What is risk?

*All management is risk management!*
Risk Management “Boot camp”

\[\text{Threat} + \text{Vulnerability} = \text{Risk}\]

\[\text{Risk} - \text{Controls} = \text{Residual Risk}\]

\[\text{Residual Risk Probability} + \text{Residual Risk Impact} = \text{Risk Rating}\]
Risk Types

- **Strategic Risks** – Inherent risks of doing business, going after new markets, regulatory
- **Finance Risks** – Treasury risks, credit risks, trading risks
- **Operations Risks** – People, compliance, process
- **Information Risks** – Operational and Technological risks
About controls…

Control Types

- Preventive
- Detective
- Corrective

Control Categories

- Administrative
- Technical
- Personnel
- Physical
How do you manage and track risks?

• Enterprise Risk Management
  – What is it?
    ERM is establishes the oversight, control and discipline to drive continuous improvement of an entity’s risk management capabilities in a changing operating environment.
  – Who is involved?
    Everyone in the organization and the Board
And you should care because…
Recent History of ERM

- Cadbury Committee (UK) (1992)
- Chief Risk Officer created at GE (1992)
Global Corporate Governance Models

**France**  
- Vienot Com.  
- Mrini Report  
- Levy-Long Com.

**UK**  
- Cadbury  
- Turnbull  
- Greenbury Rpt  
- BS 31100 RM

**All EU Countries**  
- Directives on Governance

**Germany**  
- Bill on The Control and Transparency of organizations  
- Kon TraG Bill

**Netherlands**  
- Code Tabaksblatt

**Italy**  
- Draghi Commission

**Canada**  
- Toronto Stock Exchange Committee  
- Canadian Securities Committee  
- Allen committee Report  
- COCO

**US**  
- Business Round Table  
- NYSE listing Requirements  
- Blue Ribbon Commission  
- Sarbanes Oxley Act  
- COSO ERM Framework

**South Africa**  
- Code of Best Practice  
- King Report I, II and III  
- Stakeholder Communication  
- Public Finance Mgmt Act

**INTERNATIONAL - Basel I & II; ISO 31000 & 31010**

**Japan**  
- Corporate Governance Forum of Japan  
- J-SOX

**Australia/New Zeal**  
- AS/NZS 4360:2004  
- Stock Exchange Listing  
- New Accounting Standards  
- Best Practice Stmt Mgmt

**Source:** RIMS.org

Copyright 2010 Assura, Inc. All rights reserved.
Risk Management Frameworks

Which one is best for your organization?

- Organizational
  - Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Internal Framework (ERM-IF)
  - Risk and Insurance Management Society (RIMS) Risk Maturity Model (RMM) for Enterprise Risk Management
  - Australian/New Zealand Standard (AZ/NZA 4360:2004)

- Information Technology Focused (supports Organizational)
  - Control Objectives for Information and related Technology (COBIT from ISACA)
  - Guide to Assessment of IT Risk (GAIT from IIA)

- Risk Management Publications
  - BS 31100:2008 and ISO 31000:2009
  - ISO guide 73 risk management – vocabulary
  - ISO 31010 risk assessment techniques
ISO 31000 Risk Management – Principles and Guidelines

• Provides a very general and flexible framework for best practices in ERM
• Incorporates COSO, PMI (Project Management Institute, and AS/NZS4360:2004
• Built on the premise that risk management is fully integrated into the organization and part of all decisions
• Allows for management of negative and positive risk
ISO 31000 10 Basic Principles

1. Creates value – not focused on loss
2. Integral part of the organization – in project management, strategic planning, etc.
3. Decision making through analysis and evaluation to understand risk
4. Explicitly addresses uncertainty and how it can be modified
5. Systematic, structured, timely, repeatable
10 Basic Principles (Cont.)

6. Based on available information – historic data, expert opinion.

7. Big or small – tailored to the organization

8. Includes human, cultural as well as technical factors that impact likelihood of consequences

9. Transparent and inclusive – communication and consultation with stakeholders

10. Incorporates continuous improvement and responds to changing environment
ERM Framework

- 31000 focuses on the framework that supports the Risk Management Process(es) or RMP
- Does not specify components, but gives conceptual guidance
- Aggregates information on risks, risk management, and performance of risk controls
- Must be practical and part of existing processes
ERM Framework Components
“The Lucky 7”

1. Mandate and commitment to the ERM framework
2. Risk management policy
3. Integration of ERM in the organization
4. Risk Management Process (RMP)
5. Communications and reporting
6. Accountability
7. Monitoring, review, and continuous improvement (Plan, Do, Check, Act)
Risk Management Process

Establishing the Context

- Risk Management environment defined
- Risk Appetite/Tolerance Should Be Defined
- Internal and External Context
- Risk Mgmt. Context

Risk Assessment

- Risk Identification
- Risk Analysis
- Risk Evaluation

Treat Risk

- Identify control option
- Select control option
- Implementation of control

Monitor and Review

Communicate and Consultation

Ongoing Tracking and Monitoring

Copyright 2010 Assura, Inc. All rights reserved.
How To Leverage BC in an ERM Process
Analyze Risk: Risk Mapping (a.k.a. Heat Map)

**Secondary Risks**
- Lower likelihood, but could have significant adverse impact on business objectives

**Key Risks**
- Critical risks that potentially threaten the achievement of business objectives

**Low Priority Risks**
- Significant monitoring not necessary unless change in classification
- Periodically reassess

**Secondary Risks**
- Lesser significance, but more likely to occur
- Consider cost/benefit trade-off
- Reassess often to ensure changing conditions (move to high significance)

Source: www.knowledgeleader.com
## Risk Ratings – Other types

<table>
<thead>
<tr>
<th>FREQUENCY OF OCCURANCE/PROBABILITY</th>
<th>RISK IMPACT</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IV  (Catastrophic or Emergency)</td>
<td>III  (Critical or High)</td>
<td>II  (Marginal or Medium)</td>
<td>I  (Negligible or Low)</td>
<td></td>
</tr>
<tr>
<td>4 (Frequent)</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3 (Probable)</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2 (Occasional)</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>1 (Remote)</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0 (Improbable)</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Evaluate Risks: Types of Risk Decisions

- **Avoidance** - a decision not to become involved in, or to withdraw from, a risk situation.
- **Acceptance**: acceptance of the burden of loss, or benefit of gain, from a particular risk.
- **Reduction**: actions taken to lessen the likelihood, negative, or both, associated with a risk.
- **Sharing of risk**: sharing with another party the burden of loss, or benefit of gain from a particular risk.
Monitor Risk: Tracking the Risk

- Risk Register (*Keep It Simple!*)
  - Identified Risk with Description
  - Risk Category (Type of Risk)
  - Risk Score (*Residual Risk Probability + Residual Risk Impact*)
  - Risk Owner
  - Risk Decision
**Perceived Deficiencies with ISO 31000**

Risk management policies, roles and responsibilities

- Insufficient detail of risk architecture, strategy, protocols

Risk management principles

- Confusion between what risk management is and what it delivers

Risk management specialist areas no included

- Project risk management and clinical risk management

Risk governance

- No mention of “risk appetite”
- Lack of detail for risk reporting and auditing controls

Source: RIMS.org
Final Thoughts...

• Start Small – Document and obtain agreement on the Risk Appetite – “Establishing the Context”
• There are no “right” and “wrong” answers to every risk. Make the best decision you can with the most available data!
• Engage all parts of the organization!
Karen L. Cole, CBCP, SBCI
Assura, Inc.
804.672.8714
Karen.cole@assuraconsulting.com
www.assuraconsulting.com