WolfPAC
INTEGRATED RISK MANAGEMENT

Three Principles for Creating an Excellent, Effective and Efficient Enterprise Risk Management Program

L. Randy Marsicano, CISA, CRISC

Community-based financial institutions are facing big challenges today. There are more compliance and risk management processes, policies, regulations present while the environment grows more competitive. That's why it's more important than ever to have a robust enterprise risk management program in place. By following three basic principles that cover operation, finance, and governance, your institution can create and implement an effective and efficient enterprise risk management program.

I. INTEGRATED RISK MANAGEMENT OPERATIONS

Getting the ball rolling starts with looking at how your people are working to assess and mitigate risk. Effective risk management relies on teamwork. Working in silos, which allows for threats that span more than one area of the institution to be missed or minimized, must be a thing of the past because there is no room for these kinds of errors in today's challenging environment. The people and departments in your financial institution must be committed to enterprise risk management, working together to identify and mitigate risk while eliminating silos. It takes a team to manage risk properly.

One way to create an enterprise-wide view is to structure your approach as a bottom-up risk management program. That means starting with the technologies, vendors, and functions used in each of the products and services that you offer. Once you have this inventory, you can be effective in performing risk assessments across functional areas and weigh the risks and controls using common criteria. This then allows you to optimize efforts to allocate control resources, conduct control testing, and align management's expertise to develop risk mitigation strategies for the entire institution.

II. UNDERSTANDING RISK MANAGEMENT FINANCE

A simple rule of thumb for risk management is this: If you can measure the cost of risk management, you can make it cost less. There are ways to measure the cost of risk management. You can start with the hard costs like facilities, equipment, and technology vendors and consultants. But don't forget about the soft costs of people's time. A common approach here is to take an average hourly rate for a mid-level or grade of managers, and add to it an hourly component that includes administrative costs, benefits, taxes, and other costs directly linked to the cost of the employee. This "fully loaded" hourly rate can be applied to the hours a resource spends on risk management to produce a soft cost of that resource. Once you have this soft cost, you can determine the fully loaded costs of time spent on internal

audits and other internal risk management activities. When you have an understanding of the blended hard and soft costs of each risk management area, you can then match this to your organization functional risks like credit, information security, and regulatory compliance, to create an accurate picture of your risk and risk management spending. The CRO or risk management committee can then ask questions, make adjustments, and pose strategies that will make your risk management program more effective and cost efficient.

III. RISK MANAGEMENT GOVERNANCE

Strong risk management governance is crucial to the success of your enterprise risk management program. Each community-based financial institution needs a chief risk officer whether a dedicated role or part of an exciting executive's responsibilities. This individual is the evangelist about the benefits and best practices of enterprise risk management for the entire institution. Without this role, the effectiveness of the program will diminish over time. There are various internal and external forces that drive the need for this valuable role. Internally, there are numerous risk indicators that require monitoring, changes to the business that require evaluation, and emerging risks that need to be evaluated. Externally, there are regulatory changes, growing competitive pressures, new product introductions, and increased scrutiny as an organization approaches and crosses the $1B mark.

Strong risk governance is needed to set the institution's risk appetite, establish the key risk indicators, and determine the resources to be allocated to assess and mitigate risk. The risk management governance team should do a thorough assessment of current practices for assessing risk, work to "convert" everyone in the institution to be more risk-minded, create a common language to communicate risk, and decide if the institution needs more resources and technology to address risk.

Creating a robust and highly effective enterprise risk management program will bring significant change to your institution. The process will reveal aspects of your institution that were not known before. It will also provide an accurate risk profile of the institution on which better decisions can be made by management and the Board on important matters like adding or retiring products, or acquiring an institution.

Enterprise risk management is not another compliance requirement. It's not another management practice. And, it's not going away. ERM is a powerful and effective approach to risk management that will make your institution stronger, sounder, and more successful in achieving its current and future business goals.

L. RANDY MARSICANO, CISA, CRISC
SENIOR MANAGER – WOLFPAC SOLUTIONS GROUP
Direct: 617-428-5447
rmarsicano@wolfandco.com