Enterprise Risk Management Maturity-Level Assessment Tool

Maria Ciorciari[1], MAS, FRM
Dr. Peter Blattner[2]

Copyright 2008 by the Society of Actuaries.
All rights reserved by the Society of Actuaries. Permission is granted to make brief excerpts for a published review. Permission is also granted to make limited numbers of copies of items in this monograph for personal, internal, classroom or other instructional use, on condition that the foregoing copyright notice is used so as to give reasonable notice of the Society's copyright. This consent for free limited copying without prior consent of the Society does not extend to making copies for general distribution, for advertising or promotional purposes, for inclusion in new collective works or for resale.

[1] Maria Ciorciari, MAS, FRM, risk manager, assistant vice president, BSI SA, 6900 Lugano, Switzerland, Tel: +41 (0)91 9452624, e-mail: ciorciari@sunrise.ch, maria.ciorciari@bsibank.com.
[2] Dr. Peter Blattner, IFZ der HSLU Economics, professor of Banking and Finance, 6003 Zug, Switzerland, Tel.: +41 (0)41 724 6550, e-mail: p.blattner@arcor.de.

Abstract

The increasing complexity and range of risks force organizations to recognize their importance in order to achieve the established objectives. The implementation of an enterprise risk management (ERM) framework supports and improves the risk awareness at every level, from strategic to operative, and from top management to employees.

ERM cannot be seen as a static one-time process, but it must be embedded in the organization and dynamically adapted to the changing internal and external environment.

The aim of this work is the definition of a holistic approach to assess the maturity level of ERM within an organization, following the principles defined by The Committee of Sponsoring Organizations of the Treadway Commission (2004b) in the "Enterprise Risk Management—Integrated Framework."

The approach is transferred into an application tool, EnteR, for an automated and guided maturity-level assessment.

By means of EnteR, an organization can evaluate the eight components of the framework: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring. EnteR helps organizations to assess the maturity level of the ERM, highlighting strengths and weaknesses from which a prioritized list of measures is derived, whose implementation helps to fill existing gaps in ERM.

The Enterprise Risk Management tool functionalities include:

- identification of weaknesses
- identification of strengths
- definition of a prioritized measures list
- assessment of the maturity level of ERM
- documentation of the ERM
- overview of results considering different dimensions
- multi-period assessment on different reference dates
- overview of multi-period results considering different dimensions.

The ERM evaluation tool can be used as a benchmark for assessing different organizations for equivalent comparison.

A structured collection of elements describes characteristics of ERM. The approach is composed of more than 100 elements with more than 600 corresponding criteria.

Preface

This paper is the result of the master final thesis project carried out in 2007 at Banca del Gottardo by Maria Ciorciari, as last part of her Master of Advanced Studies post-degree at Lucerne University of Applied Sciences and Arts in Switzerland. The supervisor was Dr. Peter Blattner, Financial Risk Management Course director, and co-referee was Mr. Alberto Saracino, head of Risk Management at Banca del Gottardo.

In 2007, Maria Ciorciari won the prize for best master's thesis in risk management at the Lucerne University of Applied Sciences and Arts.

In March 2008 the ownership of Banca del Gottardo, one of the leading Swiss banks offering state-of-the-art private banking services, passed from Swiss Life to BSI, a company in the Generali Group, one of the world's biggest insurance companies. BSI specializes in asset management and related services for private and institutional clients, and is present in the major financial markets worldwide.

The Lucerne University of Applied Sciences and Arts is one of seven universities of applied sciences in the country and contributes significantly to the economic and cultural development of central Switzerland. The Lucerne University of Applied Sciences and Arts is “Committed to Excellence” with a successful implementation of quality measures of the EFQM European Foundation for Quality Management.

1. Introduction

What is the adequate amount of risk that should be accepted by a firm? For every firm this is one of the most important questions in management decisions. In the past, financial risks were the focus when discussing a firm's risks. Buying insurance or hedging risks were the instruments of enterprise wide risk management. Normally financial risks are insured or hedged at time and not in time. Risk management of financial risks is more a static procedure than a dynamic consideration.

One of the most theoretical underpinnings of risk management is the capital asset pricing theory (CAPM). In the language of CAPM, portfolio considerations are the center of the argument. The shareholders can diversify their capital over many firms, sectors or countries. Only systematic risks are important for pricing risks. Unsystematic risks are not relevant for the hurdle rate of equity.

In the language of CAPM, more systematic risks or business cycle sensitive sectors of an economy can be accepted by a shareholder, who will ask for a higher rate of return. Higher risk implies a higher rate of return. There is a positive correlation between return and risk.

The chance and threat of risks are handled in a symmetric manner. Total risk is not relevant for the pricing decision on equity of a shareholder. The rate of return for shareholders is connected to systematic risks and unsystematic risks can be diversified over a portfolio.

The decision of the management of a firm is connected to more risks than in the case of the hurdle rate for equity. The going up of the cash flow of a firm is different from the going down of the cash flow of a firm. The shortfall of cash flow is important to the management of a firm. In this context, the cash flow new costs, so called (indirect) insolvency costs, are relevant for decision making. In the literature, these costs are called deadweight costs.

In the case of a shortfall of cash flow, there is a loss of reputation, the best workers leave their jobs at first, liquidity premiums are present for short run investments, restructuring will be costly, and so on. On the other hand, the downgrading in the case of a shortfall of cash flow will be relevant for the costs of capital. A downgrading of the rating is connected to higher capital costs. Decision making in the firm will be more expensive, and investments with a positive net present value cannot be undertaken with respect to the case without the presence of deadweight costs.

Other than financial risks, risks like operational, reputational or strategic risk can be relevant for management decisions too. Normally these kinds of risks cannot be diversified away on a firm basis. Constructing a portfolio is only a good idea for reducing systematic risks. For managing total risk of a firm, all stakeholders are important for pricing risks of firm projects. Discussing the preferences of all stakeholders means that total risk is relevant for the shareholders too. Deadweight costs are relevant for stakeholders and shareholders. Pricing risks in the context of CAPM underestimate the indirect costs of financial stress in a systematic manner.

Projects with a positive net present value cannot be undertaken with respect to a financial stress, and the capital costs of a firm will be higher on average over a business cycle.

For sound decision making in a firm, the tradeoff between return and risk on a total risk basis will be of interest. Managing risk in a static manner shortens the decision of the management. Managing risks over time is relevant for the management of a firm.

Discussing deadweight costs in the context of a shortfall of the cash flow means handling risks over time. Insolvency is a phenomenon in time, not at time. Reputation risk or strategic risk is connected with time. Reputation risk, for instance, implies the erosion of making good contracts with customers and other banks over time, step by step. Managing financial, operational, reputational and strategic risks is relevant for ERM on the basis of managing them on a total risk basis.

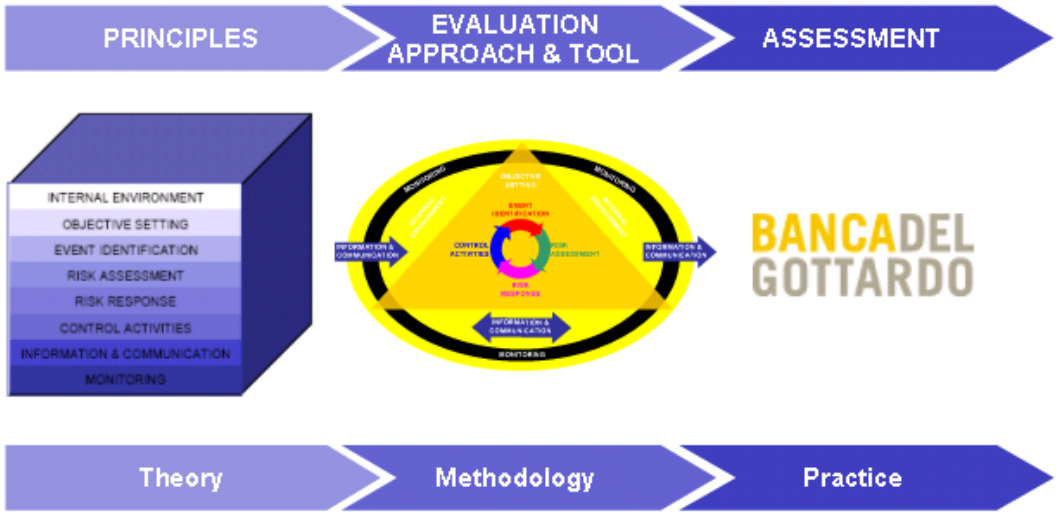
ERM must define, for instance, the overall risk appetite and has to communicate it to all parts of a firm. Clear objectives must be defined and communicated throughout the firm. The rating of a firm has to be aligned to the risk appetite.

The required amount of capital for the optimized rating with respect to the accepted risk appetite of the firm must be allocated on a marginal basis to all parts of the firm. ERM is central for the communication of the tradeoff between return and risk on a total risk basis to the whole firm. Decentralized tradeoff between return and risk must be identical to the portfolio considerations on a firm basis. Implementation and improvement of the risk culture of a firm are the most important elements of ERM. Performance evaluations must be grounded on portfolio aspects in the context of economic and organizational considerations and not only on an accounting or legal basis.

The implementation of an ERM framework supports and improves the risk awareness at every level, from strategic to operative, and from top management to employees.

The aim of this paper is to define a holistic approach to analyze an organization's ERM maturity level. The approach is transferred into an application tool, Enterprise Risk Management, for an automated and guided assessment and results overview, highlighting strengths and weaknesses in ERM.

The tool is then used to assess the ERM maturity level within a concrete organization, Banca del Gottardo. The assessment results are not included in this paper; the results shown later are based on fictitious data.



The project sponsor, Banca del Gottardo, benefits from the analysis, which allows:

- identifying the current weaknesses and strengths in ERM;
- having a list of measures that enable the maturity level enhancement;
- contributing to a more effective corporate governance;
- integrating the documentation of ERM;
- contributing to the improvement of the quality of the risk management process and risk mitigation throughout the entity.

2. Enterprise Risk Management

In 2001 the Committee of Sponsoring Organizations of the Treadway Commission initiated a project mandating PricewaterhouseCoopers to develop a structured approach to effectively identify, assess and manage risks. The project ended in 2004 with the publication of the "Enterprise Risk Management—Integrated Framework."

The Committee of Sponsoring Organizations of the Treadway Commission (2004b) defines ERM as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, 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 risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (p. 4).

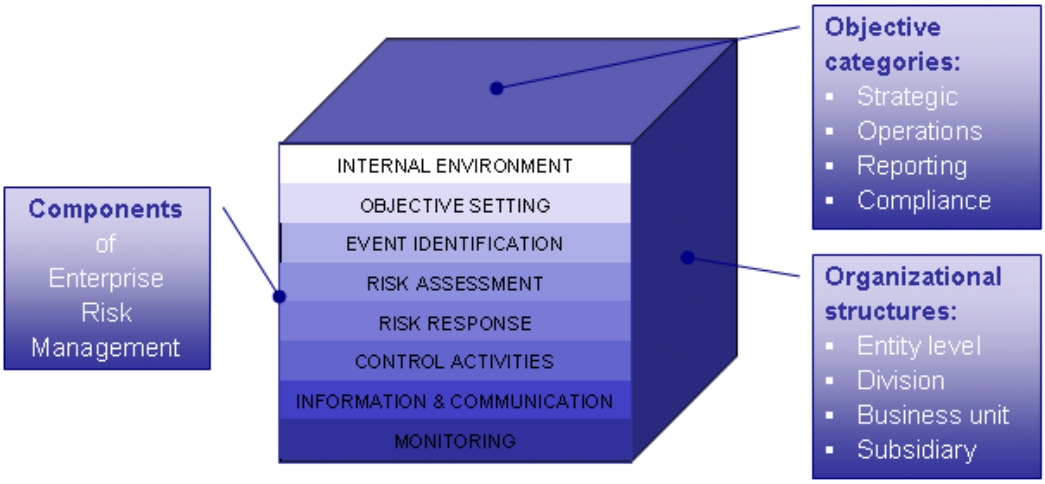
The framework aims to identify all potential events that could affect the achievement of the entity's objectives. These events can be divided into two categories: events with positive impact on objectives and events with negative impact on objectives.

The former represent opportunities, and the latter are risks. These must be managed with a clear process composed of the following three phases: identification and analysis, responses and management, control and supervision (Münzel and Jenny, 2005, p. 18).

The risk management process must be supported by a sound foundation in terms of risk philosophy, integrity and ethical values, corporate governance, competence and responsibilities, together with an objective-setting process that considers the risk dimension, a dynamic information flow and communication and an ongoing monitoring of all the framework components. Organizations should implement effective ERM because it allows them to optimize risk management by providing a systematic and holistic evaluation and control of risks.

The ERM maturity-level assessment is crucial because it enables the identification of strengths and weaknesses from which an organization can derive measures in order to fill the existing gaps and improve the corporate governance and risk management.

The concepts contained in the "Enterprise Risk Management—Integrated Framework" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004a) apply to all levels of the organization, providing a new way of looking at all risk dimensions on a corporate level, from strategy setting to day-to-day activities.



Enterprise Risk Management Framework

Just as a house needs a strong foundation, the internal environment serves as a basis for all other components of the framework. In fact, the environment reflects the overall attitude, awareness and actions that have an impact on the whole organization's activities. It is also important for management to apply healthy corporate governance that takes risks into account in every task, from strategy definition to objective setting.

A revolving risk management process can be considered the heart of the framework; risk identification and assessment are useless if no risk responses are implemented and no regular controls are in place. The strategic, business and operational processes do not work properly without information that flows in, out and across the enterprise. The monitoring component has the same importance as the other components of the framework, because it allows the determination of whether everything continues to work effectively.

2. Evaluation Principles

Each of the eight components equally contributes to ERM. A weak component can affect the entire process. The interrelationships of the framework components strengthen the role of each single component.

The risk management philosophy and the risk appetite contribute to the objective setting, which in turn allows identifying events that could affect them. Events with positive impact are channeled back to the objective-setting process, while events that could adversely affect the objective achievement are assessed, responses are carried out, and control activities are performed on their fulfillment degree. The ERM process only functions effectively if the information flows through all the components and an ongoing monitoring is performed.

The analysis is based on eight theses, one for each component, extracted from the "Enterprise Risk Management—Integrated Framework" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004a, 2004b, 2004c):

- *Internal Environment*

  Thesis 1: "Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the basis for how risk and control are viewed and addressed by an entity's people. The core of any business is its people—their individual attributes, including integrity, ethical values and competence—and the environment in which they operate" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Objective Setting*

  Thesis 2: "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" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Event Identification*

  Thesis 3: "Potential events that might have an impact on the entity must be identified. Event identification involves identifying potential events from internal or external sources affecting achievement of objectives. It includes distinguishing between events that represent risks, those representing opportunities, and those that may be both. Opportunities are channeled back to management's strategy or objective-setting processes" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Risk Assessment*

  Thesis 4: "Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with objectives that may be affected. Risks are assessed on both an inherent and a residual basis, with the assessment considering both risk likelihood and impact" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Risk Response*

  Thesis 5: "Personnel identify and evaluate possible responses to risks, which include avoiding, accepting, reducing, and sharing risk. Management selects a set of actions to align risks with the entity's risk tolerances and risk appetite" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Control Activities*

  Thesis 6: "Policies and procedures are established and executed to help ensure the risk responses management selects are effectively carried out" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Information and Communication*

  Thesis 7: "Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing, and responding to risk. Effective communication also occurs in a broader sense, flowing down, across, and up the entity. Personnel receive clear communications regarding their role and responsibilities" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

- *Monitoring*

  Thesis 8: "The entirety of enterprise risk management is monitored, and modifications made as necessary. In this way, it can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of enterprise risk management, or a combination of the two" (The Committee of Sponsoring Organizations of the Treadway Commission, 2004b, p. 22).

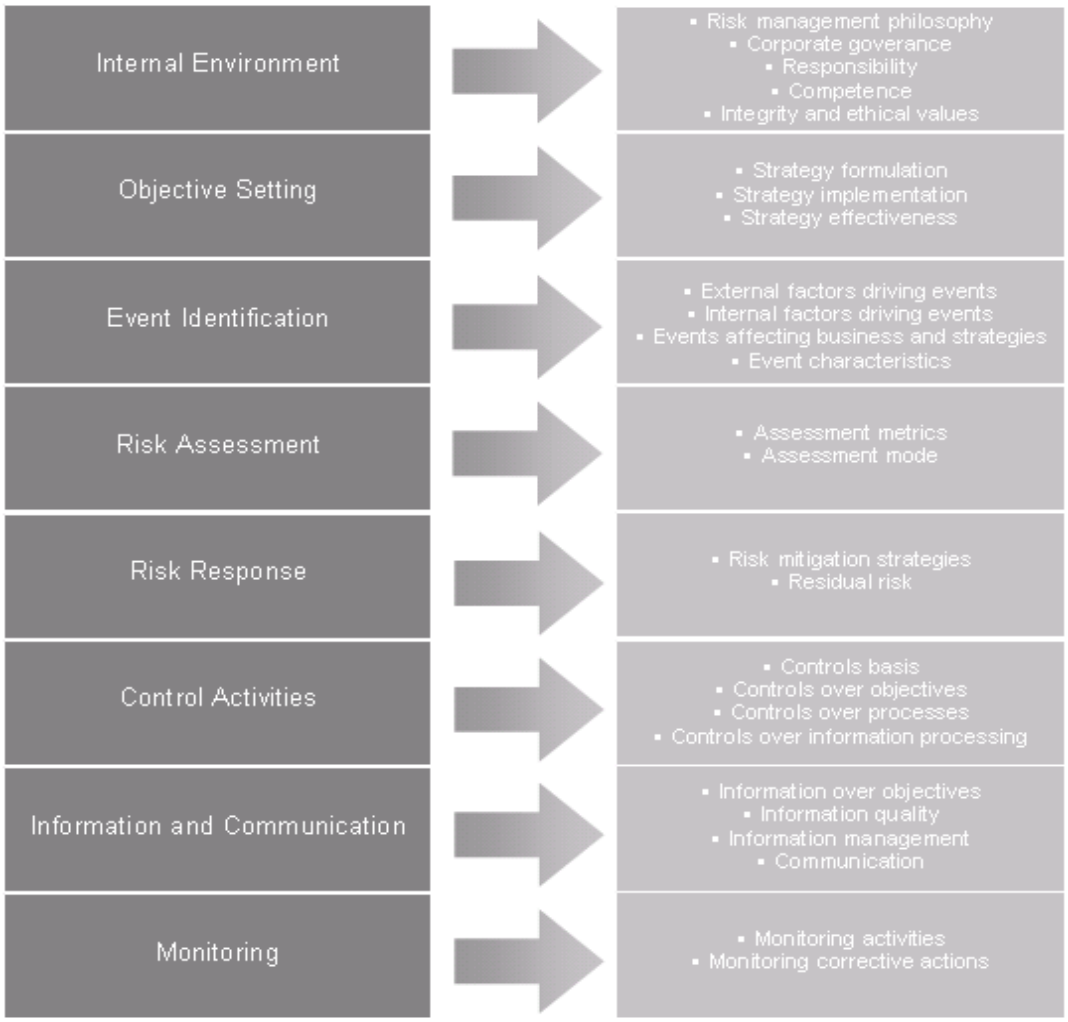
Each element of a component has the same importance and contributes to ERM; therefore it is equally weighted.

3. Methodology

All of the eight interrelated framework components are analyzed, and the theses are the basis for establishing the maturity-level evaluation criteria. The theoretical concepts enunciated for each component of ERM are translated into practical elements, each of them grouped by topic.

Evaluation Approach Structure

A set of two or more topics is defined for each component.

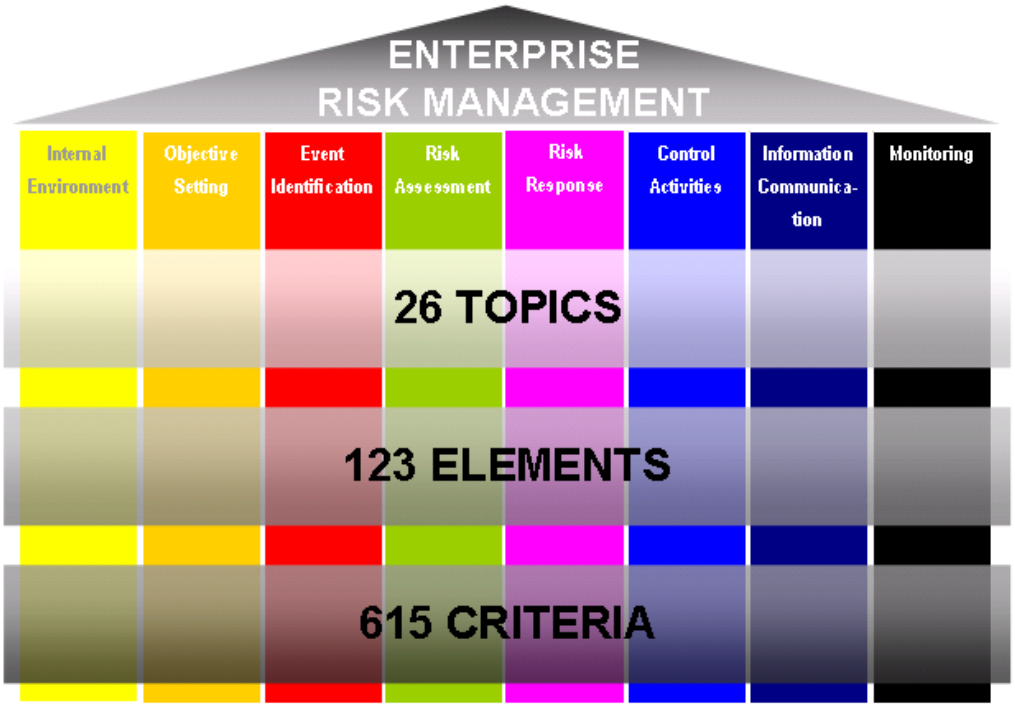


Evaluation Topics

Within the internal environment, topics such as risk management philosophy, corporate governance, competences, responsibilities and integrity and ethical values are evaluated. For the objective-setting component, it is important to evaluate the strategy

formulation, implementation and effectiveness. When identifying events that could affect positively or adversely the entity's objectives, one should analyze and characterize both the external and internal factors driving them.

The risk assessment must be based on clear metrics and methodology. Risk mitigation strategies affecting inherent risk must be carried out in order to bring the residual risk within the risk appetite. Control activities must be based on clear policies and procedures and focus on objectives, processes and information processing. Relevant information must be communicated. An ongoing monitoring must be performed on activities and on corrective actions.



Evaluation Approach Overview

A structured collection of elements describes characteristics of ERM. The approach is based on more than 100 elements with more than 600 corresponding criteria.

Each topic is detailed into three or more elements that are evaluated along the following maturity-level scale:

Maturity Level	Very Weak	Poor	Mid	Good	Optimized
	Very low formalization, no documentation available, no communication	Informally regulated, defined, still no training and communication	Standardized, principles defined and documented, basic training carried out	Supervised, principles are carried out, observance is verified and regularly improved	Optimized, risk management principles and processes are integrated in the management process

Maturity Scale

An evaluation criterion is set for each of the five maturity scale levels. The lowest maturity level implies that no documentation is available, no communication is given, and a very low formalization exists. The highest maturity level implies that the process is optimized, i.e., the risk management principles and processes are integrated in the management process.

3.1 Internal Environment

The following *Internal Environment* main topics have been identified and translated into basic ERM elements:

- *Risk Management Philosophy*
  A clear risk management philosophy is important as first step in implementing successful ERM. It defines how the entity considers risk in everything it does. The philosophy is reflected in oral and written communication from the management to the employees, in shared beliefs, but also in attitudes. The philosophy on risk management is reinforced not only with words but, more importantly, with effective actions. Risk appetite, the amount of risk the entity is willing to accept, must be defined.

- *Corporate Governance*
  Healthy corporate governance is crucial for effective ERM. With their actions, the board of directors and the senior management can heavily influence the success of the organization.

- *Responsibility*
  Clear responsibilities and authorities should be defined and communicated. Clear competences help to avoid tasks overlapping but also to optimize processes.

- *Competence*
  The employees should have the adequate knowledge and skills needed to perform the assigned tasks. The human resource management plays an important role in recruiting the right person at the right place, but also in identifying the training needs of the employee.

- *Integrity and Ethical Values*
  The entire employee should adhere to a standard of behavior that considers integrity and ethical values in order to enable a strong corporate culture.

3.2 Objective Settings

The following *Objective Settings* main topics have been identified and translated into basic ERM elements:

- *Strategy Formulation*
  Before management formulates the strategy it should conduct a situation analysis to identify the entity's strengths and weaknesses, but also the external opportunities and threats. The management should define a range of possible strategies, for which risks and opportunities are identified. The strategy setting process must be done on an ongoing basis requiring continuous reassessment and reformation.

- *Strategy Implementation*
  The strategic objectives should be accompanied by operations, reporting, and compliance related objectives. Those objectives should be measurable and understood by all employees. The objectives should be dynamically adjusted, and always support and be aligned with the entity's strategy.

- *Strategy Effectiveness*
  The management should regularly monitor the objectives' achievement degree, the employee commitment and the client satisfaction.

The entity should also compare results among peers, in order to identify improvement opportunities.

A Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis should be performed in order to identify the strategy choices. These should focus on the maximization of the strengths and opportunities and on the minimization of weaknesses and threats. This process should be performed on an ongoing basis.

Internal ▼ External ▶	Opportunities	Threats
Strengths	SO-Strategies	ST-Strategies
Weaknesses	WO-Strategies	WT-Strategies

SWOT Analysis

The SWOT analysis is a matrix in which the internal strengths and weaknesses are combined with the external opportunities and threats. The SWOT combinations result in the following four types of strategies (Lombriser and Abplanalp, 2005, p. 198):

- Strengths-Opportunities Strategy
  Exploits the internal strengths to take advantage of external opportunities.

- Strengths-Threats Strategy
  Exploits the internal strengths to reduce the external threats.

- Weaknesses-Opportunities Strategy
  Improves weaknesses to take advantage of external opportunities.

- Weaknesses-Threats Strategy
  Reduces weaknesses in order to avoid external threats.

3.3 Event Identification

The following *Event Identification* main topics have been identified and translated into basic ERM elements:

- *External Factors Driving Events*
  The entity should consider and analyze external factors driving events that could affect the achievement of strategic objectives. The analysis should consider economic, natural environment, political, social and technological factors. The factors identification process should be performed on an ongoing basis, and at every level of the entity.

- *Internal Factors Driving Events*
  The entity should consider and analyze internal factors driving events that could affect the achievement of strategic objectives. The analysis should consider infrastructure, personnel, process and technology factors. The factors identification process should be performed on an ongoing basis, and at every level of the entity.

- *Events Affecting Business and Strategies*
  The management should focus on significant and possible events that could affect positively or adversely the achievement of objectives. The opportunities, positive events, should be channeled back to the objective and strategy setting process, while the risks, negative events, should be assessed and actions taken.

3.4 Risk Assessment

The following *Risk Assessment* main topics have been identified and translated into basic ERM elements:

- *Event Characteristics*
  In assessing risk, management should consider both expected and unexpected losses. Correlated events should be assessed together.

- *Assessment Metrics*
  The entity should assess both the possibility of occurrence and the impact of potential events that could adversely affect the achievement of objectives. The risks should be ranked in order to focus first on highly significant risks.

- *Assessment Mode*
  Management should promote best-practices assessment techniques and a continuous and iterative risk management process aligned with the strategy setting process. A composite assessment of risks across the entity should be performed.

The management should promote the use of best practice assessment techniques. The quality of the supporting data and assumptions should be periodically reviewed. To gauge the quality and accuracy of the used risk assessment techniques, the entity should perform a back-testing.

The increasing complexity of the legal environment and the rapid changes in the markets force the entity to adopt more sophisticated techniques.

First Class Risk Management

The way to a first-class risk management encompasses techniques with increasing knowledge required, from the limit management, to an active portfolio management of risk (Crouhy and Galai, 2001, p. 662). There is also a growing need for risk-adjusted profitability measures (risk-adjusted rate of return or RAROC).

3.5 Risk Response

The following *Risk Response* main topics have been identified and translated into basic ERM elements:

- *Risk Mitigation Strategies*
  Management should identify the appropriate response to the identified risks considering their significance in terms of likelihood and impact. The responses can be handled by accepting, reducing, sharing and/or avoiding risk in order to align it with risk appetite. Management should develop alternative risk mitigation strategies for each of its risks. A cost versus benefit analysis is the basis for the response strategy selection. The selected strategy should be accompanied by an implementation plan.

- *Residual Risk*
  Management should assess the residual risk remaining after the responses are fully implemented. The residual risk should be aligned with risk appetite.

The management should have a portfolio view of residual risks by entity level, from unit to business divisions.

3.6 Control Activities

The following *Control Activities* main topics have been identified and translated into basic ERM elements:

- *Controls Basis*
  The entity should have in place policies and procedures and ensure that these are well-understood and implemented. The processes should be documented and assure a segregation of duties.

- *Controls over Objectives*
  The entity should establish and execute control activities over strategic, operations, reporting and compliance objectives.

- *Controls over Processes*
  The entity should establish and execute control activities over processes. It has to ensure risk responses are appropriately carried out in a timely manner, risk limits are observed, prices and models are appropriate, risk management resources are adequate, and new products can be managed. The control activities should be regularly reviewed.

- *Controls over Information Processing*
  The entity should establish and execute control activities over information systems regarding data validity, exceptions management, IT security and availability.

The entity should control performance indicators on operating or financial data, such as staff turnover rates, transaction volume and cost trend. Senior management should review actual performance versus budgets, forecasts and prior periods. This can be done through a balanced scorecard approach.

The Balanced Scorecard method of Kaplan and Norton (1996) is a strategic approach and performance management system that allows the implementation of vision and strategy, working from four perspectives:

- Financial perspective
- Customer perspective
- Internal business processes perspective and
- Learning and growth perspective.

Kaplan & Norton Balanced Scorecard

Any unexpected results should be investigated and corrective actions should be taken.

3.7 Information and Communication

The following *Information and Communication* main topics have been identified and translated into basic ERM elements:

- *Information over Objectives*
  The entity should verify and assure on an ongoing basis that relevant information over strategic, operations, reporting and compliance objectives is delivered in a timely manner, and in a form that enables the entity to carry out the ERM-related business activities.
- *Information Quality*
  The entity should assure the quality of the provided information, in terms of depth, timeliness, availability, accuracy and accessibility.

- *Information Management*
  The entity should establish enterprise-wide historical and up-to-date data management programs enabling information systems to provide the needed information. The management should promote integrated systems in order to facilitate access to information.

- *Communication*
  The board of directors, as the representative of the firm's owners, must be apprised of sensitive information on risks the entity is facing in the achievement of objectives. A continuative interaction, communication and coordination between senior and line management should be assured. Upward channels must exist to encourage the reporting of relevant information, such as violations and anomalies.

The entity should establish open communication channels with stakeholders in order to better understand the client needs, but also to inform other stakeholders about the entity's risk appetite and limits.

> Companies and their executives must be sensitive to corporate public relations and recognize that good relationships with all of those who may be termed their stakeholders, the customers, owners, staff, suppliers and local communities, take a long time to build up and only a very short time to destroy (Kendall, 1998, p. 191–192).

The entity should communicate with stakeholders providing appropriate levels of information to conform to their needs and to regulatory requirements. The entity should establish a policy that defines the relevant information and coordinates the disclosure process. To increase transparency, the regulators are requiring more and more disclosure of risks. The entity should establish a disclosure policy defining and coordinating the disclosed information.

3.8 Monitoring

The following *Monitoring* main topics have been identified and translated into basic ERM elements:

- *Monitoring Activities*
  The entity should perform ongoing monitoring activities and regular separate evaluations in order to identify weaknesses in ERM.

- *Monitoring Corrective Actions*
  The entity should report deficiencies to those positioned to take necessary actions. These should be monitored until complete fulfillment is effective.

Each identified element can be assessed along the maturity-level scale. An evaluation criterion is set for each of the five maturity scale levels.

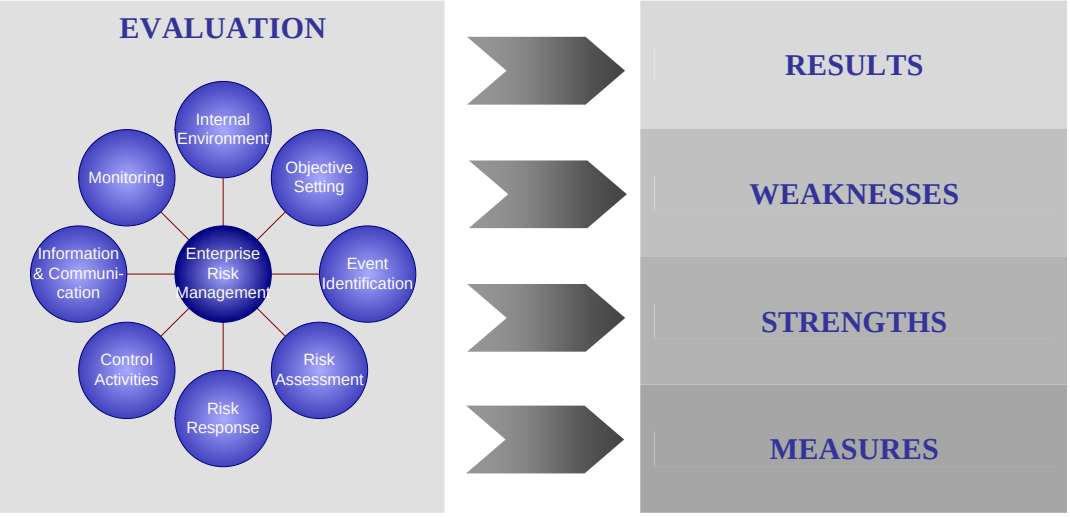
Ongoing monitoring activities differ from control activities, because the latter are performed as required steps in processes. The entity should perform periodical separate evaluations over businesses and processes, establishing an internal control system. Changes in processes, strategies, structure and systems should be monitored. The evaluation process should be based on clear methodologies and be documented.

> A well-designed system of internal controls will focus on three areas of any firm—the "front lines" where risks are taken or hedged, the independent risk management function and/or committee, and the internal audit function (Culp, 2001, p. 489).

A widely considered standard practice by regulator and auditors is the "Internal Control—Integrated Framework" approach (The Committee of Sponsoring Organizations of the Treadway Commission, 1992).

4. Assessment Tool

By means of the Enterprise Risk Management maturity-level assessment tool, it is possible to evaluate the elements of the framework's eight components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring.



Enterprise Risk Management Tool Functionalities

The Enterprise Risk Management tool allows the assessment of the ERM maturity level and highlights strengths and weaknesses from which are derived measures whose implementation helps to fill the existing gaps.

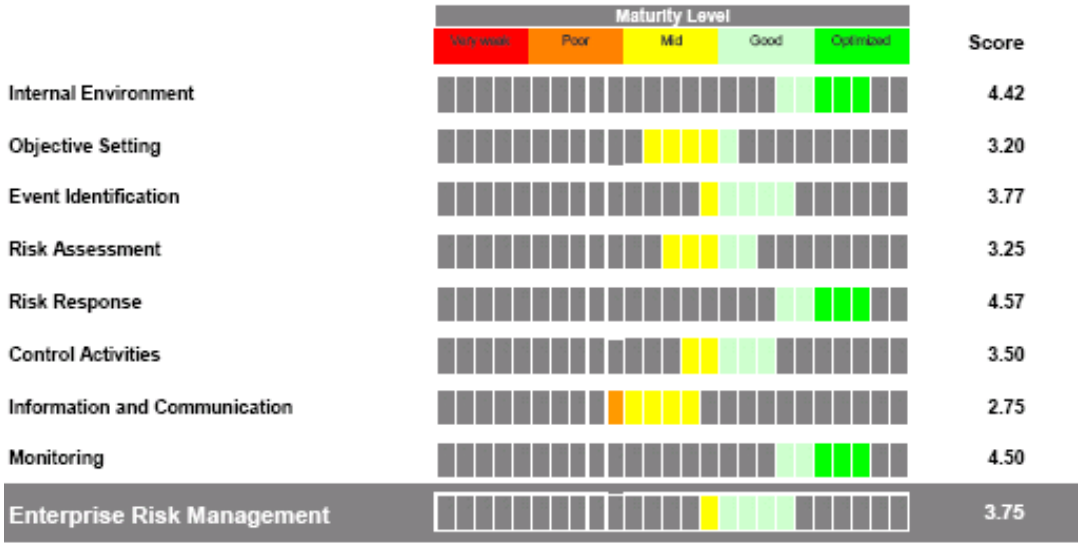
The Enterprise Risk Management tool is the solution that helps organizations to implement ERM:

- with more than 100 elements and 600 criteria, it helps organizations to evaluate the ERM maturity level
- allows identification of the weaknesses and the strengths in ERM
- helps to improve ERM by giving a prioritized list of measures whose implementation allows the organization to fill existing gaps
- provides also the possibility to document and assess the ERM maturity level at different situation dates, giving also a multi-period overview of results.

The evaluation approach can be used as a benchmark for assessing different organizations for equivalent comparison.

4.1 Results Overview

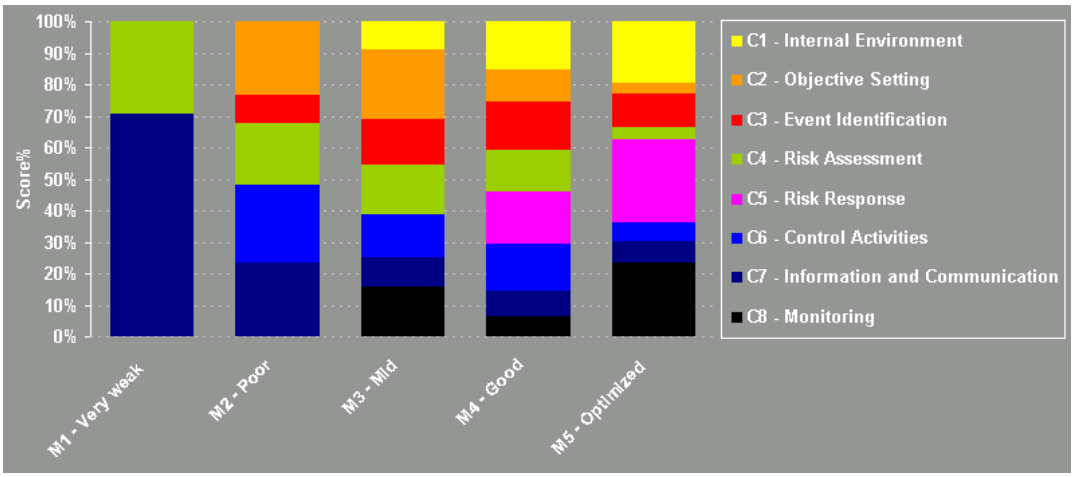
The assessment tool allows an overview on the maturity level of each single component of ERM (results based on fictitious data).



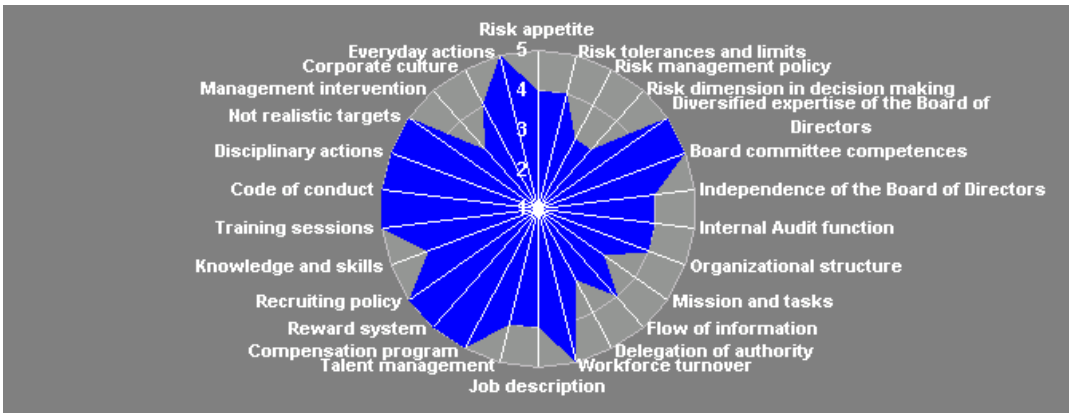
An average score with values from 1 to 5 (very weak to optimized) is computed for each component.

Low <		**Maturity level** > High		
Very weak	Poor	Mid	Good	Optimized
1	2	3	4	5

The following view allows the identification of the components which less/more contribute to the five maturity levels (results based on fictitious data).



A radar chart provides an overview of the maturity level degree for each of the identified component's elements. The following chart refers to the Internal Environment component's elements (results based on fictitious data).



The component is optimized when all the elements reach a score of 5 (optimized), i.e., the radar chart is completely blue.

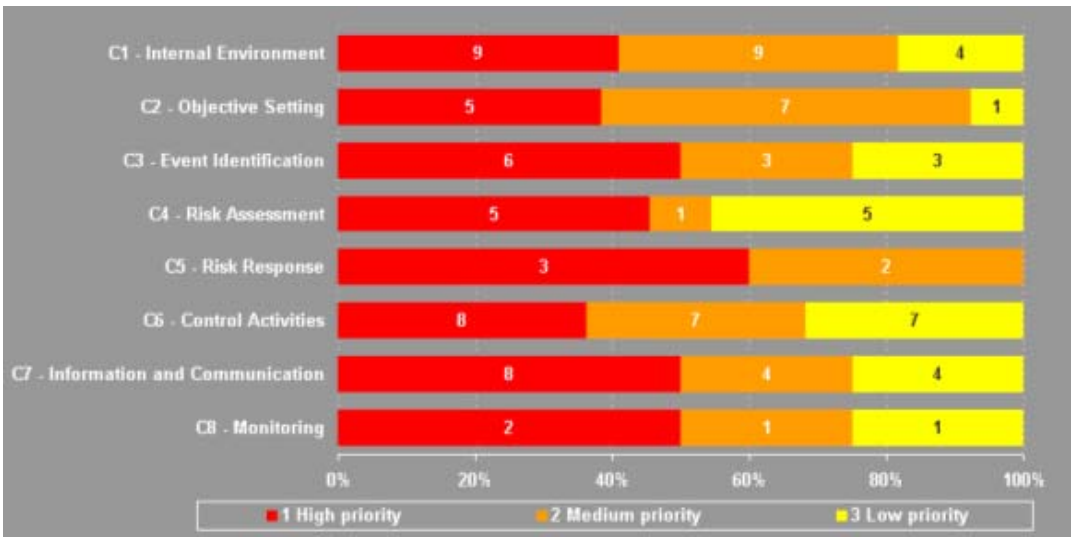
The following chart shows the difference between the component's score and the overall score. This view allows distinguishing between components which positively affect the overall score and components which negatively affect it.

In this example (results based on fictitious data), we can notice that the components which positively affect the overall score are: Internal Environment, Risk Response and Monitoring.

4.2 Strengths/Weaknesses and Measures

The assessment tool allows the identification of strengths and weaknesses in ERM at component, topic or element level.

The tool helps to improve ERM by giving a prioritized list of measures whose implementation allows filling existing gaps (results based on fictitious data).



The measures allow enhancing the ERM maturity level to a state-of-the-art level.

The measure prioritization depends on the element's maturity level evaluation.

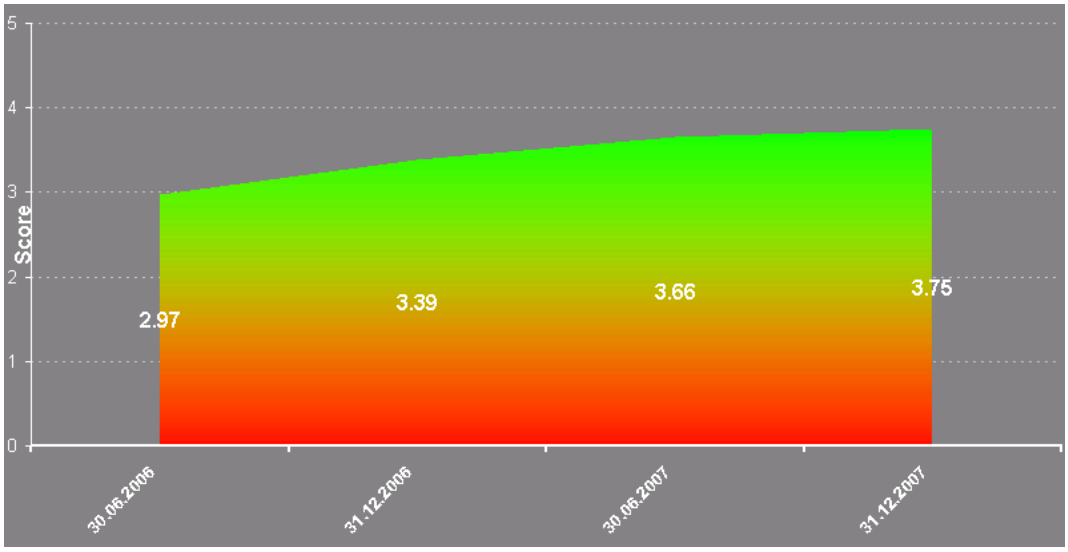
Low <		Maturity level		> High
Level 1	Level 2	Level 3	Level 4	Level 5
Very weak	**Poor**	**Mid**	**Good**	**Optimized**

High priority	**Medium priority**	**Low priority**

The high priority measures derive from elements that have been evaluated with a very weak or poor maturity level degree. The medium priority measures derive from elements that have been evaluated with a mid-maturity level degree. The low priority measures derive from elements that have been evaluated with a good maturity level degree. The degree of closeness to best practices depends on the results of a cost versus benefit analysis that has to be performed for each of the recommended measures, and is therefore the main driver for actual implementation.

4.3 Multi-Period Overview

The tool allows managing assessments for different situation dates. It is possible to monitor the ERM maturity-level over a time period enabling a dynamic assessment process (based on fictitious data).



The tool offers also the possibility to show the components maturity level.

5. Conclusions

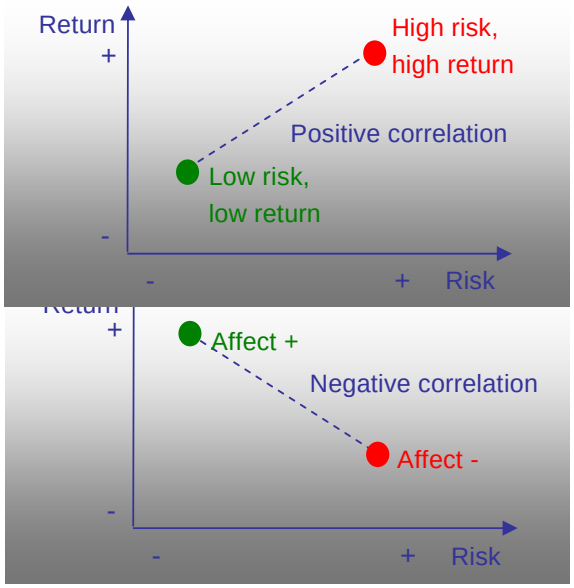
Effective ERM provides a reasonable assurance on the achievement of the entity's objectives. But a reasonable assurance does not mean absolute assurance. Even effective ERM can experience a failure. A failure can be due to judgment mistakes, collusion and illegitimate activities.

An entity is made up of people, each of them having different experiences and cultures that affect their judgments. Many studies have been performed on human judgments. In case of uncertainty, the behavior of people is not rational and causes distortions of reality, called *biases* in technical terms. In behavioral finance theories, the psychological aspects are applied to studies on financial markets. Many factors directly affect risk perception.

The risk/return relationship has a positive correlation between risk and return. An investment that bears a high return is often accompanied by high risk.

Slovic (2000) has observed that there can be an inverse relationship between perceived risk and return.

This inverse relationship is due to *affect heuristic*. If a situation is considered "positively" (Affect +), then people tend to judge risk low and benefit high. If a situation is considered "negatively" (Affect -), then people tend to judge risk high and benefit low.



Risks exist when no certainty exists, and since the future cannot be predicted with certainty, future events and situations imply risks. Even when all information and resources are available, faulty judgments can be made in decision making. This is because there is always a possibility that even the most improbable event can occur. For example, when we analyze the risk on a financial instruments portfolio and establish that the value-at-risk on a one-day time horizon with a confidence level of 99 percent is 1 million CHF, this does not mean that we will never experience a loss higher than 1 million CHF. We can have only a reasonable assurance that the loss over one day will be lower than 1 million CHF with a probability of 99 percent.

Together with people factors, resource constraint can also result in failures in ERM. The degree of closeness to best practices depends on the results of a cost versus benefit analysis that has to be performed for each of the recommended measures, and is therefore the main driver for actual implementation.

The tool, EnteR, helps organizations to assess the maturity level of ERM highlighting strengths and weaknesses from which is derived a prioritized list of measures whose implementation helps to fill existing gaps in ERM. By enabling a multi-period overview on the ERM maturity level, the tool allows evolving a static assessment into a dynamic one.

ERM cannot be seen as a static one-time process, but it must be embedded in the organization and dynamically adapted to the changing internal and external environment.

References

Crouhy, M., Galai, D., and Mark, D. 2001. *Risk Management*. New York: McGraw-Hill.

Culp, C.J. 2001. *The Risk Management Process: Business Strategy and Tactics*. Toronto: Wiley & Sons, Inc.

Kaplan, R., and Norton, D. 1996. "The Balanced Scorecard: Translating Strategy into Action." Online (April 10, 2007): http://www.valuebasedmanagement.net/methods_balancedscorecard.html

Kendall, R. 1998. *Risk Management for Executives*. London: Pitman Publishing.

Lombriser, R., and Abplanalp, P.A. 2005. *Strategisches Management. Visionen entwickeln. Strategien umsetzen. Erfolgspotenziale aufbauen*. Zurich: Versus Verlag.

Münzel, C., and Jenny, H. 2005. *Riskmanagement für kleine und mittlere Unternehmen*. Zurich: Schultess Juristische Medien.

Slovic, P. 1972. "Psychological Study of Human Judgment: Implications for Investments Decision Making." Journal of Finance 27(4): 779–799.

The Committee of Sponsoring Organizations of the Treadway Commission. 1992. "Internal Control—Integrated Framework." New York: AICPA.

The Committee of Sponsoring Organizations of the Treadway Commission. 2004a. "Enterprise Risk Management—Integrated Framework. Executive Summary." New York: AICPA.

The Committee of Sponsoring Organizations of the Treadway Commission. 2004b. "Enterprise Risk Management—Integrated Framework. Framework." New York: AICPA.

The Committee of Sponsoring Organizations of the Treadway Commission. 2004c. "Enterprise Risk Management—Integrated Framework. Application Techniques." New York: AICPA.