THREE LINES OF DEFENSE & ASSURANCE MAPPING

IIA Ottawa April 8, 2015
Sharon M. Messerschmidt, CPA, CMA, CIA
Outline

- This presentation will bring together:
  - Three Lines of Defense: A tool for dialogue and understanding
  - Assurance Mapping: A complete view of organizational assurance

- Opportunity to share knowledge:
  - How the two were used together successfully in the international public sector
  - Lessons for the Canadian public sector
Why Three Lines of Defense?

- Financial Crisis
  - Something went wrong with risk management…
- Proliferation of Assurance Providers
  - Means to identify and assign responsibilities
- Defines Management’s Role in Assurance
  - Clarifies responsibilities
- Three Lines of Defense as a dialogue on assurance
  - Opportunity for organizational learning
IIA’s Position Paper

Useful and frequently quoted publication

Internal Audit’s role in the Three Lines of Defense
Management’s responsibility

- Within a defined area; risks are owned
- To manage risk to achieve objectives through effective control systems

This includes:

- Design and implementation of policies, procedures, systems and controls
- Managerial and supervisory review
Ensure first line controls are properly designed, in place and operating as intended

Typically Include:
- Enterprise Risk Management
- Internal Control Assurance Processes (COSO/SOX)
- Controllership for Financial Risks and Reporting
- Others...
Many 2\textsuperscript{nd} lines will be unique by organization:

- Oversight over regional or field based operations
- Program Audits of grants and contributions
- Payment gating and sampling reviews
- Specialized or Regulated Quality Control functions
- Management oversight committees (IT, HR, Program)
Features of 2nd Line assurance processes:
- Separate from first line chain of command
- Reliance is placed on this oversight
- Are not completely independent... still management
- There won’t always be a second line...
- Wide variance in degree of maturity of oversight provided.
Independent Oversight

- Internal Audit is the focal or coordination point
- There may be others...
  - Independent Evaluation
  - External Audit in some cases
  - Ethics, Investigations, Whistleblower etc.

- Key is independence and reporting lines
  - Must report internally to governing body
- Recognized professional standards
IIA’s Three Lines of Defense Model

The Three Lines of Defense Model

Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41
Model with Advisory Audit Committee:

Deputy Minister

Executive/Senior Management

Audit Committee

First Line of Defense

Responsible for Risk and Control

- Internal Control Systems, Processes
- Supervisory and Managerial Oversight

Second Line of Defense

Management Oversight Functions

- ERM
- ICFR
- Oversight Commit.
- Recipient Audits
- Gating/Sampling

Third Line of Defense

Independent Advice and Assurance

- Internal Audit
- Investigations/Ethics
- Office of Evaluation
- OCG Audits
- Other Departmental Audits

External Audit
Why Assurance Maps?

Assists understanding of assurance processes:

- Provides a visual and informative summary for governing bodies and senior executive
- Categorizes and assesses assurance processes
- Identifies gaps and overlaps in assurance
- Promotes collaboration and opportunities for reliance on other assurance providers
Assurance Maps Key Elements

- Quantitative: requires a framework to support identification of assurances:
  - For Risk Management - key corporate risks
  - For Internal Audit - Audit Universe, Business Process, Functional Areas...

- Qualitative: requires a means to assess the strength of the assurances provided
  - Simple (R-Y-G)
  - Maturity Model/COSO elements
## Assurance Map – Text Based

<table>
<thead>
<tr>
<th>Entity business risks (taken from an entity’s risk management plan)</th>
<th>Source and level of assurance provided</th>
<th>Overall assessment of level of assurance</th>
<th>Is level of assurance adequate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to recruit, develop and retain sufficient skilled staff to sustain core service delivery at required levels.</td>
<td>Work Area: low, Work Area: moderate, Management committees: (Human Resource Management) moderate, Internal audit: low, Other assurance activities: moderate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure to assess, monitor and appropriately manage key organisational requirements including resource and budget management in a changing business environment.</td>
<td>Work Area: low, Work Area: low, Management committees: (Executive Board) moderate, (External review) low, Other assurance activities: moderate</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Failure to adequately manage the entity’s complex contractual arrangements.</td>
<td>Work Area: low, Work Area: moderate, Management committees: (Executive Board) moderate, Internal audit: low, Other assurance activities: moderate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ineffective financial management.</td>
<td>Work Area: low, Work Area: low, Management committees: (Information Management) moderate, Internal audit: moderate, Other assurance activities: moderate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure to work with or manage implementation partners.</td>
<td>Work Area: moderate, Work Area: moderate, Management committees: (Finance) moderate, Internal audit: moderate, Other assurance activities: moderate</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Level of entity assurance and advice provided on the entity business risks — high, moderate, low. The level of assurance provided will depend on the extent to which the controls in place and other arrangements address the business risk.
Assurance Maps - Visual

http://www.bakertilly.co.uk/SiteCollectionDocuments/Social housing/Assurance Web Presentation.pdf
## Assurance Map – By Functional Area

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Second Line Assurance Processes</th>
<th>Second Line Assessment</th>
<th>Third Line Audits and Evaluations</th>
<th>Third Line Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IT</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Finance</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>HR</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
Assurance Maps

- Can be complicated…
- Need to suit your purpose and your organization
- Challenge to describe simply but with enough information to be useful.

- Assessing the strength of the 2nd lines is important
  - Consider doing with management
  - A maturity model provides good structure
## COSO-based Maturity Template

<table>
<thead>
<tr>
<th>Maturity Model for Second Line Assessment</th>
<th>Ad-hoc</th>
<th>Defined &amp; Directed</th>
<th>Mature and Monitored</th>
<th>Provides Assurance</th>
<th>Fully Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Control Activities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information &amp; Communication</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 1 - Do your Homework...

- Consider your framework – how detailed?
- Start to fill in what you know... 1\textsuperscript{st} and 2\textsuperscript{nd} lines
  - Determine your approach (risk, function, process etc.)
- You know a lot about the 3\textsuperscript{rd} line...
  - What will you include?
  - To what extent can IA rely on this work?
Step 2: Dialogue, Dialogue, Dialogue..

- **Meet with Management**
  - Explain model and their role in assurance
  - Confirm mutual understanding of 2\textsuperscript{nd} lines.

- **Do you want to assess the 2\textsuperscript{nd} lines with management?**
  - Is identification enough…
  - Maturity Model, options here…
  - Current and Future States
# Maturity Assessment by Function

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Current State</th>
<th>Current Level</th>
<th>Future State</th>
<th>Future Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Rating</td>
<td>Evidence</td>
<td>Rating by Area</td>
<td>Desired Improvements</td>
<td>Rating by Area</td>
</tr>
<tr>
<td>Internal Environment</td>
<td>Mature</td>
<td></td>
<td></td>
<td>Assured</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Directed</td>
<td></td>
<td></td>
<td>Mature/Assured</td>
</tr>
<tr>
<td>Control Activities</td>
<td>Assured</td>
<td></td>
<td></td>
<td>Assured</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>Mature</td>
<td></td>
<td></td>
<td>Assured</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Ad-hoc</td>
<td></td>
<td></td>
<td>Mature</td>
</tr>
<tr>
<td>Summary</td>
<td>Directed/Mature</td>
<td></td>
<td></td>
<td>Mature/Assured</td>
</tr>
</tbody>
</table>
Step 3: Prepare and Share

- How you will portray this will depend on your purpose...
  - Expectations of Senior Mgmt and Audit Committee
  - Culture and appetite of organization

- Sharing is important, will help determine next steps
  - Will IA need to validate 2nd line effectiveness?
  - Impact on Audit Plan....
## Second Line Assessment by Function

<table>
<thead>
<tr>
<th>Second Line Maturity</th>
<th>Ad-hoc</th>
<th>Defined</th>
<th>Mature</th>
<th>Assured</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program A</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Program B</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Info. Technology</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Administration</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
What you might learn...

- There can be a lot of traffic in high risk areas...
  - What can IA use from 2\textsuperscript{nd} and other 3\textsuperscript{rd} line reviews

- Importance of looking at “low risk” areas
  - Are there gaps? Are things as low risk as you think?

- What 2\textsuperscript{nd} lines does management rely on?
  - Have these been tested?
  - There can be a lot of value in auditing second lines...
## Detailed Assurance Map for IA

<table>
<thead>
<tr>
<th>Program</th>
<th>Key First Line</th>
<th>Second Line</th>
<th>Management Second Line Maturity Assessment *</th>
<th>Third Line (Since 2011-12)</th>
<th>Overall Assessment **</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System of Controls &amp; Review Committees</td>
<td>Defined Oversight and Approval Committees</td>
<td>Assured</td>
<td>Evaluations (5) and Audits (3)</td>
<td>Attention</td>
</tr>
<tr>
<td></td>
<td>Program Manual</td>
<td>Program Approval Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Centralized Systems</td>
<td>Oversight and Change Control Committees</td>
<td>Directed</td>
<td>Evaluations (0) and Audits (8)</td>
<td>Immediate Attention</td>
</tr>
</tbody>
</table>
Criticisms of the Model

- As an ERM tool seen as promoting risk aversion
  - Should be a way of stating how risks will be taken...
  - As an audit tool is an aid in supporting risk assurance

- Felt to not appropriately take into account external regulators and governing bodies
  - The “Five” Lines of Defense*…
  - Governance and Tone at the Top are considered in audit planning and risk assessments

*Protiviti Bulletin
When 2\textsuperscript{nd} and 3\textsuperscript{rd} Lines Intersect…

- Can’t compromise the effectiveness of 3\textsuperscript{rd} Line
- Clearly communicate the impact and get approval

- No management responsibility
- Formalize in audit charter
- Some roles may be temporary
- Outsource audits in these areas
- Ensure Duties are segregated.

Source: IIA Netherlands White Paper
Canadian Public Sector

- ERM and ICFR are key second lines
  - Are there others?
- What second lines are institutionalized?
  - Program audits, payment controls,
- External Audits, Special Examinations
  - Audits directed to your department
- Other Department and Agency Audits
  - Central Agency, Shared Services etc.
Key Takeaways

- Dialogue with management; enhance their understanding of their role in assurance
- Mapping of all key assurance activities; opportunity to clarify roles and responsibilities
- Understand the assurances that management relies on; identify gaps and overlaps in audit coverage
- More complete audit universe and synergy with other assurance providers
Do you have any questions or comments?

sharon.messerschmidt@sympatico.ca
+1 613 816 5777
## 2nd Line Maturity Model - Example

<table>
<thead>
<tr>
<th>Maturity</th>
<th>Ad-hoc</th>
<th>Defined &amp; Directed</th>
<th>Mature/Monitored</th>
<th>Provides Assurance</th>
<th>Fully Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Environ.</strong></td>
<td>No second line activities are in place; no central owner of the functional area is defined</td>
<td>The second line is assigned overall responsibility for the business function and some guidance is provided to the first line</td>
<td>Clear objectives and accountabilities are defined for first &amp; second line</td>
<td>Proactive and structured monitoring is performed on first line activities to ensure compliance, particularly in high risk areas</td>
<td>-Full cyclical auditing is undertaken to ensure controls are working to the agreed upon risk tolerance</td>
</tr>
<tr>
<td><strong>Risk Mgmt.</strong></td>
<td>Risk management is ad-hoc, done locally and is not coordinated.</td>
<td>Second line sets risk guidance and tolerance levels that the first line is responsible to follow.</td>
<td>Second line monitors risks reported by the first line, some investigation may be conducted on rising levels.</td>
<td>Second lines conduct assurance reviews over high-risk areas to provide assurance that mitigation efforts are effective.</td>
<td>Formal processes exist to identify emerging risks and trends. Annual audits are used for management decision-making on risk management activities.</td>
</tr>
<tr>
<td><strong>Control Activies</strong></td>
<td>First line is responsible for checking compliance to their own controls</td>
<td>Second line policies and guidance are in place but may not be mandatory</td>
<td>Policies, systems and standards are communicated and implemented setting out control expectations for the first line</td>
<td>The second line monitors the effectiveness of its own policies, systems and training programs by using its own assurance processes to drive improvement.</td>
<td>Assurance is conducted according to a cyclical and risk based plan; uses a formal methodology with sample plans, testing approaches, ratings</td>
</tr>
<tr>
<td><strong>Inform. &amp; Comm.</strong></td>
<td>-No reporting outside of the first on performance, risk and compliance.</td>
<td>Reporting to second line is mainly done on an issue or as needed basis.</td>
<td>Reporting requirements are defined; are regular and are formally agreed to between the first and second lines.</td>
<td>Reporting of First Line activity and results of assurance processes are used to drive future second line focus and business improvement.</td>
<td>Performance and risk management reporting incorporate the results of assurance of compliance and quality assurance activities</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>Review and monitoring activities are the responsibility of the first line.</td>
<td>Some monitoring and oversight may be provided by second line but is not regular in nature.</td>
<td>Embedded second line monitoring activities exist to confirm completeness and consistency of first line activities.</td>
<td>The second line performs structured and embedded monitoring to test and verify compliance of first line activities.</td>
<td>Independent quality reviews are commissioned by the second line and used to drive improvement.</td>
</tr>
</tbody>
</table>
Other Sources of Information

- IIA Audit Executive Center, *Assurance Mapping – Charting the Course for Effective Risk Oversight*, 2012