

**Mental Health Mental Retardation  
Authority of Harris County**



## **ENTERPRISE RISK MANAGEMENT**

**A Framework For Assessing, Evaluating  
And Measuring Our Agency's Risk**

**A Risk-Based Audit Strategy  
November 2006  
Internal Audit Department**

*The  
Internal Audit  
Department*

*WAMRA of Harris County*

---

*ERM is a continuous process that involves  
managing risk across all parts of the enterprise.*

Enterprise Risk Management:  
Optimizing Controls While Supporting  
The Agency's Mission, Goals And Objectives

Prepared by  
Henry Webb  
Internal Auditor

Every organization has a mission, and all business involves risk. One of the roles of management is to assess the impact of potential risks to the business and to set in place management controls that will minimize the impact of the identified risk.

An effective risk management process is an important component of the Agency in its quest to perform its mission and reach stated objectives as well as the Strategic Plan. When these risks are successfully recognized, managed and mitigated through a well-orchestrated Enterprise Risk Management (ERM) approach, they become key elements in a strategic plan and offer forward-thinking organizations a tool for achieving business success.

#### **WHAT IS ENTERPRISE RISK MANAGEMENT?**

ERM, as defined in the *Risk Management Handbook for Health Care Organizations* (4<sup>th</sup> ed.), is a structured analytical process that focuses on identifying and eliminating the financial impact and volatility of a portfolio of risks rather than on risk avoidance alone. Essential to this approach is an understanding that risk can be managed to gain competitive advantage.

ERM utilizes a process or framework for assessing, evaluating and measuring all of an organization's risk. In essence, it is integrated risk management. ERM quantifies risks to determine significance, groups them into components or "domains" looking for either inter-relatedness or inter-dependency, and devises strategies to manage each.

#### **RISK DOMAINS**

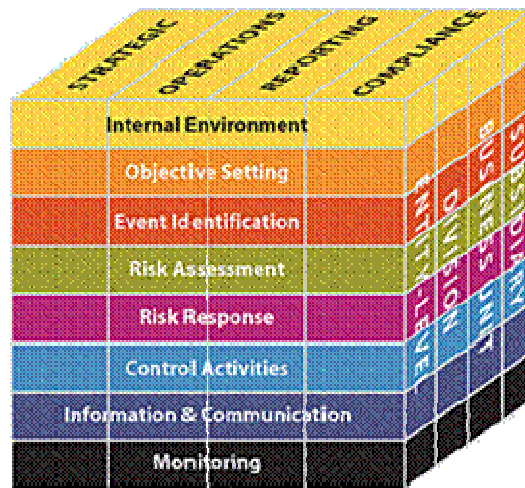
The risks facing the Agency today can be classified into domains as detailed in the *Risk Management Handbook for Health Care Organizations* that ERM recognizes:

- **Operational:** Derived from the organization's core business, including its systems and practices. Examples include clinical services and patient care.
- **Financial:** Risks related to the organization's ability to earn, raise or access capital as well as costs associated with its transfer of risk. Examples might include insurance premiums and bonds.

- **Human:** Relates to the risk related to recruiting, retaining and managing its workforce. Examples include worker’s compensation, employee turnover and absenteeism, and discrimination.
- **Strategic:** Risks related to the ability of the organization to grow and expand. Examples include joint ventures, mergers, profitability, customer satisfaction and financial performance.
- **Legal/Regulatory:** Risks related to health care statutory and regulatory compliance, licensure and accreditation. Examples include HIPPA compliance, OSHA regulations, Medicare/Medicaid-deemed status.
- **Technological:** Risk associated with equipment, devices and telemedicine. Examples include clinical/financial information systems and communications.

**The Commission of Sponsoring Organizations (COSO) ERM Framework**

- Is a process
- Is effected by people
- Is applied in strategy setting
- Is applied across the enterprise
- Is designed to identify potential events
- Manages risks to be within risk tolerance
- Provides “reasonable assurance”
- Supports achievement of key objectives



*Commission of Sponsoring Organizations of the Treadway Commission (COSO).*

The Commission of Sponsoring Organizations of the Treadway Commission (COSO) developed a model ERM program that is utilized and adapted to the unique needs of the health care organization. This COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

Entity objectives can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes

The eight components of the framework are interrelated:

**Internal Environment:**

- a) Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur.
- b) Establishes the entity's risk culture.
- c) Considers all other aspects of how the Agency's actions may affect its risk culture.

**Objective Setting:**

- a) Is applied when management considers risks strategy in the setting of objectives.
- b) Forms the risk appetite of the entity – a high-level view of how much risk management and the board are willing to accept.
- c) Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.

**Event Identification:**

- a) Differentiates risk and opportunities.
- b) Events that may have a negative impact represent risks.
- c) Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting.
- d) Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.
- e) Addresses how internal and external factors combine and interact to influence the risk profile.

**Risk Assessment:**

- a) Allows an entity to understand the extent to which potential events might impact objectives.
- b) Assess risk from two perspectives:
  1. Likelihood
  2. Impact
- c) Is used to assess risks and is normally also used to measure the related objectives.
- d) Employs a combination of both qualitative and quantitative risk assessment methodologies.
- e) Relates time horizons to objective horizons.
- f) Assesses risk on both an inherent and a residual basis.

**Risk Response:**

- a) Identifies and evaluates possible responses to risk.
- b) Evaluates options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.
- c) Selects and executes response based on evaluation of the portfolio of risks and responses.

**Control Activities:**

- a) Policies and procedures that help ensure that the risk responses, as well as other entity directives, are carried out.
- b) Occurs throughout the Agency, at all levels and in all functions.
- c) Includes application and general information technology controls.

Information & Communication:

- a) Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities.
- b) Communication occurs in a broader sense, flowing down, across, and up the organization.

Monitoring:

- Effectiveness of the other ERM components is monitored through:
  - Ongoing monitoring activities.
  - Separate evaluations.
  - A combination of the two.

**Internal Control**

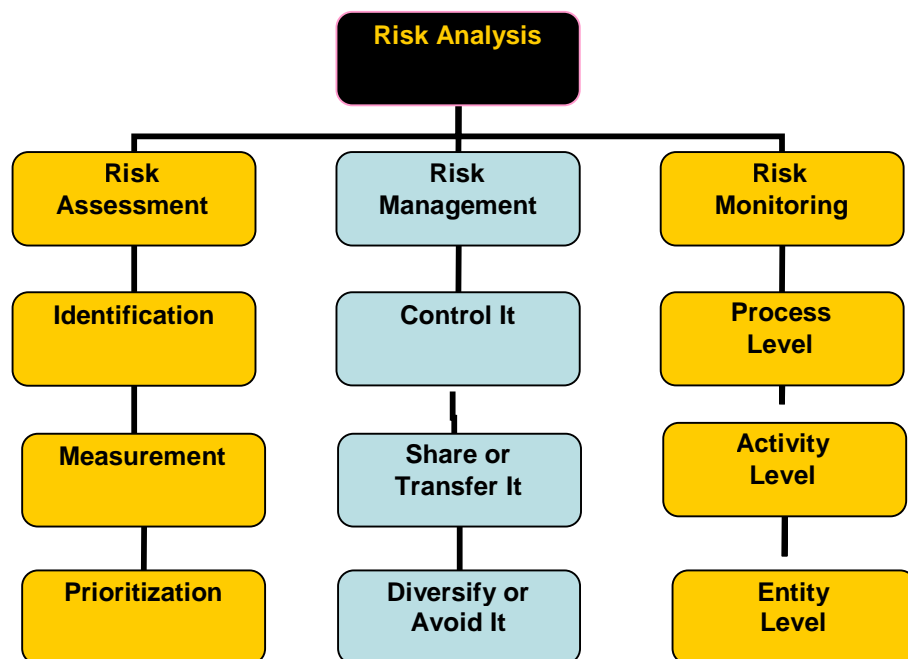
A strong system of internal control is essential to effective enterprise risk management.

**Relationship to Internal Control:**

- Expands and elaborates on elements of internal control as set out in COSO’s “control framework.”
- Includes objective setting as a separate component. Objectives are a “prerequisite” for internal control.
- Expands the control framework’s “Financial Reporting” and “Risk Assessment.”

**Standards:**

- **2010.A1** – The internal audit activity’s plan of engagements should be based on a risk assessment, undertaken at least annually.
- **2120.A1** – Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization’s governance, operations, and information systems.
- **2210.A1** – When planning the engagement, the internal auditor should identify and assess risks relevant to the activity under review. The engagement objectives should reflect the results of the risk assessment.

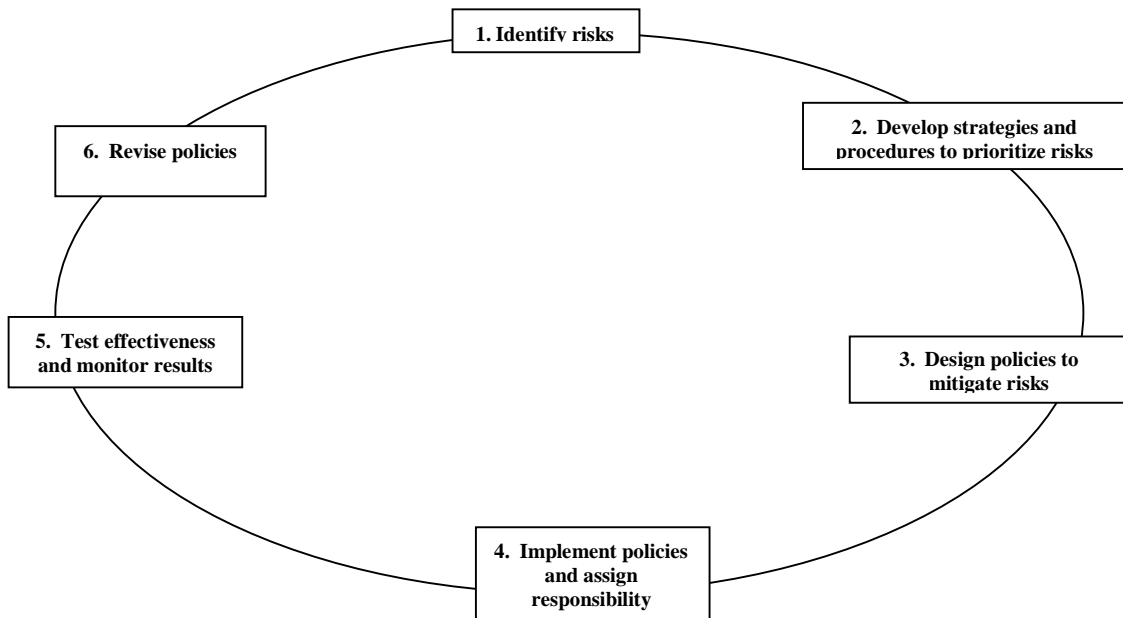


## **RISK OR OPPORTUNITY**

*A **risk** is an observable event with potential for a negative impact on the goals and objectives of the Agency.*

*An **opportunity** is an event that may have a positive impact on the Agency.*

## The Risk Management Process



Internal Audit believes the following are the “Keys to Effective Risk Management”:

- Stated mission and core values
- Motivated and confident people
- Conducive environment
- Sound methodology
- Accountability and transparency
- Security
- Performance and efficiency
- Reliable management information systems

### Clarity of Mission and Values

The key to shaping strategic success is clarity of mission. To be successful, MHMRA recognizes the importance of having organizational values and is committed to a process of developing those values. Staff need to understand what business the Agency is in and how its values drive that business. Without such understanding employees will not develop much commitment or loyalty to the organization and its success. The mission statement provides a sense of purpose and incorporates a vision of future accomplishment.

Equally important for the Agency to develop is to communicate a statement of core values or guiding principles that complements the mission statement. When both the mission and core values are understood, managing risk becomes more attainable.

### The Limitations of Internal Controls

No matter how well internal controls are designed, they can only provide reasonable assurance that objectives will be achieved. Some limitations are inherent in all internal control systems.

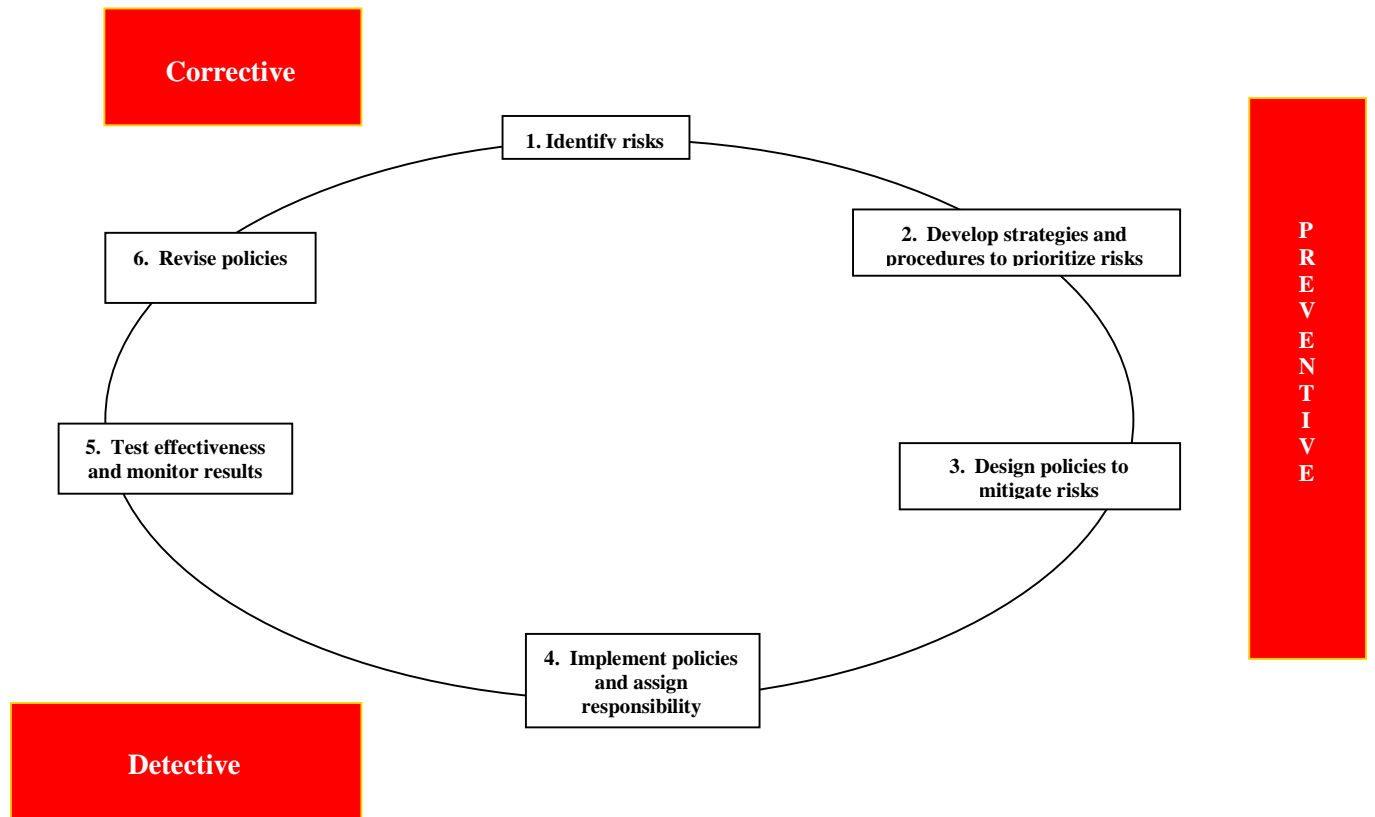
- **Judgment** – The effectiveness of controls will be limited by decisions made with human judgment under pressures to conduct business based on information at hand.
- **Breakdowns** – Even well designed internal controls can break down. Employees sometimes misunderstand instructions or simply make mistakes. Errors may also result from new technology and the complexity of computerized information systems. Controls may become obsolete with new systems and operations.
- **Management Override** – High-level personnel may be able to override prescribed policies or procedures for personal gain or advantage. This should not be confused with management intervention, which represents management actions to depart from prescribed policies and procedures for legitimate purposes.
- **Collusion** – Control systems can be circumvented by employee collusion. Individuals acting collectively can alter financial data or other management information in a manner that cannot be identified by control systems.
- **Costs** – It may be too costly to install certain controls based on the anticipated benefits of installing that control.
- **Human Error** – People can make mistakes, can be misdirected, irresponsible, can show poor judgment, or have high workloads. They might not know what to do, how to do it or where.

### General Responsibilities of Internal Audit

Internal Audit	Executive Director and Staff	Audit Committee
<ul style="list-style-type: none"> <li>• Develops a comprehensive annual work plan for board approval, including time schedule and budgets</li> <li>• Develops audit work programs that provide audit coverage of Agency operations and adhere, to audit standards</li> <li>• Designs work papers that clearly document the evidence of audit work performed and conclusions drawn</li> <li>• Maintains and develops a professional audit staff, requiring highly qualified individuals</li> <li>• Participates in field work as appropriate to ensure quality of staff work and procedures</li> <li>• Reports findings to the Audit Committee on a regular basis and assists them in fulfilling their responsibilities relating to audits</li> <li>• Follows up on previous findings to ensure that corrective action has been taken</li> <li>• Manages the audit function independent of management but maintains appropriate communication with the Executive Director and staff</li> <li>• Establishes and maintains professional ties with related professional groups</li> </ul>	<ul style="list-style-type: none"> <li>• Establishes policies and procedures within the Agency</li> <li>• Establishes an environment that says controls are important to the Agency</li> <li>• Facilitates access of the auditor to all areas of the Agency</li> <li>• Provides necessary resources</li> <li>• Receives copies of audit reports</li> <li>• Enforces response provision by affected departments and staff</li> <li>• Oversees correction and implementation of recommendations</li> </ul>	<ul style="list-style-type: none"> <li>• Oversees internal audit function</li> <li>• Monitors risk</li> <li>• Ensures that an appropriate system of controls is in place</li> <li>• Oversees job description preparation and internal audit hiring process</li> <li>• Finalizes selection of Internal Auditor</li> <li>• Must be a functioning audit committee</li> <li>• Ensures that the internal auditor reports to the Audit Committee</li> <li>• Ensures that reporting requirements are established and followed</li> <li>• Appraises the performance of the internal auditor</li> <li>• Mediates issues between management and the auditor</li> <li>• Reviews internal audit report and directs management to make needed corrections</li> <li>• Approves annual Internal Audit work plan and summary</li> </ul>

In summary, managing risk requires a continuous **cycle** of controls that are **preventive, detective and corrective**.

### The Risk Management Process



Internal Audit provides the Executive Director and the Audit Committee with an annual audit plan.

The audit plan serves as a working document that incorporates the assessments documented in the comprehensive Agency-wide business risk assessment, Executive Staff's, and department management's input and results from previous audits. As such, this plan will serve as the primary work plan to carry out the audit responsibilities in an efficient manner consistent with the priorities established by the Internal Auditor.

Due to the continual request for audit services, unknown extent of findings, and the required testing for the planned audits, the plan will be monitored and revised as necessary throughout the year.

#### **Background**

The Internal Audit Department is an independent, objective assurance and consulting activity that issues its findings and recommendations to the Executive Director, Agency Management, and Audit Committee Members. The mission of the Internal Audit Department is to provide the Executive Director, Agency Management, and Audit Committee Members with independent analyses, assurances, and

recommendations concerning the adequacy and effectiveness of the Agency's internal control structure, effective safeguarding and utilization of Agency resources, and management's performance in carrying out assigned responsibilities.

The scope of activities carried out by the Audit Department may relate to any phase of Agency activities including:

- \* Evaluating and enhancing the Agency's accounting policies and procedures that constitute its internal control structure.
- \* Assessing compliance with appropriate policies, laws, and regulations.
- \* Evaluating the accuracy of reported data utilized by departmental and Agency management in making operational decisions.
- \* Appraising the economy, efficiency, and effectiveness of the Agency's organizations, programs, functions, and activities.
- \* Assessing the efficiency of operations and developing recommendations for cost savings.
- \* Ascertaining that all Agency revenue is maximized, safeguarded and controlled.
- \* Ascertaining that all operational data is safeguarded and accurately maintained.
- \* Ascertaining the extent to which Agency assets are accounted for and safeguarded from loss.
- \* Investigating allegations of financial fraud, waste, and theft through various sources.

### **Risk Assessment**

Risk assessment is the identification and analysis of relevant risk to the achievement of an organization's objectives for the purpose of determining how those risks should be managed.

Risk assessment implies an initial determination of operating objectives then a systematic identification of those things that could prevent each objective from being attained. In other words, it's an analysis of what could go wrong.

Not all risks are equal. Some are more likely than others to occur, and as such, will have a greater impact than others if they occur. So, once risks are identified, their probability and significance must be assessed.

Finally, having identified and assessed risk, management must decide how to deal with it. In some cases, the decision may be to control it; in others it may be to accept it.

The risk management process is an ongoing one. Internal and external factors constantly develop, presenting new hazards to the Agency. Change itself is a risk, and management must continually adapt its policies and procedures to manage its changing risks to a comfortable level.

Each unit at the Agency faces its own challenges and must assess how it will manage them to meet its objectives. A good internal control system can mitigate those risks, and Internal Audit can advise how to develop good internal controls.

The Internal Audit Department assesses business risks throughout the Agency. We seek input from Executive Staff, management, and our external auditors for possible risks

and their likelihood or importance. The results of the assessment are used to prepare the annual audit plan.

The risk assessment model measured many different risk factors for each process, with the following key risk criteria factors more heavily considered in the achievement of the Agency's strategic objectives:

Nature of Operations:

- 1) Significant Changes
- 2) Pressure Meeting Objectives
- 3) Clearly Defined Objectives
- 4) Strategic Value
- 5) Inherent Risks

Nature of Transactions:

- 1) Number of Transactions
- 2) Complexity of Transactions
- 3) Accuracy of Information

Management:

- 1) Attention Given by Management
- 2) Monitoring Activities

External Influences:

- 1) Compliance With Regulations
- 2) Market Stability

Systems:

- 1) Integrity: Reliance on Information Systems
- 2) Relevance: Ability to Satisfy Business Objectives
- 3) Access: Unauthorized Access and Transactions
- 4) Availability: Level of Support
- 5) Complexity: Relative Number of Transactions, Files, and Devices

Dollar Volume/Materiality:

- Materiality

Changes in Procedures/Personnel:

- 1) Training/Experience
- 2) Adequacy of Staffing Levels
- 3) Segregation of Duties

Results of Prior Audits/Management Interest:

- 1) Audit Findings
- 2) Follow-up

Time Since Last Audit:

- Prior Audit Published

Opportunities to Achieve Operating Benefits:

- 1) Opportunity Identification
- 2) Risk Assessment
- 3) Management Interest/Request

Department processes or activities with high or moderate residual risk are noted in the Agency's current Business Risk Assessment Model.

### **Audit Focus Areas**

The Business Risk Assessment serves as a planning tool to determine the best investment for audit efforts.

Annually, the audit plan prioritizes the Audit Department's limited resources of people and budget dollars based on MHMRA's Business Risk Profile and management's need for vital information. This audit plan prioritizes audit focus on either Agency-wide processes or departments with processes or activities having high or moderate residual risk. As such, the Agency's audit function serves as a risk management tool through the development of improved control processes as a result of performance improvement and financial auditing, as well as a control with the performance of the revenue enhancement and compliance audits.

### **Audit Programs**

Audit activities will vary as a result of the differences in the nature of operations, organizational structure, and management style and by the competence, employee capabilities, and concepts of operation control. Specific audit programs will be developed from each activity to the audited within the year ending August 31, 2007.

Audit programs will be designed in regards to business services, compliance requirements, performance considerations, and specialized skills required for each project. All audit programs, workpapers and reports will be conducted in accordance with appropriate professional standards.

The Internal Audit Department will also provide any assistance to the Agency's management when they request special assignments/projects. These special assignments/projects will normally be performed in addition to the normally scheduled audit work planned.

The “Top Five” Agency risks identified by Internal Audit are based on the Fiscal Year 2007 Risk Assessment worksheet (copy attached as Exhibit A.) The following represent these top five risks and associated mitigation efforts.

**RISK DOMAINS**

<b>RISK</b>	<b>MITIGATE RISK</b>
<b>(1) Operational</b> - Lack of adherence to established policy and procedures - Management’s ability to override internal controls	- Staff to be held accountable - Open communication with ED and Board
<b>(2) Financial</b> - Accounts Receivable - Return of funds not expended - Accounts Payable - Payroll - Bad Debt	- Establish benchmarks - Require continual monitoring and requirements - Continued training and maintain high benchmarks - Fully utilize payroll module - Establish benchmarks above standards
<b>(3) Human</b> - High turn over of staff in key areas - Client care - Facility care - Professionalism, care and safeguard of assets	- Determine root cause and corrective action - Maintain higher than required targets - Continue facility reviews and Project Management - Require strict code of Conduct and Ethics
<b>(4) Strategic</b> - Continue positive financial performance under ever changing environment and demands - Clinical software venture	- Evaluate ALL financial commitments and prioritize based on funding and critical needs (objective) - Evaluate on an on-going philosophy with future State “system” in mind
<b>(5) Technological</b> - Keeping pace with required technology and equipment for both clinical and financial needs	- All IT projects should be “value driven” and prioritized