

Enterprise Risk Management (ERM) Starter Kit



Introduction

The purpose of this document is to provide preliminary guidance to companies in the early planning stages of their Enterprise Risk Management (ERM) program. This information has been compiled from interviews with several Fortune 500 company leaders who have completed or are in the process of implementing ERM. It is not meant to be a comprehensive in depth discussion of the subject matter, but rather anecdotal lessons learned from persons who have been there and done it.

ERM is not a “one-size fits all” proposition and evolves as it is assimilated into an organization. As an example, think of the early “quality” initiatives. In many companies “quality” started out as a separate department which over time was integrated into the company culture with accountability ending up with the business owners.

Initiating an ERM program is a significant investment in time and resources. Each company should take into account their ERM objectives and organization culture in planning for and tailoring a successful program to fit their environment.



Organization Design

ERM is an iterative and evolutionary process. Therefore, responsibility and accountability for your ERM program may change over time depending upon, among other things, how risk will be integrated into the company culture.

As a general guideline, the initial ERM sponsor should be a corporate-level department that already has or can obtain the requisite expertise to commence the project. For example, one company selected their Internal Audit department to identify and rationalize enterprise-wide risks based on their following expertise:

- Interviewing skills necessary to identify the risks, likelihood, impact, materiality
- Relationships at the executive and management level to conduct initial research
- Direct report to Audit Committee
- Experience with external auditors
- Accounting/auditing experience
- Prior knowledge of business processes
- Access to key documentation

A key factor in selecting an “organization home” for ERM should be based on your company’s short and longer term ERM objectives.

For Example:

ERM Objective	Organization Home
Scope compliance and operational audits and make operational improvements	Internal Audit
Strategy planning	Office of the President or Strategic Planning group
Cash and liquidity planning	Treasurer’s office

Some company specific examples include:

Organization Alignment
Independent ERM function reporting into the Audit Committee. Responsible for providing risk assessment and mitigation support to corporate level functions, including Internal Audit, Legal, HR, etc.
Corporate Strategies Group (In this company ERM supports strategic objectives)
President’s Office (In this company ERM supports strategic objectives)
ERM/Finance/Internal Audit (In this company ERM supports tactical and strategic objectives)
Internal Audit (In this company ERM supports tactical objectives)
Treasury (In this company ERM supports cash and liquidity objectives)



Resource Planning

The initial data gathering phase and development of your company-specific risk rating framework is estimated to be about 3 – 9 man-months, depending on project scope. Adjusting project scope --for example, focusing on strategic risks vs. operational risks-- reduces the project effort accordingly.

As an example, two companies, each with \$7 and \$13 billion in revenues, respectively spent approximately 3-6 man-months gathering enterprise-wide risk data, and a subsequent 3 man-months confirming their risk rating framework. Existing resources from Internal Audit were leveraged to take advantage of their business knowledge and contacts.

Once risks are identified and a risk rating framework is developed, the ongoing ERM maintenance and administrative effort is estimated to be less than 1 FTE. In addition, a company’s Internal Audit function is ideally positioned to maintain and track supplemental risk “issues” related to routine audits and one-off incidents. In other words, the 1 FTE estimate above assumes that other people in the organization, such as internal auditors, are supporting the function by contributing updated, ERM-related information by communicating the results of risk assessments, business plan reviews, internal audits or incident-specific information.



Risk Assessment

The end-game for the initial project phase includes:

- List of enterprise-wide risks (or subset of risks depending on project objectives/scope)
- Documentation of detailed risks (linked to each enterprise-wide risk) , including description(s), business owner(s), linkages to operational processes/systems, risk likelihood and business impact(s)
- Prioritization of enterprise-wide risks based on risk rating model which “accurately” predicts overall risk rating for each enterprise level risk

The ComplianceManager ERM module is pre-loaded with a comprehensive list of enterprise level risks and an automated risk calculation framework to help clients jump start their assessment stage and establish a sustainable ERM program.

Following are considerations for your company’s risk assessment:

1. Gathering Data



Risk data is best captured at the source. This means first identifying the risk owners. Once identified, the preferred approach is a direct interview or “risk assessment” with each owner. This is typically a business unit manager or executive level individual knowledgeable about existing/potential risks in their respective departments.

Advance preparation is key in order to keep interviews to 20 - 30 minutes. Start off with a list of risks/challenges that you already know “could” reasonably exist. This will serve as a catalyst for the discussion and help keep the meeting on point. Recommended wrap-up question: “Is there anything else that keeps you awake at night?”

A comprehensive assessment should also ferret out potential risks associated with strategic company-wide initiatives (often sponsored at the executive level), as well as key projects sponsored at the business unit level. Projects that involve more than one “owner” and/or multiple disciplines should be identified upfront and potential risks captured during the interview stage. Annual operating plans/budgets and quarterly updates are good sources for identifying these cross-discipline initiatives.

Some typical lines of questioning may include:

- Corporate Strategic Initiatives
 1. What is your department doing in connection with strategic initiative “X”?
 2. How important is your effort to the overall initiative?
 3. What are the things that could prevent you from achieving your part of the initiative?
 4. What’s the likelihood of these risks occurring?
 5. What are you doing to mitigate these risks?

- Business Unit/Department Projects:
 1. What are the key projects and goals for your BU or department this quarter/year?
 2. What are the things that could prevent you from achieving these goals?
 3. What's the likelihood of these risks occurring?
 4. What are you doing to mitigate these risks?

Other relevant source documents for risk assessment preparation include:

1. Business Unit/Department Budget, Quarterly "Goals" or Business Plan Presentation
2. Risk Factors in 10K; Financial Statement Notes and Related Adjustments to Financials
3. Related Audits and Audit Findings
4. Related Incidents – Media Information Items
5. Analyst Information or Concerns
6. Policy Changes

Risk assessment interviews are documented and cycled back to their respective owners for confirmation and changes. This is a dynamic process which can be performed on a periodic basis (say, annually, quarterly, etc) and/or ad-hoc based on risk type/priority.

The ERM team classifies and consolidates assessment responses at an enterprise level and recommends an initial overall "strategic" risk level (e.g. high, medium and low) for each major risk category. See #2 below for recommendations on rating risks. A typical company will have no more than about 20 risk categories. These risk categories are subsequently reviewed and signed off by the Audit Committee or other independent body to ensure the list is complete and that there are no gaps. This step is important: One company completed the assessment and determined that "Competitive Risk" was missing...a key enterprise risk category.

Lesson Learned: One company used a written questionnaire instead of a "live" interview for their assessment stage. This approach resulted in data integrity and completeness issues which was resolved by conducting follow-up interviews.

2. Rating Risks



All risks are not created "equally". A standardized risk framework/model helps companies rank and prioritize their risks, raise organization awareness/focus on top level risks and mobilize appropriate mitigation resources. Risks generally follow a normal distribution with no more than 10 -20% ranked high/low and 60 – 80% in the middle. A heat-map dashboard is a good way to visually display risks.

Building a company-relevant risk framework typically utilizes an iterative approach to select and weight appropriate risk criteria. The most common mistake is to select too many risk criteria which adds complexity and does not materially impact the result. Keep it simple and maintain an enterprise-wide level perspective.

Recommendation is to choose no more than 5 – 8 risk rating criteria. Think of risk rating criteria as potential business impacts at the enterprise level. For example:

1. Significant Financial Loss
2. Impact on Brand/Identity
3. Threat to Execution of Key Company Initiative(s)
4. Operational Downtime
5. Distribution/Supply Chain Interruption
6. Loss of Innovation Leadership

Validate your model by testing different risk criteria and adjust the weighting for each until your risk rating results converge with your judgment. Look at the “top level risks” ranked by the model and ask whether they make sense. As a final review, use external resources to validate your rating model, including:

- Sense-check your risk ratings with the Audit Committee / Board
- External Auditors
- Industry Benchmarks

The risk rating model is not meant to replace rationale judgment, but should provide a good starting point for discussion. A risk framework is dynamic and should be validated and adjusted over time as your environment changes.



Adding Value

Scope IA Audits – Using your established risk framework to design and validate the scope of your internal audit plan ensures that internal audit activities cover all major risk areas. Check planned annual/quarterly audit activity against risks.

Establish risk conscious culture – Schedule short (5 – 10 minute) Q&A meetings between accountable risk owners and the Audit Committee for “direct” debriefing sessions on highest level risks.

Scope Annual Operating Plans (AOP) – Ensure that annual plans for functional and operational groups include contingency plans for “what ifs”, as well as proactive programs and projects to manage likely risks, including mitigation, insurance, and outsourcing (shifting responsibility).



Ongoing Maintenance

In order for ERM to remain a relevant tool, risk information needs to be updated to reflect changes in your company and external environment. Ongoing activities may include the following:

- Monitor media information on the net about the company and its competitors
- Meet periodically with key “go-to” persons (operational management, process owners, risk assessment owners, etc).
- Form Business Unit relationships to discuss risks annually or quarterly. These should also include informal get-togethers to ask “how are things going?”.
- Prepare annual “risk assessment” communication, presentation or discussion forum
- Review audit reports
- Attend presentations on strategic initiatives
- Review Business Unit quarterly presentations and goals
- Review SEC risk factors, analyst reports and any debt covenant triggers



Questions

Any questions or comments may be referred to your local *ComplianceManager* representative or emailed to sales@MyComplianceManager.com.

About ComplianceManager

ComplianceManager is a leading provider of on-demand compliance solutions for corporations from small caps to Fortune 100. *ComplianceManager* offers individual or enterprise modules for Internal Audit, Risk Management, Governance, Regulatory Compliance, and Quality Assurance. The Company has locations in San Francisco, Los Angeles, Scottsdale, Dallas and Hong Kong.

For more information, please visit <http://www.MyComplianceManager.com>, or call 1-888-219-8024.

ComplianceManager does not give any representation or warranty of any kind (whether express or implied) as to the accuracy or completeness of this publication. The publication is for general guidance only and does not constitute investment or any other advice. Accordingly, it is not intended to form the basis of any investment decisions and does not absolve any third party from conducting its own due diligence in order to verify its contents.

Before making any decision or taking any action, you should consult a professional advisor. ComplianceManager accepts no duty of care to any person for the preparation of this publication, nor will recipients of the publication be treated as clients of ComplianceManager by virtue of their receiving the publication. Accordingly, regardless of the form of action, whether in contract, tort or otherwise, and to the extent permitted by applicable law, ComplianceManager accepts no liability of any kind and disclaims all responsibility for the consequences of any person acting or refraining to act in reliance on this publication for any decisions made or not made which are based upon the publication.

©2004-2009 MARK Business Intelligence Systems. All rights reserved. ComplianceManager is Patent Pending technology.