CGMA CASE STUDY

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

On the pages that follow, a hypothetical case study is presented as an illustration of how the ERM assessment tool, *How to Evaluate Enterprise Risk Management Maturity: Tool*, might be used by senior management and the board of directors to assess the effectiveness of an organisation's approach to enterprise risk management.

Gemini Motor Sports (GMS), a public company headquartered in Brazil, manufactures both on-road and off-road recreational vehicles for sale through a dealer network in both Brazil and Canada. Sales of these vehicles is largely a function of the discretionary income and available credit capacity of their targeted customer base—primarily males between the ages of 21 and 50 years of age. GMS launched an Enterprise Risk Management (ERM) programme two years ago in response to an explicit request by the chair of the audit committee (AC) of the board of directors to evaluate whether GMS' existing risk management approach could be improved by adopting a more comprehensive, enterprise-wide view of risk.

GMS Chief Financial Officer (CFO), Davi Cruz, was charged with the oversight of the development of the initial ERM framework for the company. This involved the designation of a small group of Cruz' staff as coordinators for the initial risk identification and assessment that they believed was a logical starting point for the ERM implementation based on their reading of various resources made available to them by Cruz.

The ERM team met with GMS senior management (all C-level executives and business unit leaders were interviewed) over a two-month time frame and open-ended questions were asked about risks that had been encountered that they felt had been disruptive to GMS operations and damaging to the financial health of the company. Information on how these risks were dealt with was also collected. This information was then brought together by the ERM implementation team for further analysis. Based on the number of times a specific risk event had been mentioned, and the financial loss that had been incurred as a result of that event, the ERM implementation team prioritised the risks and developed a presentation for the CFO to deliver to the AC at their next scheduled meeting.

While somewhat enlightening, the presentation was criticised by the AC chair as a rehash of past events and offered little insight or value to the board as they discussed the strategic direction of GMS. GMS follows Comissão de Valores Mobiliários – (CVM - Securities and Exchange Commission of Brazil) regulations as well as U.S. Securities and Exchange Commission (SEC) regulations since they are listed on the New York Stock Exchange (NYSE) and prepared to respond for the first time to new SEC disclosure requirements concerning their role in the oversight of the risk management function of GMS. Cruz was directed to devote additional resources to more fully develop an ERM process that would allow the AC and the full board to have a better understanding of the risk environment faced by GMS.

After meeting with staff whom he had charged with the first round of risk identification and assessment, Cruz concluded that additional training on ERM best practices was needed and sent several senior members of his staff to executive education programmes on ERM as well as personally investigating available literature to help provide additional direction to the ERM staff on enhancements and revisions to their original effort. These investments provided a more fully developed understanding of the goals of enterprise risk management to all involved with the ERM implementation.

In the second year of the ERM programme, Cruz devoted significant attention to the process that was developed for gathering information about risks across the company. He insisted that questions asked of the other members of the senior management team not only focus on risk events that had already occurred, but also on potential risks they saw as emerging within their areas of expertise. For these risks, estimates of likelihood of occurrence within the next two years were obtained along with 'best guess' income amounts for the damage such a risk event would cause the company if they were to occur. These risks were scored by multiplying the estimated probability times the income damages to rank-order the risks for additional review.

In addition to identifying the top 15 risks faced by the organisation through this process, Cruz also was able to place oversight responsibility for the ongoing monitoring of these risks with specific individuals within the company. For example, one of the risks identified in this process involved the potential development of a new type of transmission for the family of off-road vehicles that was a significant component of GMS' product line. This transmission alleviated the need for a traditional clutch mechanism and was rumoured to be under development by an industry competitor. If successfully developed, this would represent a significant threat given the ease of operation of such a vehicle relative to the GMS product line offerings. Yara Mendes, the head of new product development for GMS, was given the responsibility for monitoring the progress being made within the industry in this area as well as developing responses in the event of the introduction of this innovation into the marketplace.

In making his next report to the AC, Cruz was praised for the revisions to the ERM process that he had initiated. However, the AC chair still questioned the value of the information that she had received with respect to the usefulness to the board in understanding the risk management process (ie, its strengths and weaknesses) and precisely how the risk information that had been gathered could be integrated with the strategic plan that they had recently approved for GMS. The AC chair suggested that Cruz explore a benchmarking exercise to determine whether the ERM programme that he and his staff had developed could be further evolved into a strategic tool for the company.

Fortunately, shortly after this meeting, Cruz was made aware of the existence of an ERM assessment tool, newly available from the CGMA website. Completion of this assessment appeared to offer a path forward for identifying both strengths and weaknesses in GMS' existing ERM programme. Cruz thought it might also provide ammunition for the next round of resource allocation discussions if he could point to explicit shortfalls in GMS' risk management practices that could be addressed with additional staff or staff training that had been objectively identified through the use of the assessment tool.

Cruz obtained the ERM assessment tool and carefully responded to the 75 elements identified as components of a robust ERM program. The results of that assessment follow.

1. Risk Culture:

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.).	1
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.	1
The board of directors is supportive of management's efforts to implement an enterprise-wide approach to risk oversight.	1
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').	1
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).	1
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.	1
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	6
Percentage Score for Risk Culture (Raw Score divided by 12)	50%

Discussion: In reading through the critical elements of risk culture, Cruz was only able to respond in the affirmative to half of these. He had been explicitly tagged with the ERM effort and he did directly report to the CEO. As well, he felt that both the board and the senior management team were both supportive of and knowledgeable about the goals of ERM. However, he did not feel that the company was yet at a place to use ERM strategically, nor was the ERM philosophy well-integrated throughout the company. Perhaps most importantly, he recognised that he had not yet tapped the expertise of the board in his risk identification and assessment efforts to date, nor did they devote specific time in their meetings to discussions of significant risks.

2. Risk Identification:

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."	1
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).	1
The organisation engages in explicit (eg, identifiable, defined, formal, etc.) efforts to identify the organisation's important risks at least annually.	1
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).	1
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.	1
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	5
Percentage Score for Risk Identification (Raw Score divided by 10)	50%

Discussion: Several important insights emerge from the completion of this assessment of risk identification practices. First, it had not occurred to Cruz that the term 'risk' might need to be carefully defined to ensure consistent responses. As well, he had been framing the risk questions over the past two years as focusing only on failures. It became clear that potential opportunities may have been overlooked with this one-sided view of risk. Cruz was not aware of any effort to date to explicitly link the risk identification process to strategic goals of the company. And, it was also clear that Cruz should begin involving many more employees, and members of the board, in the risk identification process in order to ensure the most complete inventory of risks was gathered.

3. Risk Assessment:

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.	1
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.	1
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.	1
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.	1
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.	1
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.	1
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.	1
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	7
Percentage Score for Risk Assessment (Raw Score divided by 13)	54%

Discussion: Cruz felt that the assessment guidance that had been developed met many of the standards in the assessment tool. There was explicit guidance provided about the time horizon to be considered (two years) and the measurement of the impact was determined by an income loss amount that would be incurred in the event of occurrence. As well, probabilities and impacts were multiplicatively combined to produce a prioritisation score for each top risk. As in the earlier assessments, it was clear to Cruz that he needed to include members of the board in the risk assessment process. He was especially concerned about the need to carefully consider low probability, high impact events even when their risk score did not identify them as particularly risky and he needed to include questions about the speed of onset and persistence of risk events. No explicit agreement had yet been reached with the board as to whether the risks that had been identified and assessed were in fact the company's top risk exposures. As well, no attempt had been made to consider correlations of risk on a portfolio basis.

4. Articulation of 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.	1
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	1
Percentage Score for Risk Appetite (Raw Score divided by 5)	20%

Discussion: Upon completion of this assessment, Cruz realised that this was a significant area of concern. While he felt the board and senior management team had discussed risk-taking (which he interpreted as an early effort towards the articulation of an organisational risk appetite), it was clear that there is much work to be done in this area. To Cruz' knowledge, no explicit statement of the risk tolerance or appetite for risk had been developed to guide decision making.

5. Risk Response:

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).	1
The organisation has identified a risk owner for other risks identified outside the top 8–12 risks that management believes are important to monitor.	1
The organisation has documented the existing response(s) to its most significant risks (ie, its top 8–12 risks).	1
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.	1
The organisation re-evaluates its risk responses at least annually.	1
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).	1
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	6
Percentage Score for Risk Response (Raw Score divided by 12)	50%

Discussion: Cruz felt good about the level of attention paid to the top 15 risks they had identified through their identification and assessment process with respect to planned responses and delegation of responsibility. Beyond these top 15, Cruz recognised that there was additional work to be done to ensure that the next level of risks were also monitored and had been assigned risk owners. Cruz was intrigued by the possibility of conducting simulations to test the effectiveness of planned responses but had not yet implemented that approach.

6. Risk Reporting:

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).	1
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.	1
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.	1
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	3
Percentage Score for Risk Reporting (Raw Score divided by 6)	50%

Discussion: Cruz had been working with his staff to adjust risk metrics that corresponded to specific risk events that had occurred and affected the company. This assessment allowed him to recognise the need for and value of critical risk indicators that would be more predictive in nature and allow the company to more proactively respond to emerging risks. Cruz provides a report, updated quarterly, to the senior management team that consists of a roll-up of reports he receives from risk owners charged with monitoring specific risks. He has received requests for a more concise report or dashboard that provides a clear view of the status of significant risk exposures. The board does not receive any regular report other than the oral presentations Cruz makes when requested by the AC chair. Legal is responsible for the Item 1A risk factors to be disclosed in the 10-K and Cruz has never received a request for risk information from them.

7. Integration with Strategic Planning:

Description of Key Elements	Score (1= element present; 0 or blank otherwise)
The organisation has a formal strategic planning process.	1
The strategic plan is updated at least annually.	1
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.	1
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.	1
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	4
Percentage Score for Strategic Planning (Raw Score divided by 10)	40%

Discussion: Senior management of GMS engages in an annual strategic planning exercise and the newly revised strategic plan is shared with the board for their review and approval. Cruz felt that risk was a part of these discussions, but not in a formal, structured fashion. The concept of risk versus return is well understood at GMS and business units are evaluated, and capital allocation decisions are made, with risk-adjusted performance in mind. This assessment made it clear that an effort to better integrate risk information from the ERM process could improve the strategic decision-making by senior management. Cruz would currently describe this effort as much more ad hoc in nature rather than robust and definable. As noted earlier, no explicit statement of risk appetite has been developed at GMS.

8 . Assessment of ERM Effectiveness:

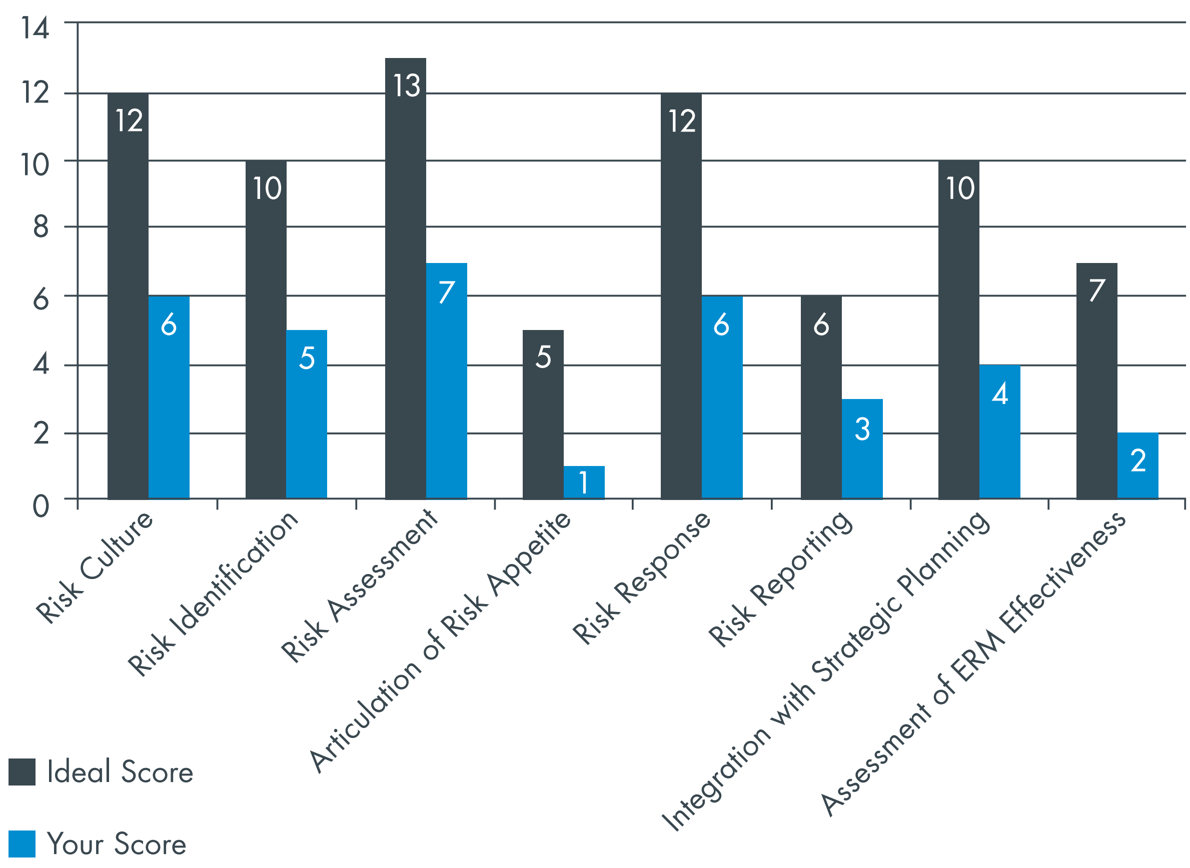
Description of Key Elements	Score (1= element present; 0 or blank otherwise)
Senior management regards ERM as an ongoing process rather than just a project.	
Senior management seeks to understand and monitor emerging ERM best practices.	1
Senior management and the board of directors have engaged in ERM 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.	1
The organisation identifies and subsequently implements changes to improve its ERM processes.	
Total Assessment of ERM Effectiveness	2
Percentage Score for Assessment of ERM Effectiveness (Raw Score divided by 7)	29%

Discussion: After completion of this final assessment, it is clear to Cruz that there remains significant work to be done to evolve the GMS ERM process to the next level. Cruz has no doubt that ERM is still largely viewed as a discrete project. He has been asked on more than one occasion when he will be finished with the ERM programme. He recognises that additional resources will still be necessary in order to involve more members of the company below senior management and business unit leaders as well as the board in the annual process of updating the list of top 15 risks that GMS faces. It may be time, Cruz realises, to draw on external expertise for assistance in designing an ERM function that can better position GMS for further growth.

SUMMARY

Category	Total Score Possible	Raw Score for Category	Percentage Score for Category
Risk Culture	12	6	50%
Risk Identification	10	5	50%
Risk Assessment	13	7	54%
Articulation of Risk Appetite	5	1	20%
Risk Response	12	6	50%
Risk Reporting	6	3	50%
Integration with Strategic Planning	10	4	40%
Assessment of ERM Effectiveness	7	2	29%
Total Score	75	34	
Grand Percentage (divide Total Score by 75	100%	45%	

ERM MATURITY BY CATEGORY



INTERPRETATION OF RESULTS

GMS' score of 34 places them within the range of 26–45, which is in the maturity level described as 'Basic ERM Practices in Place.' After two years of development, this is a reasonable result. As CFO, Davi Cruz has many important responsibilities and should be proud of the evolution of the ERM implementation he has led. That said, it is likely that this effort will need to be passed to an individual capable of devoting more time solely to the task of coordinating and facilitating the information gathering effort required for a more sophisticated ERM process to emerge. Many organisations have begun to appoint a Chief Risk Officer (CRO) or formally constitute an Executive Risk Committee to oversee their ERM processes.

Not surprisingly, two areas were identified as being rather weak: 1) the absence of a formal statement of risk appetite to help guide decision making and 2) the integration of the ERM process with strategic planning. Both of these areas are typically associated with more sophisticated, more fully evolved ERM programmes. It would be advisable for GMS to begin discussions at the board and senior management level to better articulate the appetite for risk-taking so that managers and executives can more fully understand that risk-taking is inherent to successful business operations. Better informed risk-taking is likely to lead to higher incidences of success. A robust enterprise-wide risk management approach can provide the information necessary to improve decision-making. Cruz noted that risks were a part of the discussion when the strategic plan was being debated and agreed upon at the senior management level. What may be needed is a more formal approach to ensure that all participants in the planning process have a consistent understanding of the organisation's risk profile and risk appetite.

Another area of concern that was made apparent through the ERM assessment tool was the apparent lack of significant involvement of the board of directors of GMS in the risk identification and assessment process. As well, it appears that the board does not devote formal agenda time to the discussion of significant risks. One way that the board can feel more comfortable about the discharge of their risk oversight responsibility is to actively participate in the risk information gathering conducted by the ERM staff and to document time spent engaged in discussions related to the significant risks their companies face.

These actions will also allow the board to confidently report their involvement with and oversight of the risk management function as now required for all SEC registrants as part of their proxy disclosures.

ERM must be viewed as an evolutionary process within the company. Too often, it is viewed as a compliance driven exercise to be accomplished, documented, and filed away. It is doubtful that much value will be extracted from this type of effort. The ERM process must be allowed to continually refresh the existing risk inventory and revisit assessments of probabilities and impacts to ensure that significant, potentially catastrophic, risks are not missed. To help this view of ERM become the dominant view within the company, both the board of directors and the CEO should explicitly endorse the ERM effort and provide sufficient resources to allow the ERM staff to fully implement the elements of a mature ERM process discussed herein.

Finally, it also should be understood that it is unrealistic to expect an ERM process to evolve to this state of maturity in a relatively short period of time. Many sample companies have integrated ERM programmes for some time and, to a company, tell us that they are still learning, and still refining their processes. The company profiled in this case study, GMS, has made significant strides towards developing a mature ERM process–but does still have significant room for further development, and additional value creation that derives from making better risk-informed decisions in setting the strategic direction of their company.

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**.

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

11674B-359

CGMA Chartered Global Management Accountant

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.