CGMA TOOLS

How to evaluate enterprise risk management maturity

CGMA
Chartered Global Management Accountant

Powered by
AICPA | CIMA

NC STATE UNIVERSITY
POOLE COLLEGE OF MANAGEMENT
ENTERPRISE RISK MANAGEMENT

CONTENTS

Two of the world's most prestigious accounting bodies, AICPA and CIMA, have formed a joint-venture to establish the Chartered Global Management Accountant (CGMA) designation to elevate the profession of management accounting. The designation recognises the most talented and committed management accountants with the discipline and skill to drive strong business performance.

OVERVIEW OF THIS ERM ASSESSMENT TOOL

Increasingly, boards of directors and senior executive teams are exploring the concept of enterprise risk management (ERM) to better connect their risk oversight practices with the execution of their strategic plan. ERM has become an important emerging business discipline that has attracted the attention of regulators, financial markets, and rating agencies as they examine firms within their areas of responsibility and interest. The recent financial crisis, emerging political unrest in nations around the globe, and the impact of significant natural disasters are placing even more emphasis on the importance of robust and strategic risk management practices in organisations of all types and sizes.

Despite this increased focus on ERM, organisations still find it difficult to understand both how ERM differs from traditional risk management, and what an effective ERM process looks like. Further, recent research has indicated that many organisations' risk management processes remain fairly immature and lack structure and formality. We have observed that some organisations believe that the ad hoc risk management practices they currently employ are sufficient. We believe these organisations fail to see how a more formal, enterprise-wide approach to risk management would add strategic value. Unfortunately, they often do not fully appreciate the value proposition of ERM until a major risk event occurs, which, by then is too late. In many cases, the failure to see the value of ERM is directly related to a lack of understanding of the critical components of an effective ERM process, and how they are critical to the achievement of the organisation's most important objectives.

This ERM assessment tool will help senior executives and their boards of directors evaluate the strength and relevance of their organisation's existing risk oversight processes. This tool can be used to determine whether the organisation is applying best practices in ERM, and if not, what steps are still necessary to be considered best practice.

This assessment tool is based on a number of inputs that we have found useful to our understanding of effective approaches to ERM. We have been informed by one-on-one coaching and customised training we provide to boards of directors and senior executives about ERM. Additionally, this tool has been developed, in part, by our tracking of the literature and research related to ERM contained in thought papers, research, and best practice guidance issued by numerous think-tanks and regulatory agencies. We have also been involved in a number of ERM thought leadership projects, including the development of COSO's *Enterprise Risk Management – Integrated Framework* and COSO ERM thought papers, and we have conducted extensive ERM-related research. Finally, we frequently work with boards of directors and one of us serves on two corporate boards.

HOW TOOL IS ORGANISED

The following assessment tool guides evaluators through eight focus areas that are considered to be important dimensions of an effective ERM process. In each of the eight focus areas, the tool includes brief descriptors of critical elements of an ERM process that are important to the strength of that focus area. The evaluator considers whether each of the critical elements is currently present at the organisation at the time of the evaluation. In total, there are 75 elements that the evaluator will assess for the organisation. These 75 elements are easily answered as either being present or absent in their current ERM practice.

Raw scores, in addition to a percentage score, are developed for each of the eight focus areas. In the summary section at the end of this tool, the evaluator will tally raw scores and percentage scores from each of the eight focus areas to create an overall score for the organisation. The overall score will be used to provide feedback to the evaluator about the relative maturity of the organisation's ERM processes. Percentage scores for each of the eight focus areas will help provide the organisation some direction about specific aspects of ERM that may require the most immediate attention.

In a corresponding document, we have provided a case study illustration of how this assessment tool can be used by senior management and the board of directors to assess the effectiveness of an organisation's approach to ERM.

WHAT TO DO

The evaluator will consider each of the 75 elements across the eight focus areas and will assign the organisation 1 point in the scoring column for each element that the evaluator believes is present. If the element is not present in the organisation, then the evaluator should score that element with a zero. As the evaluator completes the assessment for each focus area, he or she will total the score for each category and calculate a percentage score by dividing the raw score by the number of risk management elements for that focus area (the number of elements for each focus area is provided). At the end of the assessment tool, the evaluator will create a total score for the entire assessment. Instructions are provided to help the evaluator interpret the organisation's score. Also, a case study example of a completed assessment is presented in a corresponding document.

For purposes of this ERM assessment tool, we define ERM using the following definition contained in COSO's *Enterprise Risk Management – Integrated Framework* (2004):

> Enterprise Risk Management is a process, effected by the 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 the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

While we base our definition of ERM on the COSO framework, this assessment tool will be useful to organisations that may have developed their ERM processes by referencing other known ERM-related frameworks. We believe the eight categories of focus that are assessed through the use of this assessment tool are appropriate and critical to any set of ERM processes and are not unique to a particular ERM framework. Our goal is to help organisations recognise critical elements of an ERM programme that increase its usefulness by strengthening the oversight by management and the board of directors of the most significant risks likely to impact the strategic success of any organisation.

Let's begin the assessment process by first focusing on the importance of the organisation's risk culture regarding the usefulness of ERM processes. Please complete the version below or use the accompanying spreadsheet version. Additionally, review the accompanying case study that illustrates how this ERM assessment tool might be used by senior management and the board of directors to assess the effectiveness of an organisation's approach to ERM.

1. **Risk Culture:** Cultivation of an appropriate, "risk-aware" culture is paramount to effective ERM practices. The strong endorsement by the board of directors and senior management of the value of investing time and infrastructure into better understanding the organisation's most significant risk exposures is an important and necessary condition that must be in place. Without that endorsement, the organisation is not likely to be supportive of any efforts to obtain an enterprise-wide perspective of risks most likely to impact organisational objectives. Instead, risk management may be relegated to a low-value initiative that is viewed by management and employees as compliance oriented and bureaucratic. This focus area in the assessment tool helps the evaluator assess whether senior management and the board understand the importance of ERM and support its use throughout the organisation.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
Senior management and the board of directors have a clear understanding of the objectives of ERM relative to traditional approaches to risk management (eg, insurance, credit risk management, etc.).	
The CEO embraces the need and provides adequate endorsement of an enterprise-wide approach to risk oversight that seeks to obtain a top-down view of major risk exposures.	
The board of directors is supportive of management's efforts to implement an enterprise-wide approach to risk oversight.	
Senior management views the organisation's efforts to obtain an enterprise perspective on the collection of risks as an important strategic tool for the organisation.	
The organisation has explicitly assigned enterprise-wide risk management authority and responsibility to a senior executive or senior management committee (eg identified an internal 'risk champion' or 'risk management leader').	
The senior executive with explicit responsibilities for enterprise-wide risk management leadership is a direct report of the CEO (or, a senior executive risk committee is used to provide that leadership and the committee chair reports to the CEO).	
Enterprise-wide risk management principles and guidelines have been identified and defined by executive management and formally communicated to all business units.	
Senior management has effective risk management capabilities and competencies.	
Senior management's compensation is linked to and dependent upon critical risk management metrics.	
Senior management has formally presented an overview to the board of directors about the organisation's processes that represent its approach to ERM.	
The board of directors sets aside agenda time at each of its meetings to discuss the most significant risks facing the organisation.	
Both the board of directors and senior management view ERM as an ongoing process that will continually evolve over time.	
Total for Risk Culture – Raw Score	
Percentage Score for Risk Culture (Raw Score divided by 12)	

2. **Risk Identification:** Unfortunately, many organisations believe ad hoc and informal approaches to the identification and assessment of risks are sufficient. Therefore, they conclude that there is little benefit in implementing definable, robust, and repeatable processes which encourage the board and senior management to regularly think about risks and opportunities that may emerge and affect the organisation's achievement of objectives. This focus area of the assessment tool helps the evaluator assess the robustness of processes the organisation has in place to identify risks, particularly those risks that may be currently unknown, but emerging.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation has defined and widely communicated to members of management and the board what it means by the term "risk."	
Risks have been described in terms of events that would affect the achievement of goals, rather than simply a failure to meet goals (ie, risks can have both positive and negative aspects to the organisation).	
The organisation engages in explicit (eg, identifiable, defined, formal, etc.) efforts to identify the organisation's important risks at least annually.	
The organisation has identified a broad range of risks that may arise both internally and externally, including risks that can be controlled or prevented, as well as those over which the organisation has no control (ie, focus on more than just known risks such as IT risk, legal risk, credit risk).	
The organisation engages in identifiable processes to regularly scan the environment in an effort to identify unknown, but potentially emerging risks such as competitor moves, new regulations, changing consumer preferences, etc.	
Senior management has a documented process to accumulate information about risks identified across the organisation to create an aggregate inventory of enterprise-wide risks.	
Senior management links risks identified by the ERM process to strategic goals in the organisation's strategic plan to evaluate the impact of those risks on the strategic success of the organisation.	
Each member of the senior management team has provided input into the risk identification process.	
Each member of the board of directors has provided input into the risk identification process.	
Employees below the senior management level have provided input into the risk identification process.	
Total for Risk Identification	
Percentage Score for Risk Identification (Raw Score divided by 10)	

3. **Risk Assessment:** Many organisations find that when they engage in activities to identify risks, they identify a large number of potential risk events, sometimes numbering into the hundreds or thousands. While all risks identified may have relevance to the organisation, some risks are notably more important to the achievement of objectives than others. Therefore, organisations need some method to prioritise risks that encourages a consistent consideration of both the likelihood of the risk occurring and the impact of the event to the organisation, if the risk occurs. This section of the assessment tool guides evaluators through the consideration of a number of elements that are important to a robust risk assessment process to determine if the organisation has developed an effective enterprise-wide set of metrics to consistently assess the risks the organisation faces.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation defines the time period over which risks should be assessed (eg, the next 3 years) to ensure consistency in management's evaluations.	
The organisation strives to assess inherent risk (ie, the level of the risk before taking into account the organisation's activities to manage the risk).	
The organisation assesses not only the likelihood of a risk event occurring but also the impact of the risk to the organisation.	
Guidelines or metric scales have been defined and provided to help individuals assess both likelihood and impact so that assessments are consistently applied across the organisation.	
The organisation considers an integrated score that incorporates both the likelihood and impact assessments to create some kind of risk rating that helps prioritise the organisation's most significant risk exposures.	
The organisation's ERM wprocesses encourage management and the board of directors to consider any low probability, but catastrophic events (ie, "black swan" or "tail" events).	
The organisation considers other dimensions, in addition to likelihood and impact, (such as speed of onset or velocity of a risk or the persistence of a risk event) when assessing risks.	
Each member of the senior management team has provided his or her independent assessments of each risk identified.	
The senior management team (or other similar group with an enterprise view of the organisation) has met formally to review the results of the independent assessments and to discuss significant differences in individual risk assessments.	
The senior management team (or other similar group which would have an enterprise view of the organisation) has reached a consensus on the most significant (somewhere between 8–12 critical risks) risks facing the organisation.	
The board of directors has concurred with the assessment of the risks completed by management.	
Senior management analyses its portfolio of risks to determine whether any risks are interrelated or whether a single event may have cascading impacts.	
The ERM process encourages monitoring on a regular basis (more than once a year) any events substantially impacting the assessments of likelihood and impact.	
Total for Risk Assessment	
Percentage Score for Risk Assessment (Raw Score divided by 13)	

4. **Articulation of Risk Appetite:** The full benefits of identifying and assessing risks can only be realised if the organisation has articulated its risk appetite. Without some description of the organisation's willingness to take on risks as it seeks to achieve its objectives, the board and senior management are unable to know when risks should be taken or when risks should be managed.

While determining the organisation's appetite for risk taking can be challenging, it is important that the board and senior management make some attempt to articulate its overall appetite for risk taking. This focus area in the assessment tool helps the evaluator assess the effectiveness of the organisation in determining its risk appetite.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The board and management have engaged in discussions to articulate the organisation's overall appetite for risk taking.	
The board of directors has concurred with the organisation's risk appetite.	
The organisation has separately defined its risk appetite for different types of risks (eg, the organisation may have different appetites for engaging in mergers and acquisitions [M&A], for investing in new ventures, for gaps in succession in executive positions, and for risks related to employee health and safety).	
The organisation has expressed in writing its overall appetite for risk taking.	
The organisation has used at least some quantitative measures in defining its risk appetite.	
Total for Risk Appetite	
Percentage Score for Risk Appetite (Raw Score divided by 5)	

5. **Risk Response:** Until the organisation implements its desired response to manage risks that have been identified and assessed, the organisation's ERM efforts will be of little value towards the achievement of objectives. Organisations may choose to accept certain risks, avoid others, adopt processes to reduce the exposures to risks, or share risks with external parties. Of utmost importance, however, is to ensure that an appropriate risk response (like those mentioned above) is implemented, and then to ensure that the response is working as intended. Periodic evaluation of whether identified risk responses are effectively being carried out is will ensure an effective ongoing ERM process. This focus area of the assessment tool helps the evaluator assess the extent to which the organisation has taken appropriate steps to manage its risks to be within its risk appetite.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation has identified risk owners with responsibility for each of its most significant risks (ie, its top 8–12 risks).	
The organisation has identified a risk owner for other risks identified outside the top 8–12 risks that management believes are important to monitor.	
The organisation has documented the existing response(s) to its most significant risks (ie, its top 8–12 risks).	
The organisation has documented the risk responses for each of the other risks identified outside those deemed as the top 8–12 most significant enterprise-wide risks.	
The organisation has evaluated whether the existing response is sufficient to manage the risks to be within the organisation's risk appetite.	
The organisation has developed and is implementing plans to address those risks where the current response is insufficient.	
The organisation has separately evaluated the potential cost of the risk response relative to the benefit provided by the response towards either reducing the impact or reducing the probability of occurrence of the risk event.	
The organisation re-evaluates its risk responses at least annually.	
The organisation's ERM process helps identify potential overlaps or duplications in risk responses across the enterprise.	
The organisation conducts table top drills or other exercises to test whether responses to its most significant risks (ie, its top 8–12 risks) are working as intended.	
The organisation has objectively assessed the effectiveness of risk response plans for its most significant risks (ie, its top 8–12 risks).	
The organisation has objectively assessed the effectiveness of risk response plans for other risks that management believes are important to monitor that are outside the top 8–12.	
Total for Risk Response	
Percentage Score for Risk Response (Raw Score divided by 12)	

6. **Risk Reporting:** An objective of any ERM process is to provide information to senior management and the board about the organisation's portfolio of risks and related response to those risks. As risks are identified and assessed across the organisation, processes are needed to facilitate the communication of risk-related information so that an aggregate view of important risks and their related risk responses are provided to senior management, the board, and to critical stakeholders. This focus area of the assessment tool helps the evaluator assess the effectiveness of how the organisation communicates information regarding its most significant risks.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation has developed and monitors critical risk indicators that are lagging in nature (ie, metrics that show when risk events have occurred or are escalating).	
The organisation has developed and monitors critical risk indicators that are leading in nature in that they provide some indication that a risk event is more likely to occur in the future.	
Senior management regularly reviews a "dashboard" or other report that provides the status of critical risks and/or risk response plans.	
The board regularly receives and reviews a "dashboard" or other report that provides the status of critical risks and/or risk response plans.	
Senior management has identified thresholds or trigger points whereby risk metrics indicate that an emerging risk warrants greater management and/or board attention.	
Output from the organisation's ERM processes about significant risk exposures are an important input to the organisation's risk disclosures to critical stakeholders (eg, Item 1A Risk Factor disclosures in a public company's Form 10-K filing).	
Total for Risk Reporting	
Percentage Score for Risk Reporting (Raw Score divided by 6)	

7. **Integration with Strategic Planning:** Risk and return are interrelated concepts. Successful leaders know that risks must be taken in order to generate returns. Unfortunately, in many situations, the organisation's efforts related to risk management and the efforts related to strategic planning are distinct and separate activities. Effective ERM can be an important input and consideration into the determination and execution of any organisation's strategy. ERM provides critical insights into the portfolio of existing and emerging risk exposures that can contribute to the strategic success of the organisation. This focus area in the assessment tool helps the evaluator assess the extent to which enterprise-wide risk considerations are incorporated into the firm's strategic planning process.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation has a formal strategic planning process.	
The strategic plan is updated at least annually.	
The organisation's existing risk profile (ie, output from the ERM processes) is an important input for the strategic planning process.	
Senior management links the top risk exposures to strategic objectives to determine which objectives face the greatest number of risks and to determine which risks impact the greatest number of objectives.	
When evaluating a range of strategic options, consideration is given to the potential impact of each option on the organisation's existing enterprise-wide risk profile.	
The senior executive with explicit responsibility for enterprise-wide risk management leadership (or the chair of the committee with that responsibility) is actively engaged in the strategic planning process.	
The organisation's ERM processes encourage the consideration of opportunities where the organisation can take informed risks to generate incremental returns.	
The firm's risk appetite statement guides the goal setting process (eg, if the firm has a low appetite for M&A, it will set lower growth goals that are achievable without engaging in M&A).	
Risk-adjusted return expectations are set for each business unit and/or product/service line.	
The organisation's strategic plan has been communicated to employees so that they can understand how their actions can create or prevent risks to the achievement of strategic objectives.	
Total for Strategic Planning	
Percentage Score for Strategic Planning (Raw Score divided by 10)	

8. **Assessment of ERM Effectiveness:** While awareness of the concept of ERM has been growing over the last decade, processes and techniques involved in any ERM implementation continue to evolve and mature. Additionally, as the complexity of the global business environment continues to increase, new methodologies and procedures will be needed to effectively manage the portfolio of risks that organisations will face in the future. As a result, senior management and the board of directors need to view ERM as an evolution, not a point-in-time project to be implemented. This focus area of the assessment tool helps the evaluator assess the extent to which the organisation regularly reviews the effectiveness of its ERM processes and monitors emerging ERM best practices.

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
Senior management regards ERM as an ongoing process rather than just a project.	
Senior management seeks to understand and monitor emerging ERM best practices.	
Senior management and the board of directors have engaged in ERM related training or other knowledge enhancing activities.	
Adequate resources have been dedicated to support the ERM function.	
The organisation periodically obtains an objective assessment of its ERM processes (eg, through internal audit or third party ERM expert evaluations).	
The organisation evaluates risk events that have occurred to better understand why the risk occurred and whether there were failures in the organisation's ERM processes.	
The organisation identifies and subsequently implements changes to improve its ERM processes.	
Total Assessment of ERM Effectiveness	
Percentage Score for Assessment of ERM Effectiveness (Raw Score divided by 7)	

SUMMARY

Now that you have completed your assessment of the 75 risk management elements across the eight focus areas in this assessment tool, it is time to summarise your results. Turn back to each page of the eight focus areas and bring forward the raw score and percentage score you recorded on those pages and enter the information in the chart below. Then, tally the total for the raw score column. A perfect score would equal 75. Then, on the final row in the table below divide your total raw score by 75 to calculate an overall percentage score for your organisation.

Category	Total Score Possible	Raw Score for Category	Percentage Score for Category
Risk Culture	12		
Risk Identification	10		
Risk Assessment	13		
Articulation of Risk Appetite	5		
Risk Response	12		
Risk Reporting	6		
Integration with Strategic Planning	10		
Assessment of ERM Effectiveness	7		
Total Score	75		
Grand Percentage (divide Total Score by 75	100%		

INTERPRETATION OF RESULTS

Focus on the total score for your organisation that you calculated in the table above to determine which category your score falls into using the chart below.

Description of Current State of ERM	Range of Total Score
Just Getting Started	From 1 to 25
Basic ERM Practices in Place	From 26 to 45
Basic as well as some more sophisticated ERM Practices in Place	From 46 to 65
Robust ERM in Place	From 66 to 75

As you evaluate the implications of your organisation's score, keep in mind that this assessment tool is merely providing you some general ideas as to your organisation's overall ERM effectiveness. This is not a scientifically determined scoring outcome. Rather, you should view your score as a directional indication of the general level of maturity of the organisation's ERM. Do not be too concerned by the exactness of your score. It is more important to consider your score in general relationship to the possibility of having all 75 elements in place.

A corresponding document: *How to Evaluate Enterprise Risk Management Maturity: Case Study* provides a sample of how a fictitious company can benefit from using this tool.

For those organisations in the "Just Getting Started" stage of ERM, there are a number of the eight focus areas that may warrant immediate attention. We would especially encourage those organisations to start with focus area number 1: "Risk Culture" to ensure that senior management's and board of directors' support of ERM is in place, before taking any actions towards strengthening the other seven focus areas highlighted by this assessment tool. Once risk culture is in place, then the organisation can work its way through the other seven focus areas.

About the Authors

Mark S. Beasley, CPA, Ph.D., is the Deloitte Professor of Enterprise Risk Management and director of the ERM Initiative at NC State University (see www.erm.ncsu.edu). He specialises in the study of enterprise risk management, corporate governance, financial statement fraud, and the financial reporting process. He is a board member of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and has served on the International Corporate Governance Network and Yale University's Millstein Center on Corporate Governance's Task Force on Corporate Risk Oversight and has participated with The Conference Board's ERM Working Group. He earned his Ph.D. at Michigan State University.

Bruce C. Branson, Ph.D., is a professor of accounting and associate director of the Enterprise Risk Management (ERM) Initiative at NC State University. His teaching and research is focused on financial reporting and includes an interest in the use of derivative securities and other hedging strategies for risk reduction/risk sharing. He also has examined the use of various forecasting and simulation tools to form expectations used in financial statement audits and in earnings forecasting research. He earned his Ph.D. at Florida State University.

Bonnie V. Hancock, M.S., is the executive director of the Enterprise Risk Management (ERM) Initiative, and is also an executive lecturer in accounting at NC State's Poole College of Management. Her background includes executive positions at both Progress Energy and Exploris Museum. She has served as president of Exploris, and at Progress Energy, has held the positions of president of Progress Fuels (a Progress Energy subsidiary with more than $1 billion in assets), senior vice president of finance and information technology, vice president of strategy and vice president of accounting and controller. She currently serves on the board of directors for AgFirst Farm Credit Bank and Powell Industries.

Contact us at: **erm_initiative@ncsu.edu**.

The information herein was adapted from *ERM Assessment Tool: Evaluating Your Organization's Current State of ERM Maturity*, by Mark S. Beasley, Bruce C. Branson, and Bonnie V. Hancock, Copyright © 2011 by American Institute of Certified Public Accountants, Inc.

American Institute of CPAs
1211 Avenue of the Americas
New York, NY 10036-8775
T. +1 2125966200
F. +1 2125966213

Chartered Institute of
Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom
T. +44 (0)20 7663 5441
F. +44 (0)20 7663 5442

www.cgma.org

January 2012

CGMA
Chartered Global Management Accountant

11674A-359

The Association of International Certified Professional Accountants, a joint venture of AICPA and CIMA, established the CGMA designation to elevate the profession of management accounting globally.