With **major systems failures** at several trading firms and market centers, **increasingly volatile markets**, and an **aggressive regulatory response**, enterprise risk management has become central to strategic planning for financial institutions. ERM programs, however have often been perceived as elusive and non-value added propositions — but given the stakes in today’s regulatory and market environment, this is a road trip every well-managed institution should undertake. While ERM can be pursued as a response to known and unknown risks, when implemented properly, it can also present a strategic opportunity to better allocate resources and investment and protect the firm’s tangible and less tangible assets¹.
Why ERM?

An integrated ERM framework is an essential element of a responsible corporate governance program — identifying and isolating risks that can cause the most damage and enabling executive management to deal with future uncertainty, risk, and opportunity. ERM is a journey of continuous improvement that can be a brand differentiator.

The motivation to begin this road trip comes in different forms — a recent incident or the immediate threat of one or more concerns expressed by senior management or audit committees, among others. Every few years, there is significant attention from systematic events viewed as either unpredictable (business resilience after 9/11); unacceptable (financial scandals and the ensuing Sarbanes-Oxley Act); or extraordinary (2008 Lehman Brothers collapse and banking crisis). The risks are still present and just as threatening:

- The cost of strategic error — whether regulatory penalty or capital erosion through damage to the firm’s brand (strategic, regulatory, reputation risks) — can be a multiple of traditional risk classes. Enforcement actions, consent orders, and major fines are expensive reminders.
- Firms are less insulated from international events arising from cross-border transactions and globalization. Oil and commodity prices are recent cases in point.
- Reliance on third parties (vendor risk) and associated vulnerabilities — cybersecurity threats included — dramatically extend the reach required of risk management. The entry point for the cyberattack on the Target stores was an HVAC vendor — evidence that one weak link can have widespread impacts.
- Corporate governance pressures and investor scrutiny, combined with heightened regulatory expectations, do not tolerate poor business practices. The recent LIBOR, FX, and, auto emission scandals prove that even large firms are not immune, and that senior executives can and will fall from grace.

Reliance on third parties and associated vulnerabilities ... dramatically extend the reach required of risk management.

Even firms with strong risk capabilities should be prepared for a crisis. Siloed responses, while valuable, involve reactive crisis management which can create additional vulnerabilities. ERM programs can help avoid the lower likelihood, but high impact events can create earnings volatility and are not easily measured by single-discipline key risk indicators.
It takes courage and determination to commit to the road trip — there may be hazards along the way. A successful ERM program includes:

- Appropriate priority setting;
- Tools to support the strategy, priorities, and conclusions;
- Conviction to complete the difficult job of generating issue awareness; and
- Obtaining buy-in and acknowledging and remediating the gaps.

**ERM requires a shift from a defensive stance to a preventive one.**

**The Road Map**

No two firms are alike; no two ERM solutions are alike. ERM may differ in relevance, sophistication, and requirements depending on the firm’s organizational structure, business lines, and size. Each firm will experience the journey differently even if all are headed in the same general direction.

**WHAT’S AT THE END OF THE ROAD?**

- Top-down, Strategic Focus
- Regulatory, Investor, Shareholder Confidence
- Enhanced Corporate Governance and Risk Culture
- Improved Response and Stress Strategies
- Alignment of Risk Management
- Operational Excellence
- Link of Risks to Appetite, Tolerance, Economic Capital, and Incentives
- Enhanced Firm-Wide Risk Capabilities

ERM requires a shift from a defensive stance to a preventive one; from focus on value erosion to identifying hazards and avoiding catastrophic losses; and, allocating economic (operational) capital more effectively and efficiently. It enhances overall risk competencies and knowledge and broadens risk management (technology, process, and data) capabilities.
While concepts have been debated for over 20 years, it seems that some firms are waiting for universal guidance. There are, however, several well-tested industry standards and no absence of subject matter literature. There are also too many examples of firms damaged or destroyed by the lack of, or delayed, implementation.

**ESTABLISH RISK VISION AND STRATEGY**

**Articulate the Objectives**

Your ERM foundation should set the context and announce a “call to action” (CTA) — a compelling and shared risk management value proposition. This CTA is the link to the firm’s business strategy and long-term objectives.

A sound risk vision and strategy encourages growth and innovation, including managing new businesses and products; setting boundaries for acceptable behavior; and rewarding strategies that benefit the firm rather than one business line. It establishes accountability and management through development of policies, processes, competencies, methodologies, and reporting, and outlines initiatives to improve capabilities. The risk strategy identifies:

- Target markets, geographies, product mix, client bases;
- Financial targets adjusted for risk-adjusted returns;
- Potential events and specific threats;
- Sensitivity to events and response ability; and
- Ability to absorb losses for identified and accepted exposures.

*In ERM terms, these are the priority opportunities and outcomes.*

**ROAD SKILLS**

- Ask about the unknown exposures that can shift focus to crisis control and what can be done to avoid them.
- Reevaluate the vision periodically based on real, not perceived, capabilities.

**Define Risk Appetite**

“Risk appetite” expresses the variability of results that the firm is willing to accept in executing its strategy. It helps target commitments, risks arising from these strategies, capital needed, and where to allocate capital excesses. It reflects and influences the firm’s culture and operating style and sets boundaries for exploiting strategic opportunities. Within risk appetite, “risk tolerance” is the acceptable level of variation against specific objectives. It expresses the tactical link to the underlying measurement processes.
ROAD SKILL

- Effective risk appetite and tolerance statements are pushed down to the functional level to ground them in the firm’s culture. This action ensures that line managers act in the firm’s overall interest as they pursue their individual goals.

COSO Framework

Enterprise risk management is a process set in motion by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise. ERM is designed to identify potential events that may affect the entity, to manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.

Identify the Risk Framework

Without a framework, risk management is likely to be ad-hoc. A framework is a benchmarking tool to direct focus and discipline. Over time, the process framework will mature and gain the confidence of stakeholders in the firm’s risk management capabilities. Arguably, the most common framework in the U.S. is COSO². It is designed to be customized and is used to both describe the current (as is) as well the future (to be) state. Support is paramount. COSO states that executive management “support(s) the entity’s risk management philosophy… and that the CEO should “(ultimately) assume ownership.”

ROAD SKILLS

- Sequence implementation. Pilot one set of objectives and risks (stemming from other initiatives — Basel, Dodd-Frank Act, for example), and expand. Each successive state adds risk capabilities and attributes.
- Have processes work top-down and others bottom-up. Communication and education is top-down; working teams develop the approach and migrate it upwards.

Establish Oversight and Governance

The Board and the CEO should collaborate to promote effectiveness and performance. This collaboration is best done by converting the framework and governance processes into policies that outline the philosophy, methodologies, technology, and accountabilities that support its execution. This effort must be supported by firm-wide communication and a powerful business risk organization under a designated senior level official, typically a Chief Risk Officer.
ROAD SKILLS

- Maintaining executive accountability is key to limiting program decay.
- Keep the process immediate and reinforced with regular, proactive dialogue and executive updates mapped to real issues and opportunities.

Implement a Common Taxonomy

To reduce potential confusion and miscommunication, the firm should operate under agreed definitions for process, risk, and control. Uniform language and referential content enables diverse teams, business lines, and functions to operate and dialogue successfully and to aggregate risks and responses into more meaningful categories. There are many classification schemes available.

The reality is that many firms cannot properly link spending on risk remediation to return on capital or are unable to model their economic capital accurately to include operational and strategic risk.

Standards, definitions, and approaches should be rolled out and executed on a waterfall basis to each business unit and function, which generally differ from the idiosyncratic ones within each business. Take full advantage of any overlaps.

ROAD SKILL

- Resolve different definitions early as they will leak through the entire program.

DEVELOP RISK MANAGEMENT CAPABILITIES

Largely a matter of culture and operating style, the program does not necessarily require highly sophisticated techniques, except where the firm’s complexity or profile demands it. Usually, an incremental process is called for. All involve the following elements:

Execute Risk Assessments

ERM implementation generally commences with an enterprise-wide risk assessment to identify and prioritize risks and establish risk inter-relationships. This assessment should span the firm — business and functional areas — and encompass all objectives to create a holistic, portfolio view of risk. Assessments can be conducted in a variety of ways from interviews to surveys, in-depth process analyses, or specific business line reviews. These methods can be executed in tandem or uniquely — largely a factor of resource and experience. Identify a tool for collating the risk inventory and results in a simplified way. Risk maps are one example; they are easy to use, understand, and communicate. It is important to appreciate that this exercise must be refreshed periodically as risks and objectives change.
Prioritize Risk
The value of ERM is more tangible and specific once risks are identified and prioritized. If the risk strategy and vision have been articulated well, risks should be prioritized using that strategy as the frame of reference.

Implement Risk Response Strategies
The COSO framework offers four alternatives.

- **Avoid**: Prevent exposure by eliminating the event. Actions include barring or deferring activity; implementing preventive controls; redefining business development hurdles; or divesting in specific markets.

- **Accept**: Leave in the current state and take no additional action. Actions include re-pricing products; offsetting or hedging, including financial reserves; or self-insuring.

- **Share**: Transfer the risk to an independent party to manage. Actions include indemnification; hedging; outsourcing; securitizing; or insuring/reinsuring.

- **Reduce**: Implement countermeasures (preventive, detective processes) to lower the level of residual risk to within tolerance levels. Actions include adding controls or periodic testing to confirm them; diversifying the risk by reducing concentration in any one product, strategy, geography; or redesigning processes.

Not all risks are controllable, and unintended consequences of risk adjustment must be carefully balanced against regulation (zero tolerance in some areas, such as the Office for Foreign Assets Control) and the reliability of data / judgment supporting observations.

**ROAD SKILL**

- Set realistic goals and integrate with other parallel activities (e.g., Balanced Score Card) and leverage other control groups.

**Quantify Risks: Performance Data, Analytics, and Metrics**
This element often creates significant resistance. Data needs to be relevant, timely, reliable, accurate, and complete. Disaggregated systems and difficulties to isolate data can be overwhelming, particularly if few of the required data elements exist or can be sourced. Consequently, data cleansing and gathering is intensive with little time available for data analysis.
Risk Measurement Techniques

- Risk Indicators — ratings, scoring levels
- Historical, Monte Carlo Simulations — probabilistic analysis
- Scenario Analysis — large factor changes
- Portfolio Analysis — risk pools
- Stress Testing — modified base cases

Nevertheless, this element should not be a rationale for avoiding ERM. Capabilities can be improved over time, starting with weighting on qualitative data and migration up the difficulty spectrum to a more quantitative approach. The final goal is to build ‘gold standards’, systematic processes, and robust data models to support key risk indicators (KRIs), and eventually scenario type /stress analyses and simulations.

The most important steps are:

- Clarify purpose — performance is generally retrospective versus assessment which is generally forward looking.
- Isolate data required for the different risk factors.
- Identify KRIs for executive dashboard reporting.
- Map data requirements for both direct and indirect measures of risk.

Here is some good news. Many data elements can be built or sourced in conjunction with other regulatory-driven initiatives such as Volcker, CCAR, and regulatory reporting, among others.

ROAD SKILLS

- Approach the future state from multiple perspectives (data points) versus a single data point.
- Partner risk specialists with business lines to analyze results.
- Consider initial trade-offs between accuracy versus agility, and balance between static and forecasting type activities.
- Clearly identify and define risk factors/variables — inherent, residual, impact (expected, unexpected loss), likelihood, velocity etc.
REPORT AND MONITOR

Reporting is inherently linked to the robustness of the methodologies and applications used to assess and measure risk. The more comprehensive the ERM solution, the more likely that the reporting components will provide timely, relevant, and meaningful support for dialogue and decision-making. Like other components, these capabilities will be built incrementally.

Reporting is a means to an end but it is not the end. Reporting activities should not be solely dependent on the degree of automation but should provide consistency, clear actions for response, and the appropriate balance between data versus information and messages. This activity is as much a design and quality issue as a technical issue. Lastly, while the ‘material’ is important, the audience should be cross functional so that the audience members can appropriately talk to and challenge the information.

Monitoring the implementation of enhancement opportunities and action plans, related both to the ERM program milestones and risk response strategies, is generally embedded within ‘normal’ management activities, including risk management, and internal audit assurance reviews. However, specialized attention, expertise, and sponsorship from the senior executive will likely accelerate the program.

AVOIDING THE POTHOLES — CHALLENGES TO THE PROGRAM

A critical point of failure is not recognizing the key objectives of ERM or the cultural shift it may require. With that as a basis, the common challenges are:

- **Investment and sponsorship:** Short-term funding and change of direction and leadership can destroy momentum.
- **Safe harbor:** Highlighting risks and gaps should not be penalized. Participants who are not rewarded for identification and mitigation activities may shut down.
- **Collaboration:** Lack of coordination and cooperation across the lines of defense can derail efficiency, obscure issues, or remove transparency.
- **Scale:** One size does not fit all, and not every risk warrants sophisticated techniques. Details may drown the big picture.
- **Breadth:** ERM objectives fall beyond the traditional compliance, financial-driven ones to those focused on optimization, strategic planning, and business opportunities. Failure to make that jump may only yield known results and not focus on value driven issues.
The Importance of Technology
Every ERM implementation is linked to technology. ERM systems need to gather and consolidate information from a wide variety of sources, including operational and risk measurement systems. The nemesis for many firms is paucity of the technology architecture supporting data collection. However, data is not the only feature of a successful ERM program.

Technology-based tools must also be able to handle assessment, reporting, document retention, inventory, and exposure analysis. These are often overlooked. There are solutions for many aspects but no one tool that provide all features. In the meantime, firms can leverage Governance, Risk, and Compliance tools used in internal control groups.

Variability is the enemy of operational effectiveness. Uncertainty is the enemy of decision-making. Risk intelligence is an important weapon and guard against these factors.

END OF THE ROAD
Executed well, an ERM program will reduce surprises, provide a portfolio view of risks, strengthen shareholder confidence, and enhance risk management capabilities.

ERM calls for a focus on unexpected loss and a broader focus on economic performance; environmental and social responsibility; human capital practices; and client and product reliability. Traditional risk responsibilities still dominate risk thinking, which calls for risk reduction. Risk opportunity is nevertheless gaining recognition as a critical decision-making activity, and risk adjusted strategic planning is increasingly a part of annual budgeting processes.

Avoiding losses is a hard case to make. However, we could all agree that while it is a good strategy to have car insurance, it is even better strategy to have the skills, awareness, and ability to avoid a crash completely. This cost of prevention is low compared to that of catastrophic failure.

Reading the road signs and driving within the ‘limits’ of our ability, but still making speedy progress, is the best way to navigate risk.

---

1 Such as: reputation, business strategies, client assets, proprietary models.
3 Risk can be passed to a more specialized third party. However, the concept of ‘independence’ must be viewed with caution, especially as firms are held increasingly responsible for the actions of their vendors.
4 Office for Foreign Assets Control: economic and trade sanctions regulation.
Financial Services Advisory Practice

The financial services industry is facing unprecedented challenges and risks – compliance with various provisions of Dodd Frank and Basel III for banks, SEC registration and examination for hedge funds and private equity, and increased regulatory oversight for broker dealers and trading firms. Institutions are bearing the cost of expanding their risk management and compliance programs while dealing with volatile markets and pressures on fees and margins. Requirements for maintaining a robust and secure network and information technology infrastructure continue to grow as regulators propose new rules to protect the industry from major systems failures and cyberattacks.

Berdon’s Financial Services Advisory Practice can assist your institution in navigating these challenges by helping you integrate and strengthen your risk management programs, test and enhance compliance policies and procedures, and develop a strong risk based internal audit program.

In 2015 alone, there were over 45,000 regulatory events which financial services firms needed to review for applicability and impact to their organization and which mark the beginning of a process of analysis, policy review, reporting and distribution. The pace, volume, and impact of regulatory change continues to accelerate. Learn how your firm can “ride the wave.”

Get your copy of Riding the Regulatory Wave at: http://info.berdonllp.com/ride-the-wave
Financial Services Advisory Practice

The financial services industry is facing unprecedented challenges and risks – compliance with various provisions of Dodd Frank and Basel III for banks, SEC registration and examination for hedge funds and private equity, and increased regulatory oversight for broker dealers and trading firms. Institutions are bearing the cost of expanding their risk management and compliance programs while dealing with volatile markets and pressures on fees and margins. Requirements for maintaining a robust and secure network and information technology infrastructure continue to grow as regulators propose new rules to protect the industry from major systems failures and cyber attacks.

Berdon’s Financial Services Advisory Practice can assist your institution in navigating these challenges by helping you integrate and strengthen your risk management programs, test and enhance compliance policies and procedures, and develop a strong risk based internal audit program.

Alexander Moshinsky, CPA, Director, Internal Controls & Risk Management at Berdon LLP, brings more than 25 years of experience in the financial services and other sectors — working with major companies and government regulatory agencies. You can reach Mr. Moshinsky at 212.331.7448 or amoshinsky@berdonllp.com.

For more information, contact your Berdon advisor: New York 212.832.0400 | Long Island 516.931.3100