>Human</td>
<td>520</td>
</tr>
<tr>
<td>Accounts Payable</td>
<td>Financial</td>
<td>495</td>
</tr>
<tr>
<td>Governance (Committee Charters)</td>
<td>Governance</td>
<td>475</td>
</tr>
<tr>
<td>Credit Balances</td>
<td>Regulatory</td>
<td>465</td>
</tr>
<tr>
<td>Computer Operations</td>
<td>Technology</td>
<td>445</td>
</tr>
<tr>
<td>Wireless Network</td>
<td>Technology</td>
<td>445</td>
</tr>
</tbody>
</table>
Sample Risk Assessment Heat Map
Internal Controls “Can” and “Cannot”

- Internal controls can:
  - Promote reliable internal and external financial reporting
  - Help safeguard assets
  - Promote compliance with laws and regulations
  - Help an institution achieve its performance and profitability targets

- Internal controls cannot:
  - Guarantee the reliability of financial reporting and compliance with laws and regulations
  - Guarantee an institution’s survival or success
Things to Remember About Internal Controls

- We should not use the concepts of risk, control and governance to strangle the life out of the organization
- Risk assessment and internal controls are tools
  - We must use them wisely and in a manner that supports the mission and vision of the organization
  - Like the organizations served, these tools are as unique as they are similar
- Internal controls should be balanced to the risk addressed
- Internal controls are often better at keeping honest people honest than they are at preventing criminals
- Don’t expect to control all risks
Things to Remember

- Risk management and risk assessment are not an exact science. There is no one size fits all approach.
  - The process is unique to your organization
  - Only one component of audit plan development
  - Includes many variables
  - Scoring of individual risk factors and risk by several people will likely result in disagreement
  - Results should “feel” right, especially in terms of how risk is viewed overall and what rises as significant versus not so significant
  - Audit and Compliance Committee members should not get caught up in the details but should understand the risk process and how key risk concerns are evaluated
Who is Responsible for Risk Management?

- Everyone!
- Board of directors provide guidance, direction and monitoring
- Audit Committee or full board receive “dashboard” on risk and establish risk tolerance
- CEO has ultimate ownership and sets tone for ERM process
- Each level of management stays informed and takes ownership of risks at their level
- Chief Risk Officer, if one exists, is facilitator and challenger of process
- Risk Management Team to oversee and support process
Your Work Does Not End Here

- These are the first few steps of a solid risk management program
  - Address risk (execute the plan)
  - Monitor and report on risks
  - Respond to risks
  - Continuous improvement
Leaders…..

- Understand the risks most pertinent to their organization
- Manage the risks in an integrated fashion
- Prioritize risk management efforts around:
  » Risks having the biggest potential impact and,
  » Are most likely to occur
Thank you!
Arlene F. Baril
Director, Facility Reimbursement Services
972-904-1285
Arlene.baril@sinaiko.com