Agenda

• Introductions
• Why perform a Risk Assessment?
• What is the COSO Enterprise Risk Management Framework?
• How do you evaluate Internal Controls?
• What about Compliance?
• How do you add value to the process?
• Closing Points
Why perform a Risk Assessment?
The Changing Healthcare Operating Environment

- Essential to effective internal control
- Increased focus on Governance, Compliance and Internal Controls
- New AICPA Audit Requirements regarding assessment of Internal Controls
- Pending Legislation surrounding Non Profit Transparency
- Increased focus on 990 reporting and disclosures
- Bond Rating agencies interest in financial reporting and internal controls
- Strengthens the organizations position if a problem is identified
- Compliance problems continue to attract the OIG
Anticipated Benefits of risk assessments and internal control reviews

• Increased confidence of CEO/CFO in meeting reporting requirements
• Improved coordination of Company Management Team
• Improved and clarified Corporate Governance process
• Systematized process for early identification of business risks/whistleblowing issues/incident management
• Increased operational effectiveness
Why perform a Risk Assessment?

- How would your administrative team define risk?
- What does your organizations do to measure risk?
- How do the operational areas value the annual risk assessment?
What is the Enterprise wide COSO Framework?
Risk Assessments and Internal Controls

Assessing risk is integral to internal control and management framework

COSO Internal Control – Integrated Framework

COSO Enterprise Risk Management Framework

Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring
Compliance
Reporting
Operations
Strategic
Bringing to Life the Conceptual Framework Through Integration of Governance, Risk Management and Compliance
Aligning Risks and Controls with Business Objectives

Risks and Controls need to be integrated with processes that meet the Business Objectives of the Organization.
Key Concepts in the COSO Enterprise Risk Management Framework

- Risk Management in a Strategy Setting
- Events and Risks
- Risk Appetite
- Risk Tolerance
- Portfolio View of Risk
What is the Enterprise wide COSO Framework?

• How many people in your organization could briefly describe COSO?
• How would you begin to explain this to the Executive Leadership of your organization?
• How long do you think it will be before a ‘Sarbanes-Oxley Light’ (aimed at not-for-profits) will impact the industry?
How Do You Evaluate Internal Controls?
Sample Healthcare Company Internal Control Assessment Results

Level 1 – Unreliable: Indicates that no preventive or detective control exists.

Level 2 – Informal: Indicates that a preventive and/or detective control exists; however, it may not be documented, applied consistently, or able to identify deviations from the control’s objective in a reliable manner.

Level 3 – Standardized: Indicates that a documented and comprehensive preventive and/or detective control exists, is applied consistently, and will successfully identify any deviations from the control’s objective.

Level 4 – Monitored: Indicates that a documented standardized control is in place and is monitored.

Level 5 – Optimized: Indicates integrated internal controls
Sample Healthcare Company Assessment Results

Current State
Level 4: Monitored Control
Level 3: Standardized Control
Level 2: Informal Control
Level 1: Unreliable Control

Sample Healthcare Company

Analysis: 69% of Sample Healthcare Company’s controls are either informal or unreliable
Sample Healthcare Company Assessment Results

Scope and Summary:
2. Total of 120 major control objectives

Key Findings:
1. Policies and procedures require extensive revision
2. Inadequate segregation of duties exists
3. Formal review, approval and monitoring of reconciliations does not exist
4. Significant reliance on Excel spreadsheets
5. Significant accrual and reserve procedures are informal and unreliable
6. Signature authority and processes are not consistent for ordering
7. There is inadequate documentation for receipt of goods
8. Asset additions are often recorded to the fixed asset ledger as a group
9. There is no standardized process to track inventory and maintenance of fixed assets
10. Disposal of assets are not occurring timely or regularly due to the transition to Lawson

Analysis: Most of Sample Healthcare Company’s business process controls are either informal or unreliable

Current State
Level 4: Monitored Control
Level 3: Standardized Control
Level 2: Informal Control
Level 1: Unreliable Control
Unreliable or Informal controls lead to internal control deficiencies

Control deficiencies can range from internal control deficiencies to significant deficiencies to material weaknesses in internal control.

- **Internal Control Deficiency**
  - Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- **Significant Deficiency**
  - An internal control deficiency or combination of control deficiencies that adversely affects the company’s ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP such that there is a more-than-remote likelihood that a misstatement of the company’s annual or interim financial statements that is more than inconsequential will not be prevented or detected.

- **Material Weakness**
  - A significant deficiency or combination of significant deficiencies that results in a more-than-remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.
How Do You Evaluate Internal Controls?

• How many control objectives exist across your organization?
• Who is responsible for the effectiveness of these control objectives?
  – Accounting
  – Internal Audit
  – Department Heads
  – The External Auditors
  – Legal/Compliance officer
• How often are these control objectives tested?
What about Compliance?
Healthcare Industry Compliance: Focus Areas

Based on recent OIG publications and audit activity, the following areas represent “higher risk issues”:

- Hospital-physician financial arrangements
- Medicare Hospital Outlier Payments
- Short Inpatient Stays/One-Day Stays
- Hospital Wage Index Data
- Graduate Medical Education Costs
- Organ Acquisition Costs
- Behavioral Health
- Cardiac Rehab
## How Compliance fits into the COSO framework

<table>
<thead>
<tr>
<th>COSO Framework</th>
<th>Compliance Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective Setting</td>
<td>Program Goals / Mission</td>
</tr>
<tr>
<td>Event Identification</td>
<td>Hotline, Internal Issues</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Annual Audit Plan</td>
</tr>
<tr>
<td>Risk Response</td>
<td>Gap Remediation</td>
</tr>
<tr>
<td>Control Activities</td>
<td>Both compliance initiated and others</td>
</tr>
<tr>
<td>Information and Communication</td>
<td>Policies and Training</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Compliance reporting and review of other reports</td>
</tr>
</tbody>
</table>
Business Processes with Potential Compliance Integration

• Entity Level Controls
• Revenue Cycle
• Expenditures
• Cost Reporting
• Fixed Assets
• Real Estate
• General Computer and Computer Application Controls
• Partnerships
• Tax
Compliance and Controls

**Entity Level Controls – items to consider**

- Integrity and Ethical Values
- Board of Directors
- Audit Committee
- Management Style and Operating Style
- Organization Structure
- Assignment of Responsibility
- Human Resources
- Information and Communication
- Risk Assessment
- Monitoring
Compliance and Controls

Controls Environment

• Design and Operating Effectiveness
• Level of External Audit Testing – Controls vs. Substantive
• Control Assertions
  – Completeness
  – Accuracy (Valuation or Allocation)
  – Validity (Authorization, Existence or Occurrence)
  – Reporting (Presentation and Disclosure)
• Other Control Considerations
  – Safeguarding Assets
  – Anti Fraud
  – Maintenance of Records
What about Compliance?

- What % of the ‘C-Suite’ time is spent on Compliance in healthcare?
- If you were writing an article in Modern Healthcare, what would you list as the next ‘big thing’ in compliance?
How Do You Add Value in the Process?
Each Business Process Contains Opportunity for Added Value

Core Processes

- Revenue
- HR, Payroll, Benefits
- Procurement/Accounts Payable
- Fixed Assets

Information Technology

Example Supporting Processes - Revenue

- Patient Access and Flow
  - Scheduling
  - Pre-registration
  - Registration
  - Charity Care Eligibility

- Capture of Services and Charges
  - Clinical Service Delivery
  - Charge capture
  - CDM Maintenance

- Information Translation and Coding
  - Medical Records/Health Information Management

- Billing and Claims Processing
  - Billing/Claims Processing
  - Cash Collection
  - Cash Posting
  - Accounts Receivable Follow-up and maintenance
How Do You Add Value in the Process?

• Can a business case be made that efficiency gains can offset the cost of ‘controls / compliance’?
• How does the departmental level management view the value of a ‘control & compliance’ program?
• What can be done to enhance the perceived value of the process?
Closing Points
Some General Comments on Roles and Responsibilities

Board of Directors

• The board knows the extent to which management has established effective risk management in the organization
• It is aware of and concurs with the entity's risk appetite
• It reviews the portfolio view of risk and considers it against the risk appetite
• Is apprised of the most significant risks and whether management is responding appropriately

Management

• The chief executive has ultimate responsibility for enterprise risk management
• He/she ensures the presence of a positive internal environment, and that all enterprise risk management components are in place
• Senior managers in charge of organizational units have responsibility for managing risks related to their unit's objectives
• They guide application of enterprise risk management, ensuring application is consistent with risk tolerances
• Each manager is accountable to the next higher level, for his/her portion of enterprise risk management, with the CEO ultimately accountable to the board
Some General Comment on Roles and Responsibilities

Other Entity Personnel

• Enterprise risk management is an explicit or implicit part of everyone's job description

• Personnel understand the need to resist pressure from superiors to participate in improper activities, and channels outside normal reporting lines are available to permit reporting such circumstances

• The enterprise risk management roles and responsibilities of all personnel are well defined and effectively communicated

Parties Interacting with the Entity

• Mechanisms are in place to receive relevant information from parties interacting with the entity and take appropriate action

• Action includes not only addressing the particular situation reported, but also investigating the underlying source of the problem and fixing it

• For outsourced activities, management has implemented a program to monitor those activities

• Management considers the observations and insights of financial analysts, bond rating agencies and the news media that may enhance enterprise risk management
What Questions can we answer for you?

Mark Avery, Director  
PricewaterhouseCoopers  
Tel: 267-330-2462  
E-mail: mark.a.avery@us.pwc.com

Ray Dziesinski, Director  
PricewaterhouseCoopers  
Tel: 678-419-1436  
E-mail: ray.dziesinski@us.pwc.com

© 2004 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.
Appendix

• ERM Framework Overview
• Synergy of Compliance and Financial Controls
The COSO ERM Standard Delineates a Principles-Based Framework

The framework provides:

• A definition of enterprise risk management

• The critical principles and components of an effective enterprise risk management process

• Direction for organizations to use in determining how to enhance their risk management

• Criteria to determine whether their risk management is effective, and if not, what is needed
The COSO ERM Standard Delineates a Principles-Based Framework

The Application Techniques framework provides:

- Illustrations of how critical principles may look within an organization
- An overview of an implementation process
- Illustrations that consider varying entity:
  - Size
  - Strategy
  - Industry
  - Complexity
The COSO ERM Standard Creates a Common Language

Enterprise risk management:

• Is a process
• Is effected by people
• Is applied in a strategy setting
• Is applied across the enterprise
• Is designed to identify events potentially affecting the entity and manage risk within its risk appetite
• Provides reasonable assurance to the entity’s management and the board
• Is geared to the achievement of the entity’s objectives
The Framework Empowers Management and the Board to …

- Leverage existing risk management processes
- Ask the right questions so they can be confident of reports made to key constituencies
- Evaluate the effectiveness of their risk management
- Identify ways to improve risk management
- Integrate enterprise risk management and internal control
- Integrate entity performance management and enterprise risk management
Three Foundational Aspects of the Framework

• Starts with objectives:
  – strategic
  – operations
  – reporting
  – compliance
• Applies to activities at all levels of the organization
• Has eight interrelated components
Key Concepts in the COSO Enterprise Risk Management Framework

• Risk Management in a Strategy Setting
• Events and Risks
• Risk Appetite
• Risk Tolerance
• Portfolio View of Risk
Risk Management in a Strategy Setting – What it Means

• The entity’s strategic objectives and high-level goals align with and support its mission/vision

• Objectives reflect management’s strategic choices as to how the entity will seek to create value for its stakeholders

• Management identifies risks associated with strategy choices and considers their implications

• Management allocates resources across business units, with consideration of the entity’s risk appetite and individual business units’ strategic plans, to generate a desired return on invested resources.
Events and Risks –
What They Mean

• An **event** is an occurrence that could affect strategy implementation or achievement of objectives
  – **Risk** is the possibility that an event will occur and adversely affect the achievement of objectives
  – Events that may have a positive impact represent opportunities
• Risks are measured using the **same unit of measure** as the related objectives.
• **Time horizons** are specified and aligned with objectives
• Management **identifies events** both at the entity and activity levels
  – Events with a low possibility of occurrence are considered if the impact on achieving an important objective is great
Risk Appetite—What it Means

- **Risk appetite** is a high-level view of how much risk management and the board are willing to accept.
- Management forms a risk appetite at the entity level.
- Companies may express risk appetite as the acceptable balance of growth, risk, and return, or as risk-adjusted shareholder value-added measures.
- Entities, such as not-for-profit organizations, express risk appetite as the level of risk they will accept in providing value to their stakeholders.
Risk Tolerance – What it Means

- **Risk tolerances** are the acceptable levels of variation around objectives
- Risk tolerances are measurable, preferably in the same units as the related objectives
- In setting risk tolerances, management considers the relative importance of the related objectives
- Risk tolerances align with risk appetite
Portfolio View of Risk – What it Means

- **Portfolio View of Risk** indicates that Management considers risk from an entity-wide, or portfolio, perspective
- Management determines whether the entity’s residual risk profile is commensurate with its overall risk appetite
- Management considers how individual risks interrelate
- Management develops a portfolio view from both a business unit and entity perspective
Enterprise Risk Management Framework is Fully Aligned with the Internal Control Framework

Improvements in enterprise risk management can build on the investment made in internal control.
Relationship to Internal Control – Integrated Framework

• ERM includes objective setting as a separate component. The IC-IF sets out that objectives as a prerequisite for internal control.
• The ERM framework’s “Reporting” category of objectives expands the IC-IF “Financial Reporting”.
• ERM requires that an entity-have a portfolio view, or risks from across the entity at the entity level.
• The ERM framework expands on the “risk assessment” component of IC-IF, separating it into three ERM components.
• The ERM framework elaborates on other components of IC-IF as they relate to enterprise risk management.
• Effective internal control is necessary for effective enterprise risk management.
#1: Internal Environment

Risk Management Philosophy

- The entity’s risk management philosophy represents the shared beliefs and attitudes characterizing how the entity considers risk in all activities
- It reflects the entity’s values, influencing its culture and operating style
- It affects how enterprise risk management components are applied, including how events are identified, the kinds of risks accepted, and how they are managed
- It is well developed, understood, and embraced by the entity’s personnel
- It is captured in policy statements, oral and written communications, and decision making
- Management reinforces the philosophy not only with words but also with everyday actions

Risk Appetite

- The entity’s risk appetite reflects the entity’s risk management philosophy and influences the culture and operating style
- It is considered in strategy setting, with strategy aligned with risk appetite
#1: Internal Environment (continued)

## Board of Directors

- The board is active and possesses an appropriate degree of management, technical, and other expertise, coupled with the mind-set necessary to perform its oversight responsibilities
- It is prepared to question and scrutinize management’s activities, present alternative views, and act in the face of wrongdoing
- It has at least a majority of independent outside directors
- It provides oversight to enterprise risk management and is aware of and concurs with the entity’s risk appetite

## Organizational Structure

- The organizational structure defines key areas of responsibility and accountability
- It establishes lines of reporting
- It is developed in consideration of the entity’s size and nature of activities
- It enables effective enterprise risk management
#1: Internal Environment (continued)

**Integrity and Ethical Values**

- The entity’s standards of behavior reflect integrity and ethical values
- Ethical values not only are communicated but also accompanied by explicit guidance regarding what is right and wrong
- Integrity and ethical values are communicated through a formal code of conduct
- Upward communications channels exist where employees feel comfortable bringing relevant information
- Penalties are applied to employees who violate the code, mechanisms encourage employee reporting of suspected violations, and disciplinary actions are taken against employees who knowingly fail to report violations
- Integrity and ethical values are communicated through management actions and the examples they set

**Commitment to Competence**

- Competence of the entity’s people reflects the knowledge and skills needed to perform assigned tasks
- Management aligns competence and cost
Assignment of Authority and Responsibility

- Assignment of authority and responsibility establishes the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, and provides limits to authority.
- The assignments establish reporting relationships and authorization protocols.
- Policies describe appropriate business practices, knowledge and experience of key personnel, and associated resources.
- Individuals know how their actions interrelate and contribute to achievement of objectives.

Human Resource Standards

- Standards address hiring, orientation, training, evaluating, counseling, promoting, compensation, and remedial actions, driving expected levels of integrity, ethical behavior, and competence.
- Disciplinary actions send the message that violations of expected behavior will not be tolerated.
#2: Objective Setting

Selected Objectives

- Management has a process that aligns strategic objectives with the entity’s mission and ensures the strategic and related objectives are consistent with the entity’s risk appetite

Risk Appetite

- The entity’s risk appetite is a guidepost in strategy setting
- It guides resource allocation
- It aligns organization, people, processes, and infrastructure

Risk Tolerances

- Risk tolerances are measurable, preferably in the same units as the related objectives
- They align with risk appetite
#2: Objective Setting (continued)

**Strategic Objectives**

- The entity’s strategic objectives establish high-level goals that align with and support its mission/vision
- They reflect management’s strategic choices as to how the entity will seek to create value for its stakeholders
- Management identifies risks associated with strategy choices and considers their implications

**Related Objectives**

- Related objectives support and are aligned with selected strategy, relative to all entity activities
- Each level of objectives is linked to more specific objectives that cascade through the organization
- The objectives are readily understood and measurable
- They align with risk appetite
#3: Event Identification

Events

- Management identifies potential events affecting strategy implementation or achievement of objectives – those that may have positive or negative impacts, or both
- Even events with a relatively low possibility of occurrence are considered if the impact on achieving an important objective is great

Influencing Factors

- Management recognizes the importance of understanding external and internal factors and the type of events that can emanate therefrom
- Events are identified both at the entity and activity levels

Event Identification Techniques

- Techniques used look to both the past and future
- Management selects techniques that fit its risk management philosophy and ensures the entity develops needed event identification capabilities
- Event identification is robust, forming a basis for risk assessment and risk response components
#3: Event Identification (continued)

**Interdependencies**
- Management understands how events relate to one another

**Distinguishing Risks and Opportunities**
- Events with negative impact represent risks, which management assesses and responds to
- Events representing opportunities are channeled back to management’s strategy or objective-setting processes
#4: Risk Assessment

- In assessing risk, management considers expected and unexpected events

**Inherent and Residual Risk**
- Management assesses inherent risks
- Once risk responses have been developed, management considers residual risk

**Estimating Likelihood and Impact**
- Potential events are evaluated from two perspectives – likelihood and impact
- In assessing impact, management normally uses the same, or congruent, unit of measure as used for the objective
- The time horizon used to assess risks should be consistent with the time horizon of the related strategy and objectives.

**Assessment Techniques**
- Management uses a combination of qualitative and quantitative techniques
- The techniques support development of a composite assessment of risk

**Relationships between Events**
- Where correlation exists between events, or events combine and interact, management assesses them together
#5: Risk Response

- In responding to risk, management considers among risk avoidance, reduction, sharing, and acceptance

**Evaluating Possible Responses**

- Responses are evaluated with the intent of achieving residual risk aligned with the entity’s risk tolerances
- In evaluating risk responses, management considers their effects on likelihood and impact
- Management considers their costs versus benefits, as well as new opportunities

**Selected Responses**

- Responses chosen by management are designed to bring anticipated risk likelihood and impact within risk tolerances
- Management considers additional risks that might result from a response

**Portfolio View**

- Management considers risk from an entity-wide, or portfolio, perspective
- Management determines whether the entity’s residual risk profile is commensurate with its overall risk appetite
#6: Control Activities

Integration with Risk Response

- Management identifies control activities needed to help ensure that risk responses are carried out properly and in a timely manner.
- Selection or review of control activities includes consideration of their relevance and appropriateness to the risk response and related objective.
- In selecting control activities, management considers how control activities interrelate.

Types of Control Activities

- Management selects from a variety of types of control activities, including preventive, detective, manual, computer, and management controls.
#6: Control Activities (continued)

**Policies and Procedures**

- Policies are implemented thoughtfully, conscientiously, and consistently
- Procedures are carried out with sharp, continuing focus on conditions to which the policy is directed
- Conditions identified as a result of the procedure are investigated and appropriate corrective actions taken

**Controls over Information Systems**

- Appropriate general and application controls are implemented
#7: Information and Communication

**Information**

- Relevant information is obtained from internal and external sources
- The entity captures and uses historical and present data as needed to support effective enterprise risk management
- The information infrastructure converts raw data into relevant information that assists personnel in carrying out their enterprise risk management and other responsibilities; information is provided at a depth and in a form and timeframe that are actionable, readily usable, and linked to defined accountabilities – including the need to identify, assess, and respond to risk
- Source data and information are reliable, and provided on time at the right place to enable effective decision making
- Timeliness of information flow is consistent with the rate of change in the entity’s internal and external environments
- Information systems change as needed to support new objectives
#7: Information and Communication (continued)

Communication

- Management provides specific and directed communication addressing behavioral expectations and responsibilities of personnel, including a clear statement of the entity’s risk management philosophy and approach and clear delegation of authority
- Communication about processes and procedures aligns with, and underpins, the desired culture
- All personnel receive a clear message from top management that enterprise risk management must be taken seriously
- Personnel know how their activities relate to the work of others, enabling them to recognize problems, determine cause, and take corrective action
- Personnel know what is deemed acceptable and unacceptable behavior
- There are open channels of communication and a willingness to listen, and personnel believe their superiors truly want to know about problems and will deal with them effectively
Communication

• Communications channels outside normal reporting lines exist, and personnel understand there will be no reprisals for reporting relevant information

• An open communications channel exists between top management and the board of directors, with appropriate information communicated on a timely basis

• Open external communications channels exist, where customers and suppliers can provide significant input

• The entity communicates relevant information to regulators, financial analysts, and other external parties
#8: Monitoring

- Management determines, through ongoing monitoring activities or separate evaluations, or a combination, whether the functioning of enterprise risk management continues to be effective

**Ongoing Monitoring Activities**

- Monitoring activities are built into the entity’s normal, recurring operations, performed in the ordinary course of running the business
- They are performed on a real-time basis and react dynamically to changing conditions

**Separate Evaluations**

- Separate evaluations focus directly on enterprise risk management effectiveness and provide an opportunity to consider the continued effectiveness of the ongoing monitoring activities
- The evaluator understands each of the entity activities and each enterprise risk management component being addressed
- The evaluator analyzes enterprise risk management design and the results of tests performed, against the backdrop of management’s established standards, determining whether enterprise risk management provides reasonable assurance with respect to the stated objectives
#8: Monitoring (continued)

**Reporting Deficiencies**

- Deficiencies reported from both internal and external sources are carefully considered for their implications for enterprise risk management, and appropriate corrective actions are taken.

- All identified deficiencies that affect the entity’s ability to develop and implement its strategy and to achieve its established objectives are reported to those positioned to take necessary action.

- Not only are reported transactions or events investigated and corrected, but potentially faulty underlying procedures also are reevaluated.

- Protocols are established to identify what information is needed at a particular level for effective decision making.
Examples of the synergy

Financial Controls that benefit Compliance
and
Compliance Controls that benefit Financial Structure
## Entity Level Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishment of the &quot;tone at the top&quot;. Commitment to integrity and ethics is communicated effectively throughout the organization.</td>
<td>Written Code of Conduct distributed to each new employee. Acknowledgement of receipt and agreement to abide kept in personnel files. Dates entered into compliance database and monitored by Compliance Committee.</td>
</tr>
<tr>
<td>Assignment of responsibility and delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements.</td>
<td>Compliance approval of all contractual relationships with referral sources. Legal requires all signatures to be present before contract is drafted or reviewed.</td>
</tr>
<tr>
<td>Extent to which people are made aware of their responsibilities and expectations of them.</td>
<td>Code of Conduct (above). Compliance Orientation Training required within 30 days of hire. Dates tracked automatically by learning management system and monitored by Compliance Committee.</td>
</tr>
</tbody>
</table>
## Entity Level Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extent to which personnel policies address adherence to appropriate ethical and moral standards</td>
<td>Performance evaluations include section on Compliance. Human Resources monitors completion for all employees.</td>
</tr>
<tr>
<td>Discipline and methodology used to conduct the Risk Assessment and compile the results</td>
<td>Company has overall process. Compliance conducts annual risk assessment with input from management and external sources including OIG work-plan that results in areas to be reviewed over coming year.</td>
</tr>
</tbody>
</table>
## Entity Level Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existence and implementation of codes of conduct (&quot;Code&quot;) and other</td>
<td>Written Code of Conduct distributed to each new employee. Acknowledgement of receipt and agreement to abide kept in personnel files. Dates entered into compliance database and monitored by Compliance Committee.</td>
</tr>
<tr>
<td>policies regarding acceptable business practice, conflicts of interest,</td>
<td></td>
</tr>
<tr>
<td>or expected standards.</td>
<td></td>
</tr>
<tr>
<td>Codes are comprehensive, addressing, for example, conflicts of interest,</td>
<td>All areas addressed in Code. Potential Conflict of Interest Notification must go to supervisor and Legal. Legal and Internal Audit review and corrective action taken if direct conflict (e.g. employee cannot participate in decision to use vendor for which spouse is sales person)</td>
</tr>
<tr>
<td>illegal or other improper payments, anti-competitive guidelines, insider</td>
<td></td>
</tr>
<tr>
<td>trading.</td>
<td></td>
</tr>
</tbody>
</table>
## Entity Level Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes are periodically acknowledged by key employees.</td>
</tr>
<tr>
<td>Management responds to violations of behavioral standards.</td>
</tr>
<tr>
<td>Disciplinary actions taken as a result of violations are widely communicated in the entity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Compliance refresher training includes review of Code. Dates tracked automatically by learning management system and monitored by Compliance Committee.</td>
</tr>
<tr>
<td>All reported violations are investigated and resolved by appropriate department. Logs and case files demonstrating resolution are kept.</td>
</tr>
<tr>
<td>Consequences of violating behavioral standards are listed in the Code. Disciplinary actions are kept confidential due to liability concerns and respect for individuals involved; however, selected investigation results (and their consequences) are reported periodically via the Company newsletter, with certain information redacted to preserve anonymity</td>
</tr>
</tbody>
</table>
Entity Level Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees believe that, if caught violating behavioral standards, they'll be held accountable.</td>
<td>Annual anonymous employee survey is conducted regarding attitudes towards compliance issues, including this question. Results are published within the Company.</td>
</tr>
<tr>
<td>Hotline/Whistleblower Program for receiving and retaining information about, and treating alleged incidents involving the issuer regarding accounting, internal accounting controls or auditing matters.</td>
<td>All hotline allegations are investigated and resolved by appropriate department. Logs and case files demonstrating resolution are kept. Volume monitored monthly by Compliance Committee. Board Committee receives case summary of all allegations regarding fraud, theft, kickback, incorrect billings.</td>
</tr>
</tbody>
</table>
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>The patient's financial class upon admission is correctly determined and</td>
<td>Medicare Secondary Payor information is collected and recorded in system. System does not allow registration to proceed without information. OR Monthly check of 10 registration files performed by Business Office Manager to form completed and correct payor as primary within system.</td>
</tr>
<tr>
<td>recorded.</td>
<td></td>
</tr>
<tr>
<td>Gross patient service revenues recorded represent actual patient services</td>
<td>Reconciliation performed between schedule and charge tickets and noted and signed by person completing daily batch OR System does not allow closeout of day unless scheduled patients confirmed with charges or cancellation</td>
</tr>
<tr>
<td>provided.</td>
<td></td>
</tr>
</tbody>
</table>
# Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
</table>
| Services provided are properly coded per applicable third-party regulations. | • New coders must complete training and take competency test before start coding.  
• Four hours of coding training required annually. Information is tracked by coding supervisor.  
• Monthly quality control audit of 10 charts per coder completed by supervisor. Coders with more than one error have charts checked per day by supervisor until 5 days with no errors  
• Denial tracking reports of all denials, corrective actions plans for trends related to improper coding (e.g. chargemaster corrections, department education, payor meetings) |
# Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bills for services are in accordance with billing regulations.</td>
<td>• Pre-bill checks for NCCI, NCD, LCD and other edits, edit reports worked daily by billing staff, and corrective action plans for trends.</td>
</tr>
<tr>
<td></td>
<td>• Denial tracking reports of all denials, corrective actions plans for trends related to improper coding (e.g. charge-master corrections, department education, payor meetings)</td>
</tr>
</tbody>
</table>
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad debt write-offs are properly approved.</td>
<td>• All bad debts require approvals based on dollar amount.  Medicare bad debts require</td>
</tr>
<tr>
<td></td>
<td>documentation of collection effort. Monthly review of five bad debt approvals by BOM with</td>
</tr>
<tr>
<td></td>
<td>initials to indicate agreement. Corrective action initiated if any errors found.</td>
</tr>
</tbody>
</table>
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other write-offs are properly approved.</td>
<td>• All write-offs require approvals based on dollar amount. Additional forms required for:</td>
</tr>
<tr>
<td></td>
<td>• Financial Hardship</td>
</tr>
<tr>
<td></td>
<td>• Professional courtesy</td>
</tr>
<tr>
<td></td>
<td>• Out-of-network</td>
</tr>
<tr>
<td></td>
<td>• Monthly review of ten other write-offs approvals by BOM with initials to indicate agreement.</td>
</tr>
<tr>
<td></td>
<td>Corrective action initiated if any errors found.</td>
</tr>
</tbody>
</table>
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contracts are properly approved.</td>
<td>• Contracts require approvals for rates, billing requirements, and contract language. Managed Care does not sign contract without required approvals.</td>
</tr>
</tbody>
</table>
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th><strong>Objective</strong></th>
<th><strong>Company / Compliance Control</strong></th>
</tr>
</thead>
</table>
| Credit balances are properly analyzed on a timely basis and are properly recorded, either corrected if in error or identified as a liability and repaid pursuant to the Company's policies and applicable third-party regulations. | • Credit balance reports are run weekly and worked by dedicated team, Business Office Manager reviews monthly report on credit balances outstanding greater than 60 days and notes reason for exception. Corrective action plans initiated if internal issues.  
• Overall level of credit balances are monitored by the Compliance Committee monthly. |
Revenue Cycle Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charge description master (CDM) changes are properly approved.</td>
<td>CFO and Compliance signatures required for all changes. CDM data entry person does not enter changes without all required signatures.</td>
</tr>
<tr>
<td>All changes to the charge description master are completely processed and accurately recorded.</td>
<td>Quarterly report of all changes to system CDM is reviewed for corresponding change approvals with all required signatures.</td>
</tr>
<tr>
<td>All CPT and HCPCS codes and descriptions meet industry coding standards and all codes have a gross charge and all services and procedures performed are accurately reflected.</td>
<td>Yearly review of CDM completed by each department with sign-off of accuracy and completeness.</td>
</tr>
</tbody>
</table>
## Expenditures Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requisitions and/or purchase orders are accurately coded to the General Ledger account.</td>
<td>All Prosthetic and Orthotics must be coded to proper account. Purchases by hospital are monitored quarterly by Controller. Any hospitals with zero purchases are reviewed for accuracy.</td>
</tr>
<tr>
<td>Non-PO expenses are accurately coded to the General Ledger.</td>
<td>AP requires all expenses coded to Charitable Donations to be made out to the tax exempt organization with all donations greater than $1000 approved by Compliance.</td>
</tr>
</tbody>
</table>
# Expenditures Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amounts posted to accounts payable represent services received.</td>
<td>AP requires all payments for Medical Director services to be accompanied by timesheet and contract summary.</td>
</tr>
<tr>
<td>Non-PO expenses are accurately coded to the General Ledger.</td>
<td>AP requires all expenses coded to Charitable Donations to be made out to the tax exempt organization with all donations greater than $1000 approved by Compliance.</td>
</tr>
</tbody>
</table>
### Fixed Asset Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed asset acquisitions are appropriately authorized.</td>
<td>Any acquisitions of computer equipment or major software requires HIPAA Security Officer approval. Legal requires all signatures to be present before contract is drafted or reviewed.</td>
</tr>
<tr>
<td>Fixed asset disposals including gains or losses on sale are accurately calculated and recorded.</td>
<td>Any sales to referral sources, must include documentation of fair market value (FMV). Accounts Payable will not issue checks to referral sources without accompanying contract. Legal requires documentation of FMV to be present before contract is drafted or reviewed.</td>
</tr>
</tbody>
</table>
## Fixed Asset Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset dispositions are authorized in accordance with company policies.</td>
<td>Any destruction of computer equipment with ePHI must be documented by a certificate of destruction. Asset Management will perform an annual audit of 30 dispositions and when applicable will note deficiencies and report them to the HIPAA Security Officer</td>
</tr>
<tr>
<td>Changes to the fixed asset sub-ledger are accurate (e.g., transfers, useful lives) and are supported by adequate documentation.</td>
<td>Asset transfer forms are completed online by the sending and receiving department. Asset Management runs a report monthly and researches any incomplete transfers.</td>
</tr>
</tbody>
</table>
Fixed Asset Control Examples

<table>
<thead>
<tr>
<th>Objective</th>
<th>Company / Compliance Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>All equipment leases are identified in a timely manner. All equipment</td>
<td>• Any leases of computer equipment or major software requires HIPAA Security Officer approval.</td>
</tr>
</tbody>
</table>
### Partnerships Control Examples

<table>
<thead>
<tr>
<th><strong>Objective</strong></th>
<th><strong>Company / Compliance Control</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>All distributions made according to partnership agreement.</td>
<td>All distribution calculations reviewed by VP-Partnership Accounting. Any exceptions for must be approved by Compliance.</td>
</tr>
<tr>
<td>All loans to Partnerships at commercially reasonable terms</td>
<td>All loans approved by Loan Committee which includes Compliance. Loan terms (interest rate, length) must follow policy guidance.</td>
</tr>
</tbody>
</table>
## Computer Control Examples

<table>
<thead>
<tr>
<th><strong>Objective</strong></th>
<th><strong>Company / Compliance Control</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriately segregated of duties is logically configured within key financial applications so that user access reflects job responsibilities. Only active employees have access to key financial applications.</td>
<td>Access to systems is granted to authorized personnel by ITG only through the persons to who access is granted is determined by the Business Owner. This access includes the minimum necessary for HIPAA purposes. Annual review of user accounts on each application and system and the prompt revocation of any privileges no longer required by users. It is the responsibility of System Administrators to ensure that the person performing the review has all of the appropriate and up-to-date information on each user.</td>
</tr>
</tbody>
</table>
What Questions can we answer for you?

Mark Avery, Director
PricewaterhouseCoopers
Tel: 267-330-2462
E-mail: mark.a.avery@us.pwc.com

Ray Dziesinski, Director
PricewaterhouseCoopers
Tel: 678-419-1436
E-mail: ray.dziesinski@us.pwc.com