Deloitte.

Practical Enterprise Risk Management (ERM)

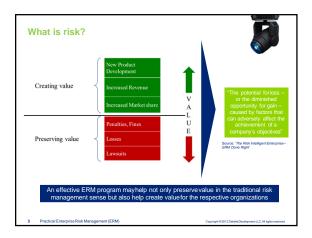
Casualty Loss Reserve Seminar, Fall 2013





| Agenda | |
|--|---|
| ERM 101 | 2 |
| Building an effective ERM program | 8 |
| Case study | 28 |
| Lessons learned | 34 |
| Q&A | 38 |
| | |
| | |
| 1 Practical Enterprise Risk Management (ERM) | Copyright @ 2012 Deloite Development LLC. All rights reserved |

ERM 101





What is ERM?

Practical Enterprise Risk Management (ERM)

- Enterprise Risk Management is a capability that involves identifying, assessing, measuring, monitoring, and responding to risks across the enterprise in a way that is aligned with the enterprise's objectives and risk appetite.
- The premise of ERM is that it attempts to present an overall and integrated view of the risks to which an enterprise is exposed.
- Effective ERM programs may ultimately lead to the Risk Intelligent Enterprise ™

| | Traditional Approach | Risk Intelligent Approach |
|---|--|--|
| Risk Interactions and Scenario Analysis | Focus only on the individual risk events without considerations for its long term impact or risk interactions | Study interactions between separate individual risks Assess risks using scenario analysis |
| Siloed Risk Management | Different risk language and risk management approaches across the organizational silos Poor communication across these silos | Define a common risk language that cuts across silos Coordinate roles and responsibilities across the organization Rationalize and standardize controls for risk management |
| Ollewalded Risk vs. Rewarded Risk | Focus on compliance, security, financial issues Mitigating risks of fraudulent activities, physical safety | Take calculated risks to obtain a competitive advantage Take risks for attracting more and high- value customers |







Why ERM?

- An effective ERM program may help:
- Identify and manage cross-enterprise risks
- Create a risk-aware culture
- Enable focus on the risks that matter most through integrated management reporting
- Reduce vulnerability to adverse events
- Align risk appetite and strategy
- Link growth, risk, and return

Practical Enterprise Risk Management (ERM)

- Decrease operational surprises and losses
- And more...

How to build an effective ERM program

| | # | Recommendations | <6 months | 6-12 months | >12 months |
|------------------------------------|----|--|-----------|-------------|---------------|
| Risk Prnan ce | | Develop a standard definition of risk and a framework to enable proactive management of risk | | | ±==> |
| Risk Governan | 62 | Rationalize and realign risk management function | | | |
| -5 | н | Develop talent management model to optimize staffing levels | | | · · · · |
| | 12 | Develop and implement a formal training and communication program | | | > |
| Risk Infrastructure Man agement | 13 | Develop a technology strategy to support the Risk and Compliance group | | | \rightarrow |
| Ris. | 14 | Improve timeliness and ease of obtaining data | | | |
| | P1 | Strengthen documentation and promulgation of policies and procedures | | | > |
| vershig | P2 | Institutionalize risk assessment and measurement | | | |
| Risk Ownership | P3 | Develop Key Risk Indicators (KRIs) tied to Key Performance Indicators (KPIs) | | | :t::::5 |
| ų, | P4 | Enhance reporting standards | | | · · · |

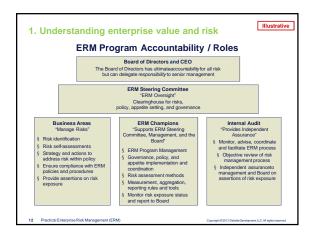


| _ | Activity | Illustrative Components |
|---|--|---|
| | Understanding enterprise risk & value | Definition of risk, policies and procedures, business strategies, organization objective |
| ~ | Develop risk framework | Risk map, rating agency framework |
| e | Develop risk appetite | Risk rating criteria (impact, vulnerability, speed of onset) |
| 4 | Assess & prioritize risk | Risk register, heat map |
| ŝ | Quantify risk | SME working groups led by CFO |
| 9 | Develop action plan | Risk limit, delegation authority |
| 2 | Monitor and reporting | Risk dashboard |
| ~ | Integrate risks into strategic decisions | Strategic planning process, internal audit plan |
| | | |

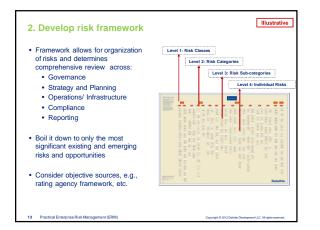




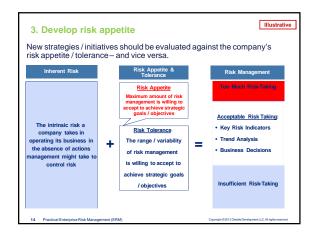




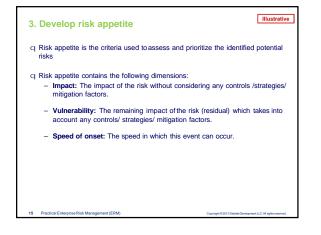










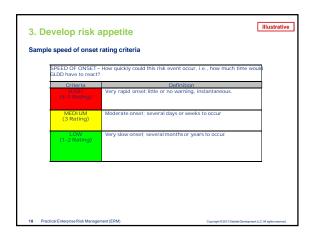


| Sample i | npact rating | criteria | | | | |
|----------------------|--|---|--|--|--|---|
| Impact Criteria | Financial | Reputation | Customers | Operations | Employees | Legal/Regulatory |
| MEDIUM (3 Rating) | 5 rating: Greater than SOX million impact on earnings before taxes 4 rating: Greater than SOX million and tess than SOX million impact on earnings before taxes 3 rating: Greater than SOX million and less than SOX million taxes | Internationalimational media attention Significant negative impact on reputation have long-laading impact Regional media attention Some negative impact on reputation and brand, not likely to have long-laading impact | Wdespread impact on customer satisfaction Serious threat to future grow th. Inability to self Decline in customer satisfaction Impact on sales | Significant Interruptions of business operations of countries 2 or more divisions of countries Detectual losses may be considered Intercoverable Moderate Interruptions of business operations of business operations of a rome divisions of countries Patential losses are roomable in the short sam (12 - 24 months) | Upplaned loss of employees Serious injury to employees and/or dangerous near mised on employee nutrations, relations near masks, and morale Upplaned loss of Serveral employees Same impact on employee relations, relations, nates, and morale | Major foderal or state sorutiny Investigations subject to substantial fines and panalite including criminal charges and/or cease-and- desist orders Possible regulatory action Moderate or routine fideral and state litigation subject to penalities, subject and substantial fines or penalities, subject and regulatory proceedings and/or hearings |
| LOW (1-2 Rating) | 2 rating: Greater than \$XX million and less than \$XX million impact on earnings before taxes 1 rating: Less than \$XX million impact on earnings before taxes | Minimal local media attention Minimal or no negative impact on reputation and brand with primarily short-term impact | Minimal of isolated impact on customer satisfaction Minimal complaints and recovery costs | | Unplanned loss of a single employee No impact on employee relations, retention rates, and motale | Unaxory or remote chance of oriminal enforcement, civil enforcement, and/or litigation |

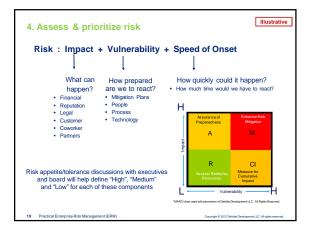
| |
|------|
| |
| |
| |
| |
| |
| |
| |
| |

| Sample v | ample vulnerability rating criteria | | | | | | |
|-----------------------|--|--|--|--|--|--|--|
| Vulnerability | Mitigation/Monitoring Complexity Decels Decessory | | | | | | |
| HIGH (4-5 Rating) | 5 rating: No mitigation/monitoring plans exist | Risk affects a high # of transactions or a high # of | Limited level of internal staff capable of managing risk potential | 5 rating: No effective process in place to manage the risk | enabled process) Major systemperformance, reliability and validity issues | | |
| | 4 rating: Mtigation/monitoring plans exist but are not consistently applied | processes Transactions are highly subject to judgment and | Limited accessto resources Significant level of change | 4 rating: Process in place but not consistently followed and/or no monitoring, testing or reporting of process | Significant security exposun Outdated and ineffective technology | | |
| | | estimation | experienced by resources as a result of risk event | Significant level of change required to business process as a result of risk event | Significant changes required to systems as a result of risk event | | |
| MEDI UM (3 Rating) | Mitigation/monitoring plans need to be updated and/or improved | Risk affects a medium # of transactions or a medium # of processes Moderate | Moderate level of internal staff capable of managing risk potential Moderate access to resources | Process is in place but is in need of improvement (e.g., may be overly complex or manually driven) Monitoring, testing and/or reporting of process needs improvement | Moderate data & system performance, reliability, and validity issues Moderate level of change required to systems as a peut of risk event | | |
| | | subjectivity to judgment and estimation | Moderate level of change experienced by resources as a result of risk event | Moderate level of change required to business process as a result of risk event | | | |
| LOW (1-2 Rating) | 2 rating: Mtigation/monitoring plans are in place, consistently applied and | Risk affects a low # of transactions or a low # of processes and low | Sustainable level of employees capable of managing risk potential | Clear, effective and consistently followed process to manage the risk is in place Any necessary monitoring, testing and/or | Minimal data& system performance, reliability and validity issues | | |
| | routinely tested; 1 rating: | subjectivity to judgment and estimation | Readily available resources | reporting of process has been effectively implemented | Minimum level of changes required to system as a resu of risk event | | |
| | Mitigation/monitoring plans are an integral part of standard operations | | Minimal level of change experienced by resources as a result of risk event | Minimal level of change required to business process as a result of risk event | | | |

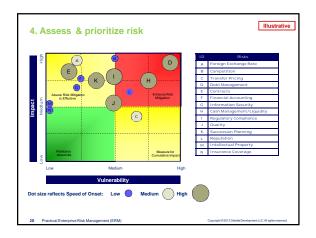








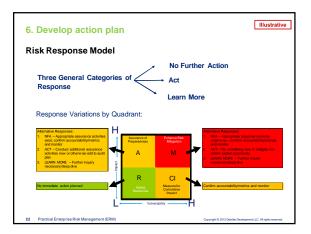




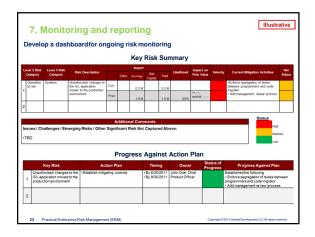














| Risk Name | | Owner: | | |
|--------------------------------|---------------------------|---|--|--|
| Risk Description | | Advisor: | | |
| Owner / Advisor Assessment: | BRAT Trend Assessment: | Key Risk Drivers: | | |
| Key Response A | ctivities/Initiatives: | Factor 2 Factor 3 | | |
| | | Factor 3 Factor 4 | | |
| • A | ctivity 1 | | | |
| • A | ctivity 2 | | | |
| • A | ctivity 3 | | | |
| | stivity 4 | Key Metrics: | | |
| • 4 | ctivity 4 | Metric 1 | | |
| | | Metric 2 | | |
| | | Metric 3 Metric 4 | | |
| | | Metric 4 Metric 5 | | |
| | | - Weble 5 | | |
| Owner / Advisor | Assessment Key | BRAT Trend Assessment Key | | |
| Stay the Cour. Modify. | Change Course Change from | Risk/Lost Opportunity Increasing Deportunity Deportuni | | |



8. Integrate risks into strategic decisions

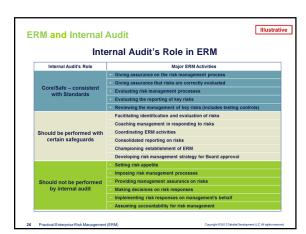
Build risk considerations into strategic planning process

Illustrative

- What are potential risks (both internally and externally driven) to the success of this strategic initiative?
- How will each potential risk be monitored?
- What contingency plans and/or mitigation mechanisms are in place to manage these potential risks?
- What new potential risks does this strategic initiative create?
- What are their potential impacts?
- How will the Company manage its vulnerability to those risks?
- What opportunities does this strategic initiative pursue?
- What are their potential impacts?

25 Practical Enterprise Risk Management (ERM)

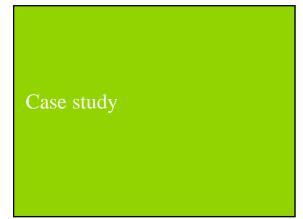
- How will the Company manage successful achievement of those objectives?
- Conduct scenario analysis focused on top priority risks





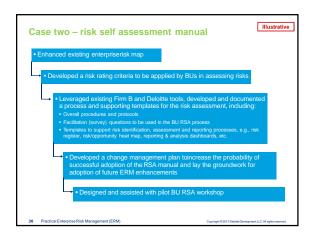






| Case – risk self assessment manual | Illustrative |
|---|---|
| Client A large Financial Services firm (Firm B) | |
| Background Firm B was seeking to develop a Risk Self-Assessment (RSA) within the business units (BU) to enable specific and consiste the assessment of risk. | |
| Project Sponsor Chief Risk Officer (CRO) | |
| | |
| 29 Practical Enterprise Risk Management (ERM) Covyrigit | ©2012 Delates Development LLC. All rights reserved. |

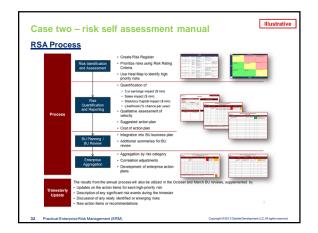
10



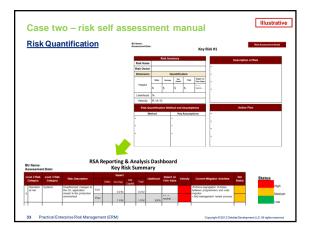


| | | | | Likelihood Rating Criteria | | | |
|---|-------------------------------|-------------------------------------|----------------|---|---|--|--|
| | | | | Likelihood Rating Description | | | |
| | | | | нан | >50% chance of occurring within the next three years | | |
| npact Rating | act Rating Criteria – Example | | | | Between 20% and 50% chance of occurring within the next times years | | |
| Impact Rating | Low (45%) | Medium (5% to 10%) | High (>195) | LOW | < 20% chance of occurring within the next three years | | |
| Sales | ~ 5x M | Sx M-Sx M | ≻5×M | | | | |
| Carnings | < 5x M | 5x M-5x M | ×5× M | 1 definition arrives that are used on the second | | | |
| Statutory Cepital | < \$x.M | \$x M-\$x M | >\$x M | | | | |
| Sales Earnings Statutory Ca | ptal | ik in the following financial calle | - | | | | |











Lessons learned

Leading practices

- Risk management should be integrated into corporate culture, starting at the Board level and with the governance capability.
- Ensure the ERM fundamentals, i.e., the framework, methodology, and tools are established before developing more advanced risk management practices
- Buy in from CEO and executive team is imperative to the program's success
- Buy inform constraints and executive teams imperative to the program sources because the program sources in the program sources in the program of the board and/or CEO, and increasing frequency of CRO executive sessions with the board
 The integration of ERM with other management practices (performance management, process management, compliance management, quality management, etc.)
- Leaders actively shape their risk culture into something purposeful that is aligned with business strategy — and where each employe takes personal responsibility for managing risk in their work every day understands how to make the right risk-based decisions
- Integration of risk discussions and ERM monitoring into everyday business is essential not a documentation exercise
- Build common language and common metrics

Practical Enterprise Risk Management (ERM)

Potential challenges

- · ERM training is still limited to risk specialists and people directly involved in the Risk Management activities
- Just in this past decade, many companies' failures were the result of bad decisions on the part of a handful of people in these cases, the human factor is the root cause
- In the midst of the recent economic challenges, many companies with well-established ERM functions, processes, and controls still failed
- · Missing the cultural and organizational components that may help guard against
- ineffective or just plain poor decision-making on the part of individuals ERM processes are implemented but organizations may still face challenges with respect to effective monitoring and reporting
- · Lack of awareness is a common barrier to effectiveness

Current trends

Practical Enterprise Risk Management (ERM)

- There is increasing link between risk and performance management
- More emphasis has been put on risk related to strategy and its execution
- The focus is shifting from the unrewarded risks to the rewarded risks
- The role of HR in managing risk is expanding Social media risk rivals financial risk as an area of concern

Practical Enterprise Risk Management (ERM)

- · Continuous risk monitoring is rare today, but on the rise
- The Changing Role of Internal Auditors is not just focused on risk mitigation but also value creation
- · Data integrity and data analysis become increasingly important as systems are
- integrated and reporting needs increase Boards have been increasingly proactive in risk management and this will likely
- continue The CRO is increasingly a more senior executive position

Q&A

