KEY PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

A set of common principles developed by RMA’s Operational Risk Council “by the industry, for the industry,” with an introduction by Spyro Karetsos, chair of the council.

The operational risk management community has traditionally relied on regulatory perspectives to establish practices and methodologies for its operational risk management (ORM) programs. As a team of ORM leaders, RMA’s Operational Risk Council decided it would be best to have a set of common principles developed “by the industry, for the industry.” The goal in drafting the principles was to make them so practical that they would resonate with any financial firm.

As chair of the RMA Operational Risk Council, I’m pleased to share our “Key Principles of Operational Risk Management.” We used our previously established operational risk framework as the foundation for the associated principles. Each principle aligns to an element of the framework to assist financial firms in establishing highly functional ORM programs.

Although the tactics required to implement and deploy the principles are expected to vary across firms to factor in local nuances, we hope these principles serve as a valuable resource for reference and benchmarking purposes.

— Spyro Karetsos
Principal, Director of Enterprise Risk Management, Vanguard

General Principles
Systemic risk in the industry is reduced and risk management activities are enhanced if institutions are given latitude to experiment with a variety of business models and organizational structures suiting their size, scale, and complexity. Enforcing identical approaches by all participants increases systemic risk.

Rapid changes in organizational structure and management approach will generate operational risk within an institution. Changes that are implemented in a measured fashion, not all at once, are more likely to be successful.

Risk management is an integral part of business management and should be incorporated into overall business and financial

October 2016 The RMA Journal 11
planning. Budgets, profit goals, and profitability targets should all be developed by fully incorporating potential risk outcomes, as well as the expenses required to administer risk controls.

Risk Culture
The basis for an effective operational risk management framework, a strong risk culture requires transparency regarding operational risk issues throughout the organization, including leadership and the businesses. Accordingly, the operational risk management function must be transparent as well.

Business culture within institutions must embrace the value of risk escalation and welcome independent challenge of risk decisions. Soliciting multiple points of view and engaging in debate result in better, more informed decisions.

Business culture must embrace constant questioning of established processes. A culture that embraces continuous, steady improvement should be encouraged.

Risk management influences a culture of proactive management that emphasizes risk-adjusted performance and incorporates regulatory compliance and best practices.

Business management should exhibit dedicated involvement in the risk management program.

Human resources practices should actively encourage rotation of talent within risk disciplines as well as to and from business leadership and risk roles. Experience in risk leadership should be considered a requirement for general management positions. Training and education programs should be developed and implemented to ensure that the business culture’s key principles are properly understood and consistently applied.

Risk Appetite
Institutions should develop and implement a risk appetite statement and relevant thresholds and limits based on the institution’s business model and tolerances. Considerations should include internal and external risk drivers and constraints.

BUSINESS CULTURE WITHIN
INSTITUTIONS MUST EMBRACE THE VALUE OF RISK ESCALATION AND WELCOME INDEPENDENT CHALLENGE OF RISK DECISIONS.

Communications
Timely, clear, and effective communication among the three lines of defense is critical to effective risk management.

Governance, Policies, and Procedures
Accountability is ensured through an effective governance structure that oversees the institution’s risk and control environment.

Senior management should provide direct oversight of current and emerging exposures. Meanwhile, risk management should be part of the normal management process and governance, not be made a separate, adjunct function.

Relationships should be established with qualified, high-performing professionals who are closely integrated with business operations and the decision-making processes.

Effective risk management is a basic responsibility of business leaders and managers, requiring them to

• Understand their institution’s risk appetite.
• Understand their actual and prospective risks.
• Define their risk exposures.
• Execute an effective strategy to mitigate controllable risk.
• Educate associates on the risks and how their responsibilities contribute to managing them.

Risk management defines, develops, maintains, and implements best-practice tools, frameworks, and risk management processes.

Risk Identification and Assessment
Institutions should strive to understand all the risks they face and their potential downside implications under a range of scenarios. They should develop control processes based on this understanding.

Moreover, institutions should develop a process to prioritize or rank risks and allocate risk management resources according to this prioritization.

Control Environment
Control development is an outgrowth of risk analysis; risk analysis should not be an outgrowth of the control environment.

Business management owns all risk mitigation activities within their respective span of operations.

The line of business uses the controls assessment framework to identify and document key controls. The strength of key controls (control design adequacy) is evaluated using the controls assessment framework’s criteria.

Control groups provide oversight of specific risk types.

There is a structured process for validating that key controls are operating effectively to meet business objectives.
In addition, there is cross-functional transparency in instances where the division relies on another division or an internal/external service provider for performing key controls. There must be clarity on accountabilities, responsibilities, and performance measurement based on agreed-upon standards.

Expert practitioners responsible for executing operations must have input into risk analysis and control design. Risk management activities dictated solely by remote oversight functions lacking detailed execution experience are highly prone to error and inefficiency.

**Monitoring and Reporting**
A well-developed risk reporting structure must be established and maintained. Emphasis should be placed on risk escalation and risk communication procedures for both current and potential operational risks.

Reporting of risk data should be supported by a sound and streamlined technology solution. Reporting systems need to provide different articulations of the contents and specific ways to develop the topics analyzed, depending on the objectives and recipients of the reports.

Risk management should partner with the business to address risk events in a timely way, escalate them as needed, and report accordingly.

**Quantification, Measurement, and Modeling**
Risk management follows a structured methodology for establishing and prioritizing its process universe and performing risk assessments based on inherent risk level.

When evaluating the risk level in a given activity, risk management practitioners should consider historical results over long periods to be an important indicator of future results, particularly if the fundamentals of the business activity and management approach have not changed.

Data should be used for analysis and modeling to support sound operational risk management practices and business decisions. A modeled approach is best suited to transactional-style risks with sufficient data points (tail-style conduct risk issues do not model well).

Risk management should have effective processes for measuring whether key exposures are increasing, decreasing, or remaining stable in order to take action as needed.

**Risk Decision-Making**
As part of sound business and strategic decision-making, operational risk implications must be assessed and considered in order to determine whether to
- Manage the risk.
- Tolerate the risk.
- Transfer the risk (for example, by insuring against the risk).
- Decline the risk.

**Incentivizing Behaviors**
Compensation practices should promote the risk culture of the institution, promote accountability of results, and incentivize appropriate decision-making and behaviors.