FMS Financial Managers Society

fmswhitepaper

Why community-based financial institutions should practice enterprise risk management.

By Michael D. Cohn, CPA, CISA, CGEIT
Director, WolfPAC Solutions Group

Unique Insights | Implementation Guidance | Strategic and Tactical Direction | Immediately Relevant

FMS Financial Managers Society

fmswhitepaper

Why community-based financial institutions should practice enterprise risk management:

Implementing a bottom-up enterprise risk management program allows financial institutions to reduce costs and achieve business goals

By Michael D. Cohn, CPA, CISA, CGEIT
Director, WolfPAC Solutions Group

Enterprise Risk Management, especially when practiced in a bottom-up approach, is an underutilized management technique that when implemented allows community based financial institutions to become more efficient, smarter, and better able to compete in an increasingly complex environment.

In the current regulatory environment, Enterprise Risk Management (ERM) is fast becoming a common practice in financial institutions as a means to better align exposure and tolerance to risk with fulfilling business objectives. While it is being accepted and practiced expertly by the large financial institutions, many smaller, community-based banks and credit unions are not practicing ERM. This is causing these institutions to incur higher operating costs which may lead them to reach a point of crisis or become vulnerable to unwanted acquisition. By implementing a robust ERM program utilizing a bottom-up approach, community-based financial institutions can reduce costs, improve delivery of their products and services, and survive in an increasingly competitive and regulated environment.

Implementing an ERM program is not hard – many of the elements needed to create a program exist in community-based financial institutions today. It's a matter of reorganizing and reorienting the institution at all levels to embrace and practice ERM.

What is enterprise risk management?

Community-based financial institutions that are not practicing ERM may regard it simply as another management practice that won't increase earnings or capital, or believe their financial institution does not require any major change in its risk management program. These characterizations of ERM are false. ***In truth, a bottom-up ERM approach is a process to organize the many threat assessment, control testing, and control remediation activities the institution has always performed***.

It's understandable that community-based financial institutions may not have a clear plan to implement an enterprise risk management program because there is no formal regulatory guidance on creating such a program.

Most expert risk managers agree that an ERM process to evaluate threats, uncertainties, and potential negative impact to earned capital is necessary to ensure that institutions, no matter their size, retain their assets, remain competitive, and achieve their business goals. To show the value of an ERM program, one must first define ERM.

The elements of the basic risk management program exist in many community-based financial institutions: risk assessment, control testing, and risk mitigation. Much of the work is documented in functional risk assessments on technologies, vendors, business operations, regulations, loan portfolios, and products. Enterprise Risk Management takes an enterprise-wide view of all of the risks at play by combining the reporting of functional risk assessments and developing an entity-wide governance structure in order to break down silos and encourage coordination among departments.

What makes current ERM programs different from risk management practices of the past is that it reveals the foreseeable risks present in the organization and offers a system-wide set of solutions to those risks that support the objectives of all departments. In the past, each department or business unit may have reviewed and worked on the risks present only to them and then moved on without thinking of the effect on the rest of the institution. This type of orientation introduces the possibility that threats that span organizational silos can be missed or under-appreciated. While these lax risk management practices may have worked before the recession, they will be inadequate to support a viable financial institution today.

The foundations of ERM are already present

There is no doubt that community-based financial institutions are working hard to manage the potential risks that surround their activities. Sometimes the risk management programs used by institutions are based on longstanding practices, applying the top-down COSO model, or by adhering to regulatory compliance.

Financial institutions currently conduct a long list of functional risk management efforts that include:

- Credit risk
- Liquidity risk
- Interest rate risk
- Information security risk
- Privacy risk
- Third party/counter party risk
- Regulatory compliance risk
- Financial reporting risk
- Strategic risk
- Reputation risk
- Multifactor Authentication risk
- Remote deposit capture risk
- ACH risk

Unfortunately, they often conduct these efforts in silos as each department assesses and then addresses the risk without taking into consideration how the fix could affect the overall performance of the institution.

Risk management in silos is not enough

The successful practice of bottom-up enterprise risk management occurs when all of the efforts above are integrated into a cohesive program that is managed with a comprehensive strategy. And when the program and strategy can be understood and explained to the most junior associate and to senior management and the board, an institution-wide acceptance of ERM is possible.

The key to bottom-up risk management is that results of the assessments must also be reorganized by product and service to provide information not previously known or understood. For instance, the risk profile of retail banking products will be different than that of credit and loan products. Knowing exactly which threats are most significant for each product is key. Most institutions know the highest threats and usually the lowest. Knowledge and remediation of more moderate level threats is less understood and typically not managed. A moderate risk may never threaten the viability of the institution, but the pain and cost of managing the impact of its occurrence could be significant. The performance of a bottom-up enterprise risk assessment will not only highlight the high and moderate risks and threats; it will change the questions your management team asks as they will be better informed about present risks and more invested in solving them.

This bottom-up approach of integrating these functional enterprise-wide risk assessments across organizational silos, optimizing the effort to conduct control testing, and aligning management's expertise to develop risk mitigation strategies for the entire institution is the most effective way to practice enterprise risk management.

With the adoption of an integrated bottom-up approach, executive management will now be able to articulate and describe to auditors, regulators, and the board the process and elements of a sustainable management program that identifies and predicts high risk threats as well as conclude on the design and

operating effectiveness of controls. Coming out of the silo mentality and executing an integrated bottom up ERM program will also allow an institution to spot and prepare for emerging risks rather than being caught off guard.

Measuring the cost of ERM

The next challenge is measuring the cost of risk management. Institutions are wondering how much they should spend on risk management and how much it will cost as new regulatory requirements are implemented. There is no hard and fast rule because there are no formal guidelines or benchmarking data. However, spending should be sufficient so the chief risk officer can assure the board and C-suite that risks are being managed and mitigated to the best of the institutions' ability.

If an institution can measure the cost of risk management then, it can take steps to make it cost less. By implementing a bottom-up approach to ERM, the inefficient allocation of resources inside the institution becomes much clearer and therefore adjustable. For example, many institutions are learning that the hours committed to traditional internal audit across all the institution's products and services are far greater than the hours committed to IT audit. This relationship may not be evident until an integrated, bottom-up risk management is completed. The value of this approach is to change the questions the management team asks. The right answer for the institution is subsequently much easier to determine.

A bottom-up ERM approach allows institutions to accurately measure the annual allocation of resources such as the number of operational controls, the breadth and depth of control testing, and the use of external consultants versus internal staff. The total resource allocation from one year to the next can then be evaluated to ensure the level of risk management resources is commensurate with changes to business strategy and external events. Level spending from one year to the next may be appropriate for many institutions, but aligning the threats and costs of risk management allows the chief risk officer (CRO) to pose questions and develop strategies not easily identified in a top-down or functional risk management approach.

Redefining management roles for effective ERM practice

To effectively maintain an ERM program, the interaction of the CRO and others such as the internal auditor and the compliance officer must be re-examined to ensure that they are operating together to the benefit of the institution.

Mastering the management of the functional risk areas listed above is not an easy task, as no one person could effectively manage and solve all of these issues on their own. That is why it is essential that the CRO promote the adoption of enterprise risk management at the institution and oversee its implementation and practice throughout the organization.

It is not enough for the CRO to implement an ERM program; he or she must be an "evangelist" about the benefits and practice of ERM to the entire institution – from the board of directors to the most junior associate. If the entire financial institution is not on board and following through on the practices necessary for the ERM program, then the effectiveness of the program will diminish progressively over time.

The internal auditor's role and their interaction with the CRO must be updated for the effective implementation of an ERM program. The relationship between the CRO and the internal auditor must be strong without compromising the internal auditor's independence. In many cases, the executive suite and board will incorrectly equate ERM and threat management with internal audit and control testing and look solely to the internal auditor for guidance. For an ERM program to be effective, the CRO must persuade the executive suite to own the risk and be responsible for controlling it. The CRO should guide management to document controls and classify them as key or secondary. The internal auditor then independently validates management's classification to ensure controls are designed to mitigate the related risks and tests the key controls for effectiveness.

The key to success in assessing and addressing the risks and controls under a successful ERM program is having the independent auditor and the chief risk officer working well together. If the relationship between them isn't productive, the opportunities to achieve an effective ERM program may not be reached.

It is also essential under an ERM program that the relationship between the CRO and the compliance officer should demarcate clear lines of responsibility for the institution to maintain compliance with laws, rules, and regulations. Very often, community-based financial institutions will incorrectly equate compliance with safety and soundness. It is very important to realize that being compliant is not synonymous with operating safely. ***A strong, competent, and efficient compliance program may prevent fines and actions from the regulators but it will not keep the institution safe*** (i.e., reduce operating losses, preserve capital, or allow a financial institution to achieve its business goals in the way an ERM program will).

Moving an ERM program forward

To begin an effective ERM program, an institution must first take stock in its current activities and organize them along the areas of the functional risks. The institution should evaluate each risk assessment and control testing result and convert or append the analysis to create a consistent residual risk measure that is used at all levels. When a common measure and language is created to communicate risk, the reporting out by the various business lines and services becomes much clearer and more effective.

The second step for the institution is to take an honest look at its practices. There will be major threats within the institution that are not being sufficiently mitigated. These must be brought to the surface and placed into view for the entire organization to see. ***The good news is that once transparent risks are uncovered they can be mitigated***.

If expertise is required that is not present in the institution, such as information technology and security, the expertise must be acquired. If the volume of data and the time to produce comprehensive reports and analysis is overwhelming, automated tools and support must be deployed. If a financial institution is understaffed and overwhelmed, it should consider measuring what it is spending now, which threats current resources are addressing, and then realign the resources based on the clearer picture of the level of threats in each area. The larger the management team the more important it is to let the analysis derived from the ERM program guide the decisions on how to allocate resources.

Because an ERM program must cover the enterprise, governance cannot be ignored. To successfully implement an enterprise risk management program it is essential to create a risk committee or further empower an existing committee. When operating optimally, the risk committee will hold an enterprise-wide view of risk assessment and management and provide guidance, oversight, and approve funding requests to allow the ERM program to operate optimally. In the absence of a risk committee, the ERM objectives will not be met.

As for compliance issues, a bottom-up approach to ERM will complement and continue to support the regulatory requirements of each functional risk assessment. Implementing a COSO version of ERM is a top-down approach. If a financial institution believes it must implement this version, and it has the resources to do so, a bottom-up and top-down ERM approach can be deployed. The results from each approach should be complimentary but the institution should recognize that the results are used for different objectives.

Emerging Benefits of ERM program

When a community-based financial institution adopts and implements a bottom-up ERM program it will soon start to see the benefits that come from taking such an important step. Three major benefits will emerge from the institutions' early efforts.

The first benefit is that the very nature and behavior of the financial institution will change as enterprise-wide awareness of major threats and the purpose of controls become evident. Line management will be more involved in threat assessment, hands-on with risk assessment issues, and assume ownership for the rating of threats and designation of key controls. Day-to-day decision making will likely change as risk across the institution is more frequently considered before actions and projects are started, not after implementation or kickoff begins.

When this happens, risk management then becomes everyone's job, not just the risk officer's. Even for a small financial institution, it is difficult for any executive to maintain comprehensive knowledge of all operational and transaction activities. But when more risk-oriented decision making is allowed and empowered in the lower parts of the organization, it results in greater speed, agility, and safety for the institution. Thus, the benefits of a bottom-up structure to an effective ERM program are realized.

The second benefit is the productive alignment of internal activities such as risk management, internal audit, regulatory compliance, information security, vendor management, business continuity, credit administration, and asset-liability management. This alignment will eliminate silos and reveal gaps in threat identification through integrated, bottom-up risk assessment.

Lastly, and most important, ERM will reduce costs. When there is overlap, extra resources are spent unnecessarily and when there are gaps, extra resources are subsequently required to fill it. Both situations are expensive and unnecessary. When the institution takes an integrated bottom-up ERM approach and measures the costs of risk management, it will plug any holes from which the institution is leaking resources.

Avoiding ERM is no longer an option

Adopting and practicing ERM is a requirement today for community-based financial institutions that want to remain viable. The current state of the economy and the increasingly complex regulatory climate requires that smaller institutions must find cost savings to compete in the marketplace. The cost saving

opportunities become evident when aligning high and moderate level risks to current year budget amounts, and analyzing emerging and receding risks to year over year resource commitments. Practicing enterprise risk management, especially when structured in a bottom-up approach, will change the DNA of an institution in a positive way and make it more successful today and into the future.

Michael D. Cohn serves as Director of WolfPAC Solutions group and is a Principal at Wolf & Company, P.C. He provides risk management advisory services and board training to community based financial institutions. WolfPAC Integrated Risk Management® is an Internet based Software-as-a-Service (SaaS) solution that provides a suite of enterprise risk assessment and risk management solutions for the financial service industry. Mike can be contacted at mcohn@wolfandco.com or (617) 439-9700.

Published by:
Financial Managers Society, Inc.
100 W. Monroe, Suite 1700
Chicago, IL 60603
312-578-1300
info@fmsinc.org
www.fmsinc.org

