Risk Management Association

Advance Your World.


THE RISK MANAGEMENT ASSOCIATION

# Reputation Risk Management Framework

JANUARY 2020

# 1 INTRODUCTION

Reputation risk is regarded as the single biggest threat to a company's market value, yet many firms struggle with managing it. In his book *Intangibles: Management, Measurement, and Reporting,* Baruch Lev noted that, in a service economy, reputation and other intangible assets can be a significant portion of a firm's assets. He also included many examples demonstrating how damage to a company's reputation can have a deeper and more lasting impact than a financial loss.

# 2 PROBLEM STATEMENT

Reputation risk is difficult to quantify and manage. But as difficult as it may be to do, managing reputation risk is not optional and firms that fail to do so can find themselves managing not just reputation but a full-blown crisis.

In the 1990s, Ford equipped its popular Explorer SUVs with Firestone Wilderness radial tires prone to tread separation and failure. The situation was made worse by the vehicle's high center of gravity. The result was a spate of accidents—many involving rollovers—that were linked to 150 deaths and hundreds of injuries in the U.S.

After the problem came to light, Ford's response was widely seen as lacking. Critics said its CEO was not actively engaged, that Ford did not put customer safety first, that the company did not have a crisis communications plan, and that it was not proactive in seeking solutions. Ford struggled for several years with a poor reputation in the marketplace.

In contrast, when Johnson & Johnson learned in 1982 that sealed bottles of Tylenol contained capsules laced with cyanide that resulted in seven deaths, its CEO became actively engaged. From the outset, Johnson & Johnson was seen as placing customer safety first. It used public relations and advertising to communicate, and the company developed the industry's first triple-safety-seal pack—a glue-closed box, a plastic seal over the neck, and foil over the bottle's mouth. Tylenol managed to recapture its market share.

The bottom line is that companies need a strategy to manage reputation. Communication and being proactive are vital to this effort. In addition, senior management must be visible and demonstrate leadership, and a crisis management framework must be in place.

# 3 KEY ELEMENTS:

## REPUTATION RISK FRAMEWORK

The Federal Reserve System's Commercial Bank Examination Manual defines reputational risk as "the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions." Thought of another way, reputation is how a firm is viewed by its stakeholders and the general marketplace, and reputation risk management includes activities to enhance a firm's reputation.

Despite the importance of a firm's reputation, there are few tools for managing the risk to it. And risk managers are split on the concept, with some classifying reputation risk as a stand-alone risk and others seeing it as a byproduct of other risks. Regardless of its taxonomy, reputation risk is dynamic—not static—and risk managers must play a role in maintaining, protecting, and, if necessary, repairing a firm's reputation with its stakeholders.

Crisis management is the set of procedures that are initiated when a significant event threatens the firm. After a crisis has already erupted, there is little room for flexibility as the company must deal with the root cause of the event. Communication is vital once a crisis occurs, and it is important that the communication be authentic and display concern, a commitment to fix the issue, and leadership.

Firms that attract, retain, develop, and empower top talent are in the best position to enhance their reputation and avoid having to manage a crisis. Many control breakdowns that erupted into full-blown crises could have been avoided had the people involved recognized the potential severity of the situation and dealt with the root causes.

Culture is a critical component of any successful company and the tone from the top is important. As firms get larger, more diverse, and increasingly complicated, it becomes harder for them to remain steadfast in applying the values that foster good corporate culture.

The Australian Securities and Investment Commission (ASIC) has identified seven key drivers of good culture: Tone from the top; Cascading values to the rest of the organization; Translating values into business practices; Accountability; Effective communication and challenge; Recruitment, training, and rewards; and Governance and control.

These seven drivers provide a useful point for boards and management to start thinking about culture. They are similar to the key drivers remarked upon by William C. Dudley, president of the Federal Reserve Bank of New York, at the Workshop on Reforming Culture and Behavior in the Financial Services Industry on October 20, 2014. At that event, Dudley said, "Firms must take a comprehensive approach to improving their culture that encompasses recruitment, onboarding, career development, performance reviews, pay, and promotion."

Similarly, the United Kingdom's Financial Conduct Authority (FCA) in a March 2014 guide, "The FCA's Approach to Supervision for C3 Firms," stated that it would examine the governance, business models, strategy, culture, frontline business processes, systems, and controls of organizations to determine how they put integrity of the market and fair treatment of consumers at the heart of their business.

However, the difficulty with corporate culture is that the concept is nebulous, subjective, and difficult to measure quantitatively. In a speech on November 20, 2015, Greg Medcraft, chairman of the ASIC, noted, "Trust and confidence is critical to the operation of the financial system. Poor culture can undermine that trust and confidence." He also remarked that "culture is important to us as regulators because it drives conduct."

To determine culture, we need a way to test the health of the internal operating environment. The next section will attempt to establish a basic framework that management can use to assess the health of corporate culture.

## 3.1 Measuring Cultural Health

### 3.1.1 Cultural Assessment

A cultural assessment is a tool that management can use to help measure the difference between the current culture and the desired culture. Management can review specific areas to determine the health of the firm's risk culture and assess its strengths and weaknesses. The assessment can also be used to ensure that the firm's culture aligns with and supports the firm's stated business objectives and corporate values.

An example of an effective cultural assessment is provided by Anthony Ciavarelli, who worked with U.S. Navy fighter pilots. Ciavarelli used a cultural assessment that helped improve flight safety, and he had to do that within a culture that accepts risk as a normal course of action.

Clearly, it's impossible to take risk out of military preparations, but Ciavarelli showed that risk can be reduced by assessing the presence of accurate perceptions, effective risk management, and awareness. His work serves as an example of how a cultural assessment can help transform an organization.

### 3.1.2 Board and Management Reporting

If a firm values risk and control, then risk metrics must be incorporated in board and management reporting. The firm can start by reviewing the board package to determine if the level of reporting is sufficient to keep the directors well informed. In addition, minutes and agendas of meetings can be reviewed to determine the depth of discussion and the coverage of risk management topics. The following areas could be included in the reports:

- Material risk events (losses and near misses) above a certain threshold, which are often referred to as high-impact, low-frequency events. What is the cause, what is the remediation, and what is the status of the remediation?

- Lower-dollar-threshold risk events, but reported by causation category. These low-impact, high-frequency events are too small to focus on individually, but at what point do a large number of small events present a systemic risk?

- Does the board have a risk appetite statement and a risk appetite scorecard? The statement allows the firm to state in a qualitative way what's in and out of scope in terms of assumption of risk. The scorecard, however, is built from a quantitative approach that allows specific risks to be measured and reported.

- Does the board have key risk indicators acting as forward measures of risk? Supporting the firm's risk appetite, these indicators can be based on the three risk disciplines and act as a consolidated view of the firm's risk profile.

- Does the board review the audit plan, regulatory examinations, failed audits, and the status of open control issues?

- This review can be combined with an analysis of the robustness of risk management reporting. Management should be able to demonstrate through its reports that it has employed risk metrics and that it is using these metrics as part of its decision-making. Posing the following questions is a good start:
- Does management reporting reflect the full span of responsibility?
- Does management have key risk indicators?
- Is management review able to control lapses and perform root-cause analysis?
- Are remediation plans monitored for follow-up?
- Does management monitor mandatory compliance and regulatory training?
- Is there a system allowing for identification and escalation of self-identified issues?

### 3.1.3 Compensation

Compensation is usually thought of as sales compensation and has become identified with incentives for overly aggressive sales practices. If possible, sales compensation should always be determined on a risk-adjusted basis. The best example is basing the compensation of a loan officer on the risk-adjusted return of a new loan.

However, some products do not have such measures, an example being pharmaceuticals. For these products, there is a relationship between fixed compensation (salary) and variable compensation (sales commissions). If compensation is heavily weighted toward the variable, there is an incentive to ramp up sales.

Conversely, if compensation is heavily weighted toward salary, there may not be enough incentive to generate sales. Human resources should conduct an analysis weighing the balance between fixed and variable compensation. The goal is to employ a risk-based input for sales such that management is comfortable with the balance and approves the compensation plan.

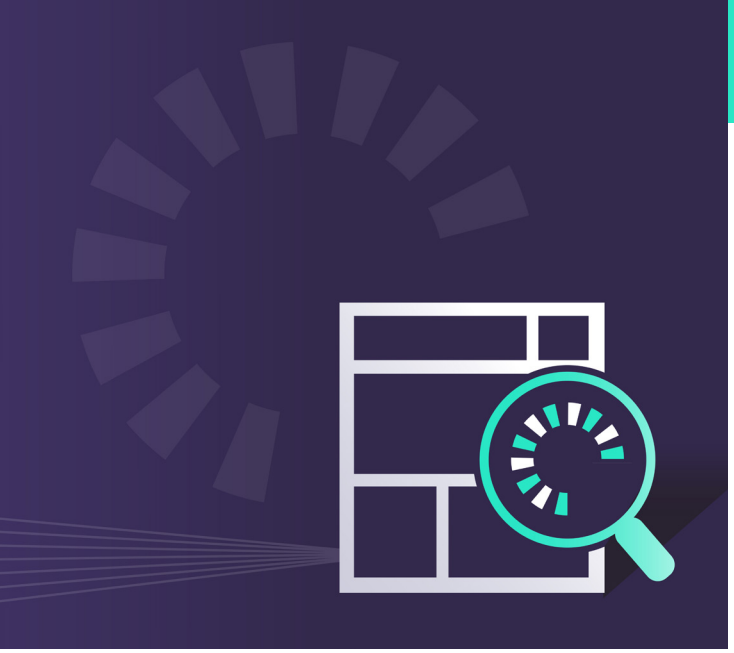
Regulators are evaluating the use of multiples for executive pay and, since the 2008-09 recession, have implemented executive pay restrictions at banks. From a cultural perspective, however, the main point for management is that if executive compensation and overall associate compensation are not aligned, some associates may feel disenfranchised. And in many financial institutions, associates in fairly junior levels have access to items of value, and they control movements of cash and other valuables.

Many studies support the premise that internal fraud is more prevalent than external fraud. Some of that can be linked to hiring practices, but some of it can also be attributed to compensation and culture. As noted previously, culture drives conduct.

### 3.1.4 Budget and Planning Processes

A review of budget assumptions and projections can be critical to determining if management is under pressure to grow revenue because of overly optimistic growth assumptions.

Growth assumptions based on sound quantitative risk management and objective economic metrics offer better probabilities. If projections are overly optimistic, the firm may find itself in a position where sales practices become questionable or, alternatively, controls could be relaxed in order to increase net income. Firms need to grow and take on risk, but overly optimistic growth assumptions can have unintended consequences.



### 3.1.5 Structure and Stature of Risk and Control Functions

Independence of risk and control functions is fairly easy to verify; one need only look at an organizational chart. But although independence is critical, it's also important to evaluate stature—and that is much more difficult. Stature in a firm can be determined in several different ways:

- Compare the seniority of titles between risk and control positions to other areas within the firm. If a firm places a high value on risk and control, one would expect those views to be represented in senior management.
- Review the agenda of recent management meetings to determine if risk, compliance, and controls are active topics.
- Look at the workspace of the risk and compliance functions and that of their business partners. Risk and compliance should be clean and functional.
- Risk, compliance, and audit functions should be evaluated to determine if staff, training budgets, and level of expertise are sufficient. The more complex an organization, the more highly trained and staffed its functions should be.
- Level of turnover and the main reasons behind the turnover can be used to evaluate whether risk and control positions are valued by a firm. To be clear, some level of turnover is healthy. But what needs to be determined is if turnover in the risk and control groups (indeed all groups) is excessive.

The above is not meant to be a one-sided assessment. Risk and control functions should have sufficient stature and be staffed by qualified people. However, if these functions actually have too much say in how a business is run, the result may be loss of business and loss of shareholder value. If risk taking is removed from the equation or if there are non-value and/or redundant controls, the result is a lower return.

The objective is to ensure risk and control functions have adequate stature, staff, and resources and can act in a constructive way to ensure the business understands the risks it is taking—and that managers have sufficient controls in place to manage the firm in a safe and sound manner.

As noted by William Dudley in his remarks at the Workshop on Reforming Culture and Behavior, "The problems originate from the culture of the firms, and the culture is largely shaped by the firm's leadership. This means that the solution needs to originate from within the firms, from their leaders."

Although culture is nebulous, management can focus on several key drivers to determine the health of a firm's culture. These measures can be combined with cultural assessments that are completed by the firm's associates. The financial sector plays a critical intermediary role in allocating capital in the global economy. And for the economy to achieve sustainable growth, we need a financial sector that is healthy and has the public's trust.

### 3.2 Fully Integrated Risk Management

A fully integrated risk management function that spans the core risk disciplines is perfectly positioned within the firm to take the lead in managing reputation risk. For that approach to work, however, the board must allow a fully independent risk function. Without this tone from the top, the effectiveness of any risk function is neutralized.

In addition, executive management must give the risk function appropriate resources and establish it as a strategic asset driven by data and analytics.

Market risk and credit risk will result in financial losses, but companies can recover as long as they have sufficient liquidity and capital. However, the perception that a firm cannot handle a significant reputational risk event that develops into a full-blown crisis can have severe consequences.

Risk management must establish monitoring systems that cover the external and internal environments. The external environment includes things like global markets, regulatory actions, clearing-houses and industry utilities, critical vendors, natural disasters, and geopolitical events. The internal environment includes systems performance, transactions processing, human capital risk, internal fraud, and cyber risk.

Data flows into risk systems and allows risk managers to monitor the external and internal environments, acting like an early warning system. The data can be categorized in three ways: 1) what you know, 2) what you don't know but should know, and 3) things you will never know.

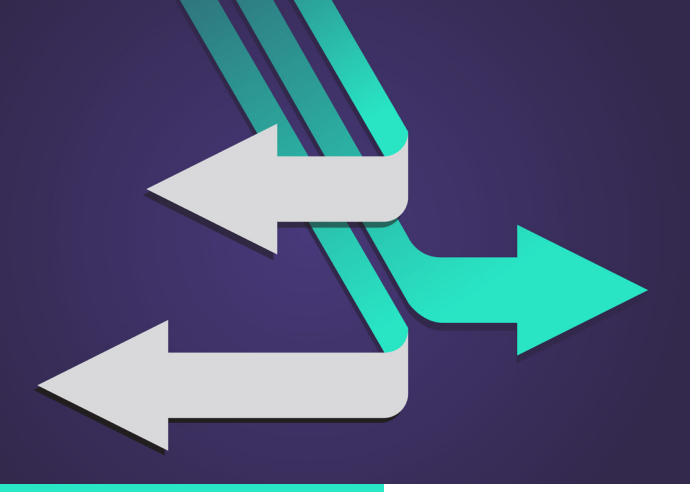
For the known data points, risk managers must identify the known risks and assess the potential impacts. This is the start of identifying emerging risks that could preclude a business from meeting its objectives. Because emerging risks could have an impact on a firm's reputation, they must be analyzed and risk-graded, and responses must be drafted.

Then there are things risk managers do not know but should know. An example would be if load/balance metrics are not being used to determine whether the capacity of critical applications and systems is constrained. In such cases, it's crucial to close the information gaps.

The risks that will never be known are largely random events. Despite their unpredictability, they still need to be addressed through business continuity and disaster recovery planning, scenario analysis and simulation exercises, and insurance coverage. It is the existence of random events and their impact that make modeling reputation risk so difficult. Operational risk is often subject to random events; thus for reputation risk to be managed, it is critical to have a fully implemented operational risk framework across the firm that is embedded in each functional area.

Known or emerging risks must be analyzed to assess their likelihood and potential severity. If a risk presents a material exposure to the firm, it must be escalated. Being able to identify risks that could preclude a firm from meeting its business objectives is critical. Whether an event is linked to an emerging risk or occurs randomly, the key is to have a coordinated response based on set criteria and escalation protocols that involve the appropriate level of management.

The above implies a difference between event management and crisis management. The vast majority of risk events never rise to the level of a crisis and are handled as part of the normal routine. Even so, guarding reputation requires a systematic way to capture data and identify material events that could preclude the firm from meeting its business objectives. Those are the events that must be escalated to executive management. Studies have shown that executive management's engagement is critical for minimizing downside impacts and avoiding dire consequences when a crisis engulfs a firm.



Risk can be defined many different ways with one definition being that risk is the potential for a deviation from an expected result. Risk management is the process through which risks are identified, evaluated, and analyzed, ultimately leading to a decision on what risk to assume, avoid, or mitigate.

Market risk is the risk of adverse movement in market factors, such as asset prices, foreign exchange, or interest rates. Credit risk is the risk of loss resulting from failure of obligors to honor their payments. Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events. Operational risk is often disaggregated into specific risk types such as follows:

- Human capital risk
- Business process risk
- Technology risk
- Financial reporting risk
- Legal and regulatory risk
- Fiduciary risk
- Dependency risk
- Business resiliency risk

Operational risk management (ORM) presents some unique challenges. Where market and credit risk decisions are based on discrete decision-making, operational risk is implicit and could come from both internal and external events. The data needed to manage operational risk is decentralized within the organization, or it could come from the external environment. On the other hand, much of the data needed for market and credit risk is market derived data.

Many institutions have adopted the Loss Distribution Approach toward calculating operational risk capital, but the predictive value of historic loss data needs further testing. While historical loss experience is helpful in quantifying loss exposure, both technology advances and process changes may result in exposure levels that differ from historical experience.

A particular key area that ORM can fill is a coordinating role among the various control groups to leverage work performed and ensure a complete front-to-back review and oversight of key processes. This is not a parallel structure. Rather it is acting as a strategic coordinating function that ensures tactical implementation is done at the business level while existing control groups perform monitoring and avoid overlap.

### 3.3 Market and Credit Risk Management

Market and credit risk management (also known as financial risk management or FRM) is a key component of an effective integrated risk management function at financial institutions. This section establishes specific coponents needed to have an effective FRM function.

Risk limits are specific boundaries that act as guardrails for business management to make decisions on those types of positions that are within the tolerance levels set by the firm. Breach protocols are established in order to have both response and escalation when tolerance thresholds are breached.

Various events and decisions can impact financial exposure. Accordingly, FRM needs to have risk identification processes in place to identify risks to management and risk management. In particular, emerging risks are potential volatility catalysts that need to be monitored and incorporated into ongoing risk management practices.

Not every risk presents a material and imminent exposure to firms. Risk activities must include an assessment and quantification of various risks to determine likelihood and impact. This quantification will lend itself to a standard risk rating scale and aggregation to ensure impact is looked at relative to the firm's risk profile.

Scenario analysis and stress testing are often used to determine the potential financial impact of extreme or tailend risk events that firms can use to measure impact to trading positions, client accounts, or earnings.

FRM typically uses various risk indicators, reporting, and escalation protocols to ensure information is disseminated throughout the firm to drive management decision-making and to inform the risk governance structures through various committees.

### 3.4 Operational Risk Management

The Basel Committee on Banking Supervision (the Committee) wrote a paper that established a set of principles for an operational risk framework. This paper, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003, can be found at (www.bis.org).

In *Sound Practices for the Management and Supervision of Operational Risk*, the Committee noted that any firm's approach to operational risk can be influenced by size and complexity, but the Committee clearly established several crucial elements that comprise an effective operational risk framework:

- Clear strategies and oversight by the board of directors and senior management
- A strong operational risk culture
- Effective internal reporting
- Contingency planning

The definition of operational risk is expansive and the Committee recognized that individual firms could adopt their own classifications. The Committee, however, established operational risk event types in order to highlight those types of events that could lead to significant losses:

- Internal fraud
- External fraud
- Employment practices and workplace safety
- Clients, products, and business practices
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery, and process management

### 3.4.1 Developing an Appropriate Risk Management Environment

The Committee places responsibility with the board of directors to understand the firm's operational risks and to periodically review the firm's operational risk management framework. The Committee notes the framework should define operational risk and establish those principles through which operational risk is identified, assessed, monitored, and mitigated. The board is also responsible for establishing a management structure that is able to implement the operational risk framework, with clear lines of management responsibility, accountability, and reporting. The board should review the framework periodically and the paper notes that risks arising from external market changes and other environmental changes are managed, as are new products, activities and systems.

The board is also responsible for ensuring the operational risk management framework is subject to internal audit and that audit has sufficient resources, but the Committee noted that internal audit should not be directly responsible for the operational risk framework.

Senior management is responsible for implementing the operational risk framework and for ensuring qualified staff is retained with necessary experience and technical skills. Management is also responsible for implementing appropriate policies, procedures, and practices for managing operational risk, and for effective remuneration plans.

### 3.4.2 Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control

Operational risk should be identified and assessed across all material products, activities, processes, and systems. This also includes new products, activities, processes and systems. There should be a process to monitor operational risk profiles and material exposure to losses, along with reporting to senior management and the board. The firm should review its risk mitigation and control strategies and make adjustments when needed, and provide for effective business continuity planning.

Tools used to identify and assess operational risk include:

- Self-assessment and risk assessments whereby a firm assesses its operations against potential vulnerabilities
- Risk mapping of various functions and process flows to risk types to determine weaknesses for prioritization
- Risk indicators comprised of statistics and metrics to provide insight on the firm's risk profile
- Measurement that tracks and records the frequency and severity of various loss and other risk events, possibly using external loss data and scenario analysis

Senior management should receive regular reports and risk reports that include financial, operational, compliance, and external market information to support decision-making. Reports should be reviewed regularly to verify timeliness, accuracy, and relevance.

For all material operational risk identified, management must decide what risk can be controlled and what cannot be controlled. For risk that can be controlled management must decide what risk is assumed and what risk is mitigated. For those risks that cannot be controlled management must decide what to accept, reduce, or avoid completely.

Some risks that are beyond a firm's ability to control, such as a server event that could impair a firm's communication and technology infrastructure, require a disaster recovery and business continuity plan to address those types of events the firm might be vulnerable to.

The Committee also highlighted the need to have the framework reinforced through a strong culture that promotes sound risk management. In addition to segregation of duties firms should ensure practices are in place for the following:

- Monitoring adherence to assigned limits and thresholds
- Maintaining safeguards for access and use of assets and records
- Ensuring associates have expertise and training
- Ensuring financial returns are not out of line with expectations
- Verifying and reconciling transactions and accounts

### 3.4.3 Role of Supervisors

Regulatory supervision requires firms to have an effective operational risk framework in place to identify, assess, monitor, and mitigate material risks as part of its overall risk management program. Supervisors also conduct reviews to determine effectiveness and deploy additional mechanisms for them to be apprised of progress.

### 3.4.4 Role of Disclosure

Firms should have adequate disclosures to allow market participants to assess the firm's approach to risk management.

### 3.5 Internal Routine and Control

The Committee also wrote a paper that established a set of principles for an internal control framework. This paper, *Framework for Internal Control Systems in Banking Organizations*, September 1998, can be found at www.bis.org.

The Committee studied control breakdowns to identify root causes for control deficiencies. These breakdowns were consigned to one of the following five categories:

- Lack of adequate management oversight and accountability, and failure to develop a strong internal control culture
- Inadequate recognition and assessment of the risk in certain activities, whether on-or off-balance sheet
- Absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance
- Inadequate communication of information between levels of management, especially escalation of problems
- Inadequate or ineffective audit programs and monitoring activities

Internal control is a continual process. It is not a single procedure completed at a point in time, and it must be implemented at all levels within a firm. The main objectives of the internal control process are:

- Performance objectives – efficiency and effectiveness of activities
- Information objectives – reliability, completeness, and timeliness of financial and management information
- Compliance objectives – compliance with applicable laws and regulations

In *Framework for Internal Control Systems in Banking Organizations*, the Committee established a clear set of principles that can be used when evaluating a firm's internal control system (the paper itself refers to banks but the principles are applicable to every firm). These principles are organized around the following inter-related categories:

- Management oversight and the control culture
- Risk recognition and assessment
- Control activities and segregation of duties
- Information and communication
- Monitoring activities and correcting deficiencies
- Evaluation of internal control systems by supervisory authorities

### 3.5.1 Management Oversight and the Control Culture

The board is ultimately responsible for ensuring there is an effective system for internal controls. The board should approve and review the overall strategy and significant policies. The board should understand the major risks facing the firm and ensure that senior management has taken those steps necessary to execute a system of internal controls.

Senior management as part of its responsibility for execution should develop processes that identify, measure, monitor, and control risks. This includes having an organizational structure with clear lines of authority, responsibility, and, when necessary, delegation.

The board and management are jointly responsible for promoting ethical and integrity standards, and the overall culture of control and compliance.

### 3.5.2 Risk Recognition and Assessment

A sound system for internal control includes an understanding of those risks that could preclude the firm from meeting its objectives, and such risks need to be continually assessed. This assessment is on the full portfolio of risks and may result in a revised internal control system.

### 3.5.3 Control Activities and Segregation of Duties

Control activities are a critical part of daily activities and an appropriate control structure with activities needs to be implemented through every level of a firm. Control activities include:

- Top level reviews
- Activity control for different parts of the firm
- Physical controls
- Checking for adherence to exposure limits
- Follow-up for non-compliance
- Properly established approvals and authorization
- A system for verification and reconciliation

There should be proper segregation of duties and potential conflicts of interest should be identified, mitigated, and subject to review.

### 3.5.4 Information and Communication

An effective internal control system should address both internal and external information that is needed to support decision-making. This information should be reliable, timely, accessible, and in a consistent format.

Information systems within the firm must be reliable, secure, and have independent monitoring and adequate contingency planning. Communication channels should ensure that all staff fully understand and adhere to policies and procedures.

### 3.5.5 Monitoring Activities and Correcting Deficiencies

Both management and internal audit must continually monitor the effectiveness of the internal control system. Key risks should be monitored as part of daily activities. Internal audit must be independent and properly trained, and the audit function should report directly to either the board or its audit committee, and to senior management. Internal control deficiencies, regardless of who identified them, should be timely reported to the proper level of management to ensure deficiencies are addressed promptly.

### 3.5.6 Evaluation of Internal Control Systems by Supervisory Authorities

Regulators should ensure that all firms, regardless of size, have an effective internal control system that reflects the complexity of the firm. Internal control systems found not to be effective should force prompt corrective action.

### 3.6 Enterprise Risk Management

Enterprise Risk Management (ERM) was introduced in 2004 when the Committee of Sponsored Organizations (COSO) issued its Enterprise Risk Management – Integrated Framework (www.coso.org). COSO defined ERM as a process performed by the board, management, and other personnel, and applied in a strategy setting across the firm. It is intended to identify potential risks that could impact the firm. ERM allows the firm to manage risk to be within its accepted risk appetite, and provides reasonable assurance regarding the achievement of firm objectives.

The integrated framework organizes firm objectives into four categories:

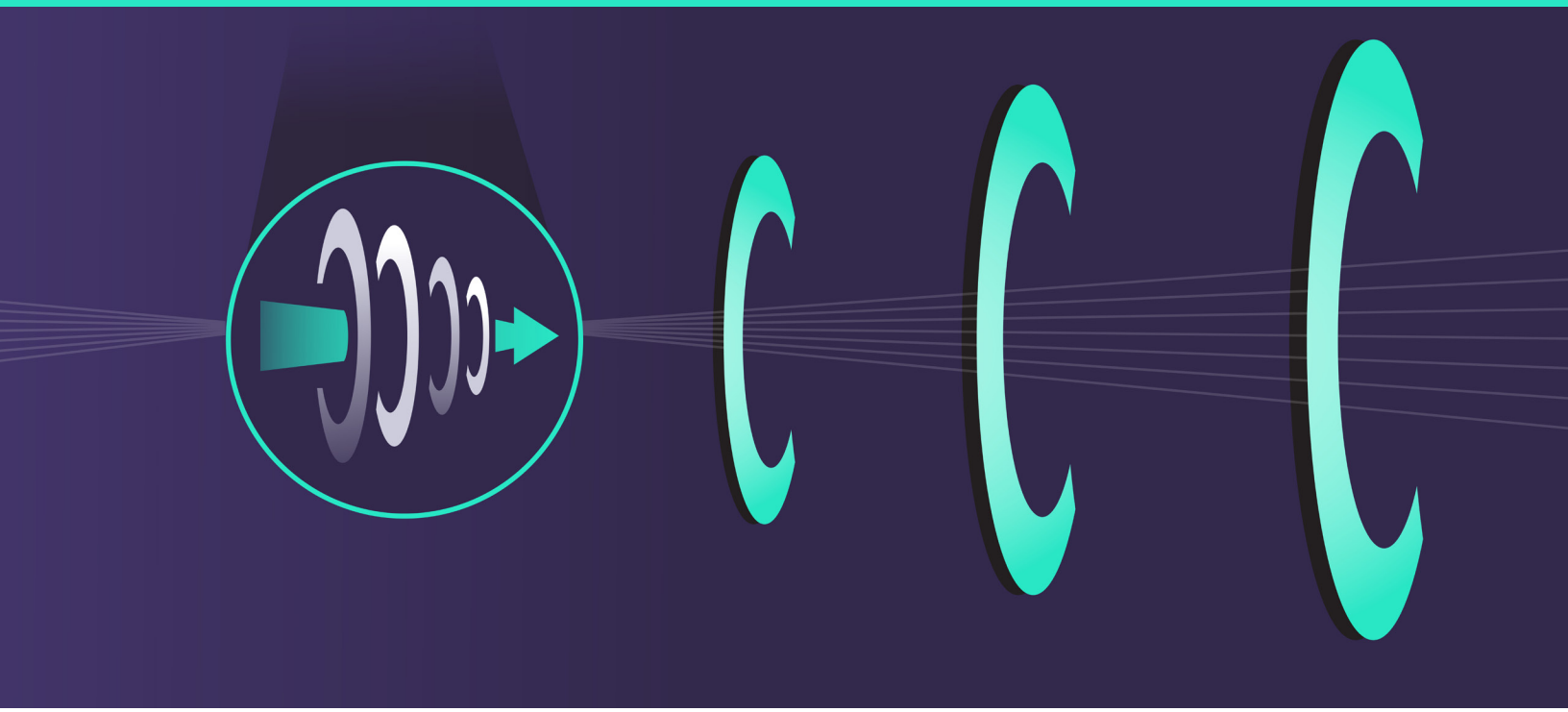
1. Strategic
2. Operations
3. Reporting
4. Compliance

Strategic objectives are part of the ERM framework and COSO defines strategic objectives as high-level goals that are aligned with and support the goals of an organization. Strategic objectives are core to the overall strategy of the firm. Strategic risk management is a critical part of a firm's overall ERM program.

Even though ERM was introduced in 2004 many firms have been slow to adopt it because of the various challenges that need to be overcome. Historically, risk has been managed in silos, and while firms have been migrating to a more integrated and enterprise-wide approach, progress has been slow. Some of the challenges for ERM teams include:

- Data Management Skills: Risk management teams need not just analysts but also people with technology backgrounds, especially in the discipline of data science. Data is an element that drives risk management and it is our ability to harness data that provides the valuable information needed for impactful analysis.
- Risk Taxonomy: There should be a consistent definition of risk throughout the firm so everybody is speaking the same language.
- Consistent Analysis: Analysis is a disciplined and formal process that associates need to be trained for in order to get a base level of skill that is required.
- Portfolio Reporting: Information resides in pockets throughout firms but it is critical for ERM to link these pockets of information and provide horizontal and vertical integration of information across the firm.

In the same way strategy requires a plan for execution, ERM must include the underlying market, credit, and operational risk disciplines to be effective. Otherwise ERM runs the risk of being isolated from the running of the business and could become an ivory tower.



### 3.6.1 What ERM Means for Risk Managers

ERM is a process in which each of the risk disciplines works within a dynamic process of gathering internal and external data that feeds into their respective risk systems, but these separate data streams become aggregated, taking into account intra-risk relationships. The output of this exercise is management information that can be used at the appropriate level to ensure each management level has sufficient information to deal with uncertainty tand has sufficient information to support decision-making.

ERM represents a portfolio view of risk that provides a holistic view of the organization and seeks to understand how all risks, internal and external, faced by the organization can ultimately impact the organization. The objective for the risk disciplines is to understand how the various pieces of risk management fit together within an accepted framework and determine how this framework can best support strategic and tactical decision-making with the goal of supporting firm strategy.

### 3.7 Crisis Management

Effective crisis management requires an integrated risk function that can spot and escalate emerging risks, as well as a fully developed event management process that handles less impactful events as routine. This filtering and escalation process allows executive management to focus on the material events. When these occur, there must be a crisis management plan in place that provides a playbook for key roles and actions. Communication should begin as early as possible and be repeated as often as needed to keep all stakeholders updated. Moreover, it should involve various channels of communication, including social media.

### 3.8 Stakeholder Analysis

Stakeholder theory is a broader concept than the traditional focus on shareholders, and it presupposes there are various groups, in addition to shareholders, whose needs the firm should address. These stakeholders can be associates, vendors, regulators, community groups, and numerous others. Stakeholder theory also includes the concept of reputation capital, in which a firm tries to quantify its reputation relative to its key stakeholders. In his rese arch paper "Reputation Risk: A Corporate Governance Perspective," Matteo Tonello of the Conference Board sought to identify key stakeholder relations in several categories:

- Enabling – provide and control resources the firm needs to operate
- Customer – demand for output
- Normative – sets rules and standards
- Peer – other firms
- Special interests – community or activist groups

Once key stakeholders are identified and organized, they can be analyzed to determine their level of criticality to the firm. In their book *Exploring Corporate Strategy*, authors Gerry Johnson, Kevan Scholes, and Richard Whittington note that assessing the importance of stakeholder expectations consists of three main issues:

1. Is the stakeholder likely to impress its expectations on the firm?
2. Does the stakeholder have the means to impress its expectations on the firm?
3. What is the likely impact?

This analysis can highlight stakeholders who have the most power and interest, which can help set the firm's engagement strategy with them during efforts to manage and enhance reputation.

## 4 CONCLUSION

Managing reputation risk requires a multifaceted approach. Risk management is well positioned to play an integral role in maintaining and strengthening a firm's reputation. A fully integrated risk framework mandated by the board and implemented consistently throughout the organization is a key component, and risk managers must establish monitoring mechanisms, tolerance levels, escalation policies, and communication protocols.

In the event reputation risk leads to a full-blown crisis, firms need to have established a crisis management plan that is embraced by senior management. Stakeholder analysis can be used to identify critical stakeholders who are in the best position to maintain and build a firm's reputation. The key role for risk managers is to develop and deploy proactive data-and-analytics techniques that provide strategic value to the firm's stakeholders.

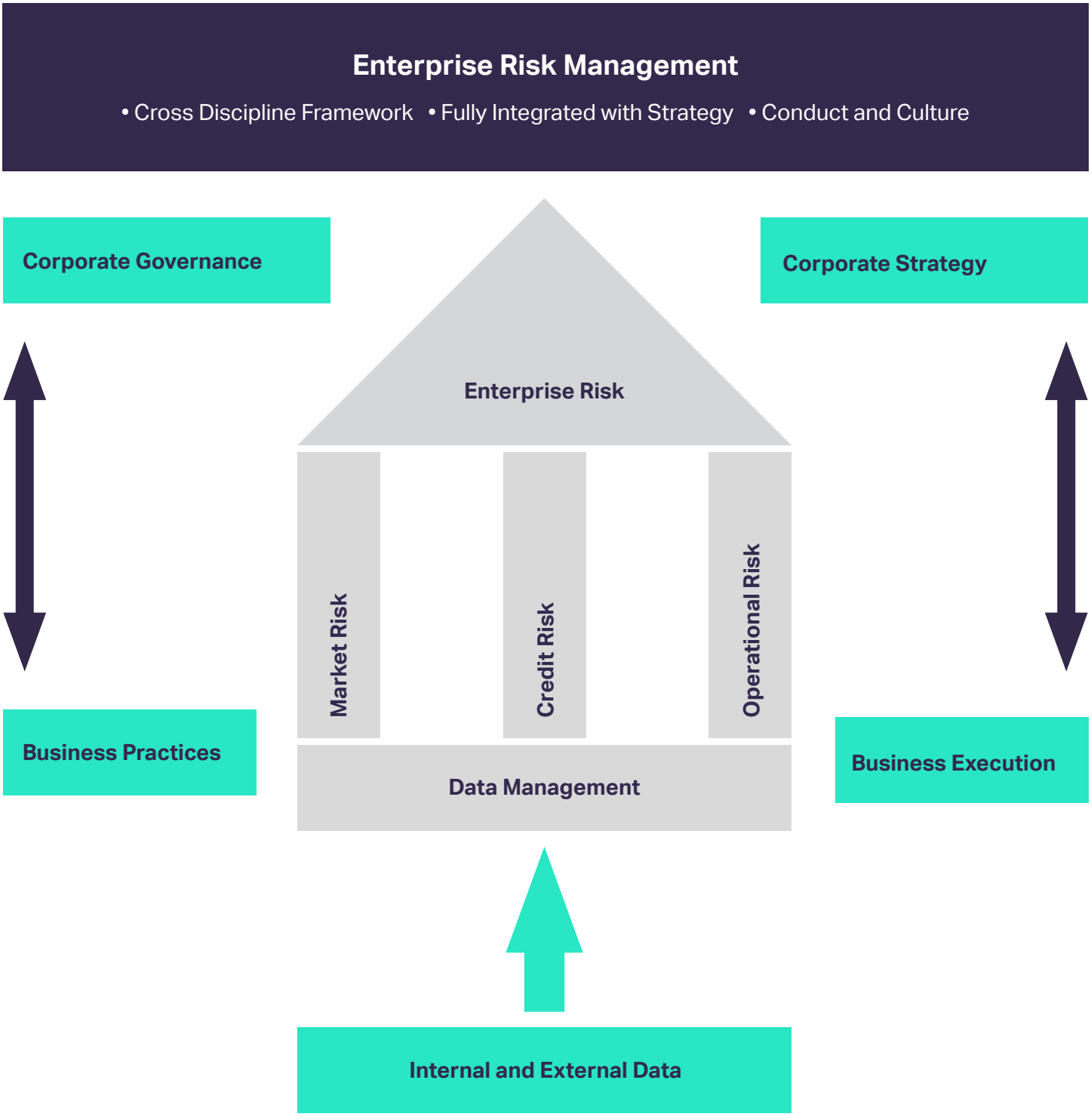
# DIAGRAM:
# ENTERPRISE RISK FRAMEWORK

**Enterprise Risk Framework**

- Culture and Risk Governance
- Strategic Risk Framework
- Emerging Risk Framework
- Reputation Risk Framework

| Market Risk Framework | Credit Risk Framework | Operational Risk Framework |
|---|---|---|
| Market Risk Policies | Credit Risk Policies | Operational Risk Policies |
| Implementing Procedures | Implementing Procedures | Implementing Procedures |

# DIAGRAM:
# ENTERPRISE RISK MANAGEMENT



# APPENDIX

We gratefully acknowledge the efforts of the members of the Operational Risk Council and Enterprise Risk Management Council:

| OPERATIONAL RISK COUNCIL |
| --- |
| Joseph A. Iraci, TD Ameritrade Holding, Chair |
| Michael Abriatis, PNC Financial Services Group |
| Erin Amerlan, Charles Schwab & Co Inc |
| Jennifer Aydelott, Wells Fargo Bank NA |
| Erika Crandall, Reserve Trust |
| Roy D'Sa, Huntington National Bank |
| Alan Freeman, Citibank NA |
| Mary M. Kapferer, KeyCorp |
| Sandra Laughlin, MidCountry Bank |
| Janet Lerch, US Bank National Association |
| Christopher Nestore, TD Bank National Association |
| Erin Straits, Wells Fargo Bank NA |
| Mark Williams, Zions Bancorporation NA |

| ENTERPRISE RISK MANAGEMENT COUNCIL |
| --- |
| Mark W. Midkiff, KeyBank NA, Chair |
| Joanne H. Aron, HSBC Bank USA NA |
| Didier Blanchard, Societe Generale |
| George Buchanan, Regions Bank |
| Lori Calhoun, Dollar Bank FSB |
| Stephen Carmichael, Discover Financial Services |
| James Dunne, TCF National Bank |
| Eric Ensmann, BBVA USA |
| Tobi Fess, TD Bank National Association |
| Anne Furlong, US Bank National Association |
| Rajesh Gopal, Bank of the West |
| Amy Jackson, TD Bank Financial Group |
| Mark Williams, Zions Bancorporation NA |
| Rajeev Lakra, JPMorgan Chase Bank NA |
| Emily Nachlas, Western Alliance Bank |
| Thomas O'Hara, Huntington National Bank |
| Jennifer O'Reilly, First Republic Bank |
| Brent M. Poley, Charles Schwab & Co Inc |
| Lori Rupp, First Citizens Bank & Trust Co |
| Edward P. Schreiber, Zions Bancorporation NA |
| Maria Teresa Tejada, Wells Fargo & Co |
| Oscar Trejo, PNC Bank NA |
| Azlina Wetmore, Capital One National Association |
| Brady Wise, PNC Financial Services Group |
| David Wright |