Core Catalysts

Enterprise Risk Management (ERM)

ERM is a unique implementation process for every organization which provides many paths to success depending on industry, regulatory oversight, culture, program maturity, and resources. However, there are a number of key concepts that drive organizational acceptance and success:

Governance

In order for ERM to be embraced organizationally, there must be internal governance and leadership to drive the program's execution and evolution. A diverse, internal ERM Committee is very effective at overseeing the implementation and execution of the program. The ERM Committee reports to executive management and ultimately the Board of Directors. The Board is responsible for corporate guidance through the establishment of an ERM Policy, Risk Appetite Statement and Risk Tolerance Framework. An internal risk management team is an effective way to handle the day-to-day ERM responsibilities.

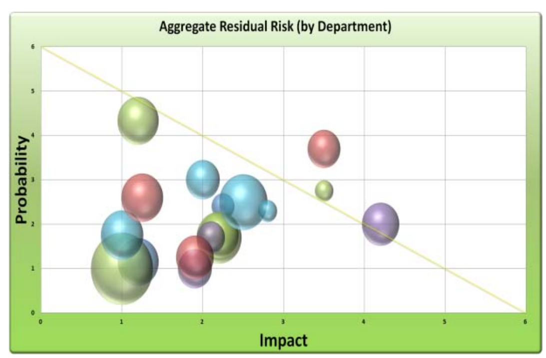
Top-Down Support

Senior leadership is an integral ERM support driver regardless of the timing of their contributions. Depending on an organization's ERM program maturity, senior leadership can adjust the timing and level of their involvement. The overall ERM framework is driven by an ERM Policy, Risk Appetite Statement, and Risk Tolerance Framework.

Bottom-Up Documentation

Leveraging all corporate resources provides a broad look into risk and allows management to evaluate and prioritize risk across the enterprise. The risk inventory can then be evaluated holistically. The inherent risk, based on the risk's probability and impact, can be measured based on the program's risk thresholds (e.g., 1 – 5 rating system). Once inherent risk is established, mitigating controls can then be identified and tied to the risk and a residual risk level can be identified.

Risk Evaluation



A chart is an effective tool to evaluate residual risk on a broad scale (see example). Residual risk can be used to evaluate each individual risk based on the Risk Appetite Statement and Risk Tolerance Framework to determine if the residual risk is acceptable or if remediation is necessary. If remediation is necessary, the program's remediation program should be implemented to bring the risk's Residual Risk within the appropriate probability and impact parameters.

Proactive Analytics

The real value of ERM is to proactively identify and prepare for risk before an event actually occurs or impacts the organization. To the extent possible, all risks should be tied to analytical metrics like (Key Risk Indicators or Key

Performance Indicators), which can then be tied to a dashboard and used as a tool. Established thresholds allow management to address issues based on trends or specific occurrences. Management can then prepare specific response(s) to the risks identified. This response and documentation is very effective for addressing the organization's regulatory needs.

Emerging Risks

An organization's risk environment is dynamic and ever changing; therefore, the organization's ERM program needs to address emerging risks and evaluate the potential probability and impact. This focus and integration into an organization's risk culture evolves management toward proactive risk identification as part of their normal operations.

Integration and Leverage

Most organizations have more than just ERM as an internal program. The holistic nature of ERM lends itself to integration with other programs. Other programs like Sarbanes Oxley (SOX) and regulatory compliance can be integrated with ERM, allowing multiple programs to leverage the same documentation (e.g., Governance, Risk Management and Compliance – aka GRC or database). A consolidated approach can drive efficiency throughout the organization, which allows management to minimize the time necessary to effectively execute each of the programs.

For more information, please contact Jim Wadella (jim.wadella@corecatalysts.com) or Greg Wallman (greg.wallman@corecatalysts.com) at 913-693-7969.