Discussion Objectives

1. Discuss factors driving interest in implementing Enterprise Risk Management ("ERM")

2. Provide Executive Management and Audit Committee a basic understanding of ERM concepts, techniques and benefits

3. Review approaches for assessing and prioritizing risks:
   - Identifying and describing risks
   - Assessing risk based on key dimensions of impact and vulnerability
   - Applying risk assessment techniques to routine operations

4. Discuss ERM implementation frameworks and roadmaps

5. Provide an overview of the organizational framework needed to support improved risk management capability
Factors Driving Organizations to Implement ERM: Why Do You Do It?

Increasing Demand for Enhanced Governance and Risk Oversight

- **2012 Dodd-Frank Act Rules**
  - compensation committee independence
  - disclosure of pay-for-performance, pay ratios, and hedging by employees and directors
  - recovery of executive compensation
  - reporting over conflict minerals essential for business
  - disclosure of government payments to resource extraction issuers, companies engaging in commercial development of oil, natural gas, and minerals

- **2010 SEC Rules to Enhance Corporate Governance Disclosures**
  - director and nominee qualifications and legal proceedings
  - diversity and director nominations
  - board leadership structure and role in risk oversight
  - accelerated disclosure of shareholder voting results

- **COSO – Enterprise Risk Management Framework**
  - Provides an organizational scope, emphasis, and program to broaden risk management to an enterprise-wide emphasis and integrate into corporate strategy

- **Sarbanes-Oxley, 2002**
  - Calls for enterprise-wide documentation and testing of controls over financial reporting risk

Many organizations’ response is to enhance their corporate governance processes by developing and implementing an Enterprise Risk Management process.
Board Responsibilities are Increasingly Focused on Risk Oversight

- The 2012 Dodd-Frank Act Rules have increased compensation controls and disclosures, and the SEC has increased Board structure and selection rules.

- Board fiduciary responsibilities should extend beyond the traditional “hard risk” areas to include all types of risk to the organization including strategy and reputation.

- Board members have a “duty of care” responsibility which includes assuring that risks are considered in decision-making and all known key risks are effectively managed.

Questions Process Ownership Should be Able to Answer

For each of your risks:

- How does this risk relate to achieving your objectives?
- What is the organization’s appetite for risk or what is its tolerance for deviating from expected results?
- What is your state of preparedness?
- How do you know? How confident are you?
- What are the risks where you really need to improve our risk management?
- Which of these risks are most likely to occur and why?
- What is your overall risk mitigation plan?
- How will you monitor the effectiveness of the plan?
- Are there other risks on or over the horizon that you need to start to prepare for now?
Most organizations rely on multiple sources for answers. However, risk oversight and an integrated approach is usually lacking.

ERM provides a means to better understand, communicate and respond to the risk knowledge that exists in the organization.

What Do We See Across Major Corporations?

Based on a 2010 GAIN Benchmark Study, the Status of ERM integration efforts are as follows:

<table>
<thead>
<tr>
<th>ERM Specific Initiatives</th>
<th>Designed and/or Implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic enterprise risk assessments performed</td>
<td>52%</td>
</tr>
<tr>
<td>Risks aggregated at the corporate level</td>
<td>49%</td>
</tr>
<tr>
<td>Enterprise-wide established policies and risk committees</td>
<td>30%</td>
</tr>
<tr>
<td>Risk management integrated into business initiatives</td>
<td>30%</td>
</tr>
<tr>
<td>Enterprise risk dashboard</td>
<td>30%</td>
</tr>
<tr>
<td>Risk training and knowledge sharing programs</td>
<td>26%</td>
</tr>
<tr>
<td>Enterprise wide risk tolerance levels and risk limits consistent</td>
<td>20%</td>
</tr>
<tr>
<td>Risk tolerances linked to strategic objectives</td>
<td>12%</td>
</tr>
</tbody>
</table>
ERM: Basic Concepts and Benefits

Authoritative Sources for ERM Approach

1. Committee of Sponsoring Organizations (COSO), comprised of the following organizations:
   • American Institute of Certified Public Accountants (AICPA)
   • American Accounting Association (AAA)
   • Financial Executives International (FEI)
   • Institute of Internal Auditors (IIA)
   • Institute of Management Accountants (IMA)

2. Control Objectives for Information and Related Technology (COBIT)
   • COBIT is an IT Governance framework used to help with regulatory compliance and gaining increased value from IT

3. Information Technology Infrastructure Library (ITIL)
   • The ITIL is a IT best practices framework that addresses service delivery and support of IT services
What is Enterprise Risk Management?

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows:

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

- COSO

What Drives Enterprise Value?

ENTERPRISE VALUE

STAKEHOLDER VALUE

Revenue Growth

Operating Margin

Asset Efficiency

Expectations
What are the Key Risk Areas?

**ENTERPRISE RISKS**

- **GOVERNANCE**
  - Ethics/Decision Authority
  - Oversight/Independence
  - Compensation/Other

- **STRATEGY**
  - Strategic/Plan/ Acquisitions/Divestitures
  - Succession Planning
  - Brand/Marketing/Pricing
  - Reputation

- **OPERATIONS**
  - Service Delivery
  - Inventory Management
  - Staffing and Employment
  - Quality Standards
  - Cost Management

- **INFRASTRUCTURE**
  - Compliance
  - Finance & Accounting
  - Tax
  - Information Technology
  - Insurance
  - BCP
  - Safety/Physical Security
  - Legal/IP/Litigation
  - Environmental / Other

- **EXTERNAL FACTORS**
  - Competition/Economic Conditions
  - Geopolitical/Regulatory
  - Activism/Public Safety
  - Natural Disasters/Other

**STRADECY**

- Strategic Plan/Acquisitions/ Divestitures
- Succession Planning
- Brand/Marketing/Pricing
- Reputation

**OPERATIONS**

- Service Delivery
- Inventory Management
- Staffing and Employment
- Quality Standards
- Cost Management

- Compliance
- Finance & Accounting
- Tax
- Information Technology
- Insurance
- BCP
- Safety/Physical Security
- Legal/IP/Litigation
- Environmental / Other

**INFRASTRUCTURE**

- External Factors
  - Competition/Economic Conditions
  - Geopolitical/Regulatory
  - Activism/Public Safety
  - Natural Disasters/Other

**REPORTING & INSIGHT**

- Board & Executive Management
- People
- Process
- Technology

**RISK TAKING**

- Strategy & Execution
- Risk Tolerating

**COMPLAINECE & RISK ASSURANCE**

- Compliance
- Risk Avoidance
- Operations

**STAKEHOLDER VALUE**

- Revenue Growth
- Operating Margin
- Asset Efficiency
- Expectations

Rewarded risk can drive value. Unrewarded risk can destroy value.
Benefits of ERM

- Align risk appetite and strategy
- Link growth, risk, and return
- Enhance risk response decisions
- Minimize operational surprises and losses
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Seize opportunities
- Support cost management efforts
- Improve operational performance
- Provide better basis for allocating resources

And thereby:
- Restore and/or retain stakeholder trust and confidence
- Protect and increase value for key constituents

Limitations of ERM

ERM is:
- A process for providing reasonable assurance about the achievability of the enterprise’s objectives
- Integrated, portfolio view of risks and vulnerabilities and their potential interactions
- Systematic and disciplined assessment of risk and reward as part of business process
- A means to improve rewarded risk taking and an aid to decision-making
- A way to redeploy existing resources
- A forward looking view

ERM is not:
- A silver bullet or absolute assurance
- A substitute for management judgment
- A stand alone initiative or a bureaucratic exercise in compliance
- Risk avoidance / risk aversion
- A call for additional resources
- A retrospective review
Assessing and Prioritizing Risk on an Enterprise-Wide Basis:

How you do it?

**Major Types of Risk and Risk Areas (examples)**

**Financial Operations**
The risks associated with the organization’s financial viability and the way the organization maintains its financial records.
- Accounting / Cost Reports / Revenue Cycle
- Treasury & Investments
- Tax – UBI, Payroll Withholding, Intermediate Sanctions, Returns -990s, and 501c3 Status
- Financing – Bonds, Public
- Internal Controls – Internal Audit
- Contracting / Purchasing (Materials Management) – Group Purchasing-Organization Relationships
- Construction

**Compliance and Legal Matters**
- Federal and state regulations
- Stark
- IRS Tax
- Anti-Kickback
- HIPAA
- Anti Trust

**Service Delivery**
The risks associated with the delivery of services
- Quality - Safeguarding of Practice
- Regulatory Compliance – EMTALA, Medical Necessity, HIPAA Privacy, Robinson/Patman
- Research/ IRB
- Institutional Licensing & Accreditation – COPs, CLIA, JCAHO, Patient Rights, Consent
- Marketing/ Community Outreach
Major Types of Risk and Risk Areas (cont.)

Employment and Staffing
The risks associated with the organization’s delivery and management of its human resources including employed, contracted and credentialed providers.
- Labor Relations
- Wage & Hourly - Compensation
- Employment Practices – Hiring & Firing, EEO, ADA
- Education, Training, Development
- Staffing – Retention, Recruitment, Performance Evaluations, Levels
- Pension & Benefits - Insurance
- Worker’s Compensation
- Contract Labor – Agency, Nurses

Organization and Strategic Environment
The risks associated with external factors, strategic direction and issues related to organizational structure and culture.
- Strategy – M&A
- Advocacy – Tax Exempt Limitations
- Public Relations
- Reputational
- Organization & Governance
- Mission
- Market forces (Competition)
- Disaster Planning
- Physical Security
- Canon Law
- Emerging Technologies (Innovations)
- Systems Integration

Major Types of IT Risk and IT Risk Areas

IT Computing Environment
Risks associated with the organization’s IT systems
- Hardware
- Software
- System interfaces
- Databases
- System and data criticality (system’s importance to the organization)
- System and data sensitivity
- Data backup and recovery process

Logical Access
- Password Administration
- Direct access to data
- Physical access to data centers/facilities/equipment
- Lack of segregation of duties

Network Security and Availability
- System security policies
- System security architecture

Operational Environment of IT systems
- Functional requirements of IT system
- Users of the IT system
- Management of data changes
Framework for Assessing Risk and Organizing Risk Response
Focus on vulnerabilities to value loss or creation - not just likelihood

Set Risk Appetite
(Thresholds)

Assess Impact
Key Performance Indicators:
- Qualitative
- Quantitative
Outcomes:
- Financial
- Reputation
- Legal/Regulatory
- Stakeholder Expectations

Assess Vulnerability
- Controls effectiveness
- Cost of risk experience
- Prevaling failure modes / contributing factors
- Complexity and change
- Risk management capability (detect, prevent, correct, escalate)

Set Priorities
- Likelihood
- Degree of difficulty
- Cost / ROI
- Time to implement

Risk Prioritization and Response Sessions
Evaluating the cost-benefit of various risk response options can be standardized using an evaluation template to standardize the analysis of different response options

Example Risk Response Evaluation Matrix: Financial Systems & Internal Reporting
Risk Description: the possibility of revenue loss or non-compliance due to poor alignment of financial systems functionality and internal reporting requirements.

<table>
<thead>
<tr>
<th>Options Available</th>
<th>Accept</th>
<th>Reduce Vulnerability</th>
<th>Reduce Impact</th>
<th>Transfer</th>
<th>Avoid</th>
</tr>
</thead>
</table>
| Costs             | -Minimal incremental cash expenses
-Continued risk of loss
-Continued or perhaps accelerated obsolescence of systems

$X Licensing fee
$X implementation
$X maintenance fee
Organizational disruption during transition
Ongoing inefficiency costs

$X implementation
$X annual fee
$X per transaction fee
Loss of organizational capability
Loss of organizational control |
| Benefits          | Lower cash outlays to address problem
Minimal organizational disruption

$X estimated avoided loss
Enhanced reporting and better business decision-making

$X estimated avoided loss
$X MM annual cost savings
Enhanced reporting flexibility and support |
| Residual Risks?   | No     | Yes                  | Yes           | Yes      | Not practicable |

©2012/CliftonLarsonAllen LLP
Inherent and Residual Risk

- Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk’s likelihood or impact.
- Residual risk is the risk that remains after management’s response to the risk.
- Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then considers residual risk.
- Effective enterprise risk management requires that risk assessment be done both with respect to inherent risk and also following risk response.

- COSO ERM 2004

Shortcomings of the COSO approach
Estimating Likelihood and Impact

“Uncertainty of potential events is evaluated from two perspectives — likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect... It is important that the analysis be rational and careful... The time horizon used to assess risks should be consistent with the time horizon of the related strategy and objectives...

For example, a company operating in California may consider the risk of an earthquake disrupting its business operations. Without a specified risk assessment time horizon, the likelihood of an earthquake exceeding 6.0 on the Richter scale is high, perhaps virtually certain. On the other hand, the likelihood of such an earthquake occurring within two years is substantially lower. By establishing a time horizon, the entity gains greater insight into the relative importance of the risk and an enhanced ability to compare multiple risks.”

COSO ERM Sept 2004 p. 58
Part 4

Implementing ERM

Phase 1
Buy-In
- Understand, Accept, Commit to Pilot
  - Value Proposition
  - Clarify ERM needs & expectations
  - Executive awareness and commitment
  - Agree on scope, criteria, process
  - Establish ERM as a priority
  - Communicate

Phase 2
Assess
- Assess enterprise risks and risk management capability
  - Pilot test
  - Set risk appetite and key performance metrics
  - Assess vulnerability to selected key risks
  - Qualify before quantify
  - Assess interactions and risk experience
  - Assess current capabilities
  - Develop risk profile
  - Identify gaps & set priorities

Phase 3
Recommend
- Detailed recommendations to resolve capability gaps in effectiveness & efficiency
  - Define authorities, requirements, resources
  - Design sustainable process
  - Identify capabilities for design
  - Design change management
  - Proof of Concept
  - Decision to proceed

Phase 4
Implement, Operate & Continuously Improve
- Implement sustainable ERM capabilities
  - Deploy tools
  - Train personnel
  - Monitor & Report
  - Integrate into core management processes
  - Change management
  - Continuously improve

A Typical Framework for Implementation
Developing the ERM implementation roadmap

- Build business cases to support implementation plan for changes to:
  - Enabling technologies
  - Organization
  - ERM processes
  - Program management

- Perform project prioritization based on business case criteria

- Develop properly sequenced implementation roadmap addressing:
  - Timeline
  - Resources requirements
  - Governance structure and responsibilities
  - High-level business cases
  - Critical success factors
  - Program enablers

Illustrative ERM Roles & Responsibilities

<table>
<thead>
<tr>
<th>Party</th>
<th>Responsibility</th>
<th>Monthly or as Needed</th>
<th>Quarterly</th>
<th>Semi-Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board / Audit Committee</td>
<td>Establish risk appetite; Review enterprise risks</td>
<td>Review all relevant risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Management Team</td>
<td>Set policy, prioritize and allocate resources for overall corporate risks</td>
<td>Review risks and allocate resources; report updates to Board / Audit Committee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERM Team (PMO, Council, Committee, etc.)</td>
<td>Manage process, tools and data</td>
<td>Coordinate and assist</td>
<td>Review all relevant risk</td>
<td></td>
</tr>
<tr>
<td>Division A Management Team</td>
<td>Identify, assess &amp; monitor risks relevant to division</td>
<td>Report/escalate significant new risks</td>
<td>Review risks with Executive Management</td>
<td></td>
</tr>
<tr>
<td>Division B Management Team</td>
<td>Identify, assess &amp; monitor risks relevant to division</td>
<td>Report/escalate significant new risks</td>
<td>Review risks with Executive Management</td>
<td></td>
</tr>
<tr>
<td>Division C Management Team</td>
<td>Identify, assess &amp; monitor risks relevant to division</td>
<td>Report/escalate significant new risks</td>
<td>Review risks with Executive Management</td>
<td></td>
</tr>
<tr>
<td>Corporate Management Team</td>
<td>Identify, assess &amp; monitor risks relevant to corporate functions</td>
<td>Report/escalate significant new risks</td>
<td>Review risks with Executive Management</td>
<td></td>
</tr>
</tbody>
</table>
Developing a Sustainable Risk Management Capability:  
*An Capability Maturity Model*

## A Model for Evaluating Risk Management Capability

1. How capable is your company today to manage its risk profile?  
2. How capable does it need to be?  
3. How can it get to its desired state?

### 1: Tribal & Heroic
- Ad-hoc / chaotic; depends primarily on individual heros, capabilities and verbal wisdom
- Reaction to adverse events by specialists
- Discrete roles established for small set of risks
- Typically finance, insurance, compliance

### 2: Specialist Silos
- Tone set at the top
- Policies, procedures, risk authorities defined and communicated
- Business function
- Primarily qualitative
- Reactive

### 3: Top-Down
- Integrated response to adverse events
- Performance linked metrics
- Rapid escalation
- Cultural transformation underway
- Bottom-up
- Proactive

### 4: Systemic

### 5: Risk Intelligent
- Built into decision-making
- Conformance with enterprise risk management processes is incentivized
- Intelligent risk taking
- Sustainable
- “Risk management is everyone’s job”

Un-rewarded Risk

Rewarded Risk

© 2012 CliftonLarsonAllen LLP
A Model for Evaluating Risk Management Capability (continued)

Categories of Leading ERM Practices

**Internal & External Environment**
- Board of Directors
- Integrity, Ethical Values & Code of Conduct
- Risk Management Philosophy
- Risk Appetite & Risk Policy
- Organizational Structure
- Assignment of Authority & Responsibility
- Commitment to Competence
- External Environment

**Decision Making & Objective Setting**
- Strategy & Execution Objectives
- Operations & Infrastructure Objectives
- Compliance Objectives
- Reporting Objectives
- Risk Appetite & Tolerances
- Risk Informed Decision-Making

**Scenario & Event Identification**
- Scenarios & Events
- Distinguishing Risks & Opportunities
- Influencing Factors
- Interdependencies
- Event Identification & Scenario Techniques

**Risk Assessment**
- Estimating Impact & Vulnerability
- Assessment Techniques
- Analyzing Interdependencies
- Prioritizing Risks for Response
- Evaluating Possible Responses

**Risk Response**
- Prioritizing, Selecting & Integrating Responses
- Assigning Responsibilities

**Control Activities & Assurance**
- Types of Control Activities
- Assurance Activities
- Policy & Procedures
- Controls Over IS and Other Infrastructure

**Information & Communication**
- Information & Reporting
- Knowledge Management
- Change Management
- Training & Continuing Education
- Communication and Disclosure

**Monitoring & Escalation**
- Ongoing Monitoring/Separate Evaluations
- Independence
- Decision Authorities, Breaches and Escalation
- Reporting Trends, Deficiencies, Exceptions
- Continuous Improvement

Enhancing Risk Management Capability

Key Strategies

- **Link enterprise risk to enterprise value**
  - Take an integrated approach that helps the organization efficiently identify and respond to unacceptable risks in the context of its key value imperatives
  - Use a consistent enterprise-wide approach to classifying and describing risks including types of risk outcomes (impacts)
  - Establish or leverage consistent qualitative and quantitative models for valuing risk impacts

- **Improve risk management capability by focusing on people, process and technology**
  - Roles, responsibilities and authorities for managing risk
  - Policies and guidelines for defining risk appetite and risk tolerance
  - Procedures and process for risk identification, assessment, prioritization and response
  - Risk centered strategic planning and resource allocation
  - Risk analysis tools and specialized skills
  - Risk management training and awareness
  - Risk aggregation, monitoring and reporting technology

- **Establish ERM as a component of the organization’s governance structure**
  - Board oversight
  - Management ownership
  - Embedded and practiced throughout the organization
The DNA of the Risk Intelligent Organization

Critical Success Factors

- Gain Board / senior executive commitment and involvement
- Establish management accountability and responsibilities
- Demonstrate tangible results and link to value objectives
- Build the process into the way the enterprise does business
- Obtain supporting charter, policies, and procedures
- Provide a competent core IERM team and adequate resources
- Focus on the cultural/change management process
- Monitor and continuously improve
Questions & Answers

Thank You for Your Time and Participation