Current Topics in Internal Audit

Presentation to
Institute of Internal Auditors
Topeka, KS Chapter

December 2010
Agenda

• Introduction and Objectives
• Current Trends in Risk Assessment
• Contract Risk
• Consideration of Fraud
Some Demographics

- How many public companies?
- How many have done SOX or FDICIA?
- What is your internal audit group primarily focused on:
  - Operations?
  - Compliance?
  - Financial Processes?
  - A combination of all 3?
Above all, understand your risks

CURRENT TRENDS IN RISK ASSESSMENT
What is Risk?

- Risk is the potential for failure
  - Loss of value or the sub-optimization of gain
  - Failure is the unacceptable difference between actual and expected performance

- Risk may be caused by an event (or series of events) that can adversely affect the achievement of your objectives.

- The objectives of the enterprise are to:
  - protect the value of its existing assets (survive)
  - create new or future value (thrive)
What’s Wrong With Risk?

Two Schools of Thought:
• Risk taking is bad and needs to be avoided
• Risk taking is good and needs to be managed

To which school of thought does your organization subscribe?
## Risk Intelligence: Deloitte’s view of Risk Management

### Unrewarded Risk vs. Rewarded Risk

<table>
<thead>
<tr>
<th>+ VALUE</th>
<th>Traditional Approach</th>
<th>Risk Intelligent Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>- Focus on compliance, security, financial issues</td>
<td>- For competitive advantage</td>
</tr>
<tr>
<td></td>
<td>- Mitigating risks of fraudulent activities, physical safety</td>
<td>- For attracting more and high-value customers</td>
</tr>
</tbody>
</table>

### Siloed Risk Management

<table>
<thead>
<tr>
<th>Traditional Approach</th>
<th>Risk Intelligent Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Different risk language and risk management approach across the organizational silos</td>
<td>- Common risk language</td>
</tr>
<tr>
<td>- Poor communication across these silos</td>
<td>- Coordinated roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>- Rationalized and standardized controls for risk management</td>
</tr>
</tbody>
</table>
Risk Intelligence: Deloitte’s view of Risk Management

Traditional Approach
- Focus only on the individual risk events without considerations for its long term impact or risk interactions

Risk Intelligent Approach
- Interactions between separate individual risks are studied
- Risk assessment using scenario analysis

Takeaway – Risk Intelligent Enterprise™
- Develops Full-Spectrum Vision
- Bridges Silos
- Speaks a Common Language
- Assesses Impact
- Weighs Vulnerability
- Considers Risk Interaction

A Risk Intelligent Enterprise™ has the ability to convert unrewarded risks into opportunities.
Understanding Risks to Value

Management is responsible for creating and preserving value in the enterprise

1. How can the enterprise fail to achieve its value objectives?
2. What would cause the enterprise to fail?
3. What would be the effects of the failure?
4. What is currently being done to prevent, detect, correct or escalate such failure?
5. What is our vulnerability to such failure?
6. What further actions are required to cost-effectively mitigate value at risk?
7. How do we get reasonable assurance existing mitigation is reliable & effective?
Impact vs. Vulnerability

- Impact, or *gross inherent risk*, refers to the risk that exists before you address it, i.e., the risk to the company in the absence of any actions the company might take to mitigate the risk.

- Vulnerability, also referred to as *net residual risk*, or exposure, is the risk that remains *after the company has attempted to mitigate inherent risk*. 
The Risk Intelligent Enterprise

• Many companies base their risk management program on the probability of certain negative events occurring.

• Unfortunately probability-based risk assessments do not always suffice.
  – As a Deloitte Research study noted, major-value losses are often high-impact, low-likelihood events.* (for example, terror attack on twin towers in NYC on September 11, 2001).

• Our new methodology therefore uses vulnerability to assess risk rather than relying solely on likelihood.

* “Disarming Value Killers,” Deloitte Research, 2005
Define Impact and Vulnerability Criteria

**Impact**
- Strategic
- Financial
- Reputation
- Legal and Regulatory
- Operational
- Stakeholders
- Competitor

**Vulnerability**
- Complexity
- Control Effectiveness
- Prior Risk Experience
- Rate of Change
- Preparedness

*Define the Impact and Vulnerability criteria which will be applied to each identified enterprise risk to determine the relative risk rankings:*
MARCI Chart

First, Effectiveness, then Efficiency

Assurance of Preparedness

Enhance Risk Mitigation

Prevent
Detect
Correct
Escalate

Redeploy Resources

Measure for Cumulative Impact

Risk Impact on Value

Vulnerability
Bridging the gap with Risk intelligence

Risk Intelligence can help an organization:

- Promote critical thought on overall risk exposure
- Identify and coordinate across risk management silos
- Promote exploration of the various impacts risks can have
- Identify potential risk interactions
- Plan assurance activities for maximum benefit
- Prioritize risk mitigation
- Make risk-based strategic decisions
Trust, But Verify

CONTRACT RISK
Objectives

• Start thinking about the extended enterprise
• What to know when establishing contractual relationships
• How to manage a relationship going forward
Extended Enterprise - Questions to Ask

• What business partners do I rely on daily?

• If a partner fails to perform, who is accountable in the market? Partner or Me?

• Which relationships are critical, both for the market for Safety & Soundness of the members?
Typically, What is an Extended Enterprise?
## Extended Business Relationships

<table>
<thead>
<tr>
<th>Supply-Side Partners</th>
<th>Demand-Side Partners</th>
<th>Licensees</th>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers</td>
<td>Franchisees</td>
<td>Original equipment manufacturers (OEMs)</td>
<td>IT outsourcing</td>
</tr>
<tr>
<td>Manufacturers</td>
<td>Distributors</td>
<td>Co-brand partners (e.g., home banking)</td>
<td>Business Continuity/Recovery</td>
</tr>
<tr>
<td>Replicators</td>
<td>Resellers</td>
<td>Joint developers</td>
<td>HR services</td>
</tr>
<tr>
<td>Integrators and installers</td>
<td>Advertising agencies</td>
<td>IP licensees</td>
<td>Travel agencies</td>
</tr>
<tr>
<td></td>
<td>Retailers</td>
<td></td>
<td>Legal services</td>
</tr>
<tr>
<td></td>
<td>Fulfillment providers (e.g., wire transfer, investment partners)</td>
<td></td>
<td>Benefit providers</td>
</tr>
<tr>
<td></td>
<td>Warranty, maintenance and repair providers</td>
<td></td>
<td>Transaction processing</td>
</tr>
</tbody>
</table>
What is Contract Risk Compliance?

Contract Risk and Compliance (CRC) is an approach to understanding and mitigating the risks in extended business relationships. It helps organizations maximize the value of the extended enterprise:

- Determine if key partner risks are identified and addressed by your own internal control framework
- Examine the integrity of your partner’s controls over contract performance and determine if the controls have been maintained and can be relied upon
- Verify whether your business partners are in compliance with their monetary and non-monetary contractual obligations
  - Recover lost revenue and identify cost savings
  - Protect your valuable brand
CRC Process Overview

CRC process reinforces the program

1. Identify Relationships
   - Identify all contractual relationships

2. Identify Relationship Objectives
   - Identify the objectives of key relationships

3. Assess Risk
   - Determine the key control points and dependencies of relationships
   - Develop processes to identify risks
   - Target relationships that pose significant risks
   - Identify the risk of not achieving key objectives

4. Evaluate Compliance
   - Determine key controls/processes at external business partners that impact your business
   - Evaluate data/records against contract terms
   - Identify process improvement opportunities

5. Mitigate Risk
   - Improve policies and procedures
   - Improve relationships and performance
   - Enhance compliance
   - Incorporate learnings
   - Train contract writers/negotiators
   - Avoid relationships that pose greater than normal risk

Inform the partner selection and contracting process
CRC Considerations

Common Concerns

• Harming the relationship

• Cost of CRC program

• Lack of audit clause

• Clearly communicated objectives
• Reviews conducted transparently
• Use of independent providers
• Deloitte: objectivity/preservation

• Significant tangible and intangible benefits
• May pass on audit costs

• Other procedures to perform
• May have other rights to exercise
• Influence likely will override
Getting Started

• Identify relationships
  • Design template for data collection
  • By function – purchasing, IT, licensing
  • Search chart of accounts
  • Engage legal, operations and finance

• Perform risk assessment
  • Determine criteria – size, strategic importance
  • Stratify population
  • Consider life cycle of relationship

• Gather internal support
  • Internal education re: benefits
  • Evaluate concerns
  • Consider long-term strategy
CRC Perspective

• The extended enterprise is today’s reality

• Exercising due diligence makes good business sense and is expected by directors

• Assessing contractual compliance is now an imperative for adequate controls assurance and revenue enhancement

In short:
“Trust, but verify”
Maybe don’t trust...

FRAUD DETECTION & PREVENTION
Fraud is ongoing...

**Occupational Frauds by Category — Frequency**

- **Asset Misappropriation**
  - 2010: 86.3%
  - 2008: 88.7%

- **Corruption**
  - 2010: 32.8%
  - 2008: 26.9%

- **Financial Statement Fraud**
  - 2010: 4.8%
  - 2008: 16.3%

---

3The sum of percentages in this chart exceeds 100% because several cases involved schemes from more than one category.

Source: Association of Certified Fraud Examiners, Inc. ©2010
...And Losses are Real

Source: Association of Certified Fraud Examiners, Inc. ©2010
And Long Lasting

Median Duration of Fraud Based on Scheme Type

Source: Association of Certified Fraud Examiners, Inc. ©2010
We’re getting better

Impact of Hotlines

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>Organizations With Hotlines</th>
<th>Organizations Without Hotlines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip</td>
<td>47.1%</td>
<td>33.8%</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>16.5%</td>
<td>11.2%</td>
</tr>
<tr>
<td>Management Review</td>
<td>15.7%</td>
<td>15.7%</td>
</tr>
<tr>
<td>Account Reconciliation</td>
<td>7.8%</td>
<td>4.7%</td>
</tr>
<tr>
<td>By Accident</td>
<td>11.9%</td>
<td>4.0%</td>
</tr>
<tr>
<td>Document Examination</td>
<td>6.5%</td>
<td>2.7%</td>
</tr>
<tr>
<td>Surveillance/Monitoring</td>
<td>2.2%</td>
<td>2.0%</td>
</tr>
<tr>
<td>External Audit</td>
<td>7.3%</td>
<td>1.4%</td>
</tr>
<tr>
<td>IT Controls</td>
<td>0.4%</td>
<td>1.4%</td>
</tr>
<tr>
<td>Notified by Police</td>
<td>2.3%</td>
<td>1.0%</td>
</tr>
<tr>
<td>Confession</td>
<td>1.1%</td>
<td>0.9%</td>
</tr>
</tbody>
</table>

Percent of Cases

Source: Association of Certified Fraud Examiners, Inc. ©2010
Address Fraud at All Levels

- Fraud Risk Governance
- Fraud prevention and detection
- Fraud risk assessment, investigation & corrective action

Risk Governance

Oversight
- Tone at the top

Common Risk Infrastructure
- People
- Process
- Technology

Risk Process
- Identify Risks
- Assess & Evaluate Risks
- Integrate Risks
- Respond to Risks
- Design Implement & Test Controls
- Monitor, Assure & Escalate

Risk Types
- Governance
- Strategy & Planning
- Operations/Infrastructure
- Compliance
- Reporting
It’s better to have a fence at the top of the cliff than an ambulance at the bottom

• Fraud Risk Assessment is fundamental
  • READ – Understand what is emerging
  • Include scenario discussion
  • Involve 3rd parties (customers, vendors, service providers)
  • Benchmark scenarios to controls
  • Refine
  • Assess and Repeat
Thank You

Brian Clark
Senior Manager
Deloitte & Touche LLP

816 802 7751 (w)
913 908 9541 (m)
bclark@deloitte.com