Enterprise Risk Management

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

Enterprise risk management is a process, applied in strategy setting 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's ERM Framework

Who Regulates Health Care

Health Care Providers

State
- Survey & Certification
- Courts
- Attorneys General
- Medicaid
- Health Boards
- Medical Boards
- Local Governments
- Licensure

Who Regulates Health Care - Providers

- DME Regional Contractors
- Regional Offices
- Intermediaries
- Carriers
- PROs
- Medicare Integrity Program Contractors
- Departmental Appeals
- GIG
- MMMR
- Regional Home Health Intermediaries
- DEA
- FAA
- OPOs
- SEC
- IRS
- EPA
- FTC
- HHS/NASH
- HHS/HRSA
- FCC
- FTC
- Homeland Security
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DEA
- DOT
- OSHA
- DOI
- DE
The Connection Compliance and ERM

- Compliance Risk Activities
  - OIG Work Plan
  - Advisories and Opinions
  - What issues are health care entities being sued for or settling out of court

- ERM
  - Regulatory/Legal
  - Finance
  - Operational
  - Reputational

Risk Activities

- Internal Audit Services
- Internal Control Evaluations
- Legal
- External Auditors
- Compliance
- Lacks coordination
- External View
Managing Risk
Usually not Integrated

- External Auditors
- Finance
- Internal Audit Services
- Information Technology
- Security
- Legal Department
- Patient Care
- Research Services
- Human Resources
- Compliance
- Environmental
- Medical School
- Board of Directors

ASSESS RISK

Risk assessment is the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed.
The Seven Elements

2. CO and Compliance Committee
3. Education
4. Monitoring and Auditing
5. Reporting and Investigation
6. Enforcement and Discipline
7. Response and Prevention
8. Risk Assessment

1 - Policies and Procedures

• What will be your process?
  • Interviews
    • Leadership
    • “Disruptors”
    • “Diverse Thought Leaders”
  • Surveys
  • Internally conducted
  • Consultant effort
  • Initial
  • Refreshing
2 - Oversight

- Board of Directors
- Audit and Compliance Committee
- Committee
- Role of CEO and/or CAO
- Risk Officer or a combination of people
  - CO
  - IAS
  - Risk Management (Hospital)

3 - Education

- Creating an ERM culture
- Focused
- Selective
- Just in time
4 – Risk Identification and Mitigation

- Reputational – Strategic
- Financial
- Operational
- Regulatory - Legal

5 - Reporting

- Ranking risk process
- Connections from year to year
- Old risks versus new risks
- Leadership Verification
6 - Commitment

- CEO and CA0
- Board of Directors
- Audit and Compliance Committee
- TIME!

7 – Response and Prevention

- Controls
- Emerging Risks
- Management Accountability
- Governance Oversight
NOW WHAT?

- Hundreds of potential risks identified
- Each person has their risk priorities
- This process is qualitative at best
- Where do you go from here?
RANKING RISKS

- Consequence
  - Financial
  - Reputational
  - Legal/compliance
  - Operational

- Likelihood
  - Past experience
  - Experience of others
  - National Trends

- Short Term < 18 months

- Long Term > 5 years

DETERMINE RISK APPETITE

- Risk appetite is the amount of risk — on a broad level — an entity is willing to accept in pursuit of value.

- Use quantitative or qualitative terms (e.g. earnings at risk vs. reputation risk), and consider risk tolerance (range of acceptable variation).
DETERMINE RISK APPETITE

Key questions:

- What risks will the organization not accept?
  (e.g. environmental or quality compromises)

- What risks will the organization take on new initiatives?
  (e.g. new product lines)

- What risks will the organization accept for competing objectives?
  (e.g. gross profit vs. market share?)

RISK EVALUATION

1. Primary Ownership within one department or work unit
2. Inter-departmental ownership occurs where risks cut across multiple departments
3. Those dependent on strategic initiatives or strategic plan
IDENTIFY RISK RESPONSES

- Quantification of risk exposure
- Options available:
  - Accept = monitor
  - Avoid = eliminate (get out of situation)
  - Reduce = institute controls
  - Share = partner with someone (e.g. insurance)
- Residual risk (unmitigated risk – e.g. shrinkage)

VALIDATING RISKS AND RANKINGS

- Core Group
  - Compliance Office
  - Internal Audit Services
  - Internal Control Activities
- Validate with CEO, CAO, CFO, CLO
PREPARE REPORTS

- Management
- Leadership
- Boards

Heat Maps

- MONITOR
- ACCEPT
- STRATEGIC CHOICES
- URGENT ACTIONS
- EVALUATE
- ALTERNATIVES
## Risk Control and Audit Matrix

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Specific Risk</th>
<th>Rating</th>
<th>Risk Owner</th>
<th>Operational</th>
<th>Governance/Committee</th>
<th>Policy and/or Procedure</th>
<th>Review Cycle</th>
<th>Audit Plan or Compliance Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C-12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Strategic Risks
- S-1
- S-2

### Financial
- F-5
- F-6

### Operational
- O-8
- O-9

### Compliance/Legal
- C-11
- C-12

---

## Risk Assessment: Prioritization and Responsibilities

<table>
<thead>
<tr>
<th>Priority Ranking</th>
<th>Business Risk</th>
<th>Senior Management Responsible</th>
<th>BOD Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mayo Clinic ERM COSO Considerations

**Internal Environment**
- Leadership (MT, BOG, ACC)
- Commitment to Risk Management

**Objective Setting**
- External benchmarking with Health Care Industry, Other Industry & External Experts

**Information & Communication**
1. ERM Heat Maps
2. ERM Risk, Control, & Audit Matrix

**Monitoring**
- Monthly Management Team meetings to include risk assessment for each risk

---

**ERM Calendar Overview**

<table>
<thead>
<tr>
<th></th>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DEC</td>
<td>JAN</td>
<td>FEB</td>
<td>MAR</td>
<td>APR</td>
</tr>
<tr>
<td></td>
<td>SEP</td>
<td>OCT</td>
<td>NOV</td>
<td>DEC</td>
<td></td>
</tr>
</tbody>
</table>

**External Benchmarking**
- Other Industry & External Experts

**Survey**
- Event Identification / Risk Assessment / Risk Response / Control Activities

**Interviews**
- 20 Leadership Interviews
- 20 Leadership Interviews
- 20 Leadership Interviews
- 20 Leadership Interviews

**Strategic Planning**

**Workgroups & Assessments**
- Establish Standardized Process & Reporting
- Ongoing Reporting to Mayo Clinic Enterprise Risk Management

**Risk Assessments (Facilitated Dialogues)**
- Monthly Management Team Meetings: Leadership Risk Assessments and Operating Objective Assessments (Strategic Planning)

**Approval / Board Communications**
- Quarterly ERM Reporting to ACC
- Quarterly ERM Reporting to ACC
- Quarterly ERM Reporting to ACC
- Quarterly ERM Reporting to ACC
RISK PROCESS

- Identify
- Rank
- Prioritize
- Assign/Recognize Accountability
- Mitigation

LIMITATIONS

- Decision making - responses
- Human failure – simple errors
- Circumvention collusion
- Ability to override controls