

WHITE PAPER

Developing An Effective Enterprise Risk Management Framework



Succeed. Transform. Compute. Perform.

Developing an Effective Enterprise Risk Management (ERM) Framework



An effective ERM provides management with a system of oversight, control and discipline affecting strategic direction, operations, reporting and compliance using eight dynamic and interdependent components.

EXECUTIVE SUMMARY

As regulators continue to focus on risk management, boards of directors and senior management face many challenges in establishing an ERM infrastructure that facilitates the advancement of risk management to provide better knowledge and information about the enterprise's key risks and its capabilities for managing those risks. Adequate risk management programs can vary considerably in sophistication, depending on the size and complexity of the organization and the level of risk that it accepts. Irrespective of the firm's size and complexity it is the expectation that a formal risk management system be in place to address their activities and to provide senior management and directors with the information they need to monitor and direct day-to-day activities.

WHAT IS ERM?

The Committee of Sponsoring Organization (COSO) defines ERM as a "process, effected by an entity's board of director's management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its appetite, to predict reasonable assurance regarding the achievement of entity objectives." ERM focuses on the establishment of oversight, control and discipline to drive continuous improvement of an entity's risk management capabilities. Enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

Eight components of ERM reflect the way management runs an enterprise and are integrated with the management process.

COMPONENTS OF ENTERPRISE RISK MANAGEMENT

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

1. **INTERNAL ENVIRONMENT** – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
2. **OBJECTIVE SETTING** – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
3. **EVENT IDENTIFICATION** – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
4. **RISK ASSESSMENT** – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
5. **RISK RESPONSE** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
6. **CONTROL ACTIVITIES** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. **INFORMATION AND COMMUNICATION** – Relevant information is identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
8. **MONITORING** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Internal control ensures effectiveness and efficiency, reliability and regulatory compliance.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multi-directional, iterative process in which almost any component can and does influence another.

ERM AND INTERNAL CONTROL

Internal control forms an integral part of enterprise risk management. Enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Authoritative guidance defines Internal Control¹ as a process designed to provide reasonable assurance regarding the achievement of business objectives.

Internal control has three main objectives:

- To promote effectiveness and efficiency of operations
- To ensure reliability of financial reporting
- To maintain compliance with applicable laws and regulations

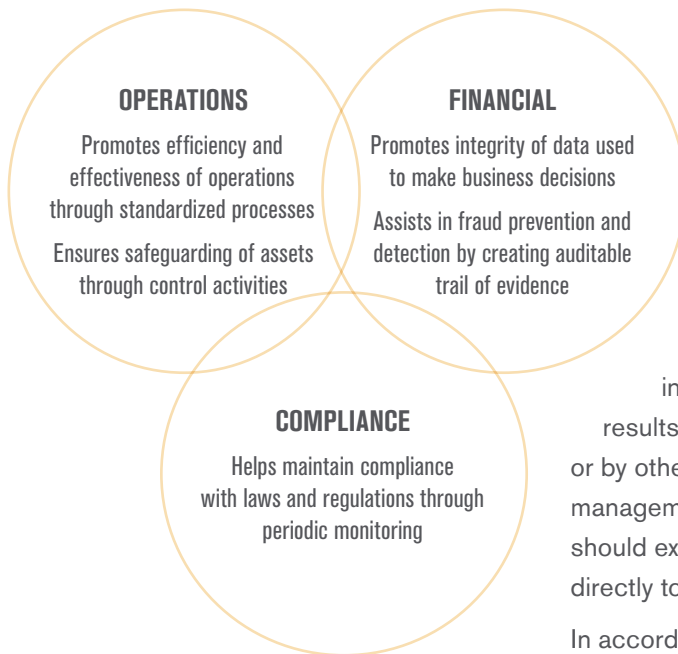
ADEQUATE INTERNAL CONTROLS

An institution's internal control structure is critical to the safe and sound functioning of the organization generally and to its risk management system, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties is one of management's more important responsibilities. Appropriately segregating duties is a fundamental and essential element of a sound risk management and internal control system. Failure to implement and maintain an adequate separation of duties can constitute an unsafe and unsound practice and possibly lead to serious losses or otherwise compromise the financial integrity of the institution. Serious lapses or deficiencies in internal controls, including inadequate segregation of duties, may warrant supervisory action, including formal enforcement action.

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting,

¹ Internal Control – Integrated Framework, Committee of Sponsoring Organizations (COSO) of the Treadway Commission

The Importance of Internal Control



safeguards assets, and helps to ensure compliance with relevant laws, regulations, and institutional policies. Ideally, internal controls are tested by an independent internal auditor who reports directly either to the institution's board of directors or its designated committee, typically the audit committee. Personnel performing these reviews should generally be independent of the function they are assigned to review. Given the importance of appropriate internal controls to organizations of all sizes and risk profiles, the results of audits or reviews, whether conducted by an internal auditor or by other personnel, should be adequately documented, as should management's responses to them. In addition, communication channels should exist that allow negative or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

In accordance with regulatory expectation, when evaluating the adequacy of a firms' internal controls and audit procedures, management should consider whether these conditions are met:

- The system of internal controls is appropriate to the type and level of risks posed by the nature and scope of the organization's activities.
- The institution's organizational structure establishes clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.
- Reporting lines provide sufficient independence of the control areas from the business lines and adequate separation of duties throughout the organization
- Official organizational structures reflect actual operating practices.
- Financial, operational, and regulatory reports are reliable, accurate, and timely; wherever applicable, exceptions are noted and promptly investigated.
- Adequate procedures exist for ensuring compliance with applicable laws and regulations.
- Internal audit or other control review practices provide for independence and objectivity.
- Internal controls and information systems are adequately tested and reviewed; the coverage, procedures, findings, and responses to audits and review tests are adequately documented; identified

material weaknesses are given appropriate and timely high level attention; and management's actions to address material weaknesses are objectively verified and reviewed.

- The institution's audit committee or board of directors reviews the effectiveness of internal audits and other control review activities on a regular basis.

LESSONS LEARNED

The lessons learned from several institutions that failed can be divided into five main areas:

- **Lack of segregation duties**
- **Lack of senior management involvement**
- **Poor control procedures**

In many institutions, not only is there a separation of operational duties between the front and back-office, but there is also a unit independent of both to provide an additional layer of checks and balances;

- **Lack of supervision**

There may be many supervisors; in reality none exercised any real control over processes; and

- **Inadequate capital**

There are two aspects to this issue - an institution must have sufficient capital to withstand the impact of adverse market moves on its outstanding positions as well as enough money to keep these positions going.