

METAVANTE WHITE PAPER

Demystifying Enterprise Risk Management

Stephan Salvador
Director, Risk and Compliance Consulting



1-800-822-6758

Table of Contents

ERM in Play: Three Essential Functions

ERM Governance

ERM Process

Technology

Summary

For More Information

Enterprise Risk Management (ERM) can overwhelm both seasoned executives at the largest financial institutions and those at community and regional banks who ask themselves whether or not ERM is a big-bank utopia they'd be better off not considering. It doesn't have to be that way.

ERM in Play: Three Essential Functions

It can help to consider ERM from the perspective of three major building blocks – *governance*, *process*, and *technology* – under which the majority of ERM activities fit and can be categorized.

- **ERM Governance** includes the organizational positions put in place to develop and oversee risk and compliance policies and processes, as well as the expected return on the program. This function usually includes the participation of the board of directors, CEO, CCO, CFO, CRO, Risk Manager, Compliance Officer, and senior leaders of the business units.
- **ERM Process** encompasses identifying, categorizing, assessing, monitoring, and mitigating the many types of risks that the bank is exposed to on an ongoing basis.
- **ERM Technology** consists of enabling systems and tools that provide for assessments, analytics, and reporting for the ERM program.

ERM Governance

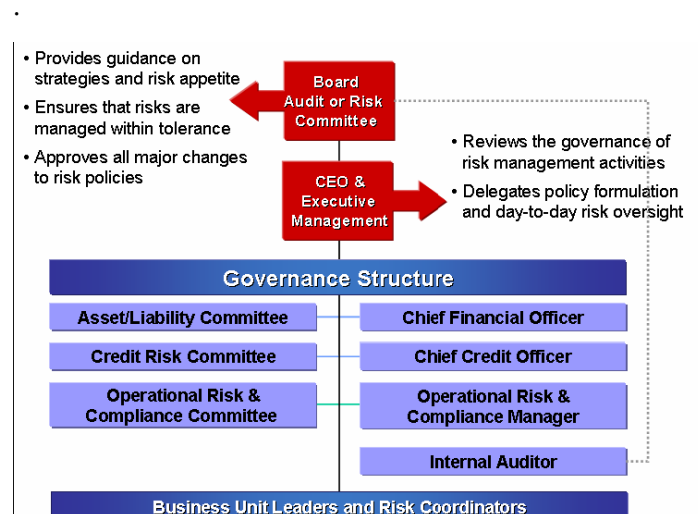
The seeds of the governance function are sown when the CEO, CRO, risk management committee, and board lay out and approve the functional structure and roles. The first rule is to not disturb what is working well; instead, focus on how to “herd cats” – those risks that impact all business units across the enterprise that no one has responsibility for and yet all are involved in trying to mitigate. The following depicts a desirable, straightforward ERM governance structure for a bank.

Many banks have seen good things develop out of this governance structure, such as:

- The establishment of formal, consistent, and interrelated policies, standards, and roles, including

oversight committees with charters, a set of guiding principles, and an operating mode.

- Leveraging existing credit and market (ALCO) managers, committees, analytics, and reporting as part of the overall ERM program.
- Joined operational risk and compliance functions with dedicated resources aligned together under a single manager to coordinate the many SOX, FFIEC, compliance, and audit risk assessments that burden business units.
- The appointment of risk coordinators (existing employees) from within each business unit to link back to the risk office – coordinators who really understand their activities and make ERM work within their business units.
- Positioning of internal audit (and loan review) as a separate unit to help ensure its independence, while remaining involved in the ERM process and drawing upon the ERM work for its own independent reviews.



Without ERM governance, business units have no guiding light to follow, no risk framework to adhere to, no leverage of risk assessments and audits, and their activities become focused on meeting minimum compliance requirements.

ERM Process

The second ERM function translates planning and governance into actions as the program begins to be carried out on a daily basis. Assuming effective communication will flow down, across, and back up the ERM governance structure, and with deployment of ERM technology, risk and compliance metrics can be monitored and exposures reduced; then this middle ingredient is how the risk program is implemented and maintained across the business units and board.

ERM represents a distinct move away from how older risk management models were deployed and managed, which assumed that risk was compartmentalized by line of business or department and devoid of interfaces to the rest of the enterprise. As ERM plays out across the organization, this philosophy has to change:

- The CEO should set the tone at the top on bankwide participation to give the CRO legs to stand on when resource constraints and competing priorities arise.
- Training workshops should be conducted with business units to roll out the ERM governance and technology and set expectations on the quality and frequency of risk assessments and monitoring.
- The various risk management committees should be conducted monthly, whereby the ERM governance, policies, and upcoming risk and compliance assessments are scheduled, reviewed, and approved.
- The business units should monitor their risks, controls, key risk indicators, and loss events in cooperation with the ERM governance function and the established framework as configured within the ERM system.
- An internal audit function, also part of the governance structure, should be involved in both independent risk assessments and control testing, with more significant failures being reported to the CEO, CRO, and the board.

The CRO should track the ERM rollout for up to 12 months and share the milestones and status reports with the board, CEO, and business unit leaders. Once stable in Year 2, the activities should move beyond rollout and be focused on reinforcing ERM governance and policies, such as providing more training workshops, helping the business units with

the quality of their risk assessments and risk indicators, enhancing risk reporting, and other refinements.

Technology

Without technology, ERM cannot exist in an optimal form. Still, the name of the discipline is Enterprise Risk Management, not Enterprise Risk Technology, for a reason. If the processes a bank puts in place are too narrow, the technology to support them won't be effective either. For example, if the process encourages a silo-based approach to identifying and managing risks, and it does not capture "enterprise-wide" operational and compliance risks, the best technology available won't be able to knit together the many components and cross-dependencies of ERM. The extent to which process influences technology should not be underestimated.

ERM technology has evolved quickly to streamline the intensive Sarbanes-Oxley 404, GLBA data privacy, FFIEC IT and vendor risk, and Basel II risk/control documentation activities; calculate economic capital; track loss events; report on key risk indicators; and provide other sustainable operational risk and compliance assessments, internal audits, and board reporting.

On the other hand, it is important to realize, especially for first-time buyers, that ERM management reporting systems may still need to be supported by credit and market risk analytical tools/spreadsheets and software packages, and they do not replace transaction monitoring (network, fraud, AML) or business continuity documentation packages. Many vendors are after this Holy Grail. But for now, the better way to view ERM technology is to drive consistencies and efficiencies in the risk assessment process, eliminate reporting redundancies, and ensure that it can integrate into your IT architecture in the future. One way to maximize the hard work accomplished in the ERM risk assessment process is to build a four-point data model within your ERM system that links business objectives to business unit risk to defined risk categories to financial statements.

Each of these definitions will vary within a bank, but if linked, all four will serve the reporting requirements of regulators, auditors, business units, and the board, as well as allow your risk analysts to ask complex queries that reveal control gaps and unmanaged exposures:

- What risks will prevent us from meeting our business and regulatory objectives, and do we have executive-level action plans and controls in place?
- What are the aggregated levels of residual risk scores across our risk categories? Do the business units have a proportional level of risk that makes sense for their products and services?
- How can we correlate business unit risk ratings to our actual loss events?
- How effective are our controls in mitigating these risks? What is the status of control testing? Are internal audit findings correlated with business unit tests, and are the opinions the same?
- What are the dependencies and linkages between risks, controls, and key financial statement accounts? Can we identify all business units, risks, controls, tests, loss events, and key risk indicators for a specific financial statement account?



Summary

The ultimate outcome of ERM is to move the bank beyond traditional consumer compliance and financial control reviews. ERM will yield a greater return and help build a better bank if properly governed, consistently implemented one step at a time, and supported with technology. Over time, business unit process transformation can happen with improved customer service, greater efficiency, better technology utilization, increased speed to market of new products, and lower risk.

Yet none of this can happen until the organization stops being awed by the idea of ERM and digs in to making it a reality within their institution. Bankers must remember to survey the ERM landscape one locality at a time, getting familiar with its components along the way and demystifying the discipline once and for all. Only then will they be able to accomplish what is best for their bank.

For More Information

Metavante Corporation's team of risk management specialists comprises practitioners in financial services, operations, technology, compliance, and risk management.

Our operational risk expertise is focused specifically on the areas of fraud prevention, compliance, information security, privacy, business continuity, IT recovery, physical security, and vendor management.

We deliver measurable results that prepare your institution for the current competitive and regulatory environment.

To learn more, call 800-822-6758 and talk to one of our consulting professionals, or visit us at metavante.com.