Maximizing value from your lines of defense

A pragmatic approach to establishing and optimizing your LOD model

Insights on governance, risk and compliance

December 2013
Contents

Introduction
Are you getting the maximum value out of your lines of defense? .......................................................... 1

Why implement a LOD model? ............................................... 2

Start with a solid foundation ............................................... 3

Integrated LOD operating model ....................................... 4

Working elements of an integrated LOD operating model... 6

Establishing and optimizing your LOD operating model.... 8

Conclusion
Mapping key risks to organizational roles and responsibilities is essential for effective risk management................................. 10
Introduction

Are you getting the maximum value out of your lines of defense?

The Lines of Defense (LOD) model has been cited extensively as an effective model to use for risk management.

The Institute of Internal Auditors (IIA) recently released a position paper stating that the “Three Lines of Defense” model provides a simple and effective way to enhance communications on risk management and control by clarifying roles and duties.1

Some of the questions we are being asked by clients include:

- How successful have companies been in practically implementing this LOD model?
- Where the model is established, how are the lines of defense coordinated, such that the board is not filtering through mountains of duplicate (and often conflicting) information but still gets assurance that all relevant risks are appropriately managed?
- Many companies have invested in identifying and prioritizing risks, but how much assurance does the board have that these risks are being managed in accordance with the company’s risk appetite?
- Has risk management been embedded in the organization not just as a tool for risk functions but as an organizational business performance enabler, and what does this look like in practice?

This paper sets out EY’s point of view on a practical implementation approach to help organizations establish and optimize the LOD operating model. EY’s Risk Agenda outlines our research into leading practices for using risk management to enable business performance. We will demonstrate how this agenda aligns with the LOD operating model.

---

The current economic environment and significant risk events over the last few years have caused companies to have a renewed focus on the effectiveness of risk management. Substantial amounts have been spent on risk management activities and reorganizing companies to best manage risk in line with various frameworks and models.

However, many companies now feel overwhelmed with the amount of risk management activity and have failed to reap the benefits of their investment in risk management. In our view, a logical and coordinated approach to risk management is integral to its success.

Companies that do not have an established or well-coordinated LOD operating model are likely to experience one or more of the following challenges:

- **Complex and inconsistent reporting makes it difficult for the board and executive management to provide effective risk oversight**
  The board and executive management receive multiple unaligned reports containing redundant and often conflicting information. They struggle to find a comprehensive view of the key risks that face the company and how these risks are being managed.

- **Gaps in risk coverage**
  Although increasing amounts are being spent on risk identification, controls, assurance and ERP systems, the company still experiences significant control failures and unexpected risk events.

- **Siloed risk functions, which reduces value and increases cost**
  There is an ineffective deployment of resources due to a lack of harmonization between risk and assurance providers — these functions are connected via informal channels and work with different risk categorizations, terminologies, approaches, rating scales and technologies. Consequently, limited resources may end up focused on the wrong areas.

- **Business fatigue**
  Multiple uncoordinated interactions between risk and assurance functions lead to confusion in the business and to questions about the value and effectiveness of these functions.

- **Confusion**
  Management has one view of an organization's risk profile, while risk functions have a different view. Risk activity consequently goes in many different directions without realizing real value.

- **Layers of redundant controls**
  Not having a holistic understanding of controls in place to manage risks and a lack of clarification of responsibilities may lead to duplication in control activities and increased cost of control.
Start with a solid foundation

In EY’s *Turning risks into results: how leading companies use risk management to fuel better performance* research report, we presented our Risk Agenda (set out below) which organizes leading risk practices into six components.

### The RISK Agenda: client issues

**Enhance risk strategy**
- Improve the overall alignment of risk with corporate goals, major initiatives and emerging market trends
- Clarify the definition of “risk” and determine the management and board’s risk appetite and overall tolerance levels
- Communicate overall risk strategy to key stakeholders
- Clarify and strengthen risk oversight at the board and executive management levels
- Deliver greater transparency and accountability at all levels in the organization

**Embed risk management**
- Define the key “risks to own” that drive growth and create value (day-to-day business, change programs, emerging business)
- Invest differentially in the strategic “risks that matter” to better enable performance
- Link risk management to business planning and performance management
- Align key risk indicators (KRI) with key performance indicators (KPI) and key control indicators (KCI)

**Improve controls and processes**
- Reduce cost of controls spend
- Leverage automated controls vs. manual controls
- Implement more prevent vs. detect controls
- Optimize controls around key business and IT processes
- Monitor critical controls and KPIs continuously to improve decision-making and performance results

**Optimize risk management functions**
- Improve the effectiveness and efficiency of individual risk management functions
- Reduce redundancies and overlap in risk coverage
- Coordinate risk activities and align skills to better leverage existing infrastructure and resources

### Turning risk into results

**Enable risk management**
- Harness technology to enhance and more effectively enable risk management, controls and processes

**Communicate risk coverage**
- Improve transparency and frequency of stakeholder communications
- Provide greater assurance to customers and stakeholders through independent, third-party verifications

### A solid foundation is essential to having an effective LOD operating model. Consequently, a framework consisting of the elements of the Risk Agenda has to form the base. At a minimum, the following should be in place:

- A strong risk culture across the organization.
- A clear definition and communication of risk appetite by the board or executive management.
- A standard language or methodology for identifying, evaluating, measuring and reporting risk.
- A robust governance risk and compliance (GRC) system to support risk identification, assessment, issue tracking, monitoring, assurance and reporting.
- A standardized enterprise-wide risk assessment process that produces a key business risk universe or register linked to business objectives and value drivers. All company entities should be covered and the nature of risks comprehensive, e.g., financial, operational, strategic, regulatory, information technology, corporate governance and ethics, and emerging risks.
- Responsibility for coordinating and reporting all risk, control and assurance activities assigned to one person or function.
- Risk owners (overall responsibility) assigned to each risk – this should not create an additional layer within the organization. The most obvious choice for risk owners are those responsible for managing a particular risk as part of their everyday jobs.
EY defines the lines of defense as follows:

- **First line (operations and business units):** Line management responsible for identifying and managing risks directly (design and operation of controls). This group has to regard risk management as a crucial element of their everyday jobs. In line with leading practices in our Risk Agenda, we also recommend optimizing controls when risks have been mapped as this activity will highlight any inefficiencies and gaps. Our recent paper on “Smart Control” provides insight into optimizing controls.2

- **Second line (management assurance):** The groups responsible for ongoing monitoring of the design and operation of controls in the first line of defense, as well as providing advice and facilitating risk management activities. These are usually management functions that may have some degree of objectivity, but are not entirely independent from the first line.

- **Third line (independent assurance):** The groups responsible for independent assurance over managing of risks. This line includes internal audit, external audit and some regulators, as long as the scope and nature of their work aligns with the organization’s risk management objectives. Again, in line with the Risk Agenda, a leading practice would be to optimize the risk management functions in the second and third lines using a risk convergence or combined assurance model.

---

2Smart Control – Transforming controls to reduce cost, enable growth and keep the business safe, January 2013.
In our view, the key to the practical implementation of an integrated LOD operating model is to focus on the organizations’ individual risks and let all activities (i.e., managing, monitoring, assurance, issue tracking, reporting) flow from the risks.

As shown in the model opposite, risks based on the organization’s business objectives and value drivers are mapped to accountabilities in each of the lines of defense. Reports are combined across the lines for each of these risks and then provided to the board and executive management. We have highlighted how elements of the Risk Agenda align: these outline the leading practices in establishing and optimizing a LOD operating model.

If a company claims to have a LOD model, but cannot produce a comprehensive mapping of risks to the lines of defense, then the effectiveness of that model is debatable. Risks should be mapped across the lines based on the company’s risk tolerance and risk monitoring strategy as communicated by the board and executive management. For example, some companies could choose to have all risks mapped to all three lines, while others focus only on significant risks and are content with mapping one or two lines for other risks.

In our experience, this risk monitoring strategy varies depending on the business sector; for example, companies in highly regulated sectors such as banking, insurance, healthcare and oil & gas, are likely to have a greater number of key risks mapped to all three lines than companies in less regulated sectors. Other factors such as the company’s risk management maturity, tone at the top, and other entity level controls, can also determine the degree of use of model lines. Regardless of the balance between the lines chosen for each risk, there should be a consolidated view of the risk measures and status of risk management for each risk.

Functions within each of the lines of defense will vary from company to company and some functions may even be split across the lines. For example, some parts of a compliance function may be involved in designing controls for the first line of defense, while other parts are monitoring controls as the second line of defense; this is often seen in the financial services sector. As long as accountabilities are mapped for individual risks, this creates clarity as to the role, regardless of the function.

The depth of risk to which accountabilities are mapped is a function of company choice, risk management strategy, and the robustness of the company’s GRC technology system. While some companies may map accountabilities to a very comprehensive risk register down to the level of business unit and processes, others fix the mapping at the entity level risks.
Working elements of an integrated LOD operating model

The key elements of an integrated LOD operating model include the following:

> Each risk has a clear link to the responsible owner in the relevant line of defense.
> Clear roles and accountabilities are assigned across the three lines and documented in the form of charters to enable work activities. Where clear accountabilities are documented, there can be no wrong assumptions as to the responsibility for risk, controls and assurance. The IIA paper states that “Clear responsibilities must be defined so that each group of risk and control professionals understands the boundaries of their responsibilities and how their positions fit into the organization’s overall risk and control structure.”
> Each line has adequate skills to discharge its responsibilities. This is usually straightforward in the first line, but can be more complex in the second and third line. Many monitoring and assurance functions do not contain deep knowledge of the business or industry, which provides a challenge in gaining the respect of the first line. A recent EY survey revealed that Internal Audit functions are increasingly expected to provide more business insight and act as strategic advisors.³
> Executive management and the board receive one combined report showing the status for individual risks. An example is shown in the graphic below.

### Individual risk status report

<table>
<thead>
<tr>
<th>Contributing factors</th>
<th>Inherent risk rating</th>
<th>Current controls</th>
<th>Lines of defense</th>
<th>Residual risk rating</th>
<th>Status and comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Inadequate management process and support for evaluation of internal controls</td>
<td>Red</td>
<td>• Internal control framework</td>
<td>Owner</td>
<td>1</td>
<td>Green</td>
</tr>
<tr>
<td>• Lack of effective documentation and tracking process for SOX 404 compliance including systems</td>
<td></td>
<td>• Management sponsorship of internal control identification and evaluation processes</td>
<td>Activity</td>
<td></td>
<td>▲ Controls testing in the last two quarters have not revealed any deficiencies</td>
</tr>
<tr>
<td>• Enterprise-level controls do not provide sufficient focus or support to enable consistent and accurate tax accounting and disclosure</td>
<td></td>
<td>• Internal control documentation and testing processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• GRC system</td>
<td></td>
<td>• Developing and operating internal controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk no. 5 — Significant or material weaknesses resulting from inadequate internal financial controls</td>
<td></td>
<td>• Control self assessment – 5 processes last quarter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Q2 Quarterly disclosure meeting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Group internal controls</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supporting development of internal control framework and processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maintaining process and control documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ongoing monitoring of processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Owner</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Group internal controls</td>
<td></td>
<td><strong>External audit</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Q2 spot testing of controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interim testing of controls</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key:
- ▲ No issues
- ★ Process improvement or increased formalization
- ★ Gap or control failure warranting attention
Clear communication protocols are established between the lines, risks, associated controls and assurance activities, defining the information to be exchanged and when.

Risk owners are responsible for collating all information from across the lines for their risks. If they have specific points of contact in the other lines, they should not have to deal with multiple requests for information.

A person or function is assigned responsibility for administering the model and overall coordination of reports.

A single technology system is used for all data input, and from which reports are generated for individual risks (as shown in the graphic below). At any point in time, the status of individual risks, associated controls assurance activities can be reviewed.

---

**Integrated risk and control reporting**

![Diagram of integrated risk and control reporting](image-url)

---

3 Matching Internal Audit talent to organizational needs: key findings from the Global Internal Audit Survey 2013.
Establishing and optimizing your LOD operating model

1. Gather information and plan
   - Define requirements, assign responsibilities for implementing and overseeing the integrated model and develop specific implementation plan, (typically the role of a company’s risk officer or the risk function)
   - Gather information to understand risk appetite
   - Understand business objectives, value drivers and key risks
   - Gather information on management assurance functions and activities, their scope of work and mandates
   - Gather information on internal and external assurance providers, their scope of work and mandates
   - Obtain an understanding of the executive and board committees and their requirements with regard to risk oversight and reporting

2. Create a risk coverage map
   - Agree on a methodology and template for mapping coverage based on the company’s risk appetite and risk management framework
   - Map risks to processes and controls (first line of defense)
   - Map risks to accountabilities for management assurance (second line of defense)
   - Map independent assurance (third line of defense)
   - Validate the risk coverage map with key stakeholders

Example of a risk coverage plan

<table>
<thead>
<tr>
<th>Critical risk</th>
<th>Link to business strategy</th>
<th>Risk ranking</th>
<th>Risk owner</th>
<th>Root causes</th>
<th>Critical controls to mitigate critical risk</th>
<th>1st line of defense</th>
<th>2nd line of defense</th>
<th>3rd line of defense</th>
<th>Assurance gap?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Control owner</td>
<td>Management monitoring of controls</td>
<td>Independent assurance providers</td>
<td>Assurance gap?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Management reviews
- Key risks
- Group compliance
- Group risk
- Group legal
- Internal audit
- Independent performance evaluation
- External legal specialists
- Department of labor
- Department of environmental affairs
- Insurance
- Special projects
3. Analyze the risk coverage map to determine adequate coverage
   ▶ Assess the completeness of risks
   ▶ Assess controls for consistency and completeness in relation to risks
   ▶ Assess competence of management and independent assurance providers in relation to the specific risks mapped
   ▶ Assess current risk, control and assurance reporting mechanisms
   ▶ Identify duplication or gaps in controls or in the management and independent assurance activities for each risk
   ▶ Develop a remediation plan

4. Implement remediation plan to optimize risk management coverage
   ▶ Streamline and optimize controls
   ▶ Clarify all roles and responsibilities and assign additional roles, as necessary
   ▶ Remove duplication in second and third lines of defense
   ▶ Train and develop skills to align with roles above
   ▶ Develop communication and reporting protocols
   ▶ Develop integrated reports for executive management and board that aggregate results from all management and independent assurance providers for each significant risk area
   ▶ Drive to get all parties on the same page about the roles and expectations of them within the model, particularly the first line of defense because managing risks is their everyday problem

5. Maintain LOD model
   ▶ Regularly review, monitor and update the LOD model to ensure it remains current
   ▶ Update on an ongoing basis with results of testing, any issues and risk events
Conclusion

Mapping key risks to organizational roles and responsibilities is essential for effective risk management.
A comprehensive mapping of key risks to organizational roles and responsibilities simplifies the effective and efficient operation of the LOD operating model.

This helps to enable the organization to operate its risk management activities on an integrated basis and provide seamless reporting to the board. A consolidated view of all risk information for each risk will provide the board with ongoing comfort that risks are being managed in accordance with the company’s risk appetite and that valuable resources are not being wasted.

EY’s suggested approach is to provide a framework that embeds risk management within the entire organization, such that a common language is spoken and that there is seamless, comprehensive coverage of risks.

Call for action

Does your company have an effective LOD operating model, and if so, are you reaping its benefits?

Boards should consider whether they can answer the following questions:

- Does executive management and the board have a clear view (in some form of risk coverage map) of how each significant risk is being managed on an ongoing basis?
- Does the board feel that the right risk and compliance activities are being performed for the organization’s key risks?
- Does management understand the board’s risk appetite, and is that evidenced in the reporting on risks?
- Does the board feel that risk management is embedded in the organization and is part of the day-to-day culture?
- Is the board comfortable that there are no gaps in risk management?
- Does the board have visibility on action being taken on any gaps in risk management?

If the answer to more than one of the above questions is negative, the board should engage with management and the risk management functions to assess the LOD operating model in the organization. If necessary, steps should be taken to transform existing processes to have a seamless LOD operating model that flows with the rhythm of the business.
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on business and IT risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at ey.com/GRCInsights

Smart Control: transforming controls to reduce cost, enable growth and keep the business safe
www.ey.com/smartcontrol

Turning risks into results: how leading companies use risk management to fuel better performance
www.ey.com/TRIRperformance

Matching Internal Audit talent to organizational needs: key findings from the Global Internal Audit Survey 2013
www.ey.com/iAsurvey2013

Unlocking the power of SAP’s governance, risk and compliance technology
www.ey.com/SAPgrc

Key considerations for your internal audit plan: enhancing the risk assessment and addressing emerging risks
www.ey.com/iaplan

Business pulse: exploring dual perspectives on the top 10 risks and opportunities in 2013 and beyond
www.ey.com/businesspulse2013
At EY, we have an integrated perspective on all aspects of organizational and IT risk. We are the market leaders in internal audit, financial risk and controls, and information security. We continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver services focused on the design, implementation and rationalization of controls that can potentially reduce the risks in our clients’ applications, infrastructure and data.
About EY’s Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our IT Risk Advisory services speak to your local EY professional or a member of our team.

Global RISK Leader

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>+31 88 40 71271</td>
<td><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></td>
</tr>
</tbody>
</table>

Area RISK Leaders

<table>
<thead>
<tr>
<th>Region</th>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>Jay Layman</td>
<td>+1 312 879 5071</td>
<td><a href="mailto:jay.layman@ey.com">jay.layman@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td>Jonathan Blackmore</td>
<td>+44 20 7951 1616</td>
<td><a href="mailto:jblackmore@uk.ey.com">jblackmore@uk.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td>Shohei Harada</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:harada-shh@shinnihon.or.jp">harada-shh@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

© 2013 EYGM Limited.
All Rights Reserved.

ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights