Fine-tuning Your Company’s Enterprise Risk Management Orchestra

Volker Pasternak, PhD
Director, Compliance and Legal, EPRI
Minel Diaz, CPA (Inactive), CGMA
Internal Audit Manager, VMware

May 17, 2019

Today’s Objectives

- How Compliance, Internal Audit, Risk, Legal, and other functions view their roles in risk management
- How assigning risk ownership can benefit the collaboration between functions
- Examples of collaboration: risk frameworks, lines of defense and reporting to the board
Agenda

ERM Refresher
Risk Ownership
Risk Management Orchestra
Example: Privacy Risk
Conclusion

What is your primary role in your organization?

- In-house (or outside) Legal Counsel
- Compliance Professional
- Risk Professional
- Privacy or Security Professional
- Internal Audit Professional
- Other
What is ERM?

"A process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and 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."

- Committee of Sponsoring Organizations (COSO)
### Why is ERM Important?

- Proactively address risks and seize opportunities
- Make better business decisions by understanding uncertainties, risks and opportunities
- An effective risk management can enhance enterprise resiliency
- Integrate ERM into company culture (transparency and risk awareness)
- Be risk intelligent vs risk averse

### Landscape of “Risk”

<table>
<thead>
<tr>
<th><strong>Types of Risks</strong></th>
<th><strong>Controls</strong></th>
<th><strong>Risk Owners</strong></th>
<th><strong>Management of Risks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational (process risks)</td>
<td>Measures to modify or mitigate risk.</td>
<td>Management holds overall responsibility for managing risk to the entity.</td>
<td></td>
</tr>
<tr>
<td>Financial (capital, financial markets, shareholder value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance (ethics, trade, regulatory, legal, environmental)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic (decision-making)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Risk Appetite**

Level of risk Management is willing to accept.
Risk Ownership

Importance of risk ownership (for every company risk)

- Ensures someone in the company is accountable for risks (and respective controls)
- Helps clarify roles for other stakeholders in support of the risk owner
- Ensures that the ERM function does NOT own the risk, but serves as facilitator

Avoid split or joint risk ownership, where possible (not always possible)

Who reports on ERM for your company?

- CEO
- Chief Risk Officer
- Chief Compliance Officer
- Legal
- Internal Audit
- Other
Fine-tuning Your ERM Orchestra

- Compliance, Internal Audit, Risk, Legal all have a legitimate role relating to company risk
- There are different roles (managing the ERM framework, owning a risk, providing support to the risk owner, monitoring a risk, auditing a risk, reporting on a risk)
- Who should have what role depends on company size, risk profile, structure and some intangible "people" aspects
- At a minimum, all stakeholders should agree that there can be no risk silos (all risks are subject to ERM)
- CEO ultimately "owns" effective risk management in the company (and can help fine-tune)

Effective Risk Management and Control – 3 Lines of Defense

Risks:
- Strategic
- Operational
- Financial
- Compliance

1st Line of Defense:
- Improve controls and processes
- Operations and Business Units
- Management Controls
- Internal Control Measures

2nd Line of Defense:
- Optimize risk management functions
- Management Assurance
- Financial Controller
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense:
- Independent Assurance
- Internal Audit

Governing Body / Audit Committee
Senior Management
## Role of Internal Audit in ERM

### Core IA roles in regard to ERM
- Give assurance on risk mgmt process
- Give assurance that risks are correctly evaluated
- Evaluate risk mgmt process
- Evaluate reporting of key risks
- Review management of key risks

### Legitimate IA roles with safeguards
- Facilitate identification and evaluation of risks
- Coach Mgmt in responding to risks
- Coordinate ERM activities
- Consolidate reporting on risks
- Maintain and develop ERM framework
- Champion establishment of ERM
- Develop RM strategy for board approval

### Roles IA should not undertake
- Set risk appetite
- Impose risk management processes
- Manage assurance on risks
- Making decisions on risk response
- Implement risk response on Management’s behalf
- Accountable for risk management

---

**Do you collaborate with your Internal Audit (IA) Department?**

- Yes, most of the time
- Occasionally
- Never/ I don’t know if we have an IA Dept
- N/A - I am apart of IA
Potential Roles of Compliance in ERM

Depending on a company’s risk role allocation, Compliance can

- "Own" certain Compliance risks (e.g., gifts, conflicts) as first line of defense
- Provide input on controls (e.g., policies) to risk owners
- Work with risk owners on training and communication
- Monitor certain Compliance risks as the second line of defense
- Highlight emerging risk areas and bring stakeholders together to address
- Report on Compliance risks to Management and the Board
- Play a broader ERM role as assigned

ERM Risk: Privacy
Privacy Risk

- What personal information is collected?
- How important is that information to organizational objectives?
- What could go wrong in collection and handling?
- What is the likelihood that the risk will occur?
- What will be the impact?
- Is this a risk with high velocity (e.g., changing landscape)?
- What are the current controls in place? What gaps are there?
- How do we "treat" the risk: a) avoid/eliminate/transfer; b) mitigate; c) accept

<table>
<thead>
<tr>
<th>Who owns privacy risks in your organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>HR</td>
</tr>
<tr>
<td>Information Security (IT)</td>
</tr>
<tr>
<td>Business Unit</td>
</tr>
<tr>
<td>Cross functional group (shared risk owners)</td>
</tr>
<tr>
<td>I don’t know</td>
</tr>
</tbody>
</table>
Potential Role Allocation

<table>
<thead>
<tr>
<th>Role Description</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk ownership</td>
<td>Business units that need the data for their business purposes:</td>
</tr>
<tr>
<td></td>
<td>- HR for employee data</td>
</tr>
<tr>
<td></td>
<td>- Customer Relations for customer data</td>
</tr>
<tr>
<td></td>
<td>- R&amp;D for research data</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Risk owner(s) with input from Compliance, Legal, Risk functions</td>
</tr>
<tr>
<td>Interpretation of current and future laws</td>
<td>Legal</td>
</tr>
<tr>
<td>Policies, training, trends</td>
<td>Compliance</td>
</tr>
<tr>
<td>Data mapping/security</td>
<td>IT / Chief Information Officer (could also be listed as risk owner)</td>
</tr>
<tr>
<td>Assurance</td>
<td>Internal Audit (could also support assessment)</td>
</tr>
<tr>
<td>Reporting</td>
<td>Risk function (if it exists) on overall ERM framework</td>
</tr>
<tr>
<td></td>
<td>Risk owner(s) on specific Privacy risk (may need consolidation)</td>
</tr>
</tbody>
</table>

Conclusion

- No one-size-fits-all ERM program
- Clarify ERM and risk ownership and roles
- Collaborate in fine-tuning the ERM orchestra
- Remember the 3 lines of defense
- Everyone is a risk manager
What is your key takeaway?

Top

Thank You!
Speaker Background

Volker Pasternak

Volker Pasternak is a multilingual attorney qualified in California, England & Wales and Germany with experience both in-house and in a “magic circle” law firm Compliance & International Legal at the Electric Power Research Institute. He works as Director of the Electric Power Research Institute (EPRI) in Palo Alto, California, with a broad range of legal, compliance, risk management, and strategic business responsibilities. Prior to joining EPRI, he was a solicitor in Freshfields Bruckhaus Deringer’s IP/IT and China practice groups, based in Hong Kong and the firm’s London headquarters, with stints in Beijing, Shanghai and Frankfurt. Volker holds a Ph.D. in Chinese studies, international law and philosophy of law from the University of Göttingen, Germany, and recently completed the Stanford Certificate in Strategic Decision and Risk Management. He knows a number of European and Asian languages, and enjoys speaking and writing on emerging issues in compliance, risk management and international law.

Minel Diaz

Ana Melita “Minel” Diaz is a Certified Public Accountant (currently inactive) in the State of California, and has over 15 years of experience in providing accounting, auditing and business advisory services to clients. She currently works as Internal Audit Manager – Americas, at VMware in Palo Alto, California, helping the AMER business navigate through risks and opportunities by ensuring the effectiveness of controls and processes. Prior to VMware, she was Corporate Audit Manager at the Electric Power Research Institute (EPRI) in Palo Alto, CA, where she was responsible for the internal audit function, and championed the ERM program at EPRI in collaboration with Ethics & Compliance. Minel started her career working for a regional CPA firm in Southern California. She earned her Bachelor of Science degree in Accountancy at Loyola Marymount University in Los Angeles, California.

The contents of this presentation represent the presenters’ personal interpretations, thoughts, and applications of published concepts, and do not represent their employers’ views.

COSO, the IIA and RIMS have created an impressive body of knowledge in this area. All references herein are to publicly available information and respect the owners’ respective intellectual property rights.