ENTERPRISE RISK MANAGEMENT FRAMEWORK

WHAT IS ERM?
Increased Focus on ERM

Although the concept of enterprise risk management (ERM) has existed for a number of years, it wasn’t until the 2008 financial crisis that ERM gained significant prominence as an integral component of an institution’s overall business strategy.

Despite the increased focus on ERM, many in the industry struggle to precisely define it. As a result, the RMA ERM Council embarked on an effort to create highly practical guides for implementing a robust ERM framework that will help institutions (of any size) manage their risk holistically.

The council defines ERM as “the management capability to manage all business risks in pursuit of acceptable returns.” With that definition as a guide, the council adopted a strategy that would help management and boards of directors answer relevant business questions pertaining to an institution’s risk appetite, business strategy and risk coverage, governance and policies, risk data and infrastructure, measurement and evaluation, control environment, response, and stress testing.

At the center of the ERM framework is culture. If an institution lacks the right culture and strong leadership at the top, none of the other elements will matter. Simply put, firms that comprehend and adopt ERM as a “way of thinking” typically outperform those that do not.

Ultimately, ERM can provide answers to three basic business questions:

• Should we do it (aligned with business strategy, risk appetite, culture, values, and ethics)?
• Can we do it (people, processes, structure, and technology capabilities)?
• Did we do it (assessment of expected results, continuous learning, and a robust system of checks and balances)?
The framework was designed to help management and boards of directors answer these relevant business questions:

1. What are all the risks to our business strategy and operations (coverage)?
2. How much risk are we willing to take (risk appetite)?
3. How do we govern risk taking (culture, governance, and policies)?
4. How do we control the risks (control environment)? How do we know the size of the various risks (measurement and evaluation)?
5. What are we doing about these risks (response)?
6. What possible scenarios could hurt us (stress testing)?
7. How are the various risk interrelated (stress testing)?

The framework applies regardless of the size of the institution or how an institution wishes to categorize its risks. The circular depiction of the framework is highly intentional. The individual components (such as coverage or risk appetite) are not meant to be sequential, but rather a dynamic flow in both directions. Additionally, culture is depicted as the center/heart/foundation since, without the right culture, the other components are somewhat irrelevant.

1. Although there are similarities between the RMA ERM framework and the COSO ERM, the RMA ERM framework is adapted to be highly specific to financial services with practical implementation guidance.
The RMA ERM Council’s approach for developing this ERM framework and associated ERM competencies is to develop a series of highly practical workbooks for risk management professionals. These workbooks are:

1. Risk Appetite Workbook (published November 2010).
3. Risk Data and Infrastructure (to be developed).
5. Responses (addressed as part of the Governance and Policies Workbook).

**DESCRIPTION OF ERM COMPETENCIES**

1. **BUSINESS STRATEGY AND RISK COVERAGE**

Risk management must function in the context of business strategy and answer the basic question, “what is our business strategy and associated risks?”

Before an institution can articulate its risk appetite, it must first determine its goals and objectives, i.e., its business strategy. The institution must define what it wants to achieve in terms of markets, geographies, segments, products, earnings, and so on. From there, the institution assesses the risk implied in that strategy and determines the level of risk it is willing to assume in executing that strategy. Regardless of a specific business strategy, an institution is exposed to the following risks:

- Credit
- Liquidity
o Strategic/Business/Reputation
o Market
o Operational
o Compliance/Legal/Regulatory
o Financial
o Capital Adequacy

RMA’s Risk Appetite Workbook provides a very detailed roadmap for explaining what a risk appetite is and how an institution can develop one. In this workbook, RMA has defined risk appetite as “the amount of risk (volatility of expected results) an organization is willing to accept in pursuit of a desired financial performance (returns).”

The concepts of risk appetite and risk tolerance are often used interchangeably, but they have distinct differences in meaning. Risk appetite represents the acceptance of volatility an institution is willing to assume in executing its business strategy. Risk tolerance refers to day-to-day operational limits developed within the context of an organization’s stated risk appetite (for example, concentration limits).

It is important for management and the board of directors to understand the critical links among strategy, business plans, and risk. A risk appetite statement is one tool that facilitates this linkage. In this context, the risk management function is an integral part of the institution’s overall strategies and specific business objectives—an essential part of the institution’s success, returns, and value creation.
Culture can be described as “what people do when they are not being watched.” As previously mentioned, culture is the most important aspect of any good ERM competency. RMA’s Governance Workbook is devoted to the full description of “what a good risk management culture looks like” and covers governance and policies as well as providing various examples of board and management level governance committees to oversee risk taking activities.

Policies express the risk appetite of the company to the masses. They describe to all stakeholders what the company is willing to do and not to do. The statement of risk appetite is executed through policies (what to do?) and procedures (how to do them?). Simply put, culture, governance, and policies collectively help an institution manage its risk-taking activities.

Boards of directors and management accomplish their risk management responsibilities through a deep understanding of the company’s risk profile. The risk data and infrastructure refers to how the information is collected, integrated, analyzed, and translated into a cohesive story. This area is probably the most challenging aspect of ERM. Some companies have spent $200 to $300 million without yielding the appropriate business results. Any good risk management infrastructure requires a highly robust management information system. Given its importance, the ERM Council plans to devote an entire workbook to this topic.
5

**CONTROL ENVIRONMENT**

The internal control environment is one of the most important tools in the management toolbox for management of risks. Internal controls help reduce the level of inherent risk to a level acceptable to management. The system of internal controls includes culture, governance, policies, preventive and detective controls, and scenario planning.

Management relies on internal controls to manage residual risk to an acceptable level. Residual risk is defined as the level of inherent risks reduced by internal controls. Building an effective internal control environment allows management to control what can be controlled.

6

**MEASUREMENT AND EVALUATION**

At any given time, boards of directors and management must manage a portfolio of risks (from asset quality, liquidity, interest rate, to business continuity, information security, privacy, etc.). The science and art of measurement in ERM is about concluding which risks are significant and which ones are not, and where to invest time, energy, and effort. In order to accomplish the goal of measurement and evaluation, an institution may adopt a simple model of color rating (green, yellow, and red) to a highly sophisticated risk adjusted return on capital (RAROC), or perhaps a middle-of-the-road failure mode and effect analysis (FMEA) model.

Regardless of method used, measurement and evaluation help boards and management answer the question, “so what?” The process of
measurement and evaluation must include the system of internal controls and must determine how well can the risks can be managed. Given the importance and complexity of this subject, an entire workbook will be devoted to this topic in order to help risk management professionals choose the right methodology for their company.

**7**

**SCENARIO PLANNING AND STRESS TESTING**

The art of ERM is the ability to answer the question, “what can go wrong and, hence, create deviation from expected outcomes?” In that pursuit, management must address known, knowable, and unknowable risks. Scenario planning and stress testing are tools that focus on the knowable and, perhaps, some unknowable risks. A robust scenario planning and stress testing discipline is a must from a capital planning perspective.

RMA recently published a workbook dedicated to this subject.³

3. RMA published the Scenario Analysis and Stress Testing Workbook for Community Banks, February 2012.

**SUMMARY**

Enterprise Risk Management, essential for any financial institution, encompasses all relevant risks. An ERM framework supports a management competency to manage risks well, comprehensively, and with an understanding of the interrelationship/correlation among various risks. The successful institution incorporates a robust ERM capability as part of its culture by integrating what already exists to create a comprehensive and integrated view of the institution’s risk profile in the context of its business strategy.

*You can access RMA’s Enterprise Risk Management Workbooks on our website at http://www.rmahq.org/risk-management/enterprise-risk/workbooks.*
About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues.

Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country’s banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, these 18,000 individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

RMA University

In today’s rapidly changing financial services industry, you need practical, day-to-day knowledge that will help you excel in your profession. RMA provides quality education to advance sound risk principles in the financial services industry. Traditional classroom training and online learning resources are available as open enrollments or in-bank training. Visit
http://www.rmahq.org/events-training/rma-university/rma-university to learn more.

eStatement Studies

RMA’s eStatement Studies® is the only source of comparative data that comes directly from the financial statements of small and medium-size business customers of RMA’s member institutions. Round-the-clock online access gives you the ease and flexibility to use this wealth of information at your convenience. Visit
http://www.rmahq.org/tools-publications/tools/estatement-studies to learn more.

Are you an RMA member?

An RMA membership provides many benefits. In addition to a free subscription to The RMA Journal® and discounts on RMA events, products, services, and training, membership also provides countless networking opportunities and exposure to the industry’s key decision makers and manager. RMA’s local and national events keep you up to date on industry trends and issues while allowing you to meet new people and swap successes with peers. Visit
http://www.rmahq.org/joinrma to learn more about membership.

No part of this publication may be reproduced, by any technique or process whatsoever, without the express written permission of the publisher.
Phone: 800-677-7621
Fax: 215-446-4101
Website: www.rmahq.org