CONTINUITY CENTRAL.COM
Business continuity, enterprise risk & resilience updates

Portal Publishing Ltd, PO Box 1393, Huddersfield, HD1 9TN, England

Enterprise Risk Management and Business Continuity

Published: Friday, 14 July 2017 08:23

Alberto G. Alexander, Ph.D, MBCI, looks at enterprise risk management, its relationship to business continuity management, and how organizations can integrate the two disciplines.

Introduction

Enterprise risk management was formalized largely because of initiatives of the Committee of Sponsoring Organizations (COSO). COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission) following several cases of fraudulent accounting in corporations. The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control.

"COSO is a voluntary private sector organization, dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient and ethical business operations on a global basis" (Rittenberg, 2013). It sponsors and disseminates frameworks and guidance based on in-depth research analysis and best practice.

Events, risks and opportunities

The impact of an event 'occurrence or change of a particular set of circumstances' (ISO 22301:2012), may be negative, positive or both. Events with a negative impact represent risk, which can prevent value creation or erode existing value.

Events with a positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities 'back to its strategy or objective-setting processes, formulating plans to seize the opportunities' (Hiles, 2011).

Enterprise risk management definition:

Enterprise risk management "Is the process of identifying major risks that confront an organization, forecasting the significance of those risks in business processes, addressing the risks in a systematic and coordinated plan, implementing the plan, and holding key individuals responsible for managing critical risks within the scope of their responsibilities," (Hampton, 2015).

The definition reflects certain fundamental concepts, ERM is:

- A process, on-going through an entity;
- Effected by people at every level of the organization;
- Applied in strategy setting;
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk;
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;
- Able to provide reasonable assurance to an entity's management and board of directors;
- Geared to achievement of objectives in one or more separate but overlapping categories.

Risk management

The updated COSO framework, of 2013, contains five control components needed to help assure sound business objectives. The control components are:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities.

Scandals such as Enron, Tyco and WorldCom led to demands for stronger corporate governance and risk management. The result 'was the Sarbanes – Oxley Act, which requires internal control systems and the certification of them by management and the independent auditor,' (Wells, 2017).

COSO's Internal Control Integrated Framework remains the commonly accepted standard for the reporting requirements.

Business objectives

COSO's enterprise risk management framework aims to achieve corporate objectives. It includes three categories:

- **Operations:** effective and efficient use of its resources;
- **Reporting:** reliability of reporting;
- **Compliance**: compliance with applicable laws and regulations.

The categorization means that a risk may fall in more than one category, so that it may be seen from different perspectives.

The ERM framework provides reasonable assurance of reporting and compliance requirements. For those events outside the organization's control, ERM provides reasonable assurance that management and the board are made aware of the organization's progress towards its objectives and of any obstacles in its way. The possible obstacles, according to ISO 31000, would be considered risks. In ISO 31000, risks are defined as "the effect of uncertainty on the accomplishment of objectives".

Components of the COSO ERM framework

The ERM COSO framework consists of five components that are depicted in figure one, below:

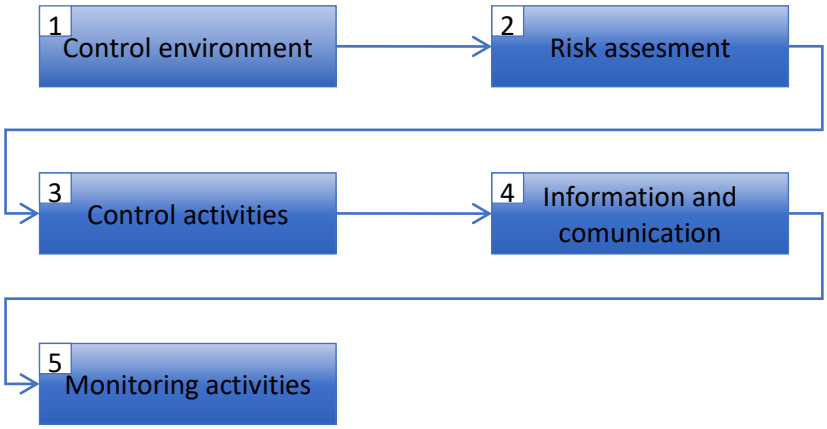

Figure one: Components of the COSO ERM framework.

A brief description of the five components follows:

- **Control environment:** The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and Senior management establish the tone at the top regarding the importance of internal control, including expected standards of conduct.
- **Risk assessment:** Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis. A precondition to risk management is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyse risks to those objectives.
- **Control activities:** Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks for the achievement of objectives are carried out. Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and communication:** Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Relevant information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
- **Monitoring activities:** Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles with each component, is present and functioning.

Relationship of objectives and components

A direct relationship exists between *objectives*, which are what an entity strives to achieve, *components,* which represent what is required to achieve the objectives, and the organizational structure of the entity (operating units, legal entities, and other).

The relationship can be depicted in the COSO cube diagram, which is shown in figure two.

Figure two: the COSO cube diagram.

- The three categories of objectives are shown at the top of the cube: the columns represent operations, reporting and compliance;

- The five components are represented by the rows;
- An entity's organizational structure is represented by the third dimension.

This portrayal shows a holistic view of the entity's enterprise risk management and at the same time permits views by category, component, entity unit or any subset of these.

Effectiveness

The components of the COSO cube can be used as a basis for assessing the effectiveness of an organization's risk processes. If the components are present and working effectively, the risks must have been brought within the entity's risk appetite.

When ERM is accepted as being effective in each of the three categories of objectives, the board of directors and senior management are reasonably confident that they understand progress towards objectives and their reporting is reliable and compliant with relevant laws and regulations.

Risk categories

Risk categories relevant to the organization are identified. The following risk categories are common to all organizations (Nazir, 2007):

- **Natural hazards** (fire, earthquakes, hurricanes.)
- **Man-made hazards** (wars, terrorism)
- **Financial risk** (credit risk, liquidity risk, bankruptcy risk, interest rates, prices, costs.)
- **Operational risk** (production breakdowns, supply chain issues, distribution issues etc)
- **Strategic risk** (fluctuations in demand, technological advances, economic cycles etc)
- **Information risk** (incorrect information, access to confidential information by unauthorized persons.)
- **Compliance risk** (penalties and fines due to non-compliance, law suits, reputation losses etc).

Some risks categories will be more important for some organizations while other risk categories will be more important for others.

ERM and BCM

Business continuity management is an important part of ERM and will continue to be so: it covers, or partly covers, several of COSO's risk categories. But, by itself, BCM cannot protect an organization from all the categories of risk that faces it.

COSO describes ERM as a process (1) that is established and implemented by an entity's board of directors, management, and other personnel; (2) that is applied in strategy setting and across the enterprise; (3) that is designed to identify potential events that could negatively affect the entity; (4) that manages risk to contain them within the organization's risk appetite; and (5) that provides reasonable assurance regarding the achievement of entity objectives.

ERM's mission is to identify, assess, monitor, and report major risks that could impede or otherwise negatively affect achievement of an organization's strategic goals and operational objectives. ERM enhances an organization's ability to make risk–informed decisions.

Business continuity management can be described as a process of identifying and responding to fast – approaching, high – impact interruption risks that can overwhelm inherent operational resiliency.

Business continuity management's mission can be described as to enhance enterprise resiliency and help an organization respond and recover from both unanticipated and anticipated business interruptions.

Business continuity management has the added value of helping the organization identify operational resiliency improvements that can greatly enhance their ability to weather interruptions that would otherwise significantly challenge competitors.

ERM and business continuity management share the common goals of identifying, assessing, and managing interruption risks that could serve to prevent achievement of their strategic objectives.

Strategies for linking ERM and BCM programs

Following a series of well-coordinated ERM and business continuity management integration activities makes it possible to realize the full value of optimized BCM. Some vital integration examples could include:

- Align the BCM program to the ERM program by sharing governance and steering committee members.
- Obtain ERM input on suggested resiliency improvements and possible recovery strategies to keep the right focus on cost – versus – risk reduction benefits.
- Obtain BCM enterprise interruption impact insight when planning and performing ERM risk scenario analysis.
- Use the more impactful and more likely ERM identified interruption risks as the basis for BCM exercise scenarios.
- Perform post–interruption event analysis to determine the effectiveness not only of BCM program response capabilities but also of ERM program risk identification and management.
- Leverage ERM's risk impact information to keep BIA interviews focused on relevant impacts of operational process interruption.
- Use the BCM program's resiliency and recovery capability assessment reporting to improve the ERM program's analysis and reporting of overall risk management effectiveness.
- Use the more impactful and more likely ERM identified interruption risks as the basis for BCM exercise scenarios.
- Obtain BCM enterprise interruption impact insight when planning and performing ERM risk scenarios analysis.
- ERM and BCM risk assessment scopes align for areas related to operational interruption risks.
- Management's risk appetite and tolerance decisions are informed by BIA results.
- The BCM program's effectiveness analysis provides a feedback loop to the overall ERM program, thereby providing comfort that resiliency and recoverability efforts reduce interruption risk impact.

Conclusions

Business continuity management and enterprise risk management complement one another, and both are necessary in today's high-risk business environment. ERM and BCM share the common goals of identifying, assessing, and managing interruption risks that could serve to prevent achievement of their strategic objectives.

Business continuity professionals should understand the principles found in the enterprise risk analysis process in order to deliver higher levels of value with the objective of managing risk likelihood

and impact. Additionally, BCM professionals should recognize that they are key team members focused on managing availability and reputational risk.

It is important to be clear that BCM cannot protect an organization from all the categories of risk that face it. To do this, we need a wider framework.

A holistic approach is needed to all risks within the categories (natural hazards, man-made hazards, financial risks, operational risks, strategic risks, information risk, compliance risk), with perspectives across all units, holding key individuals responsible for managing critical risks within the scope of their responsibilities.

The author

Alberto G. Alexander, Ph.D, MBCI is an international consultant. Dr. Alexander holds a Ph.D from The University of Kansas and a MA from Northern Michigan University. He is the Managing Director of the international consulting and training firm Eficiencia Gerencial y Productividad SAC, located in Lima, Perú. He is a member of the Business Continuity Institute. Contact him at alexander@egpsac.com

Bibliographical references

- Wells, Joseph. *Corporate Fraud Handbook: Prevention and Detection* 5th Edition. Willey. 2017.
- Hampton, John. *Fundamentals of Enterprise Risk Management* Second Edition AMACOM 2015
- ISO 22301:2012, *Societal security – Business Continuity Management Systems - Requirements*
- ISO 31000:2009, *Risk management – Principles and guidelines*
- Hiles, Andrew. "Enterprise Risk Management". *The Definitive Handbook of Business Continuity Management*, Wiley, 2011
- Nazir, Muhammad, Mubashir, *Implementation of ERM under COSO Framework* ACCA, CISA, CIA, June 2007
- Coleman, Thomas. *A Practical Guide to Risk Management* CFA 2011
- Decker, AL. Galer, Donna. *Enterprise Risk Management: Straight to the Point.* 2013. ERMSTTP
- Lam, James. *Enterprise Risk Management: from Incentives to Controls* Second Edition Wiley 2014
- Rittenberg, Larry. *COSO Internal Control Integrated Framework Turning Principles into Positive Action* 2013 The Institute of Internal Auditors Milwaukee Chapter