Collaborative Risk Management

The Risk Management Value Proposition
Dan Clayton CIA, CPA, CKM
University of Texas System
My IA journey...

**Internal Audit History** *

- Controls based - extension of external audit (up to 1980’s)
- Process based - added effectiveness and efficiency (1980’s)
- Risk based - added “why should management care” (1990’s)
- Risk management - added “optimizing risk” top down (late 1990’s)
- Objective Based** - True Top Down, Objective Priorities “at Risk”

*Paul J Sobel “Auditors Risk Management Guide”
** Tim Leech and other thought leadership (ISO 31000)
My IA journey...

**Risk Management**

- Evaluated 12 ERM implementations in Healthcare 2008-2009
- Advised on Risk Management Consulting Approach for IA
- Created Risk Management Based Risk Assessment & Audit
- Coordinated UT Systemwide Taxonomy and Risk Assessment Update
- Working towards collaborating with Risk Peers; Compliance, Information Security, Police, insurable Risk Management, Legal, etc.
Presentation Objectives

**Discuss Risk Management Concepts**
- Set the modern context for RM
- Be able to define the flavor of RM at your organization

**Assessing Collaborative RM Opportunities**
- Discuss assessing RM
- Define Collaborative RM Maturity Model
Presentation Objectives

Risk Management Concepts

- Definitions
- Risk Perspectives within the Lines of Defense
- Risk History and Context for RM
- RM at your Organization
Risk Management Concepts - Definitions

• ISO 31000 Risk Management
  • Risk - the effect of uncertainty on objectives
  • Risk Management - identification, assessment and prioritization of risk... followed by... application of resources to minimize, monitor and control impact
Risk Perspectives - 3 lines of Defense

The Three Lines of Defense Model

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Governing Body/Board/Audit Committee
Senior Management

External audit
Regulator
Risk Perspectives - 3 lines of Defense

MANAGEMENT – 1st LINE
- Risk is Assumed
- Objectives Defined/Managed (controlled)
- Operations Developed (control capabilities)
- People, Process Technology Aligned (Efficiency)
- Performance is Measured (Outcomes)
Risk Perspectives - 3 lines of Defense

2nd LINE FUNCTIONS

Risk is defined by function objective; Compliance, Legal Impact, External Event, Safety Incident, IT Breech, etc.
Risk Is Assessed, Issues Identified and Management Response Required
Risk Is Managed through Programs to aid in continual assessment, education or response
Risk Perspectives - 3 lines of Defense

3rd LINE FUNCTIONS
Enhance and Protect Organizational Value
Risk Is Assessed to evaluate Governance,
Risk Management and Control
Audit and Consulting used to define issues
in Governance, Risk Management and Control
The management system: Linking strategy to operational planning

1. Develop the Strategy
   - Mission, values, vision
   - Strategic analysis
   - Strategy formulation

2. Plan the Strategy
   - Strategy map/themes
   - Measures/targets
   - Initiative portfolios
   - Funding/STRATEX

3. Align the Organization
   - Business units
   - Support units
   - Employees

4. Plan Operations
   - Key process improvement
   - Sales planning
   - Resource capacity plan
   - Budgeting

5. Monitor and Learn
   - Strategy reviews
   - Operating reviews

6. Test and Adapt
   - Profitability analysis
   - Strategy correlations
   - Emerging strategies

Performance measures:
- Results

Execution:
- Process
- Initiative

Functional Business Objective
- Management Oversight Mechanisms
- People
- Process
- Technology

Purpose
- Management & Monitoring
- Resource Alignment
- OUTPUT
The Business Case for Integrated GRC

Integrating governance, performance, risk, internal control and compliance management (GRC) activities yields a number of benefits. These interrelated activities have much in common; and an integrated approach can improve performance while reducing costs. Importantly, integration does NOT mean consolidation. Rather, the various GRC areas should adopt a common vocabulary, methods and, if appropriate, shared technology and shared services to be more effective, efficient and agile.

CURRENT STATE

- LACK OF EFFECTIVE OVERSIGHT
- ORGANIZATIONAL & FUNCTIONAL SILOS
- DISJOINTED STRATEGY
- LACK OF VISIBILITY
- COMPLEXITY
- SLIPPING THROUGH THE CRACKS
- LACK OF INTEGRITY

FUTURE STATE

- EFFECTIVE OVERSIGHT
- INTEGRATED REPORTING & ANALYTICS
- INTEGRATED GRC STRATEGY
- INTEGRATED RISK & CONTROL ACTIVITIES
- INTEGRATED QUALITY INFORMATION
- SHARED TECHNOLOGY
- COMMON METHODS
- COMMON VOCABULARY

GRC ASSESSMENT TOOLS™ Version 3.0
Questions?

- Risk and Risk Management definitions
- The first line of defense, Management’s Role and Risk Perspective
- The second line of defense, Roles, Risk Perspectives and GRC
What is Risk Management at your Organization?

• A Executive Risk Management Committee? (COSO-based)
• A GRC Process for gathering all risks and managing them
• One dominant Risk Function, leading the rest?
• Something better?
• Something worse?
Assessing Collaborative RM Opportunities

• Start with principled definitions and perspectives
• Defining existing risk management
• Understanding the appetite for improvement
• Defining IA role in influencing and collaborating on risk management
• Use Collaborative Risk Management Maturity Model
Where do we begin? (3rd Line of Defense)

• Start with ISO 31000 definitions and Principles
• Recognize its about objectives
  • Value comes from new information for management to leverage
  • Aligning risk organization and treatment with these realities is risk management

• **Internal Audit can encourage the right structure;** and add risk management to risk assessments and audits

• Validate your understanding of Risk Management happening at your organization
Where do we begin? (3rd Line of Defense)

Understand RM and the appetite for improvement

• Mgmt. Not likely to say “I need risk management,” but may say:
  • Isn’t there one place where I can see all the risks and issues and who is managing them?
  • I wish I had better insight into that area, but everything is so new I don’t have a feel for their chances of success
  • Shouldn’t we be vetting all of the major concerns across our organization as they occur? How do we get that information

• What is the perspective of existing Risk information, who is getting it?
• How far up and down the ladder does important risk info flow?
Defining IA Risk Management input

• Can we help seed/develop the structure of general risk management?
  • Who is talking to who?
  • How are risks and issues organized; can it fit with what management sees?
  • Are there any existing Risk Committees to leverage?

CAPABILITY MATURITY MODEL?

• Measure the current state and identify roles to play
  • Advocate, Evangelist, Assessor, Collaborator...
### COLLABORATIVE RISK MANAGEMENT MATURITY MODEL

<table>
<thead>
<tr>
<th>Initial</th>
<th>Adequate</th>
<th>Enhanced</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unclear Risk Organization</strong></td>
<td><strong>Risk Awareness in Silos</strong></td>
<td><strong>Integrated Risk Operations</strong></td>
<td><strong>Risk Part of Business Operations</strong></td>
</tr>
<tr>
<td>MANAGEMENT -Delegates risk to 2nd Line -Address major risk events</td>
<td>MANAGEMENT -Executive Risk Committee -Top risks identified -Risk Event Management</td>
<td>MANAGEMENT -Proactive Exec. Risk Committee/business aligned -Reporting from bottom up and top down -Risk and Issues managed by shared terms (taxonomy)</td>
<td>MANAGEMENT -Risk/Issue Reporting at all levels -Enhanced state is furthered by technology -Renewal processes exist for innovation and effectiveness</td>
</tr>
<tr>
<td>2nd LINE -Immature risk functions -Siloed goals/processes</td>
<td>2nd LINE -Chartered risk functions -goals, measures, reporting -Interactive Processes</td>
<td>2nd LINE -Risk functions specialize -Risk function processes draw on all risk/issue sources -Defined roles exist for shared processes</td>
<td>2nd LINE -Enhanced state is furthered by technology -Organized common risk and issue data for all</td>
</tr>
<tr>
<td>INTERNAL AUDIT -Annual Risk Assessment produces only audit plans -Audits focus on validating compliance, policy or process efficiencies</td>
<td>INTERNAL AUDIT -Annual Risk Assessment draws from 2nd Line functions, shares findings -Audits begin with detailed area risk assessment</td>
<td>INTERNAL AUDIT -Ongoing Risk Assessment draws from all risks -Audits evaluates risk management -Findings flow into RM activities and follow-up</td>
<td>INTERNAL AUDIT -Enhanced furthered by technology -Real-time Risk and Issues sharing, live risk assessment -Audit expertise for risk management operations</td>
</tr>
</tbody>
</table>

- **Risk Awareness in Silos**
  - MANAGEMENT
    - Executive Risk Committee
    - Top risks identified
    - Risk Event Management
  - 2nd LINE
    - Chartered risk functions - goals, measures, reporting - Interactive Processes

- **Integrated Risk Operations**
  - MANAGEMENT
    - Proactive Exec. Risk Committee/business aligned
    - Reporting from bottom up and top down
    - Risk and Issues managed by shared terms (taxonomy)
  - 2nd LINE
    - Risk functions specialize
    - Risk function processes draw on all risk/issue sources
    - Defined roles exist for shared processes

- **Risk Part of Business Operations**
  - MANAGEMENT
    - Risk/Issue Reporting at all levels
    - Enhanced state is furthered by technology
    - Renewal processes exist for innovation and effectiveness
  - 2nd LINE
    - Enhanced state is furthered by technology
    - Organized common risk and issue data for all

- **Unclear Risk Organization**
  - MANAGEMENT
    - Delegates risk to 2nd Line
    - Address major risk events
  - 2nd LINE
    - Immature risk functions
    - Siloed goals/processes

- **Risk Awareness in Silos**
  - MANAGEMENT
    - Executive Risk Committee
    - Top risks identified
    - Risk Event Management
  - 2nd LINE
    - Chartered risk functions - goals, measures, reporting - Interactive Processes
• Management - delegates “risk management” to 2nd Line
• Management - address major “issues” (risks) as they occur
• 2nd Line - functions informal and/or immature
• 2nd Line - Siloed and redundant at times
• Internal Audit - Our Risk Assessment serves our audit plan only
• Internal Audit - Audits mostly validate compliance, policy or process efficiency
Adequate

- Management - risk committee exists, reviews 2nd Line data
- Management - top risks (risk events) formally identified/managed
- 2nd Line - Clearly Chartered functions, with goals and measures
- 2nd Line - Interactive (across risk peers) processes defined
- Internal Audit - Our Risk Assessment draws from 2nd Line, shares...
- Internal Audit - Audits start with risk assessment of area
Enhanced

- Management - risk committee at Executive Level prioritizes and assigns risk management activities
- Management - risk management reporting - common components
- Management - risk and issues managed with shared terms/taxonomy
- 2nd Line - functions specialize in area of expertise
- 2nd Line - shared processes and defined roles across all functions
- Internal Audit - Ongoing risk assessment, connected with 2nd Line
- Internal Audit - Risk Assessment Reporting, shared perspective of whole
- Internal Audit - Audit findings flow into risk management processes
• Management - Enhanced state is furthered by technology; risk and issues reporting at all levels
• Management - Renewal and innovation processes added
• 2nd Line - shared technology eliminates redundancy
• 2nd Line - shared reporting moves towards one perspective of the whole
• Internal Audit - Risks and Issue shared in real time improving periodic risk assessment and audit planning risk assessment
• Internal Audit - Expertise developed to assess ideal risk management in the 1st and 2nd lines
Defining IA Risk Management input

WHERE ARE WE... are we mature enough to contribute...

• Controls based - extension of external audit (up to 1980’s)
• Process based - added effectiveness and efficiency (1980’s)
• Risk based - added “why should management care” (1990’s)
• Risk management - added “optimizing risk” top down (late 1990’s)
• Objective Based** - True Top Down, Objective Priorities “at Risk”

*Paul J Sobel “Auditors Risk Management Guide”
** Tim Leech and other thought leadership (ISO 31000)
Defining IA Risk Management input

- How can we adjust our processes to better fit risk management?
  - Taxonomies that match organizational area (ORGANIZATION)
  - Adding Risk Management questions to audit planning
  - Using Capability Maturity Models to define risk and control
  - Others?
**Taxonomy Example**

- Aligning risk and control buckets with business management
- A Taxonomy all can understand

<table>
<thead>
<tr>
<th>UT Audit Taxonomy</th>
<th>Taxonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance</td>
<td>1. Governance</td>
</tr>
<tr>
<td>1.1. Organizational Structure &amp; Accountability</td>
<td>1.1.  Board of Regents</td>
</tr>
<tr>
<td>1.1.2. Board Subcommittees</td>
<td></td>
</tr>
<tr>
<td>1.1.3. Institutional Leadership</td>
<td></td>
</tr>
<tr>
<td>1.1.4. Institutional Audit Committee</td>
<td></td>
</tr>
<tr>
<td>2. Finance</td>
<td></td>
</tr>
<tr>
<td>2.1. Financial Reporting</td>
<td></td>
</tr>
<tr>
<td>2.2. Asset depreciation</td>
<td></td>
</tr>
<tr>
<td>2.3. Accounts Receivable</td>
<td></td>
</tr>
<tr>
<td>2.4. Debt Service</td>
<td></td>
</tr>
<tr>
<td>2.5. Travel and Entertainment</td>
<td></td>
</tr>
</tbody>
</table>
**Capability Maturity Model Example**

- Evaluating Risk Management in the Audit
- **TERM ALIGNMENT**
- **MODEL ALIGNMENT**

### Management Oversight - Capability Assessment Tool

<table>
<thead>
<tr>
<th></th>
<th>Least Capable</th>
<th>Written and Communicated</th>
<th>Written</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective (Initiative or Business)</strong></td>
<td>Not written</td>
<td>Not written, but verbally communicated</td>
<td>Written</td>
</tr>
<tr>
<td><strong>Metrics Defined</strong></td>
<td>Not written</td>
<td>Implied Metrics</td>
<td>Defined Metrics</td>
</tr>
<tr>
<td><strong>Monitoring Robust</strong></td>
<td>No monitoring</td>
<td>Inconsistent monitoring</td>
<td>Defined Monitoring Processes and Reports</td>
</tr>
<tr>
<td><strong>Policies and Procedures</strong></td>
<td>No relevant policies or procedures</td>
<td>Verbal policies and procedures</td>
<td>Documented current policies and procedures</td>
</tr>
<tr>
<td><strong>Communications</strong></td>
<td>No formal communication channels</td>
<td>Meetings structured to provide communications</td>
<td>Defined Meetings and Communications Processes utilized to push down and pull up critical operational needs and risk</td>
</tr>
<tr>
<td><strong>Culture</strong></td>
<td>No culture management</td>
<td>Some emphasis on organizational ethics</td>
<td>Defined expectations to operate ethically and within organization standards</td>
</tr>
</tbody>
</table>

**Least Capable**
- Objective (Initiative or Business): Not written
- Metrics Defined: Not written
- Monitoring Robust: No monitoring
- Policies and Procedures: No relevant policies or procedures
- Communications: No formal communication channels
- Culture: No culture management

**Least Capable**
- Objective (Initiative or Business): Not written, but verbally communicated
- Metrics Defined: Implied Metrics
- Monitoring Robust: Inconsistent monitoring
- Policies and Procedures: Verbal policies and procedures
- Communications: Meetings structured to provide communications
- Culture: Some emphasis on organizational ethics

**Most Capable**
- Objective (Initiative or Business): Written and Communicated
- Metrics Defined: Defined Metrics
- Monitoring Robust: Defined Monitoring Processes and Reports
- Policies and Procedures: Documented current policies and procedures
- Communications: Defined Meetings and Communications Processes utilized to push down and pull up critical operational needs and risk
- Culture: Defined expectations to operate ethically and within organization standards

**Most Capable**
- Objective (Initiative or Business): Written, Communicated and Monitored
- Metrics Defined: Metrics Defined, Reviewed, and Innovated as necessary
- Monitoring Robust: Monitoring, focused on most critical objectives, operations and risks
- Policies and Procedures: Living policies and procedures, routinely adjusted and communicated as necessary
- Communications: Open Communications, with empowered employees capable of blowing the whistle and getting an immediate and appropriate response
- Culture: Engrained cultural expectations, exemplified by organizational leadership
Summary

• The world is changing, Risk alignment is happening
• How can we best add value to Risk Management
  • Educate
  • Assessments, 1st and 2nd Line of Defense
  • Improving our Services
  • Aligning our Services

• How else?
Be the Change Agent
Add Value with Collaborative Risk Management