CRMA®

EXAM PRACTICE QUESTIONS

CERTIFICATION IN RISK MANAGEMENT ASSURANCE®

EXAM PRACTICE QUESTIONS

CRMA®
Certification in
Risk Management Assurance™

Thomas F. O'Connor, CIA, CRMA, CGAP

Dorothy Dordelman Pearson, MPP

Goli A. Trump, CRMA, MBA

The Institute of Internal Auditors
Research Foundation

Published by The Institute of Internal Auditors Research Foundation

247 Maitland Avenue

Altamonte Springs, Florida 32701-4201

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN-13: 978-0-89413-914-7

CONTENTS

FOREWORD

In response to growing interest and requests, The IIARF developed this publication of 150 practice questions for those planning to take the Certification in Risk Management Assurance® (CRMA®) exam. As the exam is *closed*, these 150 questions are not directly from the bank of exam questions but, very importantly, represent questions judged by The IIARF—after careful review—to be *plausible* for the exam. The IIARF's existing *CRMA Exam Study Guide*, 1st Edition (2013) offers those planning to take the exam with an excellent reference for study and includes an additional 50 practice questions.

The practice questions are aligned with the four domains of the CRMA exam related to enterprise risk management (ERM): (I) organizational governance related to risk management, (II) principles of risk management processes, (III) assurance role of the internal auditor, and (IV) consulting role of the internal auditor. Consistent with the extent of exam coverage, more questions are included for Domains I and II than for Domains III and IV.

In developing these practice questions as an addition to the 50 available in the *CRMA Exam Study Guide*, The IIARF not only expanded the *number* but also the *nature* of the questions. Specifically, they include scenario-based or practical questions in addition to those of a theoretical nature. Moreover, care was taken to include consideration of the ways in which ERM processes can and do differ dependent on the type of organization, whether in the private, public, or not-for-profit sectors.

This publication, coupled with adequate study of available, relevant literature on the widespread recognition of ERM as a key component of effective governance, should be invaluable to CRMA test takers. Also

included is an appendix that includes additional references beyond those cited in the *CRMA Exam Study Guide*.

The IIARF and the three authors wish you great success as a future CRMA!

ACKNOWLEDGMENTS

The three authors wish to acknowledge The Institute of Internal Auditors (IIA) for permission to use various publications, which gave us a solid base from which to glean collective experiences to develop this set of practice questions. In addition, many members of The IIA and The IIA Research Foundation (IIARF), as well as risk management professionals from other entities, offered advice and ideas, which were invaluable. The list of those who helped is more than can be presented herein.

We do wish to single out the technical advice, continuing support, and encouragement from Lillian McAnally, Jennifer Selix, and Lee Ann Campbell. Members of the IIARF Committee of Research and Education Advisors (CREA), who served us graciously and extremely well, were Urton Anderson, Sezer Bozkus, and Ulrich Hahn. Our practice questions are heavily aligned with the *CRMA Exam Study Guide*, 1st Edition, by Francis Nicholson and Chris Baker, and we thank them for paving the way. In the later stages of this project, Chris Baker stepped forward to offer timely and insightful comments, which helped us immensely.

On a personal level, like most people, each author has other responsibilities and commitments to family members and friends. We would not have been able to complete this project without their understanding and support, as it consumed significant time and energy. Thus, our families and dear friends share in its successful publication.

Ms. Trump wishes to thank her children, Daniel and Nathalie, who showed infinite grace as she balanced her writing hours with their hours of school, sports, and opportunities to play, laugh, and travel. Ms. Pearson expresses special thanks to her son, Taylor, and daughter, Kathryn, for their continued love and support of her endeavors. Mr.

O’Connor expresses sincere appreciation to his wife, Gail, and their four children and beautiful grandchildren, especially the small one who gave up many hours with “Papa.”

Thank you, one and all!

ABOUT THE AUTHORS

Thomas F. O'Connor, CIA, CRMA, CGAP, CPA, CFGM, CMA, CFE, MPA, is a self-employed consultant, trainer, and researcher. He had a 34-year career as an auditor, investigator, and evaluator, including 30 years with the U.S. Government Accountability Office (GAO). In that career, Mr. O'Connor continuously assessed internal controls, including consideration of relevant risks.

He currently instructs preparatory courses for the Certified Internal Auditor (CIA) and Certified Government Auditing Professional (CGAP) exams, both of which necessitate a sound understanding of risk management. Mr. O'Connor is the author/co-author of the following IIARF publications: *Emerging Strategies for Performance Auditing* (2014), *CGAP Exam Study Guide*, 4th Edition (2012), and *CGAP Exam Study Questions* (2010). He also assists The IIARF in various other research.

Dorothy Dordelman Pearson, MPP, has 27 years of experience combining strategic analysis, information technology solutions, and best practices in risk management in the private, nonprofit, and public U.S. sectors. In addition to conducting internal control audits of the United States Environmental Protection Agency (EPA), Ms. Pearson also served on the U.S. congressionally mandated engagement to train the Internal Revenue Service (IRS) and its contractors to develop performance-based task orders. She served on groundbreaking initiatives to devolve governmental authority to create institutional capacity within local jurisdictions in a foreign government.

She has served on multiple engagements training top-tier management in best practices in procurement, contracting, and performance

management. Building upon her tenure in the U.S. government technology markets, she served as a founding executive of e-fense, Inc., an information security business conducting risk audits and forensic analyses and developing integrated security programs. Her most recent work with The IIARF was as lead analyst on its 2014 publication *Emerging Strategies for Performance Auditing: Insights from City Auditors in Major Cities in the U.S. and Canada*. Ms. Pearson has spent her career building the organizational infrastructure necessary to anticipate and manage change and to leverage opportunity.

Goli A. Trump, CRMA, MBA, is the director of enterprise risk management (ERM) at a U.S. national nonprofit that oversees a $2 billion program. Ms. Trump aligns ERM to corporate strategic planning, while executing a governance, risk, and compliance (GRC) framework, developing a progressive ERM-to-audit lifecycle that requires an objective risk-based audit activity, and performing internal audits in accordance with the enterprise's risk portfolio. Ms. Trump leads risk analyses in areas of operations, governance, technology, operations, new business initiatives, legal, regulatory, ethics, and compliance. Additionally, she develops and delivers training on implementation of ERM and internal audit best practices for her nonprofit's 500-member organizations.

She has lectured at universities and presented to internal audit and ERM associations. In addition, Ms. Trump's career experience also includes roles as a chief financial officer, board treasurer, and consultant in strategic planning and communications. She has held positions in private firms and nonprofit organizations in the United States and the United Kingdom, and has served on boards of a venture capital-backed U.S. organization and a small nonprofit.

QUESTIONS

DOMAIN I—ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

1. Risk management processes in entities in the governmental sector and private sectors should be generally similar. However, due to a different environment, and dissimilar characteristics and objectives, risk management processes may differ. Which of the following is most true?

a. Organizational objectives are more diverse in government.
b. Even with constrained budgets, government entities may easily exceed private sector entities' established "risk appetites."
c. Private sector entities face more laws and regulations than government agencies.
d. The governance organizations will bear the same names (e.g., "the board," "audit committee," "a CAE") and functions the same way in both sectors.

2. A newly appointed risk officer begins an environmental scan by conducting interviews with key staff. She finds out that there is a strong sense of territory and she continues to hear the same issues raised at each department's meetings. The risk officer also has discovered that action items are not shared among the various departments or management. What would be the most likely conclusion of the risk officer's environmental scan?

a. The organizational structure does not promote integration of

activities across departments.

b. It is likely that the CEO does not believe in the nonprofit's mission.
c. The organizational structure is not designed to allow for agile and innovative responses to the external environment.
d. The managers are not given enough resources to help achieve the strategic goals.

3. Stakeholder analysis is an important component of risk management planning. Which of the following two factors are most likely to result in conflicting interests and expectations among primary *internal* stakeholders?

I. The responsibility to accommodate the extra work and the level of skills and financial resources necessary to implement risk management.
II. A corporate culture that focuses management on personal or short-term gain while owners' interests tend to be focused on long-term returns on their investment.
III. Whether a stakeholder is represented in the development of risk management processes.
IV. Whether the organization is in the private sector or the public sector.

a. I and II only.
b. II and III only.
c. I and III only.
d. III and IV only.

4. Within an organization's structure, there is one process by which risks can be managed by increasing flexibility and creating opportunities for team members when assigning tasks to subordinates. What is this process?

a. Creating cross-functional teams.
b. Succession planning.
c. Mandatory work breaks.

d. Delegating authority.

5. **A company is planning a risk assessment of the IT systems that process, store, and transmit its litigation data. In accordance with GAIT-R, the first and most important planning task the assessment team should undertake is:**

   a. Ensuring that the risk management team or assessment contractor has access to the technical expertise necessary to understand system configurations and software vulnerabilities.
   b. Conducting a thorough review of information security (InfoSec) policies and procedures.
   c. Interviewing key C-suite (CEO, CIO, CFO, legal) executives and operational managers to identify and rank threats to the business.
   d. Determining the types and proper mix of manual and automated controls needed to provide reasonable assurance.

6. **An adjudicatory board makes decisions in cases where unsuccessful vendors contend that procurement officials treated them unfairly. Both parties appear before the board. An audit of the board identified unjustified sole-source procurements; costly, unneeded renovation work; disparity in personnel work assignments; and the establishment of a council unrelated to the board's mission and funded by vendors and procuring offices. Which creates the most serious reputational risk to the board?**

   a. Wasteful spending on procurements, travel, and renovations.
   b. Questionable, inappropriate, or unfair personnel practices.
   c. Establishing a council unrelated to the board's mission.
   d. Seeking funding from those who appear before the board.

7. **Hard controls are affected by policies, processes, and structure. Soft controls rely on the behavior and attitude of individuals. Identify the controls below as hard (H) or soft (S) and decide whether an auditor would find it difficult (D), slightly**

challenging (C), or relatively easy (E) to assess the effectiveness of the control.

a. Physical counts (S)/(E).
b. Policies (H)/(C).
c. Openness (S)/(D).
d. Shared values (H)/(E).

8. **A small toy company was challenged to find a way to prioritize its risks, and the owners looked to its senior managers to help make decisions about new products. New products were considered in light of factors such as price, regulatory requirements, consumer demand, and time to market. The factors were given a weight for relative importance. Each prospective new toy was scored against each of the factors. Once numerical values were attributed to each of the toys, the elements were multiplied to determine an overall value for each toy. The toys with the highest value were deemed the best business choices for the next manufacturing and development cycle. This type of decision-making is known as:**

a. Monte-Carlo simulation.
b. Grid analysis.
c. ISO 31000.
d. Chunking.

9. **Value engineering (VE) is a technique to reduce cost while still achieving the desired end result, product, or service. A company has a formal policy to use VE in developing new products and provides VE training and incentives. One division's reported VE savings lag, and that division head supplements formal policies with his personal views on VE. What is the most likely explanation of the disparity in VE savings?**

a. Reported VE savings data in one division are unreliable.
b. The VE training programs need improvement.

c. Informal comments by the head of one division disparaged VE, increasing the risk that VE goals would not be reached.
d. Staff in one division has a cultural bias against the use of VE.

10. Unable to rely solely on its own factories, toy company PlayGo contracts with foreign-owned manufacturers. Despite its requirement that factories use materials provided by certified suppliers, a foreign manufacturer uses lead paint and PlayGo issues a recall. What are the two most effective strategies to limit PlayGo's reputational damage and reduce the likelihood of future product defects?

I. Participating in a highly publicized initiative by the Toy Industry Association and Consumer Product Safety Commission to introduce new regulations requiring more stringent safety checks.
II. Issuing a statement that the toys were made in factories in a foreign country, and that PlayGo had met its risk management responsibilities by issuing the requirement that contractors use material provided by certified suppliers.
III. Reducing the number of toys it makes through contract factories.
IV. Refining further its memoranda of understanding with contractors and partners to include stricter monitoring and tougher penalties for noncompliance.

a. I and II only.
b. II and III only.
c. I and III only.
d. I and IV only.

11. For a board, a member's independent status can be a disadvantage because his or her knowledge of staff operations and daily governance is limited to what is revealed at board meetings and other timely information. When thinking about documentation to the board, which of the following is false?

a. It contributes to openness and transparency.
b. It provides information that can support the decision-making, planning, and analysis of strategic initiatives.
c. It tilts the balance of power so that the board has more information than the CEO does about risk management.
d. It allows stakeholders to have timely and relevant information to make decisions.

12. A defense department assigned its highest priority to developing an advanced aircraft using materials not previously used and untested technologies. A firm fixed-price contract was awarded to a qualified vendor. Controls were in place at all levels, and progress reports—noting challenges—were sent to top officials. Top officials reported that progress was excellent, but the project failed due to enormous expenditures with no aircraft developed. Which risks were not adequately considered?

I. Because the requirements were not specific, the use of a firm fixed-price contract made the project risky.
II. The personnel at many levels sent false reports forward on cost incurred and progress made.
III. The contractor lacked adequate technical skills to deal with technology that was still evolving.
IV. Top procurement officials did not act on “red flags” due to a “can do” mentality on a high priority of the program.

a. I, II, III, and IV.
b. II and III only.
c. I and IV only.
d. I only.

13. A developed country runs a program to send volunteers overseas to assist less-developed countries in education, health, and community development. Statutory objectives include assisting country development and enhancing cross-cultural understanding. This program is popular but faces many risks.

Of the following four risks, which one would likely be the most challenging?

a. Health care for volunteers.
b. Inadequate in-country representation of the agency that manages the program.
c. Inadequate housing for volunteers.
d. Developing clear ways for measuring performance against the statutory objectives.

14. The internal environment of the enterprise risk management (ERM) framework and the control environment of the internal control framework provide positive contributions to the governance process and organizational performance. What is *not* one of the applications of the frameworks to achieve an organization's goals?

a. A board of directors is given authority to define the controls required to execute the strategy.
b. ERM is applied to strategy setting to identify and mitigate risks to strategy.
c. Internal control addresses the risks identified and provides assurances that strategy can be met.
d. One principle of both frameworks is the establishment of boundaries that delineate the roles and responsibilities of the board and management.

15. OWA, Inc. wants to determine the optimal scope and scheduling of its IT risk assessment. What is the most efficient sequence of pre-assessment planning activities?

I. Define the impact values of operational threat scenarios to OWA.
II. Determine the vulnerability of OWA's hardware and software to hacker exploits or internal abuse.
III. Identify the data that affect OWA's ability to be a safe and reliable source of water, and determine the criticality of the

confidentiality, integrity, and availability of each class of OWA data.

IV. Identify where and how critical data are stored, transmitted, and processed.

a. III, I, II, and IV.
b. I, III, IV, and II.
c. III, IV, II, and I.
d. II, IV, I, and III.

16. Objectives of the risk management process include all of the following except:

a. To link growth, risk, and return.
b. To act as a reasonable "brake" on strategic growth.
c. To look for ways to take advantage of opportunities.
d. To comply with laws and regulations.

17. The following are definitions of risk management terms:

I. The amount of risk an organization accepts.
II. The level of risk remaining after treatment.
III. Acceptable variance from appetite.
IV. Overall "picture" of risk across categories.

Match the above definitions to the terms below:

a. I. Appetite. II. Risk profile. III. Residual risk. IV. Inherent risk.
b. I. Appetite. II. Residual risk. III. Risk profile. IV. Risk tolerance.
c. I. Appetite. II. Residual risk. III. Risk tolerance. IV. Risk profile.
d. I. Risk profile. II. Risk tolerance. III. Residual risk. IV. Appetite.

18. A nonprofit microfinance organization wants to establish a for-profit subsidiary. Which of the following are the greatest organizational risks that must be assessed before the organization commits to the initiative?

I. Determining whether the organization has the appropriate governance structure to support the proposed expansion in its

activities.

II. Determining whether the nonprofit's existing skill set is transferrable and applicable to the activities of the proposed for-profit subsidiary.

III. Assessing whether the nonprofit's "Theory X" view of its workforce is appropriate for a for-profit operation.

IV. Assessing whether a for-profit subsidiary is consistent with the values (tone at the top) and strategic objectives of the nonprofit.

a. I and IV only.
b. II and III only.
c. I, III, and IV only.
d. II and IV only.

19. CCC has recently separated from its parent company. The CEO recently appointed herself as chair to the newly formed board of directors. The board will have the responsibility for oversight of strategy, so the CEO believes the role as chair will allow her to make decisions more quickly. She does not believe there has to be a formal documentation and decision-making process. Given this scenario, what are some of the likely key reasons that CCC's structure may *not* succeed?

I. As board chair, the CEO can make decisions quickly without the interference of a collaborative decision-making process.

II. Decision-making that is not integrated with risk analysis and a methodical process for providing information that is timely and relevant will not foster transparency to the key stakeholders.

III. Without documentation, a historical record for experience-based decision-making in the future will limit timely oversight and management accountability.

IV. The organization's governing body is not being provided with clear decision-making records and is not able to collaborate on strategic oversight.

a. I and IV.
b. II and III.

c. II, III, and IV.
d. I, II, and III.

20. After a country significantly increased the budget for its military services, the defense department accumulated "excess" spare parts valued at US $33 billion. Examples included a 14,000-year supply of one aircraft part and 126 sizes of women's shirts. Which one of the following risk management approaches would likely have had the best chance of avoiding the risk of the large wasteful expenditures?

a. Limiting the budgetary resources approved (and made available) for procuring spare parts, and rigorously monitoring related expenditures.
b. Reducing the number of spare part items managed by each item manager, thereby reducing their individual workloads.
c. Improved and updated methods of computing valid requirements for spare parts procurement.
d. More reliable and current information on existing spare parts for decision-makers.

21. PTP receives 95% of its project funding from donor BD. PTP draws down funds as needed through BD's letter of credit (LoC) and submits its rationale for the project drawdowns at the end of each quarter. The board of directors directs PTP to broaden its funding base, which PTP does using existing BD funds. An external audit discovers that PTP has used program funds to solicit new donors. As a result, BD terminates the LoC and PTP goes out of business. Which of PTP's deficiencies was the *least* critical threat facing PTP?

a. The policies and procedures for the use of the LoC, which allowed PTP to draw down funds as needed but not report until the end of the financial quarter.
b. No findings reported by the external auditor. Whether these accounting irregularities were the result of intentional fraud or honest mistakes, the external auditor should have been fluent in

BD's contractual requirements and flagged the misallocation of expenses.

c. Senior management and the board were so focused on the risk of PTP's reliance on BD funding that they failed to explore the risks associated with its efforts to find other funding. Consultation with program managers and contract specialists would have made the board aware that it could not fund its exploratory efforts using BD program funds.
d. Senior management and the board failed to ensure that the three lines of defense in risk management were operational.

22. A charitable organization that provides shelter to the homeless is defining its value drivers. Which one of these is *not* one of its primary activities in Porter's Value Chain model?

a. Operations—all the main activities that are needed to create the service or product, such as finding and providing shelter and food.
b. Client intake—the activities that are performed to identify the clients in need and bring them to the shelters.
c. Social work—including counseling the clients.
d. Grants administration—the writing and securing of grants to fund the charity.

23. A corporation staffs its foreign sites with its own country's employees (two to four years) and local employees (longer). Local employees who separate voluntarily are entitled to a lump-sum payment to be computed under a clear agreement between the local employees and the corporation. Yet, separating local employees are being paid 40% more than in the agreement. Rank the risks that likely led to overpayments.

I. The computation method is not well understood.
II. The employee who makes the computations is deliberately increasing the amount in exchange for kickbacks from local employees, or a personal belief that the local employees "deserve" more.

III. The supervisor(s) of the individual who computes and makes separation payments was not adequately reviewing the computations and payments.
IV. The comptroller is exhibiting an impoverished management style over local employees.

a. III, IV, II, and I.
b. I, II, III, and IV.
c. IV, III, II, and I.
d. II, IV, III, and I.

24. A biomedical company is marketing its new protocol to treat early stage cancer. Absent the new treatment, a patient's risk of the cancer recurring is 80%; with the treatment, the risk of recurrence drops to 2%. In risk management terms, the situation before treatment is called [fill in the blank} and the patient's prospects after treatment is [fill in the blank] :

a. Inherent risk and risk tolerance.
b. Inherent risk and residual risk.
c. Risk profile and risk tolerance.
d. Risk-aware and risk-managed.

25. Porter's Five Forces model is widely used to determine the degree of marketplace rivalry. Which of the following is *not* a factor in Porter's model?

a. The bargaining power of suppliers and their ability to dictate prices and keep customers locked into their offerings.
b. The threat of substitute products or services becoming available.
c. Government regulations or incentives that influence the ability to introduce a competing product or service into the market.
d. The bargaining power of customers and their ability to dictate prices or switch suppliers.

26. Recently a large nonprofit organization performed a risk

assessment to identify the top risks to achieving strategy. The risk assessment identified that the organization does not have a good grasp on what its core capabilities are, which may protect it from external funding competition. Core capabilities are best defined as:

a. An organization's unique range of products and services, resources, and processes.
b. A mechanism by which employees are trained and given roles they can best perform.
c. The translation of services and products into a cost that customers are willing to pay.
d. The physical assets and systems that can be transformed into value for the organization.

27. Literature and guidance recognize primary stakeholders and three lines of defense for operational and effective risk management as follows:

I. Internal auditors' assurance.
II. Operational management.
III. Senior management and governance body.
IV. Risk management and compliance functions.

Which is the correct hierarchy of the above four elements?

a. I, II, III, and IV.
b. III, II, IV, and I.
c. IV, III, II, and I.
d. IV, I, III, and II.

28. A software company, MIB, wants to increase sales of its products in a market segment. It conducts stakeholder analysis and categorizes potential customers according to their awareness of MIB's software and their ability to influence purchasing decisions. Which types of stakeholders should MIB target for its new marketing and sales campaign?

a. Apathetics.
b. Latents.
c. Supporters.
d. Promoters.

29. When a supplier does not deliver a product needed for the final manufacturing of a consumer good, the manufacturer is responsible for nonconformance to the delivery timeline. The mitigating activity should be on the exposure to what type of risk?

a. Emerging.
b. Financial.
c. Third party.
d. Inventory.

30. A firm operates under a "tall/hierarchical" organizational structure. The only employees with information security (InfoSec) technical expertise are in the IT department. The risk manager has completed a review with business units to update its InfoSec policy. What is the most effective approach for developing effective InfoSec procedures consistent with the firm's strategic vision?

a. Solicit input from each business unit regarding the resources required to implement the InfoSec risk management policy.
b. Emphasize the importance of information security in obtaining the strategic business and risk management goals of the company.
c. Task the information security department with writing enterprise-wide procedures because they are the technical experts.
d. Develop different sets of procedures that are consistent with overarching InfoSec policy yet tailored to the different needs and responsibilities of the various business units.

31. Below are characteristics of common ways to subdivide entities:

I. Finance, marketing, research, etc.
II. Product lines, geographic regions, customers, etc.
III. Cross-functional teams.
IV. Teams with various focuses.
V. Organizations joining together in common objectives.

Match these characteristics to the terms below:

a. I. Matrix. II. Functions. III. Networks. IV. Divisions. V. Teams.
b. I. Functions. II. Divisions. III. Matrix. IV. Teams. V. Networks.
c. I. Divisions. II. Functions. III. Matrix. IV. Teams. V. Networks.
d. I. Functions. II. Divisions. III. Networks. IV. Matrix. V. Teams.

32. In a government contract, the prime contractor who is awarded the contract assumes all the risks associated with delivery and performance of the government's requirements. Prime contractors carve out performance and delivery to third parties, known as subcontractors. What is the most effective activity to manage the risks in a subcontractor arrangement?

a. Create checklists that will make the subcontractor aware of its responsibilities.
b. Execute an agreement between the prime and subcontractor that flows down the terms and conditions of the government's requirements.
c. Require weekly reports and meetings between the prime and subcontractors.
d. Have the subcontractor manage the government's requirements and the prime contractor provide administrative and contract support.

33. Two partners rush to launch an Internet services firm using their own funds rather than waiting to secure investors. They assess risk by analyzing their business pipeline. There is no board of directors. The company wins many contracts but

requires ongoing partner capital. After 18 months, one partner, who expected to cash out within a year, refuses to invest further and the partners sell the company at a significant loss. Which of the following factors were the *two most significant* drivers of the startup's collapse?

I. The decision to launch the firm by self-funding; if the partners had waited until it secured investor financing, they would have had the cash flow to weather downturns in business and could have hired more staff to develop new business.
II. The partners' failure to establish and articulate their risk appetite and tolerance before launching the firm.
III. The lack of a board of directors.
IV. The firm's "produce or perish" management style as articulated by Blake and Mouton.

a. I and II.
b. II and III.
c. III and IV.
d. IV and I.

34. Recently Interlock, Inc. was informed by an outside consultant that 63% of its current workforce that conducts day-to-day functions of one of its operational areas is set to retire in the next three years. The consultant recommended workforce planning that identifies critical skills to meet future needs, defines skill gaps, and considers succession planning. However, Interlock, Inc. has not created a workforce plan to manage retirements or hire staff with needed skills. What are the necessary steps that Interlock, Inc. can take to address staffing risks?

I. Develop a succession plan that identifies workforce needs and addresses future program goals.
II. Wait to see where the largest gap will occur once the workforce begins to retire and then make decisions about where to align human capital and budget considerations.

III. Conduct a risk assessment to anticipate the areas where critical skills are needed most to address emerging risks.
IV. Develop strategies that address gaps in the number, skills, and competencies of staff.

a. I and II.
b. I, III, and IV.
c. I and III.
d. I, II, and III.

35. What is the difference between risk appetite and risk tolerance?

a. Only risk appetite can be expressed as the product of likelihood and impact.
b. Risk appetite is a higher-level statement expressing levels of risks that management deems acceptable, while risk tolerance sets the acceptable level of variation from particular objectives.
c. Risk appetite is tactical and operational, while risk tolerance is a broad statement of an acceptable enterprise wide portfolio of risk.
d. Risk tolerance is an acceptable variance from risk capacity.

36. To ensure compliance regulations on conflict minerals, an organization's risk management strategy for its supply chain should include which of the following?

a. A written code of conduct and business ethics policy.
b. Transparency in the manufacturing suppliers that extends all the way down the supply chain.
c. A memorandum of understanding that binds the supplier to the manufacturing distributor.
d. Manufacturing several sources of the mineral products.

37. In a period of great civil unrest about economic decline and perceived disparities, a national government established an *antipoverty* program with fixed amount grants to cities. Two

broad provisions of the national law received much attention: funds were "to improve the conditions under which residents live, learn, or work," and "maximum feasible participation of the areas and groups served" was required in implementation of activities. Using current concepts, which of the following are valid observations?

I. The program includes an unlimited risk appetite.
II. An expected risk would be difficulties choosing activities and agreeing on meaningful performance measures.
III. Due to the importance of the program, political risks are likely to be minimal.
IV. The antipoverty program's eventual success will be largely dependent on whether the external environment had been appropriately considered.

a. I, II, III, and IV.
b. I and II only.
c. III and IV only.
d. II and IV only.

38. In risk management, the acronym PESTEL refers to _____ and stands for _____:

a. An organization's risk culture: Pervasive, Enabled, Stakeholder-focused, Ethical, Linked to strategy.
b. An organization's capabilities or competitive environment: Processes, Employees, Systems, Technology, Entrepreneurship, Leadership.
c. A means to evaluate the external drivers and trends affecting an organization: Political, Economic, Social, Technological, Environmental, Legal.
d. An organization's legal and organizational structure: Private vs. public, Employee-owned, Subject to regulation, Taxable, Equity, Liability for losses.

39. A condominium association has 125 members and an elected

board. Two studies have concluded a major, costly renovation project is needed, and governing documents require a vote by owners. The vote outcome is in doubt due to the board's lack of enforcement of rules and alleged favoritism of board members. Which board action will likely be the most powerful catalyst to obtain owners' approvals?

a. Newsletters and door-to-door marketing campaign.
b. A preliminary survey(s), before moving ahead, to judge the likelihood of majority approval.
c. Distribution of all detailed specifications of renovation.
d. Issuance and distribution of a new or enhanced code of ethics and value statement for the board.

40. The IT department of a membership association has been asked to implement a pricing solution to assist in pricing the spices the member firms produce for sale for its food kits for overseas deployment. Multiple member firms have manufacturing and production plants for the spices, each with its own costing elements. The government is rejecting many of the member firms' proposals for spices because it cannot understand the rationale behind the pricing. The COO of the association believes that if a single pricing system is used by all the member firms, then the pricing will be more consistent and more understandable. The COO's decision is not based on a critical decision-making process. What are the outcomes that can be expected if a single pricing system is put in place without critical analysis?

a. The problem is identified; however, the intended goal is not the right one, and the final decision is not the right solution.
b. The problem is identified, the right information is collected, and the available options are analyzed.
c. The relevant factors are identified before the new pricing system is implemented.
d. The cost for implementing a single pricing system will be far

less than the cost of the lost opportunities in sales to the government.

41. The way that an organization structures itself can contribute to its culture of risk management. There are many different types of structures from which to choose. If a firm is reorganizing to better align its staff and strategic objectives, what would be one of the benefits of a hierarchical structure?

a. Culture that fosters innovation.
b. Shorter chains of command.
c. Clear demarcation of roles and responsibilities by teams and individuals.
d. Decentralized control.

42. Telegiant financed acquisitions using its own stock. When the telecomm market sank, management resorted to non-GAAP accounting methods to project profitability. Investigators later discovered that Telegiant's assets were inflated by billions of dollars. Telegiant filed for Chapter 11, the CEO was convicted of fraud, and investors also sued Telegiant's external auditor. The external auditor settled out of court. What were the two most significant risk factors that enabled the fraud?

I. Failures in governance, as documented in the "Report of Investigation" prepared for the Federal Bankruptcy Court that included a lack of effective checks and balances on the power of senior management.
II. Telegiant's overreliance on stock-based, rather than cash-based, financing of its acquisitions.
III. Insufficient federal regulations regarding the preparation, reporting, and retention of financial statements and records of publicly traded companies.
IV. Failures of scope and possibly integrity of external audits.

a. I and II.
b. II and III.

c. III and IV.
d. I and IV.

43. In making a decision on a major capital investment, the technique most likely to be used by a business would be:

a. The 80-20 rule.
b. Cause and effect.
c. Chunking.
d. Cost-benefit analysis.

44. When Solid Financial Group (SFG) reported financial and investment losses of US $30 million, the shareholders filed a suit claiming that SFG's board failed to provide oversight of its investments and financial decisions and breached its fiduciary duty of care. Which of the following facts may be relevant to claim that the board did not breach its fiduciary duty?

a. SFG's CEO was the board chair.
b. The external auditors failed to address obvious concerns like large risk derivatives that were not hedged.
c. The company's ethics and compliance programs were not assessing risks effectively.
d. After the losses, SFG replaced its board members with new directors who possessed expertise in finance and investments.

45. Motown Motors (MM) recently recalled 6 million cars due to faulty third-party ignition switches that were linked to 13 deaths. For more than a decade, MM decided against a very inexpensive switch upgrade and continued to use the vendor's ignition switches even though they did not meet MM's performance specifications. A growing number of lawsuits ensued and MM's stock sank due to heavy media attention, congressional inquiries, and a Department of Justice criminal investigation. The *most* significant risk management lesson to date from the MM recall is:

a. An organization that ignores or mistreats its external stakeholders does so at its own peril.
b. Reliance upon third-party vendors results in unacceptable levels of residual risk.
c. MM failed to develop an ethical organizational culture that guided its strategic planning and daily operations.
d. Cost-benefit analysis is an ineffective decision-making technique, as demonstrated in GM rejecting a 57-cent fix for the ignition switches.

SOLUTIONS

DOMAIN I—ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

Question 1
Source: ***CRMA Exam Study Guide*****, I.B.4**

Solution: a

a. Correct. Government programs are more complex and address a wider range of issues than a typical private sector entity.
b. Incorrect. Legislative bodies limit what governments can spend, making it less likely that risk appetites will be exceeded.
c. Incorrect. While the private sector must comply with many laws and regulations, government has even more.
d. Incorrect. Private firms generally have "boards" and "audit committees," whereas government entities have a range of governance bodies, e.g., central managers, legislatures, etc.

Question 2
Source: ***CRMA Exam Study Guide*****, I.B.4**

Solution: a

a. Correct. Cross integration and communication with departments reduces redundancy, advances effective assignment of tasks and resources, and creates efficiencies in achieving the organization's strategic goals.
b. Incorrect. The CEO created the risk officer position to help reduce the risks to achievement of mission goals.

c. Incorrect. While this may be true, the risk officer did not assess the structure's ability to mitigate risk factors of the external environment.
d. Incorrect. Not enough information to make this determination.

Question 3
Source: *CRMA Exam Study Guide*, I.B.8

Solution: a (I and II only)

I. Correct. Stakeholder analyses should consider whose interests risk management would affect negatively or positively. One party's efficiency gain might be another's cut income.
II. Correct. In the "agency view" of organizations, mechanisms of corporate governance should include a system of controls that are intended to align the incentives of managers with those of shareholders.
III. Incorrect. Representing a stakeholder in the development of risk management processes is a good way to surmount stakeholder conflicts, but it does not explain them.
IV. Incorrect. Whether the organization is in the public or private sector, there are still inherent differences among internal stakeholders.

Question 4
Source: *CRMA Exam Study Guide*, I.B.4

Solution: d

a. Incorrect. Creating cross-functional teams can enhance enterprise-wide communications among managers and departments, but teams are not required to assign tasks to subordinates.
b. Incorrect. Succession planning is a risk management activity to ensure gaps in roles and responsibilities.
c. Incorrect. Requiring work breaks is not a process to assign tasks to team members.
d. Correct. Delegating authority is one process by which an

organization can increase its flexibility in assigning tasks and increasing opportunities for subordinates as part of succession planning. However, there is a risk of failure or delayed timelines if the task is passed on to someone who does not know how to complete it.

Question 5
Source: *CRMA Exam Study Guide*, Domain I; GAIT for Business and IT Risk (GAIT-R)

Solution: c

a. Incorrect. Having the correct expertise is important, but one must first determine which systems require assessment before determining the expertise necessary.
b. Incorrect. Reviews of InfoSec policies and procedures are part of the assessment but not the planning stage.
c. Correct. The first principal of GAIT-R states the failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business. GAIT advocates a top-down assessment of business risks, risk tolerance, and the controls required to manage or mitigate business risk.
d. Incorrect. Key manual and automated controls "should be identified as a result of a top-down assessment of business risks, risk tolerance and the controls … required to … mitigate risk." Identifying and assessing the key controls are steps 2 and 3 in GAIT-R (GAIT-R Executive Summary).

Question 6
Source: *CRMA Study Guide*, I.B.8 and I.B.9

Solution: d

a. Incorrect. While these issues should be addressed, the impact is not as significant as other issues.
b. Incorrect. Appropriate, fair personnel practices are required by law and regulation but are not likely to have a big impact on the board's reputation.

c. Incorrect. This issue is significant but would not necessarily have an adverse impact on the board's reputation.
d. Correct. Soliciting funds from affected parties who might appear before the board could easily be (or at least appear to be) a conflict of interest. The chief judge was forced to resign.

Question 7
Source: *CRMA Exam Study Guide*, I.B.1

Solution: c

a. Incorrect. Physical counts are hard controls.
b. Incorrect. Policies are often soft and may be difficult to assess, but some policies (e.g., travel, attendance) can be seen as hard, and thus not challenging to assess.
c. Correct. Due to subjectivity and lack of clear evidence in some cases, openness is more soft and challenging to assess than the other options.
d. Incorrect. Shared values are a soft control.

Question 8
Source: *CRMA Exam Study Guide*, I.B.5

Solution: b

a. Incorrect. Monte Carlo simulation is a mathematical process to simulate risks through the use of algorithms and random sampling. The decision-making process used by the toy company did not do this.
b. Correct. Grid analysis is an effective decision-making process that helps analyze the available options and weigh risks that can influence governance.
c. Incorrect. ISO 31000 is a set of standards to help organizations manage risks.
d. Incorrect. Chunking is a decision-making process that breaks down a problem into "chunks."

Question 9

Source: *CRMA Exam Study Guide*, I.B.2 and I.B.3

Solution: c

a. Incorrect. There is no basis for this conclusion.
b. Incorrect. There is no indication that training is inadequate.
c. Correct. The informal comments of the division head could have been negative about VE.
d. Incorrect. There was no particular reason to suggest that one division had an anti-VE culture.

Question 10
Source: *CRMA Exam Study Guide*, I.C.1 and I.C.2

Solution: d (I and IV only)

I. Correct. This collaborative initiative can improve assurance of product safety throughout the supply chain.
II. Incorrect. "The engagement of a third party to undertake some activity does not absolve the organization of responsibility for risk." This statement is not the strongest public relations approach because it sounds as if PlayGo is denying responsibility for and not being proactive in redressing the problem.
III. Incorrect. While there may be a higher probability of unacceptable risk when dealing with organizations operating in different regulatory and cultural environments, the company determined it cannot rely solely on its own factories. Playgo is better served by reducing residual risk through stronger enforcement of penalties for third-party contractual noncompliance and participating in an industrywide effort to strengthen safety monitoring.
IV. Correct. As long as Playgo continues to determine that the benefits of lower cost offshore manufacturing capacity exceed the risks, enforcing stronger penalties and leveraging better industry monitoring will be sound elements of its residual risk equation. Playgo should, however, use this incident and findings from enhanced monitoring to consider whether it should

outsource to different foreign manufacturers.

Question 11
Source: *CRMA Exam Study Guide*, I.B.5

Solution: c

a. Incorrect. Documentation is an appropriate governance tool to ensure openness and transparency.
b. Incorrect. When independent board members are selected, they need to have access to information that will enable them to govern effectively and make knowledgeable decisions.
c. Correct. For a board to be effective when it has limited day-to-day interaction with management and staff, its independent members must be given enough information to allow them to make decisions. Balance of power refers to a situation where there is appropriate oversight and the CEO is not also the board chair.
d. Incorrect. Timely and relevant information allows for effective decision-making.

Question 12
Source: *CRMA Exam Study Guide*, I.B.1, I.B.2, and I.B.3

Solution: c (I and IV only)

I. Correct. For weapons development that will employ embryonic technology, cost-based contracts are preferable to firm fixed price.
II. Incorrect. There is no basis presented to suggest that risk 2 was present.
III. Incorrect. There is no basis presented to suggest that risk 3 was present.
IV. Correct. Given the extensive monitoring and reporting, senior procurement managers were not responding appropriately to "red flags."

Question 13

Source: ***CRMA Exam Study Guide*****, I.A.2**

Solution: d

a. Incorrect. While this is a real risk, the program can, and did, assign medical staff to the foreign countries.
b. Incorrect. Justifying budget resources can present a challenge, but that problem is not unique to this government program.
c. Incorrect. Finding adequate housing is a problem, but onsite pre-approvals and monitoring are available options.
d. Correct. The broadness of the objectives, and the frequent difficulty of gathering sufficient, reliable, relevant information, makes it hard to assess achievement of objectives.

Question 14
Source: ***CRMA Exam Study Guide*****, I.B.**

Solution: a

a. Correct. The board of directors does not define the controls. The board demonstrates independence from management and exercises oversight of the development and performance of internal control.
b. Incorrect. When strategic planning is integrated with ERM and includes internal control, it deals with alternative risk responses to achieve value as part of the governance process.
c. Incorrect. Risk reduction is a goal of internal control, which assures management and the board that the organizational goals are being met.
d. Incorrect. The internal environment component of the ERM framework and the control environment principle of the internal control framework both articulate the importance of boundaries between board and management in the context of managing risks.

Question 15
Source: GAIT-R

Solution: b (I, III, IV, and II)

I. Incorrect. Action III translates the results of action I into the data that must be protected to maintain OWA's financial sustainability and operational security.

II. Correct. The first step is to identify and rank the severity of threats to OWA's ability to continue to serve as part of the nation's critical infrastructure.

III. Incorrect. Again, one needs to understand all existential threats to OWA first, map those threats to the data that must be protected, identify where those data reside, are acted upon, and travel, and, finally, identify and remediate relevant hardware and software vulnerabilities.

IV. Incorrect. Action II is the last step after identifying existential risks, the type of data that must be protected for OWA to remain viable and secure, and the systems that store, process, and transmit these data.

Question 16
Source: *CRMA Exam Study Guide*, I.A.1

Solution: b

a. Incorrect. This is an accepted objective of risk management processes.

b. Correct. This is a common misconception concerning objectives of risk management processes.

c. Incorrect. Again, this is an accepted objective of these processes.

d. Incorrect. Again, this is an accepted objective of these processes.

Question 17
Source: *CRMA Exam Study Guide*, I.B.1

Solution: c

a. Incorrect. See definitions in the *CRMA Exam Study Guide*.

b. Incorrect. See definitions in the *CRMA Exam Study Guide*.

c. Correct. Aligns with risk management literature.
d. Incorrect. See definitions in the *CRMA Exam Study Guide*.

Question 18
Source: *CRMA Exam Study Guide*, I.B.1, I.B.3, and I.B.6

Solution: a (I and IV only)

I. Correct. Determining that sufficient governance exists is essential before the organization can launch a successful for-profit undertaking.
II. Incorrect. Ultimately, the for-profit employee skill set must be aligned with the demands of the new subsidiary, but a strong management team and governance structure will identify and fill skill gaps through training or new hires. Alternatively, management can forego the undertaking if it cannot meet the skill requirements of the for-profit subsidiary by training existing staff or hiring new employees.
III. Incorrect. A Theory X approach translates into a work environment that mitigates risk and maximizes performance using a set of hard controls, but is not inherently consistent or inconsistent with establishing a new for-profit.
IV. Correct. The nonprofit must ensure that establishing the for-profit subsidiary is not out of the scope of its organizational mission and that it will not alienate the nonprofit's core donor base.

Question 19
Source: *CRMA Exam Study Guide*, I.B.5

Solution: c (II, III, and IV)

I. Incorrect. Balance of power does *not* exist when the CEO is also the board chair, which is an ineffective organizational structure.
II. Correct. A reason that the organization's structure may not succeed is that the CEO is not using a methodical process for decision-making. Transparent decision-making with timely and relevant information is needed to ensure risk oversight by the

board.

III. Correct. Without documentation that provides a historical record, future decisions could take longer to make and it will be difficult to hold anyone accountable for risks as a result of bad decisions.

IV. Correct. The board is left in the dark and cannot provide strategic oversight that can lead to a better decision.

Question 20
Source: *CRMA Exam Study Guide*, I.B.2, I.B.5, and I.B.6

Solution: a

a. Correct. If the agency has more budgetary resources than needed, it would likely use resources wastefully for fear of having next year's budget decreased.

b. Incorrect. This action may help to make better procurement decisions, but not as directly as A.

c. Incorrect. Again, this action may mitigate procuring unneeded parts over time, but option A is more direct.

d. Incorrect. This action may also mitigate unneeded procurements, but the decision-makers may not use the available information.

Question 21
Source: *CRMA Exam Study Guide*, I.B.2 and I.B.5

Solution: a

a. Correct. Even though the ability to access funds as needed and report later is akin to "shutting the barn door after the horse got out," had the three lines of defense and external audit functioned appropriately, PTP would not have been able to misuse the LoC.

b. Incorrect. A thorough examination and report by the external auditors would have been especially important given the lack of internal audit and PTP's requirements to report to big donor.

c. Incorrect. Consultation with program directors (the first line of

defense) would have made the board and executive team aware that it could not fund its exploratory efforts using BD program funds. Operational management, as the "owners" of the contracts, should have known, for example, that while certain program development costs such as proposal preparation were allowable overhead, other development activities such as fund-raising, direct mail, and travel to non-program sites were not allowable uses of BD program funds.

d. Incorrect. PTP's lack of a three lines of defense risk management structure proved to be a critical contributor to its failure.

Question 22
Source: *CRMA Exam Study Guide*, I.B.6

Solution: d

a. Incorrect. Primary activity that has a direct bearing on adding value; operations requires skills and resources to deliver its products and services.
b. Incorrect. Primary activity that has a direct bearing on adding value; client intake requires skills in assessing and selecting the right clients.
c. Incorrect. Primary activity that has a direct bearing on adding value; social work requires qualified training and special skills.
d. Correct. Grants administration is a support activity that facilitates the primary activities that serve the clients directly.

Question 23
Source: *CRMA Exam Study Guide*, I.B.1 and I.B.2

Solution: a (III, IV, II, and I)

a. Correct. The computation method is likely well understood, so the other three (II, III, IV) are ranked higher.
b. Incorrect. Again, the computation is likely well understood, so this is not the most likely sequence.
c. Incorrect. Risk IV implies that the comptroller has an overall

impoverished style; not only one weakness is identified—but likely a pervasive style that had a negative effect on all supervisors' attitude on control.

d. Incorrect. Considering risk II first tends to point a finger prematurely at the individual who does the computations.

Question 24
Source: *CRMA Exam Study Guide*, I.A.3

Solution: b

a. Incorrect. "Inherent risk" is correct as it is the level of risk in the absence of any response, but "risk tolerance" is incorrect in this scenario because it is the "acceptable variance from risk appetite."
b. Correct. This is the proper usage of both "inherent risk" and "residual risk," which is "the level of risk remaining after a risk treatment."
c. Incorrect. "Risk profile" is the overall picture of risk across a range of categories. "Risk tolerance" is also applied incorrectly as stated above.
d. Incorrect. These terms refer to levels of organizational risk maturity.

Question 25
Source: *CRMA Exam Study Guide*, I.C.1

Solution: c

a. Incorrect. The power of suppliers is a key factor in the Five Forces model.
b. Incorrect. The threat of substitute products or services entering the market is a key factor in the Five Forces model.
c. Correct. While organizations should address the needs and expectations of the government and regulators, these are not explicit factors in Porter's rivalry model.
d. Incorrect. The power of customers is a key force in Porter's model.

Question 26
Source: *CRMA Exam Study Guide*, I.B.6

Solution: a

a. Correct. Core capabilities arise from the organization's unique range of products and services; its resources, including time, people, systems, and capital; and its processes.
b. Incorrect. When employees are in roles where they have the skills to perform, this is the core capability of the employees.
c. Incorrect. An organization will deliver products and services at a cost perceived to be their value, and value is driven by core capabilities. Cost is not driven by value alone.
d. Incorrect. Physical assets and systems are only two of the capabilities that add value to an organization. Others include capital, time, processes, and people.

Question 27
Source: *CRMA Exam Study Guide*, I.B.2

Solution: b (III, II, IV, and I)

a. Incorrect.
b. Correct. This is the only option that is consistent with IIA guidance.
c. Incorrect.
d. Incorrect.

Question 28
Source: *CRMA Exam Study Guide*, I.C.2

Solution: b

a. Incorrect. While MIB could increase apathetics' awareness of their offerings, apathetics are least likely to be interested in MIB software and have little power to affect change.
b. Correct. Latents, while they may presently have no particular interest or awareness of their products, have the power to influence it greatly if they become interested. MIB's objective

should be to make latents understand that its products will make their company, and thus their careers, more successful.

c. Incorrect. Supporters already have a positive view of the product but can do little to compel their organization to buy the product.

d. Incorrect. Promoters are already keen advocates of their products and they have done what they can to make sure their company buys MIB's products. While MIB cannot take its clients for granted and must continue to "win" their business, the primary objective of MIB's new marketing and sales campaign should be to increase awareness and convert folks on the sidelines to becoming active clients. Focusing on promoters would be like "preaching to the choir."

Question 29
Source: *CRMA Exam Study Guide*, I.B.7

Solution: c

a. Incorrect. Mitigating emerging risk is the focus of strategic risk management.

b. Incorrect. Financial risk will be an effect of the negative event that could result in loss of revenue, but it is not the primary risk to mitigate in the supply chain relationship.

c. Correct. Third-party relationships require risk management processes to control a supplier's activity or otherwise mitigate by having secondary suppliers in the event a product is not delivered.

d. Incorrect. Inventory levels will be affected if supplier relationships are not managed first.

Question 30
Source: *CRMA Exam Study Guide*, I.B.4

Solution: d

a. Incorrect. Identifying resources necessary to implement InfoSec's risk management policy should be part of the firm's

strategic planning and budget processes, but the business units are not always capable of translating InfoSec policies into technical procedures.

b. Incorrect. Articulating the importance of InfoSec to achieve business objectives is a key element of policy, not procedure. It is true, however, that procedures must be in alignment with policy, and employees' full understanding of policy can promote compliance with resulting procedures.

c. Incorrect. The company's technical expertise will be most germane for its own operations, i.e., the testing, monitoring, and remediation of systems and application vulnerabilities. However, the operating units will need procedures focused primarily upon access control, password management, working remotely, and use of wireless and personal technology devices. These types of procedures would be best defined by the risk management department because it has a more holistic view of primary stakeholders' and operational managers' needs to balance security with availability and continuity of operations.

d. Correct. This is the most effective approach, especially given the "tall/hierarchical" organizational structure, which is marked by high vertical differentiation and high degrees of vertical specialization as well as a clear demarcation of roles and responsibilities by teams. This approach does not burden operating units with procedures that are not germane to their operations and thus relevant procedures are more likely to be remembered and used consistently.

Question 31
Source: *CRMA Exam Study Guide*, I.B.4

Solution: b

a. Incorrect. Characteristics and terms are not aligned.

b. Correct. Characteristics and terms are aligned.

c. Incorrect. Characteristics and terms are not aligned.

d. Incorrect. Characteristics and terms are not aligned.

Question 32
Source: *CRMA Exam Study Guide*, I.B.7

Solution: b

a. Incorrect. Checklists are a quality control process.
b. Correct. A formal agreement confirms responsibilities, deliverables, timelines, authority, and controls, thus sharing the risks with the third party.
c. Incorrect. Effective communication is critical in a third-party relationship, but it is not the best way to manage the risks.
d. Incorrect. The prime contractor is liable for all risks associated with the contract and should manage the requirements with direct involvement.

Question 33
Source: *CRMA Exam Study Guide*, I.B.3

Solution: b (II and III)

I. Incorrect. While the probability of success may have been improved with the advantages of investor capital and expertise, a self-funded firm could have flourished. The partners should have assessed their appetite for future financial injections into the firm and should have adopted a continuous risk management approach throughout the life of the business.
II. Correct. Defining risk appetite is a formal starting point for risk management, which the firm never developed. Risks are about the future and not about the present; relying solely on business pipeline analysis does not provide a comprehensive analysis of internal and external threats to a firm's competitive positioning.
III. Correct. A board of directors could have contributed much-needed connections as well as insight into the ways to finance and operate the company so that the partners could meet their goal of selling the company quickly.
IV. Incorrect. We do not know the culture and the effect it had on employees. While the firm's culture could have become produce or perish because of failures stated in II and III, the culture

would have been the product, not the driver, of risk management failures.

Question 34
Source: *CRMA Exam Study Guide*, I.B.6

Solution: b (I, III, and IV)

I. Correct. Development of a succession plan that is predicated on the actions in III and IV is a crucial element of risk management.
II. Incorrect. Interlock will not be proactive in addressing workforce risks if it takes a "wait and see" approach.
III. Correct. Conducting a risk assessment will help Interlock develop mitigation strategies to address workforce gaps.
IV. Correct. Developing strategies that address these gaps is critical for workforce risk management.

Question 35
Source: *CRMA Exam Study Guide*, I.A.3

Solution: b

a. Incorrect.
b. Correct. For example, a company that says that it does not accept risks that could result in a significant loss of its revenue base is expressing appetite. When the same company says that it does not wish to accept risks that would cause revenue from a particular product or sales channel to decline by more than 10%, it is expressing tolerance.
c. Incorrect. The definitions are reversed. Risk tolerance is tactical and operational.
d. Incorrect. Risk tolerance is an acceptable variance from risk appetite.

Question 36
Source: *CRMA Exam Study Guide, Domain* I.B.5

Solution: b

a. Incorrect. A written code of conduct and ethics statement will

not guarantee compliance nor ensure integrity in third-party activities.

b. Correct. A framework for compliance that includes transparency through the supply chain will better enable companies to identify risks with all the suppliers in the mineral sourcing chain and identify whether products contain conflict minerals.

c. Incorrect. A memorandum of understanding will not guarantee that companies will comply with the regulations. A broad risk management framework is needed that includes a memorandum of understanding or other contractual agreements to identify how compliance will be monitored.

d. Incorrect. While manufacturing several of the components needed in a product's supply chain can lead to efficiencies and cost savings, it will not alone manage the compliance risks with mineral suppliers.

Question 37
Source: *CRMA Exam Study Guide*, I.B.1-2

Solution: d (II and IV only)

I. Incorrect. Grants are limited to specific amounts approved.

II. Correct. Determining the appropriate activities and programs to fund and agreeing on meaningful performance measures are critical success factors for the initiative.

III. Incorrect. When citizens are given more power, there will likely be more political conflict.

IV. Correct. If the environment is misunderstood, the success of the antipoverty program will be in jeopardy.

Question 38
Source: *CRMA Exam Study Guide, Domain* I.B.5

Solution: c

a. Incorrect. Although risk culture is defined as "the prevailing attitude and approach to risk," these would be desirable elements of risk culture.

b. Incorrect.
c. Correct.
d. Incorrect.

Question 39
Source: *CRMA Exam Study Guide*, I.B.3

Solution: d

a. Incorrect. The risk to a vote of approval is more about trust of the board than advocacy of this project.
b. Incorrect. This tactic could "backfire" as owners may feel "pressured."
c. Incorrect. Details of the corrective action are not as important as getting community agreement on the legitimacy of the need.
d. Correct. Overcoming the past history, and thus getting members to trust the board, is critical.

Question 40
Source: *CRMA Exam Study Guide*, I.B.6

Solution: a

a. Correct. While the problem of inconsistent and understandable pricing was identified, the best goal may not be to have uniform pricing, but it could be any other goal such as lean manufacturing, supply chain management, or consolidating production to regional plants, any of which could help streamline pricing and bring more transparency.
b. Incorrect. The COO's decision did not bear any additional options for the IT department to analyze.
c. Incorrect. The decision did not include any analysis of relevant factors to understand the root cause of the problem and find the optimum solution.
d. Incorrect. There was no cost-benefit analysis performed and this conclusion cannot be made.

Question 41

Source: *CRMA Exam Study Guide*, I.B.4

Solution: c

a. Incorrect. Hierarchical structures tend to have a risk of lower innovative cultures.
b. Incorrect. Shorter chain of command is a benefit of a flat organizational structure.
c. Correct. Organizations wishing to create structures with high degrees of specialization and easily understood roles and responsibilities tend to implement hierarchical teams and chains of command.
d. Incorrect. Hierarchical organizational structures tend to have centralized control and management lines.

Question 42
Source: *CRMA Exam Study Guide*, I.B.3, I.B.5, I.B.8, I.B.9, I.C.1

Solution: d (I and IV)

I. Correct. In fact, such failures in governance are fertile ground for fraud.
II. Incorrect. If Telegiant operated with adequate governance and thorough external auditing, the risks associated with stock-based financing could have been mitigated or detected earlier.
III. Incorrect. Similar scandals in the past resulted in comprehensive regulations on the preparation, reporting, and retention of financial statements and records of publicly traded companies.
IV. Correct. The external auditor should have been more diligent, especially given the deteriorating strength of the telecommunications sector and Telegiant's reliance upon stock-based acquisitions. The auditor's settlement was widely viewed as an admission that the evidence against the auditor was very damaging.

Question 43
Source: *CRMA Exam Study Guide*, I.B.5

Solution: d

a. Incorrect. The 80-20 technique points the focus away from the "trivial many" to the "vital few."
b. Incorrect. Cause and effect diagrams possible causes and assesses relationships, looking for the cause of known problem.
c. Incorrect. Chunking is related to a "series of decisions," as opposed to a single decision.
d. Correct. Cost-benefit analysis is common in choosing among several high-cost and complex alternatives.

Question 44
Source: *CRMA Exam Study Guide*, I.B.5

Solution: d

a. Incorrect. When the CEO is the board chair, it can be an ineffective organizational structure, but it does not indicate that the board breached a duty of care for fiduciary responsibility.
b. Incorrect. The board is not held accountable for not questioning the procedures of the external auditors.
c. Incorrect. The court did not believe it should second-guess a director who says he or she believed the compliance and ethics programs were adequate.
d. Correct. The previous board was not made up of experts in investments or finances. Thus, the court's opinion was that the board did not act with actual or constructive knowledge that its inaction would harm the corporation.

Question 45
Source: *CRMA Exam Study Guide*, I.A.2 (esp. IRM, 2012), I.B.1, I.B.5 (Table 1.3), I.B.7, I.C.2

Solution: a

a. Correct. MM cannot escape the effects of private lawsuits, congressional and Department of Justice inquiries, and extensive media coverage on its reputation and financial health.
b. Incorrect. While third-party vendors can introduce elements of

inherent risk, the residual risk can be reduced so that it falls within an organization's risk appetite. MM ignored even the most basic elements of risk management by accepting parts that did not even meet its own standards.

c. Incorrect. While an ethical culture is of paramount importance to risk management, until internal and external investigations prove otherwise, it is premature to conclude that a failure of culture caused MM's problems.

d. Incorrect. Cost-benefit analysis is just a decision-making tool. How MM chose to use the cost-benefit results could be evidence of a flawed ERM culture and strategy.

QUESTIONS

DOMAIN II—PRINCIPLES OF RISK MANAGEMENT PROCESSES

1. A ministry of health wants to assess its ability to respond to an outbreak of cholera. The ministry assesses the inherent risks associated with cholera and with different scenarios under which an epidemic might unfold, such as an earthquake or a severe weather event. Which risk criteria best describe the ministry's expanded "terms of reference against which the significance of risk is evaluated?"

I. Volatility.
II. Correlation.
III. Velocity.
IV. Interdependency.

a. I and IV.
b. II and IV.
c. II and III.
d. III and IV.

2. HAL, a leading software and hardware vendor in the private sector, is weighing the pros and cons of expanding into the public sector. Which are the most appropriate terms to describe the risks that HAL is evaluating?

I. Speculative risk.
II. Market risk.

III. Enterprise risk.
IV. Technology risk.

a. I and II.
b. I and III.
c. II and IV.
d. III and IV.

3. The state assembly decrees that the state's Pension Investment Division (PID) must divest of all holdings related to a certain country. Soon after, the financial markets soar on unexpected predictions of a dramatic economic recovery. In response, PID sells large positions of its portfolio at a premium and covers its losses from the mandated divestiture. According to the bowtie diagram analysis methodology, what two terms best describe the risk factors leading to the sale?

I. Consequence.
II. Trigger event.
III. Risk event.
IV. Intermediate event.

a. II and IV.
b. I and III.
c. I and II.
d. III and IV.

4. An advertising agency that has experienced steady growth for a decade gathers its staff together for a control risk self-assessment (CRSA) and identifies the following top concerns:

I. Heavy reliance "legacy" on former clients rather than cultivating new clients.
II. High staff turnover. Only the CEO and the award-winning creative director have been with the firm since inception.
III. Effects of the economy on each business sector they serve.
IV. The firm's new focus on a global, rather than a regional, market.

Which of the above risks represents a potential single point of failure?

a. Risk I.
b. Risk II.
c. Risk III.
d. Risk IV.

5. **Two real-estate investment partners are assessing the relative risks of a prime property in Los Angeles, California, and a comparable property in a similarly vibrant area of Brooklyn, New York. One partner discounts heavily the value of the Los Angeles property because of the potential for earthquake damage. The Los Angeles-averse partner is most likely influenced by which element of risk management analysis?**

a. Risk psychology.
b. Risk prioritization.
c. Risk severity.
d. Risk response.

6. **Which of the following is *not* a benefit of risk mapping and prioritization?**

a. The results help an enterprise to communicate better its risk aggregated risk profile to key external stakeholders.
b. Ranking risks by their level of severity helps an organization determine the optimal allocation of resources devoted to risk response or treatment.
c. Risk maps are key graphical representations of the variance in risk appetites across different divisions within an organization.
d. Helping the enterprise identify how certain risks can offset other risks to ensure that the enterprise maintains an overall risk profile that remains within risk capacity.

7. **A city comptroller was the sole signatory on the city's accounts. Over two decades she embezzled $30 million from the**

municipality by shifting public funds through multiple city bank accounts before hiding them in a secret account. Despite regular external audits, her fraud went undetected until a colleague discovered the secret bank account. What are the *most likely* reasons that this fraud was perpetuated over such a long time?

I. Incomplete understanding of the risk conditions leading to a faulty risk response mechanism.
II. The cost of treating the risk to keep the level within appetite outweighed the benefits gained from treating the risk.
III. Inadequate directive controls.
IV. Inadequate preventative controls.

a. II, III, and IV.
b. I and III only.
c. I and IV only.
d. I, II, and III.

8. **Community Hospital Systems (CHS) set a goal that all patients be seen within 30 days of their requests. Employees who met the scheduling goal were rewarded with bonuses. Unbeknownst to senior executives, schedulers were entering fraudulent data into the scheduling system to disguise the much longer actual wait time. Significant numbers of patients experienced deteriorating health, and several died before seeing a medical professional. Which of the following were the primary drivers behind the fraudulent reporting?**

I. A bureaucracy that had been taught over time to hide its problems from senior management.
II. Incomplete or inappropriate reliance on performance metrics.
III. Reducing treatment wait time was an inappropriate operating objective. Therefore, CHS did not deploy its resources effectively to achieve its strategic objectives.
IV. Lack of alignment between its organizational objectives and risk management processes.

a. I and II only.
b. II and III only.
c. III and IV only.
d. II and IV only.

9. A summer camp is known for its expertise in wilderness training and adventures. The camp carries $50 million of liability insurance, and parents of campers must sign liability waivers. All counselors are certified in wilderness first aid and activity instruction and are required to undergo periodic refresher training. All campers receive training and must meet stringent skill and safety requirements before embarking on a wilderness trip. Which two response options best summarize the camp's risk response strategy?

I. Avoid.
II. Transfer.
III. Mitigate.
IV. Tolerate.

a. II and III.
b. I and II.
c. II and IV.
d. III and IV.

10. The term *risk escalation* refers to:

a. Risks that have materialized as events.
b. Weaknesses in the internal control system that raise residual risks beyond the limits of the risk appetite.
c. The increase in an enterprise's risk profile resulting from previously unknown risks arising from changes in the internal or external environments or changes to the organization's objectives and activities.
d. The process of and procedures for reporting risk incidents up the chain of command.

11. Put the following risk identification activities in the proper sequence:

I. Develop initial risk register.
II. Conduct Control Risk Self-Assessment (CRSA).
III. Calculate risk severity.
IV. Define the risk universe.

a. I, II, III, and IV.
b. II, IV, I, and III.
c. II, III, IV, and I.
d. III, IV, II, and I.

12. An information broker, InfoMart, suffered an information security breach that exposed hundreds of thousands of customers' sensitive personal information. The breach was a result of fraud perpetrated by criminals pretending to be legitimate customers. In addition to heavy fines and redress costs, the company is now on probation subject to 20 years of external auditing by the Federal Trade Commission. What would be the *most important* improvement that InfoMart should make to avoid future breaches?

a. Implement better IT general controls and IT application controls, with special emphasis on automating controls that force employees to adhere to policies affecting change management and access rights as well as authentication and authorization of system users.
b. Make the chief information security officer (CISO) responsible for monitoring vulnerabilities in business processes and IT.
c. Strengthen business processes for vetting customers and their activities and create offices of customer credentialing, compliance, and privacy that would report directly to the board of directors' privacy committee.
d. Eliminate products that contain personal data regarding an individual's financial assets, criminal and employment histories, and known associates/family members.

13. Risk severity is often calculated as a function of likelihood, categorized as "unlikely," "possible," or "likely," and impact, categorized as "catastrophic," "disruptive," or "problematic." Using the InfoMart case above and the study guide's definitions of likelihood and impact categories, one would most likely assign a likelihood of _____ and an impact of _____ to a future InfoMart data breach:

a. Unlikely, disruptive.
b. Unlikely, catastrophic.
c. Likely, problematic.
d. Possible, disruptive.

14. What is the greatest challenge that is unique to conducting and interpreting risk prioritization exercises?

a. Likelihood and impact are not the only risk criteria that the organization needs to consider.
b. The assumption that different risk criteria (such as likelihood and impact) carry equal weight in the analysis.
c. Attaching numbers to measures of risk requires a degree of subjectivity and judgment.
d. Risk analysis, evaluation, and prioritization are processes that require regular updates.

15. According to COSO guidance, the term *sweet spot* refers to:

a. Identifying and investing the optimal amount of money devoted to risk management.
b. The point at which the aggregate risk exposure of different divisions in an enterprise are balanced in accordance with overall risk appetite.
c. An enterprise achieving a state in which overall risk profile is equal to its total risk capacity.
d. The point at which an organization's risk-taking results in the highest net gain in value.

16. Review or audit of risk management processes has three primary goals. Which of the following is *not* one of the three goals?

a. To identify and repair weaknesses and faults.
b. To avoid impugning the reputation of top management.
c. To identify changes in the organization's objectives and environment and ensure alignment.
d. To determine that the organization is achieving its goals (because risk management is working).

17. A corporation uses a risk management plan form that includes a section on methodology with the following steps:

I. Control risks.
II. Monitor risks.
III. Risk response tracking.
IV. Risk response planning.
V. Prioritize risks.
VI. Risk identification.
VII. Categorize risks.
VIII. Risk impact assessment.

Which is the logical sequence of the above steps?

a. I, II, III, VIII, IV, VII, VI, V.
b. VI, VII, VIII, V, IV, III, II, I.
c. VIII, VII, VI, V, IV, III, II, I.
d. VI, VII, IV, III, II, VIII, V.

18. In a school cafeteria, an employee was accused of stealing $500 a day in cash by operating a *cash only* line for a la carte items, without a cash register. The employee was charged with stealing more than $1 million over 20 years. Effective monitoring should have identified the following as red flags *except:*

a. Large amounts of an asset (cash) with inherent risk.
b. Absence of a cash register in the a la carte line.
c. Lack of monitoring of ratio of inventory consumption for the a la carte line to the ratio for four cash receipts lines.
d. Lack of an annual ethics briefing for all employees.

19. Some literature and guidance advocates assessing the context as an early step in the risk management process. In using the term *context*, what are important considerations?

a. Mapping the social scope of risk management (what are stakeholders facing?).
b. What are the objectives of the stakeholder (financial impact, programmatic impact, other)?
c. What resources are available to mitigate resources?
d. All three of the above are elements of *context*.

20. An investment company is constructing a complex of four residential rental buildings that will have more than 100 units. The complex is in a geographic area that has a long rainy season. Which of the following steps would likely be most essential to monitoring and mitigating the risk of rain damage?

a. Assuring compliance with local codes during construction.
b. Establish a reserve for capital expenditures, if needed.
c. Monthly inspections by internal maintenance staff and annual assessments by external engineering firms.
d. Actively encouraging renters to report possible problems.

21. Risk management processes can fail. Which of the following accurately identifies three reasons why the processes are prone to failure?

a. All systems will naturally fail; systems designed to solve problems may generate new problems; complex systems tend to defeat themselves.

b. Systems do not attract systems people; individual interactions squeeze out large systems; effective systems do not need information.
c. Simple systems are too elemental; individuals are too rigorous in doing what they are supposed to do; systems are not allowed enough "mission creep."
d. Issues or problems are changed by the systems that are designed to solve them; systems do not develop their own goals; complex systems always avoid self-defeat.

22. In reporting risk incidents, there is a value in reporting near misses. Which of the following would *not* be considered a near miss?

a. A restaurant was bombed by a criminal organization during the hours it was closed.
b. A poisonous snake was stolen from a zoo and taken aboard a crowded city bus, but it was killed by a policewoman before it could bite any passengers.
c. A tornado warning system was not functioning, but the residents of the area were all attending church services and not in residences that were struck.
d. Citizens reported a gas leak, but the investigators did not arrive in time to avoid a major explosion.

23. A national legislature provides authority and foreign aid funds to be spent on constructing schools in a country that is prone to rebel attacks. The risk of the schools being destroyed is deemed very high. In this situation, which of the four responses is likely *not* an option?

a. Avoidance.
b. Transference.
c. Mitigation.
d. Acceptance.

24. A manufacturing firm with a range of locations and products is hierarchical. For 10 years, clear but detailed criteria were used to report up through many layers. Due to voluminous reporting, the firm simplified the criteria allowing judgment so that only a very few risks get to the top. Some managers are concerned that the revised system may not be effective. What would you suggest?

a. Revert to the old system, because important risks might be missed.
b. Continue with the new system to show confidence that managers' judgments at all levels are trusted at the top.
c. Start over with a completely new third approach.
d. Involve managers in developing a *hybrid* of the old and revised systems.

25. A corporation has 10 regions and offices in 90 countries. The firm annually assesses risks on an entity-wide basis. Broad guidance is sent from the corporate level, but wide latitude is permitted in the field—from very informal to very structured, with no requirement for documentation. What is needed?

a. The corporate office should establish a consistent approach.
b. Every office needs supporting evidence, and it should be subject to a minimum review process from a higher level.
c. The timing should be clear and the same (or similar) format should be used for input.
d. All of the above.

26. Risk assessment reviews can be qualitative or quantitative. In periodic reviews of risk management, use of these two types should be taken into account. In this regard, which of the following statements is true?

a. Quantitative assessment techniques include interviews and workshops.
b. Benchmarking assessment techniques include sensitive analysis,

scenario analysis, and stress tests.

c. Non-probabilistic models using subjective assumptions include cash flow at risk, earnings at risk, and back testing.
d. Quantitative assessments are more complex than qualitative assessments but typically yield more precise measures.

27. A list of common pitfalls in risk assessment would likely *not* include which of the following?

a. Limiting risk assessment to financial hazards.
b. Oversimplifying risk quantification.
c. Limiting the number of significant risks to be managed.
d. Developing risks in a vacuum.

28. When assigning responsibilities for monitoring risk mitigation plans, which of the following criteria is most important?

a. To insure an independent attitude, monitoring responsibility should be limited to higher levels rather than at levels where detailed processes occur.
b. Those with monitoring responsibility can generally minimize consideration of cost-benefit analysis.
c. To properly assess the monitoring process, those doing the monitoring must hear from those close to the risks/controls.
d. Monitoring should focus on established, not emerging, risks.

29. In considering risk mitigation plans for supply chain management, assume the following four items are identified and labeled as shown:

I. Government legislation—External risk.
II. Every employee is considered a *risk manager*—Internal risk.
III. Market volatility—Not considered a risk.
IV. Asset productivity—Internal risk.

Which of the above four items is/are accurately labeled?

a. I and IV.

b. I, II, III, and IV.
c. I only.
d. I, II, and IV.

30. A large agricultural firm produces crops that rely on honeybees for cross-pollination to increase and enhance production. An unknown, uncontrolled disease has killed large numbers of bees (diminishing crops) and is now moving toward the firm's fields. What is the best response to this emerging risk?

a. Acceptance/toleration.
b. Avoidance/termination.
c. Sharing/transference.
d. Treatment/reduction.

31. What is the most likely reason that an organization may fail in its efforts to implement enterprise risk management (ERM)?

a. ERM is not uniformly applied across the company and there is not a comprehensive focus on all key business risks.
b. ERM is not driving everything that management drives.
c. It was not implemented in a discrete time frame, usually 12 months or less.
d. The organization did not adhere to regulatory requirements for ERM use.

32. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management – Integrated Framework* states, "Where potential events are not directly related, management assesses them individually." However, when correlation exists between events, management must take which of the following actions first?

a. Make a judgment about the priority of risks through executive decision.
b. Segregate the events and assess the effects, impact, or contribution to the severity of another event.

c. Quantifying the risks of the events and deciding which risks to mitigate using the results.
d. Complete a gap analysis.

33. How is the COSO ERM framework different from the ISO 31000 guide?

a. The COSO framework is applicable only in the United States, while ISO guidance is used internationally.
b. The COSO framework describes ERM as an iterative process and ISO 31000 guidance describes ERM as a serial process.
c. The COSO ERM framework is broad and includes ISO 31000 as a source of its input to the development of the ERM framework.
d. ISO 31000 views risks as loss events, while COSO ERM views risks as related to uncertainty.

34. The COSO ERM framework encompasses more specific frameworks relating to specific risks to corporate objectives. How is The IIA's Guide to the Assessment of IT Risk (GAIT) incorporated into the COSO ERM framework?

a. Once key risks are identified in a risk assessment, an organization can use an appropriate framework for IT risks. GAIT would be used in developing best practices and measures to manage and monitor IT risks.
b. GAIT should be used to manage risks that impact financial reporting and should not be used as part of an ERM discipline.
c. The ERM framework incorporated the four key principles of GAIT into components.
d. GAIT does not require that key IT controls be identified as a result of a top-down assessment of business risks and the controls required to mitigate enterprise-wide risks. Instead, the ERM framework calls for management to take risk mitigation into account.

35. ISO 31000 and COSO's ERM provide frameworks that help organizations with framing their risk management activities.

Which of the following is the best approach in assessing an organization's risk management approach?

a. Create inventories of the ISO and COSO frameworks and align them with the organization's activities to determine gaps.
b. Find out what is the most common framework being used by competitors in the industry.
c. Meet with the internal auditors to find out which approach they assess as the best.
d. Consider multiple components of an organization's industry, culture, and objectives to determine the most effective risk management approach.

36. When evaluating the risk management process using a process elements approach, ISO 31000 identifies seven components that must exist for a risk management process. Which of these components is *not* one of the process elements?

a. Risk identification.
b. Risk analysis.
c. Risk evaluation.
d. Risk deliberation.

37. Internal audit can play a key role in evaluating risk management processes. Which of the following are possible roles that internal audit should take when evaluating an organization's risk management processes?

I. Assurance on the risk management process itself.
II. Follow up on risk treatment plan status.
III. Setting the risk appetite.
IV. Assurance on significant risks and management assertions.

a. I, II, and III.
b. I, II, and IV.
c. II, III, and IV.
d. I, III, and IV.

38. Which of the following is *not* one of the formal components of COSO's ERM framework?

a. Management must consider internal and external events that create threats and opportunities.
b. Consider how objectives can be achieved by assessing the likelihood and probability of events that may affect the achievement of objectives.
c. An entity's tone at the top, ethical values, and operating style will help management establish a risk management philosophy and risk appetite.
d. Risk appetite is defined and communicated as part of the entity's mission statement.

39. Strategic objectives are generally set for three or more years and cascade down to operational objectives, which are usually shorter in term. Determine which of the options below is stated first as a strategic objective, then next as an operational objective:

a. We will end world hunger by creating partnerships with other nations to integrate resources. We will set goals to end hunger globally by working with hunger organizations in other countries.
b. Creating new job opportunities for people with the most severe intellectual disabilities. Identifying choices that consider the strengths of the person with intellectual disabilities and matching him/her up with employers.
c. We want to be the place that everyone calls home when they are away from theirs. We will make our bedding choices wider so that guests can choose from several options.
d. Our science and medicine will end cancer. Find a cure for cancer, one survivor at a time.

40. A mid-size firm has set up its ERM framework and wants to assess whether its ERM components are working properly. To do this, what are some of the ways to judge "effective" ERM?

a. Assess whether risks have been controlled across COSO's ERM framework components with reasonable assurances that risk management will allow the firm's objectives to be achieved.
b. Review the firm's operational objectives and determine if each of them has been met.
c. Assess ERM effectiveness by using the results of the financial auditor's report.
d. Use the corporate scorecard results as an indicator of the effectiveness of ERM.

41. Some companies are not mature in identifying risks that will prevent them from meeting their strategic objectives. What is *not* a way that ERM can help with achieving strategic objectives?

a. ERM can help companies achieve objectives by assigning priorities and resources that help achieve operational objectives, which push the strategy forward.
b. With proper internal controls, companies have reasonable assurance that risk management is working effectively, which provides a continuous basis for achieving objectives at all levels.
c. Once the ERM vision and the related goals and objectives are articulated, management can conduct a risk assessment to decide how to manage the risks to achieving the goals across all levels of the organization.
d. Companies should make a list of all their risks and assign ownership to a department that can routinely monitor and manage them.

42. You are the risk officer for an organization that has a social mission. Resources are limited, so the organization must set strategic objectives that represent options that consider the potential for uncertainties as well as the opportunities that exist and could exist to achieve objectives and goals. As the organization sets goals, it cascades the importance of SMART

objectives down through the organization. What does the mnemonic SMART stand for?

a. Success, Maturity, Appropriateness, Resources, Talent.
b. Specific, Measurable, Achievable, Realistic, Time-limited.
c. Specific, Measurable, Achievable, Repeatable, Tested.
d. Stated, Measured, Achievable, Risk-averse, Time-sensitive.

43. When an organization uses training and written manuals to guide and supervise behavior and control outcomes of its accounting functions and responsibilities, this is a control method for treating risks. Which type of control is this?

a. Preventative control.
b. Detective control.
c. Directive control.
d. Corrective control.

44. Internal controls need to be considered for their effectiveness in reducing or eliminating the risks for which they are intended to control, but also the cost effectiveness of the internal control. To assess cost effectiveness, what does the analysis need to include as part of the risk treatment decision?

I. The cost of implementing the control.
II. The effect of the control on external stakeholders.
III. The cost of internal auditors assessing the effectiveness of the control.
IV. The cost of not implementing the control.

a. I and II.
b. II and III.
c. I and III.
d. I and IV.

45. When an organization focuses on short-term tactics that provide some protection from risks, it can destroy shareholder

value and result in being overly risk-averse. Value-creating organizations focus on long-term risks and develop far-reaching strategies to address them. Which of the following is *not* an example of issues that an organization addresses in value creation?

a. Short-term market fluctuations.
b. Nonfinancial value.
c. Environmental and social issues.
d. Innovation.

SOLUTIONS

DOMAIN II—PRINCIPLES OF RISK MANAGEMENT PROCESSES

Question 1
Source: *CRMA Exam Study Guide*, II.B.3.iii

Solution: c (II and III)

I. Incorrect. Volatility refers to situations in which conditions vary greatly and therefore make it harder to predict the likelihood of a given event. The ministry is controlling its risk variables by accounting for different scenarios.

II. Correct. The ministry uses correlation analysis to determine *both* the increased impact and likelihood of a cholera outbreak due to weather or natural disaster-related disruptions to the food supply and emergency medical intervention.

III. Correct. The ministry's primary objective is gauging risk velocity as it measures how much time it will have between the trigger events and the impact or onset of cholera.

IV. Incorrect. While interdependency is similar to correlation in that it "relates to the connection of two or more risks," interdependency relates to the "mutual dependency of risks precipitating *new and potentially unexpected* risks." The ministry is focusing on how its ability to *respond* to a cholera outbreak will vary under different geological and weather scenarios.

Question 2
Source: *CRMA Exam Study Guide*, II.B.3.i

Solution: b (I and III)

I. Correct. “Risks that can be exploited for gain can be called speculative risk (or upside risk or opportunity).”
II. Incorrect. Market risk relates to changes in the value of the stock (share price.)
III. Correct. Enterprise risk is a business risk associated with selecting and undertaking business activities.
IV. Incorrect. Technology risks are those that new technology brings to all aspects of activity. HAL faces technology risks regardless of whether it remains focused on the private sector or expands to include the public sector.

Question 3
Source: *CRMA Exam Study Guide*, II.B.3.iii

Solution: a (II and IV)

I. Incorrect. The consequence—the PID’s profits covering its losses —occurs after the risk has materialized.
II. Correct. Trigger event is the correct term for the divestment mandate.
III. Incorrect. The risk event is the PID’s decision to sell.
IV. Correct. The intermediate events were the unexpected predictions for a long-sought upturn in the economy.

Question 4
Source: *CRMA Exam Study Guide*, II.B.2

Solution: b

a. Incorrect. Business development needs to be addressed but is not a single point of failure. The agency can implement a business development plan to address this issue in the time frame necessary.
b. Correct. The critical human capital asset is the firm’s creative director, both in terms of talents and relationships with clients. If the creative director leaves, the agency will lack the key talent that differentiates it from its competitors.

c. Incorrect. This is an ongoing risk that should be addressed by the agency as changes in the economy warrant.
d. Incorrect. This is an ongoing risk that should be addressed by the agency but is not a single point of failure.

Question 5
Source: *CRMA Exam Study Guide*, II.B.3.viii

Solution: a

a. Correct. Risk psychology addresses the perceived level of acceptable risk based on an individual's personal perceptions and thus individual risk appetite. Risk psychology also notes that the "psychological weight" that an individual associates with a risk is based primarily upon impact and not likelihood, and that the perceived impact is dependent upon one's ability to control or intervene in an event.
b. Incorrect. Although one partner may prioritize the risk of an earthquake higher than the other partner, risk prioritization is an aggregated profile of all risks in the enterprise's portfolio consistent with the general attitude of the enterprise.
c. Incorrect. Risk severity measures the "level of the inherent risk, defined as the magnitude of a combination of risks, expressed in terms of the … consequences and likelihood." In this instance, likelihood is (correctly or incorrectly) distorted due to the psychological weight of the potential impact.
d. Incorrect. Risk response refers to the level of response an enterprise feels is appropriate to take as a result of a risk materializing.

Question 6
Source: *CRMA Exam Study Guide*, II.B.3.v

Solution: c

a. Incorrect. This is a key benefit of risk mapping and prioritization as external stakeholders are interested in the overall, not the segmented, risk profile of the organization.

b. Incorrect. This is a key benefit for management that arises from risk mapping and prioritization.
c. Correct. While risk appetite may well vary in different divisions of an organization, the objective of mapping and prioritization exercises is to compare the overall risk profile against the total risk capacity of the enterprise.
d. Incorrect. This is a key benefit for management that arises from risk mapping and prioritization.

Question 7
Source: *CRMA Exam Study Guide*, II.B.3.v, II.B.3.iii, and II.B.4

Solution: c (I and IV only)

I. Correct. Fraud is often considered a low probability/moderately high impact risk and, as such, the municipality should have considered adjustments to routine operations and other treatments. Given that the comptroller was in a very powerful position and the only signatory on the accounts, this risk could also have been elevated to a medium probability risk that required closer attention. Regardless of the classification, the municipality appears to have tolerated the risk when it should have treated the risk.
II. Incorrect. Low-cost preventative and detective controls, such as requiring an additional signatory and having periodic internal reviews of the comptroller's books, would have been a good investment, especially compared to the significant loss of public funds and the likely attendant loss of public confidence in its government.
III. Incorrect. Directive controls, such as accounting manuals, training and supervision, and strategic plans, encourage desired behaviors and outcomes. While these are valid controls, the comptroller's senior position and lack of a co-signer translated into a lack of supervision. These longstanding conditions left the city vulnerable to fraud. It is unlikely that manuals, training, or strategic plans would have been strong enough deterrents given the lack of meaningful preventative and detective controls.

IV. Correct. These are controls designed to stop or limit the possibility of an undesirable event from happening. Key examples are segregation of duties, access controls, and authorization procedures.

Question 8
Source: *CRMA Exam Study Guide*, II.B.2 and II.B.3.i (esp. operational risks)

Solution: d (II and IV)

I. Incorrect. The bureaucratic culture should be examined to determine whether it was a factor contributing to the fraud, but the scenario's stem does not give us the data to determine whether this was the case.
II. Correct. CHS placed primary emphasis on the treatment wait time metric and, as a result, the system did not reward CHS for the quality of its service and outcomes, but rather by metrics that were easily manipulated.
III. Incorrect. The desire to reduce treatment wait time is not an inherently incorrect operating objective. The failure to recognize and monitor the risks introduced by its organizational objectives (IV) and its flawed performance and incentive structure (II) are the primary conditions that enabled the fraud.
IV. Correct. Achieving alignment between organizational objectives and risk management processes is key to ERM. CHS failed to recognize and monitor the risks introduced by its organizational objectives, performance metrics, and reward structure.

Question 9
Source: *CRMA Exam Study Guide*, II.B.4

Solution: a (II and III)

I. Incorrect. The activities that give rise to the risks are core to the purpose of the organization. The camp cannot avoid or terminate these risks.
II. Correct. Both the required liability waivers and the liability insurance covering the camp apportion some of the risk to a

third party.

III. Correct. Ensuring that counselors are highly trained instructors, leaders, and athletes and requiring that the campers demonstrate adequate preparedness before participating in a wilderness trip are strong mitigation responses for inherently risky activities.

IV. Incorrect. The option to tolerate or accept a risk is best suited for low-probability, low-impact risks. The camp correctly assessed that risk levels associated with its core activities require more proactive responses.

Question 10
Source: *CRMA Exam Study Guide*, II.B.7

Solution: d

a. Incorrect. This is the definition of "risk incidents."
b. Incorrect. Still, identification of such weaknesses is a critical component of strong risk management reporting.
c. Incorrect. This is the definition of an emerging risk.
d. Correct. The purpose of escalation is "partly to keep managers informed of risk incidents as well as to precipitate implementation of a contingency plan."

Question 11
Source: *CRMA Exam Study Guide*, II.B.2

Solution: b (II, IV, I, and III)

I. Development of the risk register is the *third* in the series of activities. The risk register documents the results of risk identification and the definition of the risk universe. It also assigns risk owners who are responsible for monitoring, responding, and reporting. As risk analyses and evaluations are conducted, and risk monitoring and response plans are developed, the risk register will also be updated to incorporate these data.

II. CRSA is a highly structured, participatory approach to

identifying risks. A CRSA could include a variety of risk assessment exercises such as questionnaires, brainstorming sessions or workshops, and vulnerability assessments. A CRSA or its components would be the *first* activity in this risk identification series of events.

III. Determining risk severity is the *last* step in the series and occurs after risk identification exercises are conducted or updated.

IV. Defining the risk universe is the *second* step in the series. Sobel and Reding's steps to move from a list of identified risks toward a more detailed articulation of the risk universe include consideration of the possible outcomes of the risks and defining and grouping risks according to similar sources, causes, or related impacts.

Question 12
Source: *CRMA Exam Study Guide*, Domain II

Solution: c

a. Incorrect. While strong IT controls are critical elements of risk management, there is no evidence that the criminals exploited vulnerabilities in IT policies, architecture, or software.

b. Incorrect. While CISOs have come to be regarded as protectors of information, no matter the threat, the CISO must work in concert with a number of divisions tackling privacy and security from different angles, such as a corporate credentialing center, a compliance and privacy division, and internal audit.

c. Correct. InfoMart should create the organizational infrastructure and policies that will allow it to employ an integrated monitoring and detection defense against fraud.

d. Incorrect. These knowledge services were core to the businesses' mission, and the elimination of these data would be an existential threat to InfoMart.

Question 13
Source: *CRMA Exam Study Guide*, II.B.3.iv

Solution: d

a. Incorrect. *Unlikely* is defined as "May occur once in a working life, such as premises being destroyed by fire." The nature of security threats is that they always evolve and require ongoing offensive and defensive measures. Realistically, InfoMart can only decrease the likelihood of another breach to *possible*.
b. Incorrect. *Catastrophic* is defined as "requiring nearly all of the management team to focus all of its attention on responding to the problem such as destruction of main premises or financial losses that threaten total reserves." See also the discussion of unlikely in rationale a.
c. Incorrect. *Likely* is defined as "May occur more than once a year, such as being unable to access emails." InfoMart's responses to its prior data breach should decrease likelihood to *possible*. Furthermore, *problematic* is defined as requiring "a few of the management team to focus some of its attention on responding to the problem." Maintaining the integrity of InfoMart's data requires that key members of InfoMart's management continue to focus on an enterprise-wide response.
d. Correct. *Possible* is defined as "May occur every few years, such as an industrial action or terrorist (intruder) incident." The nature of data security is that data are constantly exposed to threats, which can, however, be mitigated to within acceptable levels. *Disruptive* is defined in part as requiring "some of the management team to focus the majority of their attention to responding to the problem." Repeated breaches will weaken InfoMart's brand as a provider of reliable data. Key members of InfoMart's management will need to focus on maintaining the real and perceived integrity of the data it supplies to its customers.

Question 14
Source: *CRMA Exam Study Guide*, II.B.3.v

Solution: b

a. Incorrect. There are other criteria to consider, but analysts can add columns to the matrix to account for other factors such as

volatility and velocity.

b. Correct. For example, a high likelihood multiplied by medium impact comes out with the same numeric severity score as medium likelihood multiplied by high impact.
c. Incorrect. While subjectivity presents challenges, it can be redressed if practitioners articulate clearly the parameters associated with a numeric score, especially if aided with examples.
d. Incorrect. Regular review, revision, and updating are essential to all risk management processes to ensure they are aligned with the organizational context. These requirements are *not* unique to conducting and interpreting risk prioritization exercises.

Question 15
Source: *CRMA Exam Study Guide*, II.B.4

Solution: d

a. Incorrect. Optimal risk management requires more than determining the desired amount of resources devoted to determining, implementing, and monitoring risk and risk responses.
b. Incorrect. While an organization must ensure it has a balanced portfolio of risk that meets the general risk attitude, having a balanced portfolio is not necessarily sufficient to obtain the sweet spot. It is possible that an enterprise that has balanced its risks across divisions is nonetheless so risk averse that it fails to achieve better net results in return for undertaking additional risk (insufficient risk-taking). Conversely, an organization with a balanced portfolio of risk may have an overall risk attitude that translates into excessive risk-taking.
c. Incorrect. While this is a goal of risk management, it is not COSO's definition of the sweet spot.
d. Correct. Furthermore, "finding the sweet spot and manipulating risk to keep it there is the purpose of risk management."

Question 16
Source: *CRMA Exam Study Guide*, II.B.8

Solution: b

a. Incorrect. Identified as a goal in *Enterprise Risk Management: Achieving and Sustaining Success* (Sobel and Reding, 2012).
b. Correct. Not identified as a goal by Sobel and Reding.
c. Incorrect. Same as a.
d. Incorrect. Same as a.

Question 17
Source: *CRMA Exam Study Guide*, II.B.5

Solution: b (VI, VII, VIII, V, IV, III, II, I)

a. Incorrect. Illogical sequence, i.e., consideration of risks precedes those of control.
b. Correct. Logical (and found in use).
c. Incorrect. Illogical sequence, e.g., risk identification precedes planning.
d. Incorrect. Illogical, e.g., prioritization cannot be the last step.

Question 18
Source: *CRMA Exam Study Guide*, II.B.6

Solution: d

a. Incorrect. A commonly recognized red flag.
b. Incorrect. Again, a common red flag, especially when cash is the only form of revenue.
c. Incorrect. This should have been an additional red flag in view of a and b.
d. Correct. It is unlikely that an annual ethics briefing would influence the behavior of a long-term thief.

Question 19
Source: *CRMA Exam Study Guide*, II.B.5

Solution: d

a. Incorrect. Option d is best because it is inclusive of the other three options.
b. Incorrect. Option d is best because it is inclusive of the other three options.
c. Incorrect. Option d is best because it is inclusive of the other three options.
d. Correct. Option d is best because it is inclusive of the other three options.

Question 20
Source: *CRMA Exam Study Guide*, II.B.6

Solution: c

a. Incorrect. Codes may be lax and compliance may be minimal.
b. Incorrect. While it is important to have reserves, the amounts may be insufficient, and this is a reactive approach.
c. Correct. This would be the most proactive and aggressive approach.
d. Incorrect. This approach is too passive.

Question 21
Source: *CRMA Exam Study Guide*, II.B.8

Solution: a

a. Correct. All three of these are possible reasons.
b. Incorrect. None of these three are possible reasons.
c. Incorrect. None of these three are possible reasons.
d. Incorrect. Only the first of these three is a possible reason.

Question 22
Source: *CRMA Exam Study Guide*, II.B.7

Solution: d

a. Incorrect. Customers were unhurt.
b. Incorrect. Passengers avoided injury or death.

c. Incorrect. At least fatalities and injuries were avoided.
d. Correct. The ineffective or untimely response allowed property damage, personal injury, or worse.

Question 23
Source: *CRMA Exam Study Guide*, II.B.4

Solution: a

a. Correct. A law authorizes this program and provides funds.
b. Incorrect. Partnering countries with similar projects (and thus risks) may agree to join in (share) monitoring.
c. Incorrect. More creative controls (e.g., aerial videotaping, etc.) might be added.
d. Incorrect. The legislature and the president may be willing to accept *some* risk.

Question 24
Source: *CRMA Exam Study Guide*, II.B.7

Solution: d

a. Incorrect. The old system had information overload and did not sufficiently separate the more serious risks from the lesser ones.
b. Incorrect. It appears that important risks may not be identified at a high enough level to get attention.
c. Incorrect. Starting over may be inefficient and does not take advantage of years of experience.
d. Correct. This approach takes full advantage of years of experience and involves a wide range of managers.

Question 25
Source: *CRMA Exam Study Guide*, II.B.7

Solution: d

a. Incorrect. Incorporated in option d.
b. Incorrect. Incorporated in option d.
c. Incorrect. Incorporated in option d.

d. Correct. This is consistent with the content in II.B.7 in the *CRMA Exam Study Guide*.

Question 26
Source: *CRMA Exam Study Guide*, II.B.8

Solution: d

a. Incorrect. Interviews and workshops are *qualitative*.
b. Incorrect. These three models are called *non-probabilistic*.
c. Incorrect. These three models are called *probabilistic*.
d. Correct. This is a correct comparison of the two types.

Question 27
Source: The IIA's CIA Learning System, Part 1, Chapter 3

Solution: b

a. Incorrect. Considering only financial risks is a typical pitfall.
b. Correct. The typical pitfall is *overcomplicating* quantification.
c. Incorrect. Citing too many risks is a typical pitfall.
d. Incorrect. Developing risks in a vacuum and blindly selecting from a generic risk framework are both typical pitfalls.

Question 28
Source: *CRMA Exam Study Guide*, II.B.6

Solution: c

a. Incorrect. Monitoring must consider levels close to the risks.
b. Incorrect. Cost-effectiveness is generally a key consideration.
c. Correct. Effective monitoring needs to consider detailed levels (i.e., operational, financial, etc.) where risks/controls have key impacts.
d. Incorrect. Effective monitoring must go beyond previously established risks and also look forward to those emerging.

Question 29
Source: *CRMA Exam Study Guide*, II.B.5

Solution: a (I and IV)

I. Correct. This item is identified in a logical manner that is consistent with authoritative sources.
II. Incorrect. Item II is not a risk but is really a solution.
III. Incorrect. Item III is an external risk.
IV. Correct. This item is identified in a logical manner that is consistent with authoritative sources.

Question 30
Source: *CRMA Exam Study Guide*, II.B.6

Solution: c

a. Incorrect. The firm's crops will suffer greatly, leading to significant economic losses.
b. Incorrect. The firm relies on agricultural revenue and likely would not easily transition to other types of business.
c. Correct. Bringing in healthy bees from other geographic areas can help, but it can also add (share) risk to the areas from which the bees were transported.
d. Incorrect. A treatment of the disease is unknown, so no viable treatment exists.

Question 31
Source: *CRMA Exam Study Guide*, II.A

Solution: a

a. Correct. ERM must be applied with a holistic approach and has to truly be enterprise-wide. Unless ERM implementation is tightly linked to the assessment and formulation of business strategy, it is not meeting the COSO requirements.
b. Incorrect. ERM is integral to managing a company, but as COSO explains, many management decisions are not part of ERM. For example, management's choices as to the relevant business objectives and the allocation of entity resources are management decisions and may not be part of ERM.
c. Incorrect. While ERM is no different from the standpoint of

applying project management discipline, it is a growth process. Thus, the length of time to implement ERM varies from organization to organization depending on many variables.

d. Incorrect. While a regulatory requirement on internal control over financial reporting highlights the development of risk management in the reliability of financial reporting, and COSO's ERM framework would facilitate compliance with these requirements, any regulatory requirements would not be the only driver of effective risk management implementation.

Question 32
Source: *CRMA Exam Study Guide*, II.A

Solution: b

a. Incorrect. Correlated events must be assessed by asking what effect one event will have on another event.
b. Correct. By asking how the occurrence of one event, either individually or in combination with other events, will affect whether another event will happen, or affect the severity of another event, then management can understand them and make decisions to mitigate them.
c. Incorrect. It is important to quantify the risks as part of the risk assessment; however, quantification alone is not the mitigation strategy for correlated risks.
d. Incorrect. A gap analysis should be part of the overall risk assessment of the correlated events.

Question 33
Source: *CRMA Exam Study Guide*, II.A

Solution: c

a. Incorrect. Both the COSO and the ISO guide are used internationally.
b. Incorrect. ERM is a multidirectional, iterative process, and both COSO and ISO 31000 describe the objectives of ERM with this in mind.

c. Correct. ISO 31000 is a widely recognized set of principles and framework and is considered by the COSO ERM framework as a set of principles in achieving ERM.
d. Incorrect. Both ISO 31000 and COSO ERM view risk as related to uncertainty rather than loss.

Question 34
Source: *CRMA Exam Study Guide*, II.A

Solution: a

a. Correct. If IT risks are identified, GAIT provides an organization with a methodology to identify IT general controls that need to be tested to manage IT risks.
b. Incorrect. While GAIT methodology is widely used to identify IT general control risks, the GAIT framework is much more effective when considered as part of an ERM framework.
c. Incorrect. While the COSO ERM framework included other frameworks into its development and implementation, COSO did not incorporate specific control elements specific only to GAIT, nor any other framework, into the COSO ERM framework.
d. Incorrect. GAIT fosters risk mitigation as part of its key principles but not in a vacuum. Instead, the objectives of the COSO ERM framework consider all business risks, and any identified IT risks are assessed for their impact on the business.

Question 35
Source: *CRMA Exam Study Guide*, II.A

Solution: d

a. Incorrect. Creating comprehensive inventories and lists is an exhaustive exercise and does not lead to a qualitative opinion about best practices in risk management.
b. Incorrect. ERM is not a one-size-fits-all approach. Any framework should be assessed against the culture, size, and resources of the organization.

c. Incorrect. Internal audit should not be a key stakeholder in the best risk management framework. Management and the chief risk officer should make this decision.
d. Correct. Reviewing multiple frameworks in relation to an organization's principles, culture, objectives, and industry is the best approach.

Question 36
Source: *CRMA Exam Study Guide*, II.B

Solution: d

a. Incorrect. Identifying the risks should be a formal, structured process that considers sources of risk, areas of impact, and potential events and their causes and consequences.
b. Incorrect. The organization should use a formal technique to consider the consequence and likelihood of each risk.
c. Incorrect. The organization should have a mechanism to rank the relative importance of each risk so that a treatment priority can be established.
d. Correct. Deliberating risks is not a formal process element.

Question 37
Source: *CRMA Exam Study Guide*, II.B

Solution: b (I, II, and IV)

I. Correct. Assurance on the risk management process itself can be performed to provide reasonable assurance to senior management and the board that an organization's risk management program is effectively designed, documented, and operating to achieve its objectives.
II. Correct. Monitoring risk treatment and control remediation performance against the risk management plan should be designed to provide management with an assessment of progress against milestones and validate risk treatment plan status reports to the board.
III. Incorrect. Setting the risk appetite is not an activity that internal

audit should perform. Risk appetite is set by management and the board to identify the risk exposure that the organization will accept to achieve its strategic goals.

IV. Correct. Reports to management (and the board) can describe the potential exposure and management's assessment of current risks (with the implied value of the controls in place) together with the audit evaluation of the risk ratings.

Question 38
Source: *CRMA Exam Study Guide*, II.B

Solution: d

a. Incorrect. This describes event identification, which refers to management's consideration of internal and external factors that have potential negative or positive impact, or both.
b. Incorrect. This describes risk assessment, the formal application of considering how events will affect objectives.
c. Incorrect. This describes elements of the internal environment, which are integral to advancing ERM.
d. Correct. While it is critical to establish a risk appetite that allows for management to understand which risks it will take, establishing a risk appetite is not one of the components of the COSO ERM framework.

Question 39
Source: *CRMA Exam Study Guide*, II.B.1

Solution: b

a. Incorrect. These statements repeat the same operational objective to build partnerships with other countries, which can be an activity-based objective.
b. Correct. The objective is specific enough that it can be achieved through operational activities, such as in the second statement, which is a short-term task that can be initiated in less than 12 months.
c. Incorrect. The first statement is very broad and is a vision

statement. The second statement is very narrow and is an operational objective.

d. Incorrect. Both of these statements are vision statements, which tend to be aspirational in nature.

Question 40
Source: *CRMA Exam Study Guide*, II.B.1

Solution: a

a. Correct. Management and the board should have reasonable assurance that risks have been controlled across all the ERM framework components with no material weaknesses.

b. Incorrect. The operational objectives are not a driver for ERM effectiveness. Effective risk management will help drive operational objectives.

c. Incorrect. The financial auditor's report will provide management with information on how it is doing on financial controls, not ERM.

d. Incorrect. While the corporate scorecard can provide metrics that could be traced to effective risk management, using a metric approach to determine how well ERM is applied across strategy will limit the holistic approach to ERM implementation.

Question 41
Source: *CRMA Exam Study Guide*, II.B.1

Solution: d

a. Incorrect. Risk analysis can help companies identify, measure, and prioritize risks to all levels of objectives, which will allow the company to decide which risks to take and which to mitigate other ways.

b. Incorrect. Internal controls are one way to manage risks to organizational objectives.

c. Incorrect. Risk assessments are an important tool to identify, measure, and prioritize risks.

d. Correct. A "risk list" is not enough to achieve strategic goals, and assigning each of the risks to an owner is not an effective technique. Only by implementing an ERM framework and performing comprehensive risk analyses across all the objectives of the company will a company effectively manage its risks to stated objectives with resources that are aligned to the risk owners.

Question 42
Source: *CRMA Exam Study Guide*, II.B.1

Solution: b

a. Incorrect. See b.
b. Correct. SMART is the mnemonic that every team and individual should understand is expected of them with regard to contributing to the goals of the organization.
c. Incorrect. See b.
d. Incorrect. See b.

Question 43
Source: *CRMA Exam Study Guide*, II.B.4

Solution: c

a. Incorrect. A preventative control is designed to stop or limit the possibility of an undesirable event from happening. An example is segregating duties of the treasury function from the disbursement function in an accounting department.
b. Incorrect. A detective control would detect the occurrence of undesirable events, such as a control total run after the end of a disbursement batch of checks.
c. Correct. Accounting manuals that describe specific accounts receivables procedures and training that encourages staff in appropriate business expense transactions are examples of directive controls.
d. Incorrect. After the occurrence of an undesirable event, such as an accounting software crash, corrective controls are necessary

to restore normality, such as business continuity plans for processing payments manually instead of through the accounting software.

Question 44
Source: *CRMA Exam Study Guide*, II.B.4

Solution: d (I and IV)

I. Correct. First, the cost of implementation has to be established. This has to be calculated with some accuracy because it quickly becomes the baseline against which cost effectiveness is measured.
II. Incorrect. While external stakeholders may feel the effect of an internal control, it is not a primary consideration that can be measured alone, but it is instead part of the cost of implementing or the cost of not implementing the control.
III. Incorrect. This is not a risk treatment consideration.
IV. Correct. The loss to be expected if no action is taken must also be estimated, and by comparing the results, management can decide whether or not to implement the risk control measures.

Question 45
Source: *CRMA Exam Study Guide*, II.B.4

Solution: a

a. Correct. Short-term fluctuations in share prices should not be the focus of long-term value creation. This can lead to risk-averse strategies.
b. Incorrect. Focusing on nonfinancial values such as intangible assets—goodwill, brand—help build long-term value.
c. Incorrect. Creating value for multiple stakeholders, including the community, regulators, and customers, supports the extent of value creation.
d. Incorrect. Value creation is maximized when organizations create new mechanisms to sustain strategic advantage or generate new outcomes.

QUESTIONS

DOMAIN III—ASSURANCE ROLE OF THE INTERNAL AUDITOR

1. Internal audit plays several key roles in enterprise risk management (ERM). Which of the following is not a legitimate role for internal audit to undertake?

a. Identifying the risk universe.
b. Offering consulting services in support of risk management.
c. Providing assurance that the management of key risks, including internal controls, is effective.
d. Constructing an annual plan based upon the identification and prioritization of an organization's risks.

2. Which of the following data or events is/are the best example(s) of a key risk indicator (KRI) for pharmaceutical company Big Pharma?

I. A 15% drop in same sales-channel sales from 2013 to 2014.
II. The estimated cost to Big Pharma of a pending lawsuit.
III. The expiration of patent protection for Big Pharma's blockbuster prescription drug ABC.
IV. The U.S. dollar appreciates 20% against the euro in one week.

a. I only.
b. II only.
c. III and IV.
d. II and III.

3. Consider the following events:

I. A nationwide retailer's information systems are attacked one month before winter holidays, and hackers steal millions of customers' credit card data.
II. Negative publicity and customer fear resulting from the breach resulted in winter holiday sales dropping 45% from the prior year.
III. The retailer promises customers that they will not be responsible for any fraudulent charges and offers free credit monitoring for three years.
IV. Costs resulting from lost sales, lawsuits, and customer outreach efforts are estimated to run into the billions.

Which of the following statements assigns the correct Mainelli risk indicator to the different elements of the scenario?

a. Statement I is a challenge indicator.
b. Statement II is an action indicator.
c. Statement III is a risk incident indicator.
d. Statement IV is a health indicator.

4. Which of the following statements is correct?

a. Positive assurance is based on a statement noting confirmed evidence of effective processes.
b. Positive assurance is based on a statement noting evidence of effective and ineffective processes.
c. Negative assurance is based on a statement that the auditor found evidence of ineffective processes.
d. Negative assurance refers to the inability to give total confidence that all controls are effective and will remain so.

5. The CAE of Offshore Manufacturing (OMI) Incorporated suspects that its largest third-party manufacturer is not adhering to OMI's risk management requirements in its production processes. To reinforce the whistleblower's observations, the CAE conducts assurance reviews of risk

management processes for all manufacturing plants in which internal audit:

- **Sets the scope of audits to focus on whether risk management processes related to production are effective.**
- **Uses statistically significant sample sizes of documentation for review at each plant.**
- **Conducts focus groups and one-on-one interviews.**

What is the *biggest* error that the CAE is making?

a. The scope of the audit is too narrow and should have included assurance reviews of financial reports.
b. The sampling method is too expensive and resources should have been focused on the suspected third-party company.
c. Focus groups are wasteful if employees are scared to voice concerns in front of colleagues about observed weaknesses in risk management.
d. The CAE's primary objective is to validate suspicions regarding OMI's largest third-party manufacturer.

6. **Which of the following statements is not true when internal audit provides reasonable assurance about the effectiveness of risk management processes?**

a. The opinion meets The IIA's definition for reasonable assurance.
b. Reasonable assurance recognizes the human element to risk management.
c. Reasonable assurance denotes that the findings are accurate given a statistically acceptable standard of deviation (e.g., +/- 2%).
d. Reasonable assurance opinions are possible when assurance activities happen in accordance with management's prescribed schedule.

7. **Internal auditors at Creative Digits read about the fraud and reputational risks associated with using digital channels such**

as social media and web applications to connect with their customers and stakeholders. Although Creative Digits has a strong social media marketing campaign, digital marketing risks are not currently included in the risk register. What should the auditors do?

a. Audit the costs and benefits reported for each digital channel.
b. Notify the board that the risk is not addressed in the risk register.
c. Perform a risk assessment and determine the appropriate risk response.
d. Notify management involved in digital campaigns of the risks and provide advice.

8. A multinational bank relies on internal audit during its mergers and acquisitions (M&A) lifecycle. For which of the following M&A activities is internal audit best suited?

I. Identifying target companies.
II. Providing assurance regarding the financials of target private companies.
III. Conducting cybersecurity risk assessments of the target company.
IV. Performing a Foreign Corrupt Practices Act compliance review of newly acquired or merged businesses.

a. I and II.
b. I and III.
c. II and IV.
d. III and IV.

9. The city government of Hometown USA has an innovative staff and a culture that encourages continuous improvement in its programming and processes, including its embedded ERM. Each year, the city manager tasks management and internal audit to pursue opportunities for innovations in city programming. Which would be the best risk management assurance model for

Hometown to employ?

a. Maturity model approach.
b. Process elements approach.
c. Key principles approach.
d. Comprehensive assessment approach.

10. **Metro Power and Light (MPL) places safety as its first risk management priority. Management identifies safety risks, develops policies and procedures, and provides regular safety training for employees, partners, and citizens. MPL's risk management group conducts safety audits to ensure management conducts its safety duties. Internal audit provides assurance that MPL has developed the correct safety controls and that they are working as intended. Which of the following statements about MPL is true?**

a. MPL enjoys comprehensive integrated coverage across the full spectrum of assurance providers.
b. MPL relies on all three lines of defense to own, manage, oversee, and provide independent assurance over its safety risks.
c. MPL employs an integrated approach that avoids gaps and overlaps in assurance coverage.
d. MPL's risk management approach provides for adequate regulatory or legal compliance.

11. **Following COSO's ERM framework, the board's responsibilities for effective reporting of risks should include which of the following?**

a. Inserting specific engagements relating to risk management into the annual audit plan.
b. Selecting the specific techniques regarding event identification to be considered in the risk management process.
c. Assuring success in management of key risks.

d. Regularly reviewing the key risks against risk appetite.

12. According to IIA Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, in providing confidence on process design, delivery, and documentation, the following categories of questions should be included except:

a. Senior management involvement.
b. Only stand-alone processes.
c. Staff skills and knowledge.
d. Responsiveness to change.

13. A 100-year-old manufacturing firm has had an excellent reputation for high-quality products, with all sales to the private sector. Recently, the firm expanded sales to the government's defense department, and high profits rapidly declined. Historically, (1) personnel practices have been popular with employees—flexible work schedules and limited supervision (resulting in high morale), and (2) security in warehouses and production has been limited (yet minuscule pilferage occurred). In analyzing why profits have declined, which of these risks would be of least concern?

a. A very loyal workforce is being replaced by a younger workforce with less loyalty and more likelihood of abusing attendance requirements and engaging in pilferage.
b. In contract sales to the defense department, the firm is subject to tighter controls over classified inventories, and the loose controls needed improvement.
c. The past lack of locks, fences, and barriers to the firm's plant will risk more theft of expensive defense-related inventories, and may violate defense security regulations.
d. A younger workforce will likely be less educated and trainable.

14. An internal auditor assigned to an assurance engagement of risk management processes should understand and appreciate the technical language—concepts, principles, and terms—of

risk management processes. An auditor may also need to consider broader natural barriers to effective risk management. Which of the following is a natural barrier?

a. An ERM framework that is not applicable for a particular entity.
b. Reluctance by the CEO to share negative information.
c. An inadequate event identification approach.
d. An outdated risk register.

15. In an assurance engagement of risk management, an internal auditor identifies several potential problems that, in the auditor's judgment, need further exploration. Of the following, which should the auditor be least concerned about?

a. The board monitors risk directly without sharing with any committees.
b. Reporting of key risks is on an as-needed basis rather than periodically.
c. The designation of key risks is from a standardized list applicable to any entity.
d. The number of key risks is limited to a defined number.

16. An assurance engagement of risk management processes by the internal audit activity should start by doing all of the following except:

a. Proposing revision of the entity's mission, strategy, and objectives.
b. Understanding the internal and external environment.
c. Gaining knowledge of the risk appetite, risk capacity, and risk tolerance.
d. Identifying inherent risks and residual risks.

17. As a function within the organization, the internal audit activity must generally comply with the organization's policies and procedures, including risk management processes. However, there may be some differences. Which of the

following statements about the risk management processes of the internal audit activity itself is accurate?

a. Due to its nature and independence, the internal audit activity is immune from risks.
b. The only risk of concern to an internal audit activity is that it might provide false assurance.
c. The internal audit activity is subject to all the same risks of any other function.
d. Risk management methodologies should be used in internal audit practices.

18. In delivering assurance on risk management, an IIA Practice Guide identifies three approaches auditors might follow: (1) process elements, (2) key principles, and (3) maturity. A textbook identifies only two: (1) comprehensive, seen as a combination of (1) and (2) in the Practice Guide, and (2) maturity. Rigid, specific rules for choosing an approach do not exist for an audit activity, but general guidelines do exist. Which of the following statements is valid?

a. Regardless of approach, if the internal auditor is not wholly independent of the risk management function, assurance should be provided by a source other than internal audit.
b. A process, key principles, or comprehensive approach is suggested when ERM has been in use and found to be effective, but further improvements are desired.
c. The maturity model approach identifies three levels, from "risk-aware" to "risk-managed."
d. The maturity model approach is applicable when ERM has been introduced fairly recently.

19. Assume an internal auditor is assigned to an assurance engagement over the risk management process. The auditor discovers that the entity does not have an established risk management process and has not adopted a recognized framework, such as COSO or ISO 31000. Which is the best

explanation of the approach the auditor should take?

a. Select an appropriate framework and advise the entity to adopt it before continuing the assurance framework.
b. Ignore the absence of the framework and proceed with the engagement.
c. After discussing the issue with the CAE, and consideration of input from senior management and the board, decide if the assurance engagement must be adjusted.
d. Proceed with the engagement, but consider it to be a consulting engagement.

20. If internal auditors are to be effective in providing assurance on risk management processes, they must be knowledgeable of common concepts and terms used in these processes. This knowledge should include awareness of quantitative and qualitative risk assessment techniques and related terms. Match the specific techniques to the categories:
Categories: Non-probabilistic (NPM), benchmarking (B), probabilistic model (PM)
Techniques: Best in class (BIC), cash flow at risk (CFR), scenario analysis (SA)

a. CFR is in NPM.
b. BIC is in B.
c. SA is in PM.
d. CFR is in B.

21. For an internal audit plan to be appropriately risk-based, which of these must the CAE consider?

I. Residual risks, key risks, and key controls.
II. The work of other assurance providers.
III. That the organization has communicated the risk appetite.
IV. Individual risk factors where there are significant reductions from inherent to residual controls.

a. I and II.
b. II and III.
c. I and IV.
d. II and IV.

22. An auditor wants to review the organization's management of key risks, so he looks at risk mitigation implementation plans to find evidence of effective risk management. What should he be considering by looking at the risk implementation plans?

a. If the risk mitigation implementation plans identify owners, timelines, and evidence of action plans that were implemented.
b. If the plans follow COSO's ERM framework.
c. The plans should show evidence of board approval.
d. That he has enough information in the risk mitigation implementation plan to perform a walk-through.

23. The following are key design features of KRIs except:

a. The organization should use KRIs consistently in all its lines of defense.
b. KRIs should be tied to the organization's strategic scorecard.
c. Risk owners should be held accountable for risk mitigation activity of key risks over which they have responsibility.
d. Implementing KRIs creates additional costs and should be embedded into the annual budgeting cycle in advance.

24. The program office for grants administration informed the internal auditors that its organization has a robust ERM culture and discipline. However, the auditors found that key risks were not properly analyzed and managed by the organization. What are the most likely reasons that there are weaknesses in managing key risks?

I. Key risks are identified, but they are not prioritized and monitored.

II. Management has not acted in areas where residual levels of risk are above the organization's risk appetite.
III. Key risk indicators are not appropriately identified with the use of stress points.
IV. The risk responses assigned by management do not get to the root cause of the risk, thus the responses are ineffective at managing risk.

a. I, II, and III.
b. I, III, and IV.
c. II, III, and IV.
d. I, II, III, and IV.

25. The chief risk officer at Soups International has been reporting to senior management and the risk committee of the board regularly on the organization's key risk indicators, including risk ratings and responses. Management and the board are surprised, however, when it is revealed that one of Soups International's major suppliers has been investigated and found guilty of food contamination. What should the internal auditors do so surprises are avoided?

a. The auditors need to implement management's risk responses.
b. Internal audit should give assurance that risks are correctly evaluated.
c. Internal audit should define the risk appetite so surprises are avoided.
d. Reorder the risk ratings to ensure that supplier risks are exposed.

26. The board of any nonprofit or private organization should receive reports about key risks. What are some of the key elements that make risk reporting relevant for board oversight?

I. Risk reporting is repeatable over time.
II. A rigorous method and an analytical framework support risk reporting.

III. Reporting is applied periodically and regularly, as opposed to as needed.
IV. A separate committee sees the risk reports and then reports to the full board.

a. I, II, and III.
b. I, II, and IV.
c. II, III, and IV.
d. I, III, and IV.

27. Internal auditors should consider the reporting of risks as part of the assurance they provide on risk management activities. Which of the following is not a best practice in risk reporting that auditors would provide assurance on?

a. An organization limits the number of risks in a risk report to 5 to 20.
b. The information in the risk management plan and risk report flows up and down.
c. The report out on risks occurs when they have fallen outside the acceptable risk tolerance levels.
d. The risk report is separate from the annual report or performance report.

28. Which of the following is the most likely responsibility of the CAE in assuring that an organization's risk are adequately evaluated?

a. Hiring subject matter experts in all operation areas to fill out the internal audit team and manage risks in operations.
b. Coordinate the activities of risk, compliance, and internal audit to ensure resources are being used effectively and efficiently.
c. Ensure that the risk management activities are effective.
d. Develop review teams to oversee risk management activities in the organization.

29. Kipper Co is a Canadian company with offices throughout the

country. Kipper's risk management approach includes an enterprise risk matrix that allows senior management and the board to view the top 10 risks to achieving the company's strategic goals, risk owners, mitigation activities, and residual risks. The CAE of Kipper wants to perform an assurance mapping exercise. Which of the following is not a step she would perform in assurance mapping?

a. Identify which of the risk management activities and residual risks fall within Kipper's risk appetite.
b. Identify which assurance providers are responsible for assessing the risks or control activities tied to each of the 10 risks.
c. Provide assurance across the entire enterprise and its operations after considering the coverage by all assurance providers.
d. Ensure that the internal auditors are the only source from which the board will seek assurance.

30. While performing an assurance audit on the risk management process of International Flora Group, the auditor evaluated the organization using the eight components of COSO's ERM framework as a benchmark. The auditor found defined responsibility for the internal environment and robust policies and procedures protocols and documentation. Yet the risk management philosophy was informal and not communicated uniformly. Using a maturity model approach to the audit, what is the most likely rating the auditor would use on the maturity-level scale?

a. Very weak.
b. Poor.
c. Mid.
d. Good.

SOLUTIONS

DOMAIN III—ASSURANCE ROLE OF THE INTERNAL AUDITOR

Question 1
Source: *CRMA Exam Study Guide*, Introduction to Domain III

Solution: a

a. Correct. Identifying and managing risk is the role of management. It is crucial that internal audit not assume a direct role for identifying risk to ensure internal audit's independence and objectivity when performing assurance activities.
b. Incorrect. Advisory services or consulting, while subject to standards and safeguards, are legitimate roles for internal audit.
c. Incorrect. This function is a key role for internal audit.
d. Incorrect. "The CAE prepares … the audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization."

Question 2
Source: *CRMA Exam Study Guide*, III.A

Solution: c (III and IV)

I. Incorrect. This is a lag indicator.
II. Incorrect. This is a key risk with the potential for significant impact. A KRI is a lead indicator of risk-triggering events or conditions.

III. Correct. The end of patent protection introduces the opportunity for other firms to introduce less expensive versions of ABC and weaken sales of this key source of Big Pharma's revenue and profit.
IV. Correct. KRIs are evidence of conditions that could trigger risks to an organization's objectives. Depending on how much of Big Pharma's revenue comes from Europe and how it hedges foreign exchange, this development could well pose an upside or downside risk.

Question 3
Source: *CRMA Exam Study Guide*, III.A

Solution: a

a. Correct. Statement I tells us the trigger event has occurred.
b. Incorrect. Statement II is a health indicator because it lets us know how the risk event has started to affect the retailer's performance. Statement III is the action indicator, telling us whether responsive actions have been taken.
c. Incorrect. Statement III is the action indicator, telling us whether responsive actions have been taken. Statement IV is the risk incident indicator because it communicates the ultimate impact of the breach on the retailer's value.
d. Incorrect. See above.

Question 4
Source: *CRMA Exam Study Guide*, III.C

Solution: b

a. Incorrect. This is only part of the correct definition of positive assurance, which is "Assurance based on a statement noting confirmed evidence of effective or ineffective processes."
b. Correct. See explanation above.
c. Incorrect. Negative does not equate to ineffective. Negative assurance is a statement noting the absence of evidence to the contrary.

d. Incorrect. See above. Furthermore, the statement refers to auditors' inability to provide absolute assurance because an audit opinion is provided at a moment in time and is usually based on a sample.

Question 5
Source: *CRMA Exam Study Guide*, III.C

Solution: d

a. Incorrect. Due to limited time and money, assurance reviews may not be able to cover every item in one engagement. As long as all parties understand and agree to the scope of the review, a limited set of objectives is legitimate and may help to prevent "mission creep."
b. Incorrect. Selecting a statistically valid sample size is a cost-effective method to ensure integrity of the resulting analysis. Furthermore, auditors should use statistically valid sample sizes at all production plants under review.
c. Incorrect. While it is important for internal audit to acknowledge and control for a potential "peer pressure effect," focus groups are not an inherently flawed tool in the internal audit toolkit.
d. Correct. Objectivity requires that internal audit follow the evidence without preconceived ideas or the desire to prove a point.

Question 6
Source: *CRMA Exam Study Guide*, III.C

Solution: b

a. Incorrect. There is no IIA definition for reasonable assurance.
b. Correct. Reasonable assurance allows for the uncertainty that human error or bad intentions may result in control failures.
c. Incorrect. Reasonable assurance, defined as "strong but not absolute assurance," is not tied to a universally acceptable standard deviation or margin of error.

d. Incorrect.

Question 7
Source: *CRMA Exam Study Guide*, III.C

Solution: d

a. Incorrect. Analyzing the costs and benefits of a marketing channel may help identify unrealized gains (waste) or fraud, but it should be the responsibility of management (for example, the chief marketing officer).
b. Incorrect. The auditors should contact appropriate members of management before bringing the concern to the board.
c. Incorrect. Internal auditors should not conduct the risk assessment or determine the risk response.
d. Correct.

Question 8
Source: *CRMA Exam Study Guide*, Introduction to Domain III

Solution: c (II and IV)

I. Incorrect. Identifying target companies is a strategic role of management. Internal audit's appropriate role is limited to auditing the organization's target identification process.
II. Correct. Auditing and providing assurance on the financials of the target company during the due diligence of a potential merger or acquisition is a core internal audit function.
III. Incorrect. While cybersecurity vulnerability or risk assessments should be a part of the due diligence process, this function belongs to the technical and business process managers and not to internal audit.
IV. Correct. Conducting compliance audits, or coordinating with a stand-alone compliance unit if it exists, is a key internal audit assurance function.

Question 9
Source: *CRMA Exam Study Guide*, III.D

Solution: a

a. Correct. Hometown's ERM is established and supported and management is ready and motivated to seek further improvements in its programming and ERM strategy and processes.
b. Incorrect. Process elements is a more rudimentary approach. Process elements is better suited to an entity that has introduced ERM relatively recently or has not assessed its ERM systems for several years.
c. Incorrect. Key principles is a more rudimentary approach. Like process elements, key principles is better suited to an entity that has introduced ERM relatively recently or has not assessed its ERM systems for several years.
d. Incorrect. Sobel and Reding's comprehensive assessment approach operates like a combination of the process elements and key principles approaches. Therefore, the same comments apply as in b and d.

Question 10
Source: ***CRMA Exam Study Guide*****, III.C**

Solution: b

a. Incorrect. For this statement to be true, MPL should also present evidence of strong relationships with external assurance providers such as external auditors, regulators, and safety inspectors.
b. Correct. Management (1st line), risk and compliance (2nd line), and internal audit (3rd line) all play integral roles in ERM with respect to safety.
c. Incorrect. We have no evidence that MPL conducts periodic assurance mapping. Assurance maps show the coverage offered by the main classes of assurance providers and help the organization to "ensure proper coverage and minimize duplication of efforts."
d. Incorrect. Documentation of MPL's strategy and practices should provide stakeholders with confidence that MPL is

meeting regulatory and legal obligations with respect to safety.

Question 11
Source: *CRMA Exam Study Guide*, III.B

Solution: d

a. Incorrect. The CAE has primary responsibility for developing the annual audit plan.
b. Incorrect. Selecting specific techniques for event identification is the responsibility of management, perhaps with input from others, such as a risk officer.
c. Incorrect. While the board should analyze how well ERM is operating in the management of key risks, it would be unrealistic to assure success.
d. Correct. The board should perform regular review/continuous monitoring.

Question 12
Source: *CRMA Exam Study Guide*, III.C

Solution: b

a. Incorrect. Senior management involvement is important.
b. Correct. Embedded processes should be considered.
c. Incorrect. Staff members need the right skills and knowledge.
d. Incorrect. Responsiveness to change is a key element to consider.

Question 13
Source: *CRMA Exam Study Guide*, III.B

Solution: d

a. Incorrect. This risk should be considered due to the firm's popular personnel practices, and perhaps changes in demographics of the new employees.
b. Incorrect. This is a likely risk in defense sales and should be considered.

c. Incorrect. This is a likely risk, especially if inventories are expensive and/or related to national security and risk of theft by terrorist groups.
d. Correct. Younger employees are likely more educated and flexible to new technologies, so this risk would be lower than the others cited.

Question 14
Source: *CRMA Exam Study Guide*, III.B

Solution: b

a. Incorrect. Framework is a technical term related to risk management.
b. Correct. Reluctance to share bad news is common and not solely related to risks.
c. Incorrect. Event identification is a technical term in risk management.
d. Incorrect. Risk register is a technical term related to risk management.

Question 15
Source: *CRMA Exam Study Guide*, III.B

Solution: d

a. Incorrect. The board is generally too far from activities and should share duties.
b. Incorrect. Risk reporting should generally be on a regular, periodic basis.
c. Incorrect. Designation of key risks should be tailored to the organization.
d. Correct. Key risks should be limited to a defined range (e.g., 5 to 20) for simplicity.

Question 16
Source: *CRMA Exam Study Guide*, III.D

Solution: a

a. Correct. Proposing revisions in these three areas would be beyond the auditor's role, especially at the start of the engagement.
b. Incorrect. This is consistent with the relevant standard and practice advisory.
c. Incorrect. Same as for option B.
d. Incorrect. Same as for option B.

Question 17
Source: *CRMA Exam Study Guide*, III.D

Solution: d

a. Incorrect. IIA guidance explicitly states the internal audit activity is not immune from risks.
b. Incorrect. Three broad categories are audit failure, false assurance, and reputation risk.
c. Incorrect. The risks relate to the internal audit activity's unique mission and objectives.
d. Correct. Risk management methodologies should fit the environment.

Question 18
Source: *CRMA Exam Study Guide*, III.D

Solution: a

a. Correct. Independence of the internal audit activity would potentially be impaired in this case.
b. Incorrect. The approaches noted apply when ERM is fairly new and not in place long enough to be deemed effective.
c. Incorrect. The five levels in the maturity model approach are risk-naïve, risk-aware, risk-defined, risk-managed, and risk-enabled. (Terms may vary.)
d. Incorrect. See the rationale for option B. The maturity model approach is used when ERM has been used for a period of time.

Question 19

Source: *CRMA Exam Study Guide*, III.D

Solution: c

a. Incorrect. While facilitation or advisement on establishment of a framework may be performed as a consulting engagement, it should not be performed as an assurance engagement.
b. Incorrect. The auditor should carefully consider the circumstances before proceeding, so ignoring the absence of a framework would be inappropriate.
c. Correct. The CAE needs to use judgment as to the best approach to follow after consideration of input from senior management and the board.
d. Incorrect. A decision as to whether to initiate a consulting engagement should be made by management and properly coordinated with the charter and annual audit plan.

Question 20
Source: *CRMA Exam Study Guide*, III.D

Solution: b

a. Incorrect. CFR is in PM.
b. Correct. BIC is in B.
c. Incorrect. SA is in NPM.
d. Incorrect. CFR is in PM.

Question 21
Source: *CRMA Exam Study Guide*, III.A

Solution: c (I and IV)

I. Correct. Residual risks are those that exist after controls have been implemented, and key risks are usually those with the highest ranking based on likelihood and impact. Once a CAE considers the residual risks and the key risks that have been identified, the internal audit plan can be developed to provide assurance of control activities.
II. Incorrect. The work of other assurance providers must be

considered as the CAE is providing assurance across the entire enterprise when multiple parties manage risks, and the internal audit plan and activity would feed into this assurance.

III. Incorrect. Once an organization develops a risk appetite and communicates it, the internal audit activity must then consider the key risks that are identified as outside the risk appetite and the responses to the risks.

IV. Correct. This highlights controls that are important to the organization.

Question 22
Source: *CRMA Exam Study Guide*, III.A

Solution: a

a. Correct. Any risk mitigation implementation plan should show evidence of accountability and timelines, as well as provide action-based plans that can be traced to outcomes.

b. Incorrect. A risk mitigation implementation plan is not a prescribed work document of COSO's ERM framework. The plan should be specific to the organization and show that risk mitigation activities were carried out.

c. Incorrect. The board has an active role in oversight of effective risk management, but individual risk mitigation implementation plans are operational in nature and not for board approval.

d. Incorrect. There are many methods used for information gathering by auditors in reviewing the management of key risks. A walk-through does not need to be dependent on a risk mitigation implementation plan.

Question 23
Source: *CRMA Exam Study Guide*, III.A

Solution: d

a. Incorrect. A key design attribute of KRIs is the consistency of application across the organization.

b. Incorrect. When the corporate scorecard and KRIs are

comparable, the management of risks as aligned to strategic goals becomes more effective.

c. Incorrect. Tying performance measurement indicators to KRIs will strengthen risk management.

d. Correct. Key risk indicators should be designed so that they are cost effective to implement and measure.

Question 24
Source: *CRMA Exam Study Guide*, III.A

Solution: d (I, II, III, and IV)

I. Correct. Robust risk analysis requires several stages to be performed, including risk identification, risk prioritization, risk mitigation, and risk monitoring.

II. Correct. If inherent risks for fraud are controlled via key controls, but residual risks remain above the organization's risk appetite and management does not pay attention to these risks, this is a flaw in key risk management.

III. Correct. Understanding what key risk indicators are by identifying the trigger events, conditions, or intermediate events is best done by identifying the stress points, which permit the organization to be able to identify stages of fraud in grant appropriations.

IV. Correct. It is critical that the risk responses are appropriate to mitigating the risk of fraud. If management chooses the wrong risk response, then the inherent risk of fraud will not be controlled.

Question 25
Source: *CRMA Exam Study Guide*, III.B

Solution: b

a. Incorrect. This is not a legitimate role for internal audit to perform.

b. Correct. Auditors can assess exposures in the risk management process, including an evaluation of the risk ratings.

c. Incorrect. Management and the board are responsible for setting risk appetite.
d. Incorrect. The risk ratings are assigned through a management process with input from the auditors. The auditors do not determine the ratings, management does.

Question 26
Source: *CRMA Exam Study Guide*, III.B

Solution: a (I, II, and III)

I. Correct. Risk reporting should be repeatable.
II. Correct. Regardless of what methodology and analytical framework is used, risk reporting should include evidence of rigor and analytics to support the report.
III. Correct. The reports should be updated regularly and the board should know annually when to expect the risk report.
IV. Incorrect. It is not a requirement for a separate committee of the full board to review the risk report first for effective reporting.

Question 27
Source: *CRMA Exam Study Guide*, III.B

Solution: c

a. Incorrect. Risk reporting should be kept simple; only the key risks should be reported out. There is no defined limit of risks to report.
b. Incorrect. Information on risks needs to be shared so that stakeholders and employees are aware of the risk appetite, the importance of key risks, and the activities that are occurring to eliminate redundancies.
c. Correct. Risks have to be promptly identified and assessed, but risk reporting should be regular and not reported only when risk tolerance thresholds have been crossed.
d. Incorrect. Even though the risk reporting process should be embedded within core management systems, risk reporting should be separate from the annual financial report or

performance report.

Question 28
Source: *CRMA Exam Study Guide*, III.C

Solution: b

a. Incorrect. Management takes responsibility for operation risk management. Therefore, the assurance of risks by management would be considered in the CAE's assessment, but the CAE does not manage risks in operations.
b. Correct. Many organizations have distinct roles to oversee assurance activities, including internal audit, compliance, and risk management. The CAE has the skills and knowledge to provide coordination and reporting over all assurance functions to ensure they are effective.
c. Incorrect. It is management's responsibility to ensure that risk management activities are effective. Internal audit evaluates effectiveness and offers the board the appropriate level of assurance for the nature and levels of risk that exist in the organization. There is a difference between ensuring effectiveness and evaluating effectiveness to provide assurance.
d. Incorrect. Oversight of risk management activities is a role for the board.

Question 29
Source: *CRMA Exam Study Guide*, III.C

Solution: d

a. Incorrect. Without coordination of assurance providers, key risks may be misjudged and ineffective control activities may go unnoticed.
b. Incorrect. The assurance map will show the coverage provided by the providers and help identify and address gaps in the risk or control activities.
c. Incorrect. The CAE must understand the independent assurance requirements of the board and the organization to provide

information about each assurance activity by coordinating assurance providers and reporting on gaps.

d. Correct. The board will use multiple sources to gain reliable assurance, including assurance from management, external auditors, and internal auditors.

Question 30
Source: *CRMA Exam Study Guide*, III.D

Solution: b

a. Incorrect. The organization has formal controls communicated, so its ERM approach would not rate this low.

b. Correct. While the control environment is strong, the internal environment is a necessary first step to the maturity of ERM, and without formal risk management philosophy, the rating would likely be poor.

c. Incorrect. The organization's lack of communication would not lend itself to a mid-level ERM approach.

d. Incorrect. Principles for ERM cannot be carried out regularly if the risk philosophy is informal.

QUESTIONS

DOMAIN IV—CONSULTING ROLE OF THE INTERNAL AUDITOR

1. Which of the following statements about the differences between the assurance and the consulting roles of the internal auditor are correct?

I. Internal audit's involvement in a consulting engagement is generally at the request of management.
II. During consulting engagements, internal audit is able to implement improvements in ERM.
III. During consulting engagements, internal audit can only recommend improvements, and management is free to accept or reject the proposals.
IV. Unlike assurance activities, consulting does not have to be defined in the internal audit charter.

a. I and II.
b. I and III.
c. II and IV.
d. III and IV.

2. Internal audit uncovered significant cost overruns plaguing a high-visibility contract to modernize a federal agency's IT systems. The CAE directed that the CIO rework each element of the contract into performance-based work orders, a collaborative, cross-functional procurement approach with which the agency is not familiar. Which of the following

statements is correct?

a. Due to the conflict of interest safeguard, the CIO cannot request training or coaching assistance from internal audit for 12 months following the audit.
b. Management should follow internal audit's directive regarding the level of resources to be allocated to mitigating procurement risk.
c. Management should seek training to ensure that the new work orders establish vendor responsibilities consistent with internal audit's revised procurement risk appetite.
d. If internal audit provides training and facilitates collaborative work sessions among government and vendor parties, it must wait at least 12 months before it may give assurance on any part of the resulting framework for which it was responsible.

3. Which of the following statements is/are true about the similarities and differences between assurance and consulting engagements regarding risk assessment processes?

I. The nature and number of parties are the same for both.
II. Assurance engagements are generally delivered when everything needed is in place, whereas consulting engagements are more likely performed where there are no processes, or the processes are new or incomplete.
III. If needed skills are not available for assurance, they must be obtained to deliver the engagement, but consulting may need to be declined if skills are absent and not obtained.
IV. Either type must be based on risk assessment and take into consideration error, fraud, and noncompliance.

a. I, III, and IV.
b. II and III.
c. II, III, and IV.
d. II only.

4. Which of the following requirements in IIA guidance is least

related to assuring objectivity and independence in performing consulting engagements?

I. Governance, risk management, and control processes *may* be included in the scope of consulting engagements but *must* be included in *assurance* engagements.
II. Auditors must disclose potential impairments to objectivity before accepting proposed engagements.
III. Consulting engagements should not be accepted simply because management made a request.
IV. Internal auditors may consider general observations (even if not part of a specific engagement) from consulting in developing audit plans.

a. I and IV.
b. I only.
c. IV only.
d. I, II, and III.

5. An internal auditor following The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) should be familiar with the definition and nature of consulting and assurance, how the two categories may be interrelated, and possible subcategories within each category. With which of the following statement(s) would you agree?

I. Consulting engagements have subcategories of formal, informal, special, or emergency. Assurance can have various subcategories.
II. The two categories are distinct and cannot be "blended."
III. An assurance engagement should not be performed to circumvent a consulting engagement.
IV. In either category, when laws and/or regulations prohibit following certain standards, auditors need to comply without explanation.

a. I, III, and IV.
b. I, II, and III.

c. I, II, III, and IV.
d. I only.

6. **While assurance and consulting engagements have common features, there are significant differences. All of the following are true about comparisons *except:***

   a. The internal auditors should not take on a consulting role separately from the delivery of assurance.
   b. The extent of consulting should be coequal with assurance.
   c. Internal auditors must incorporate knowledge of risks gained from consulting engagements into evaluating risk management processes.
   d. Internal auditors should incorporate knowledge of controls gained from consulting engagements into evaluating control processes.

7. **A company wants internal audit advisory services to help it identify and evaluate the risks associated with entering into a new market. What statement about internal audit's advisory qualifications and roles is *incorrect*?**

   a. As experts in facilitation and risk management identification and evaluation, internal audit should determine the requirements of the advisory engagement.
   b. Internal audit's knowledge of the risk management maturity of the client organization can help to determine the appropriate risk identification and evaluation techniques and benchmarks to be used.
   c. Internal audit is well positioned to identify who should attend and what resources are needed to conduct sufficient risk identification exercises.
   d. Internal audit can teach clients strengths, weaknesses, opportunities, and threats (SWOT) analysis and other competitive analysis techniques.

8. **A home appliances manufacturer is considering adding web-**

enabled technology into its products. The CEO asks the CAE to undertake a month-long consulting engagement to identify and evaluate the risks of adopting this product development change. Which of the following statements is *true* regarding the involvement of the CAE in the consulting engagement?

a. The CAE must determine if there is sufficient expertise in internal audit to conduct the engagement on its own. If not, he or she should hire additional consultants to augment internal audit's skill set.
b. The CAE should ensure that the objectives, scope, and approach of the consulting engagement are achievable within a month.
c. The CAE must determine if the scope of the engagement is sufficient to achieve the desired objectives before committing to the task.
d. The CAE is ultimately responsible for the objectives and scope of the engagement.

9. **Which of the following is *not* a key activity that internal audit can engage in facilitating risk identification and evaluation with a management group?**

a. Asking the group to spontaneously come up with any risks that may exist.
b. Distributing a set of questions in advance to draw input from the group anonymously.
c. Gathering data from other industry groups or from leading metrics.
d. Creating a risk checklist and distributing it to the group members for ranking.

10. **Which of the following statements correctly describes why internal auditors are well positioned to coach management on responding to risk?**

a. Internal auditors are accustomed to dealing with confidential matters and thus provide a safe environment in which a client

can talk about all matters of concern without fear of repercussion.

b. Internal audit may have been responsible for identifying that management's current response to risk is an area of weakness within the risk management framework.
c. Internal audit has the appropriate experience and skill set in governance and risk management to teach management about the areas in ERM that are not working and need improvement.
d. Internal audit's analytical training and audit experience enable it to find solutions for weak systems or controls.

11. Consider the following potential consulting roles for internal audit to improve management's capability to respond effectively to risk. Which of the following would an internal auditor most likely suggest in each of the following situations?

I. The deputy CRO is being groomed to replace the CRO when he retires in six months.
II. An employee will be reassigned to a role in the CRO's office with a new added responsibility of developing event inventories.
III. All employees, some with more significant roles than others, will be introduced to a new regulatory ERM with new terms and procedures.
IV. The CAE is asked to temporarily assign an internal auditor to prepare the management report on risk.

Choose from the following: Coaching, Training, Mentoring, Other

a. Training for I, Coaching for II, Mentoring for III, and no role for IV.
b. Coaching for I, Mentoring for II, Other for III, and Training for IV.
c. Coaching for I, Mentoring for II, Training for III, and no role for IV.
d. Mentoring for I, Coaching for II, Training for III, and Other for IV.

12. One event demonstrates the negative impact of ignoring the likelihood and impact of risks. A state internal auditor identified the lack of an effective system to identify and treat mentally ill citizens. The state auditor recommended (twice) that a corrective system be in place to ensure timely, effective responses. Two years later, after no state action, an untreated mentally ill person committed two murders. Which of the following actions by the CAE would *most likely* have avoided this?

a. Early discussion with management of a potential consulting engagement to facilitate implementation of the auditors' recommendations.
b. The CAE's offer to allow the auditor who performed the review to join management temporarily to implement the revised system.
c. Lobbying the legislative branch to enact a law for corrective action.
d. The internal audit activity did all it could, and the CAE has no further requirement.

13. Internal audit is sometimes asked to coach management, as a whole or individually, on how to respond to risks. Which of the following is a legitimate expectation of coaching?

a. It should be seen as a way to fix a problem.
b. A program of training in risk-related matters may require coaching to ensure full benefits are realized.
c. It tells management what is wrong and what needs improvement.
d. Its focus is primarily on getting someone through a challenging period.

14. Which of the following "audits" is least likely to be performed by internal auditors solely as consulting, rather than an assurance or "blended" category?

a. Business process mapping.
b. Financial statement.
c. Systems development review.
d. Control self-assessment.

15. Two audit categories identified by The IIA are *operational* and *performance*. These two categories have some similarities. However, which of the following statements describe how the characteristics of these two categories *differ*?

a. Operational audits focus on economy and efficiency, while performance audits focus on whether key performance indicators (KPIs) are being achieved.
b. Performance audits cannot be consulting engagements, whereas operational audits can be either assurance or consulting engagements.
c. Both categories place equal emphasis on evaluating the specific indicators on how well objectives are being achieved.
d. The stakeholders are likely to include external parties for both categories of audit.

16. A business in a highly regulated sector discovers it has different practices and language for identifying, evaluating, monitoring, and responding to and reporting on risks. Which of the following is *not* an appropriate advisory role for internal audit?

a. Reviewing all internal and external sources of assurance (management, external auditors, health and safety inspectors, and compliance officers) to ensure that there are no significant gaps and no unnecessary overlaps and duplications.
b. Making recommendations to management about training and coaching needs to achieve standardized approaches to risk management.
c. Determining the holistic risk management framework to be used across the enterprise.

d. Having discussions with risk owners and other stakeholders to challenge risk identification and evaluation.

17. Regarding the internal auditor's role in coordination of risk management activities, which of the following four statements are true?

I. The move to ERM has brought a greater degree of centralized control and coordination and, coincidentally, likely more requests from management for advisory help from the auditors.
II. Internal auditors are not allowed to deliver assurance on operations for which they had responsibility, including risk management.
III. Internal auditors, in an advisory capacity, seek to ensure common use of terminology used in the risk management process.
IV. In the coordinating role, internal auditors are in a good position to identify training needs of employees throughout the organization.

a. I only.
b. II only.
c. I, II, and III.
d. I, II, III, and IV.

18. In a systems development and cycle review, consulting engagements could be involved in several places. The internal auditor's focus will vary depending on which of four broad phases of development is involved:

	PHASE	**AUDITOR'S FOCUS**
a.	Systems analysis (SA)	Ensure controls are included in the design.
b.	Systems design/selection (SD)	Ensure objectives/acceptance criteria are met.

c.	Conversion/implementation (C/I)	Ensure there are economical operatic
d.	Post-project design/acquisition (PD/A)	Review for continuous improvement and/or process in general.

In the table above, which one of the four phases is correctly matched with the auditor's focus?

19. An organization needs reports in order to monitor risk events as well as the ongoing risk management plan. What would be the appropriate consolidation of reports by a CAE?

a. Significant events should be reported immediately, periodic written reports should cover key risk indicators on a scheduled basis, and the ERM plan should be reported during periodic presentations.
b. Significant events should be reported on a scheduled basis and periodic written reports and presentations should cover only risks that require immediate attention.
c. The CAE only needs to report to the board at meetings at intervals, while the risk owners need to report risk events more frequently.
d. The risk owners should report every risk event timely, and the CAE is responsible for ensuring that risk owners communicate their risks.

20. TLKT international has set its risk tolerance levels for customer returns of its handheld tools at 16%. The internal auditor notices a lag indicator in the inventory reports from the warehouse. The warehouse is restocking handheld tools at a 24% increase since the same period last year. What would be the appropriate action for the internal auditor to take to make management aware of this indicator?

a. The internal auditor needs to disclose the risk tolerance

disruption to the external stakeholders.

b. An outlier to risk tolerance is significant enough to be reported immediately, and the internal auditor should make the board aware.
c. The lag indicator should coordinate with risk owners to deliver status updates to the appropriate level of authority and determine if escalation is needed.
d. The internal auditor should do some research on the external environment to determine if the lag indicator needs to be reported.

21. While a successful risk management strategy can and should involve a wide range of internal and external parties, some of these parties have special roles and responsibilities. In this regard, which of the following responsibilities is correct?

a. High-level influence to ensure ERM is managed at an acceptable level is a responsibility of the operations team.
b. Facilitation of risk management reporting protocol is the responsibility of the CRO.
c. Implementing ERM in a coordinated, consistent manner is the responsibility of the board.
d. Risk management is never to be outsourced to external service providers.

22. Which of the following is an *inappropriate* trigger for internal audit to perform consulting?

a. An organization enters into a new market or activity.
b. Management wants to progress further along the risk maturity spectrum.
c. Management performs a PESTEL (P-Political; E-Economic; S-Social; T-Technological; E-Environmental; L-Legal) analysis and identifies new external risks.
d. A key risk management player leaves the organization and management wants to save time and money by having the

internal auditor fill the second line of defense role via consulting.

23. Which of the following are *true* statements about the appropriate advisory activities for internal audit?

I. Internal audit has a legitimate role in establishing risk responses.
II. Internal audit has a legitimate role in maintaining or developing the risk management framework.
III. Internal audit can play an advisory role in organizational governance.
IV. To maintain its objectivity, internal audit should not support risk management champions or good practices from other sections of the organization.

a. II and III.
b. I, II, and III.
c. I and III.
d. II and IV.

24. Federal agency X has determined its appetite for different types of risk across the organization. The agency also accounts for both upside and downside risk in its planning and develops strategic solutions to risks based on the interests of its multiple stakeholders. Based on this information, Pickett would consider agency X to be in which phase of developing its risk management framework?

a. Phase 1.
b. Phase 2.
c. Phase 3.
d. Phase 4.

25. The risk profile of an organization includes compliance with regulatory requirements as its highest-ranking risk. The CAE reviews the risk management plans for a lag indicator of regulatory compliance and notices that management has

neglected to implement remedial plans after several complaints about a wage and payroll matter. In light of the KRI, what is the best way for the CAE to communicate to management?

a. The CAE must bring the matter to the attention of the board because of the high risk ranking of this risk indicator, in accordance with IIA *Standards*.
b. The CAE must engage in an assurance audit to determine if management is at risk of failure to comply.
c. The CAE does not have to take any action because management is in charge of risk management for the organization.
d. The CAE should try to convince management to implement appropriate remedial or contingency plans.

26. What is the *least* effective step in a successful risk management advocacy project plan?

a. Identifying the target audiences for advocacy.
b. Demonstrating the value of integrating risk management into routine activities related to finance, procurement, and IT and advocating to extend that methodology to other departments and activities in an organization.
c. Reviewing the resources that can be applied to advocating risk management.
d. Setting and monitoring KPIs to assess the impact of advocacy.

27. When an internal auditor's report highlights risks for a client in a new line of business and makes recommendations beyond the mechanical level of formal systems, such as the client's project planning system in new business lines, what is the benefit to the client with regard to risk management?

a. The client will have an advantage over its customers in entering the new line of business because of the additional recommendations.
b. The client can rely on the auditor to act as the risk officer for its company.

c. Promotion of risk responses that go beyond the prescribed areas of responses can create valuable risk management activity for the client.
d. The internal auditor's report will save the client money in future audits by considering uncertain risks rather than favored risk responses.

28. The CAE of Yolo, Inc. has taken a strategic position that a disciplined risk management culture would benefit her organization. To advocate for the establishment of risk management, what are some of the steps that she can take?

I. Stakeholder analysis.
II. Develop key messages.
III. Select a framework.
IV. Set targets and KPIs.

a. I, II, and III.
b. I, III, and IV.
c. II, III, and IV.
d. I, II, and IV.

29. "To Facilitate Communication of Risks Across all Stakeholders and Risk Owners in Order to Reduce Silos and Increase Disciplined Risk Management" is an example of which of the following in building a risk management strategy?

a. Rationale and principles.
b. Role and purpose.
c. Risk policies.
d. Action plan.

30. Which of the following is *not* a role that internal audit can perform when supporting an organization in developing its risk management strategy?

a. Consult with management and the board to clarify the

objectives of the risk management strategy.

b. Identify key standards and frameworks that management could consider in implementation of the risk management strategy.
c. Conduct a gap analysis to help management identify the areas that the board and management will need to enhance and execute to achieve the desired risk management strategy.
d. Impose risk management processes that must be implemented.

SOLUTIONS

DOMAIN IV—CONSULTING ROLE OF THE INTERNAL AUDITOR

Question 1
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: b (I and III)

I. Correct. This is a key difference.
II. Incorrect. Implementing improvements is management's responsibility.
III. Correct. This is a key difference.
IV. Incorrect. Both assurance and consulting engagements must be defined in the internal audit charter.

Question 2
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: d

a. Incorrect. Internal audit can provide training or coaching in an area that it had previously audited. The opposite is not true, however. Internal audit cannot audit an area in which it provided advisory services within the previous 12 months.
b. Incorrect. Internal audit should never make final decisions regarding resource allocation to control or mitigate risk.
c. Incorrect. Internal audit should never establish risk appetite.
d. Correct. This is an essential safeguard to ensure that the internal audit activity and risk management responsibility remain

separate.

Question 3
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: b

a. Incorrect. Assurance engagements have three main parties—internal auditor, owner of activities, and recipient of assurance; consulting engagements have two main parties—internal auditor and recipient (client) of the advice.
b. Correct. This statement about differences is correct.
c. Incorrect. I and II are correct. IV is a true statement for assurance engagements but not for consulting.
d. Incorrect. This statement is true about assurance but not consulting.

Question 4
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: a (I and IV)

I. Correct. This is true about consulting engagements but not directly related to objectivity.
II. Incorrect. This statement is clearly related to objectivity and independence.
III. Incorrect. Auditors should not perform consulting without considering whether the engagement aligns with organizational objectives—a potential threat to independence.
IV. Correct. This is true and not a threat to objectivity or independence.

Question 5
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: a (I, III, and IV)

I. Correct. See The IIA's CIA Learning System for these four common consulting categories, and other IIA guidance and literature for multiple assurance categories.

II. Incorrect. Components of one audit can be a "mix" of the two categories.
III. Correct. The reverse of this is the case, i.e., consulting should not be used to circumvent assurance engagements.
IV. Correct. If this is the case, a disclosure is required.

Question 6
Source: *CRMA Exam Study Guide*, Introduction to Domain IV

Solution: b

a. Incorrect. This could lead to a conflict of interest.
b. Correct. The primary value of internal auditing comes from delivery of assurance. There should not be an "even split" between the two.
c. Incorrect. See IIA Standard 2120.C2.
d. Incorrect. See IIA Standard 2130.C1.

Question 7
Source: *CRMA Exam Study Guide*, IV.A

Solution: a

a. Correct. The auditors should work jointly with management to determine the requirements of the engagement.
b. Incorrect. This knowledge is a great asset that internal audit can contribute in an advisory capacity.
c. Incorrect. These are also key benefits to having internal audit act in an advisory capacity. Note, however, that internal audit can only make informed suggestions and cannot dictate the level of participation or the level of resources dedicated to an engagement.
d. Incorrect. Internal audit can teach the client competitive analysis techniques without imposing on management's responsibility to determine strategic direction.

Question 8
Source: *CRMA Exam Study Guide*, IV.A

Solution: c

a. Incorrect. While the CAE should determine if internal audit has the appropriate skill set and available labor, management (not the CAE) should decide whether to hire external consultants.
b. Incorrect. Objectives, scope, and approach of the consulting engagement should be agreed upon between the client and the internal auditor.
c. Correct. The auditor must ensure that the scope of the engagement is sufficient to address agreed-upon objectives. If the scope is insufficient, internal audit must discuss its reservations with the client to determine whether to proceed with the engagement. If the client and the CAE cannot reach an acceptable compromise, the CAE should decline the engagement.
d. Incorrect. The client is ultimately responsible for the objectives and scope of engagement.

Question 9
Source: *CRMA Exam Study Guide*, IV.A

Solution: d

a. Incorrect. This is a brainstorming activity and is common for facilitating risk identification.
b. Incorrect. Sending out questions or a survey in advance helps build a risk universe to be discussed in follow-up facilitation of risk identification.
c. Incorrect. Benchmarking in a firm's industry is a valuable source of information for identifying risks.
d. Correct. Internal audit should not be telling management what the risks are.

Question 10
Source: *CRMA Exam Study Guide*, IV.B

Solution: b

a. Incorrect. While clients should be able to talk freely with

internal audit without worrying that conversations will be reported up the chain of command, if significant control weaknesses or potential wrongdoing are identified, the client should not have an expectation of confidentiality.

b. Correct. Furthermore, it is not a conflict of interest for auditors who identified a material weakness in risk management to coach management in ways to redress the weakness.
c. Incorrect. When internal audit is in a coaching rather than a training situation, it does not tell management what is wrong and needs improvement, but it does help management identify the areas that need improvement and the goals needed to get there.
d. Incorrect. Coaching should not be seen as a way to fix a problem but as a process of helping others develop through personal growth and discovery. Coaching contributes to "a culture of continuous improvement and increasing risk management maturity."

Question 11
Source: *CRMA Exam Study Guide*, IV.B

Solution: c

a. Incorrect. Training is not the most appropriate for I, nor is Mentoring for III.
b. Incorrect. The choices for III and IV are not the most appropriate, and none of the three roles are appropriate for IV.
c. Correct. All choices are the likely the most effective and appropriate for the situation.
d. Incorrect. The only effective and appropriate choice here is Training for III.

Question 12
Source: *CRMA Exam Study Guide*, IV.B

Solution: a

a. Correct. Consulting seems the most practical action because two

assurance engagements had already led to relevant recommendations, the risks were great, and action was not taken.

b. Incorrect. Standards do not permit the auditor to assume a management role.
c. Incorrect. This approach would usually be seen as beyond the role of the internal audit function. In addition, enacting legislation is often a very slow process.
d. Incorrect. This would not be seen as "adding value." A nonchalant attitude, if discovered, could harm internal audit's reputation.

Question 13
Source: *CRMA Exam Study Guide*, IV.B

Solution: b

a. Incorrect. Coaching contributes to a culture of continuous improvement and increasing risk management maturity.
b. Correct. This is a situation that is likely to have the most appeal for providing coaching.
c. Incorrect. Identifying what is wrong and what needs improvement is an expectation of a training session.
d. Incorrect. Its primary focus is equipping him or her for continued success in the future.

Question 14
Source: *CRMA Exam Study Guide*, Introduction to Domain IV and IV.B

Solution: b

a. Incorrect. Internal auditors are often involved as consultants.
b. Correct. The objective is assessing the fairness/reliability of financial statement information, and approaches are structured. Also, external auditors are often extensively involved.
c. Incorrect. Internal auditors are often involved as consultants and must avoid making management decisions.

d. Incorrect. The IIA states that the range of involvement by internal auditors is from *intense* (maybe assurance) to *minimal* (likely consulting).

Question 15
Source: *CRMA Exam Study Guide*, Introduction to Domain IV, IV.B and IV.C

Solution: a

a. Correct. By definition, this is correct.
b. Incorrect. In performance audits, for example, a consulting engagement can advise management on whether the measures in use are appropriate.
c. Incorrect. This is true of performance audits, but operational audits have a broader focus (e.g., overall effectiveness, continuous improvement, etc.).
d. Incorrect. Certain stakeholders (e.g., the board and management) would be interested in both categories, but it is likely that external stakeholders would be interested in the results of performance audits.

Question 16
Source: *CRMA Exam Study Guide*, IV.C

Solution: c

a. Incorrect.
b. Incorrect.
c. Correct. While internal audit is often fluent in the spectrum of standards and the operations of the enterprise, establishing effective enterprise-wide risk management is one of the principal responsibilities of management and the board. Internal audit can advise management of available options but not dictate the best approach to risk management that meets the needs of the organization and reflects its size, culture, goals, and capabilities.
d. Incorrect.

Question 17
Source: *CRMA Exam Study Guide*, IV.C

Solution: d

a. Incorrect.
b. Incorrect.
c. Incorrect.
d. Correct. All four options are true about coordination.

Question 18
Source: *CRMA Exam Study Guide*, Introduction to Domain IV and IV.C

Solution: d

a. Incorrect. SA focus is to evaluate feasibility, not to ensure controls are included in the design.
b. Incorrect. SD focus is to ensure controls are included in design, not to meet criteria.
c. Incorrect. C/I focus is to assure project objectives and acceptance criteria are met.
d. Correct. These are correct for audit focuses in post-project/acquisition.

Question 19
Source: *CRMA Exam Study Guide*, IV.D

Solution: a

a. Correct. Events that have a major impact need to be escalated immediately; monthly or quarterly reports should cover risks needing attention; and periodic presentations can be timed with board meetings to cover non-critical changes to risk profile and risk indicators.
b. Incorrect. Significant events should be escalated immediately, not just at scheduled or periodic intervals.
c. Incorrect. The CAE should consolidate the risk owners' reports and ensure that they are rolled into periodic written reports or

presentations, or when significant, escalated.

d. Incorrect. The CAE does not ensure that risk owners communicate their risks but should take the role of consolidating the risk owners' reports.

Question 20
Source: *CRMA Exam Study Guide*, IV.D

Solution: c

a. Incorrect. Reporting lag indicators should first be coordinated with internal reporting.
b. Incorrect. Outliers to risk tolerance may have to be escalated at times, but the internal auditor should coordinate with risk owners to find out what levels of reporting exist and how risk events are communicated.
c. Correct. When risk events threaten to disrupt operations, the internal auditor should determine the system for reporting that already exists.
d. Incorrect. It is important to understand the external environment, but the role of the internal auditor is to coordinate any research and reporting that the organization has in place or report to the appropriate level when reporting does not exist.

Question 21
Source: *CRMA Exam Study Guide*, IV.D, IV.G

Solution: b

a. Incorrect. The board has high-level influence, not the operations team.
b. Correct. This option is consistent with IIA guidance. Note that risk management cannot be delegated.
c. Incorrect. The CEO has to ensure implementation in a coordinated, consistent manner.
d. Incorrect. Risk management may be outsourced as needed under the direction of the board.

Question 22
Source: *CRMA Exam Study Guide*, IV.E

Solution: d

a. Incorrect. This is a legitimate reason that organizations request internal audit advisory services.
b. Incorrect. This is a legitimate reason that organizations request internal audit advisory services.
c. Incorrect. This is a legitimate reason that organizations request internal audit advisory services.
d. Correct. To maintain independence, internal audit should not assume responsibility for managing risk. Therefore, any internal audit consulting role in the second line of defense should only be an interim solution for a fixed time period.

Question 23
Source: *CRMA Exam Study Guide*, IV.E and IV.F

Solution: a (II and III)

I. Incorrect. See the IIA "Fan." Internal auditors can promote risk responses but not establish them.
II. Correct. As long as stringent safeguards are in place and everyone understands that the managing risk is the responsibility of management, internal audit can provide consulting to help the organization improve its risk management.
III. Correct. The governing body needs independent assurance and consultative services of internal audit with respect to governance. Standard 2100 states that internal audit must contribute to the improvement of governance.
IV. Incorrect. These are key ways that internal audit can promote risk management and move the organization forward in the maturity of its risk management processes. Internal audit does not compromise its objectivity by highlighting better practices in risk management, even if the practitioners are from the same organization.

Question 24
Source: *CRMA Exam Study Guide*, IV.E

Solution: c

a. Incorrect. An organization in Phase 1 views risks as threats to achieving its goals without proactive measures to identify or address risk.
b. Incorrect. Agency X has defined risk appetite, which is not achieved until Phase 3.
c. Correct. Agency X has satisfied the conditions of Phases 2 and 3.
d. Incorrect. There is no evidence that agency X integrates risk management in its operations.

Question 25
Source: *CRMA Exam Study Guide*, IV.E

Solution: a

a. Correct. When the level of risk that management has accepted is deemed unacceptable by the CAE, the CAE must communicate his or her observations to the board.
b. Incorrect. The information given indicates that the risk of noncompliance is deemed high already, so an additional assurance audit will not be an effective action by the CAE. The CAE must address management's current risk response with the board.
c. Incorrect. The CAE is responsible for reviewing risk management activities of its organization and reporting exceptions to the board.
d. Incorrect. Option a is better.

Question 26
Source: *CRMA Exam Study Guide*, IV.F

Solution: b

a. Incorrect. Advocacy is the art of inspiring others to take action. Therefore, advocacy is improved by tailoring messaging to each

audience or set of stakeholders.

b. Correct. To be the best advocate for risk management, internal audit must move beyond reliance on traditional (finance, procurement, IT) internal controls and risk responses. Internal audit should strive to be conversant with and advocate the most current best practice developments in risk management across the enterprise, including traditional and nontraditional activities.
c. Incorrect. Planning an advocacy project, like any other project, requires an understanding of the time and money available to advocate for risk management.
d. Incorrect. Establishing and monitoring progress against KPIs is critically important to understanding and communicating progress made as a result of the advocacy initiative.

Question 27
Source: *CRMA Exam Study Guide*, IV.F

Solution: c

a. Incorrect. There is not enough information in risk identification alone for the client to gain advantages in market entry.
b. Incorrect. While the internal auditor needs to advocate for risk management, there would need to be clear delineation of his or her role in an advisory capacity.
c. Correct. When the internal auditor provides responses based on uncertain risk factors rather than specific risks, he or she advocates for more robust risk management.
d. Incorrect. There is not enough information to make a direct correlation between an audit report that highlights uncertain risk responses and the need for or cost of future audits.

Question 28
Source: *CRMA Exam Study Guide*, IV.F

Solution: d (I, II, and IV)

I. Correct. Determining who should be involved and what their

respective interests and needs are is critical in getting support from the stakeholders.

II. Correct. As part of the timeline to advocate for risk management, a well-thought-out communication plan that includes what and to whom messages should be broadcast is critical.

III. Incorrect. Selecting a framework is a key element after a disciplined risk management culture and project plan is developed and initiated.

IV. Correct. As is true of any project, establishing metrics and performance indicators will help advocate for risk management in order to build confidence in its value.

Question 29
Source: ***CRMA Exam Study Guide*****, IV.G**

Solution: b

a. Incorrect. Rationale and purpose is needed after the role and purpose is documented; this is when the risk management strategy is clearly aligned to the needs of the organization.

b. Correct. Creation of a mission statement for risk management will support the board's overall objectives of supporting organization effectiveness.

c. Incorrect. Policies are the details by which a risk management strategy will be guided and measured.

d. Incorrect. An action plan is one of the last steps needed in developing a risk management strategy. It describes the detailed steps for execution.

Question 30
Source: ***CRMA Exam Study Guide*****, IV.G**

Solution: d

a. Incorrect. Consulting engagements are an acceptable role of internal audit to gather information that management can use in its risk management strategy development.

b. Incorrect. Internal audit has the knowledge and understands the recognized standards and guidance that may be best for the organization's unique structure, values, and objectives.
c. Incorrect. Before the execution of a risk management strategy, internal audit can facilitate a gap analysis to determine where the organization's position in risk management maturity currently is and identify where it needs to grow.
d. Correct. Internal audit cannot impose risk management processes; this is the responsibility of the board and management.

REFERENCES

DOMAIN I: ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

IIA. 2008. *GAIT for Business and IT Risk (GAIT-R)*. (Q. 5 and Q. 15)

COSO. February 2004. *Improving Organizational Performance and Governance, How the COSO Frameworks Can Help*. Committee of Sponsoring Organizations of the Treadway Commission. (Q. 14)

National Security Agency. *Information Security Assessment Methodology* (IAM). (Q. 15)

AIRMIC, Alarm, and IRM. 2010. *A Structured Approach to ERM and the Requirements of ISO 31000*. (Q. 30)

KPMG International. 2012. *Conflict Minerals and Beyond, Part II*. (Q. 36)

The Conference Board. February 2010. *The Duty to Monitor under Delaware Law: from Caremark to Citigroup*. (Q. 44)

DOMAIN II: PRINCIPLES OF RISK MANAGEMENT PROCESSES

COSO. 2012. *Risk Assessment in Practice*. Committee of Sponsoring Organizations of the Treadway Commission. (Q. 15)

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Q. 16)

The IIA's CIA Learning System, Part 1, Chapter 3. The Institute of Internal Auditors. (Q. 26 and Q. 27)

COSO. 2004. *Enterprise Risk Management – Integrated Framework*.

Committee of Sponsoring Organizations of the Treadway Commission. (Q. 26, Q. 33, Q. 35, Q. 38, and Q. 40)

International Organization for Standardization. ISO 31000:2009, *Risk Management – Principles and Guidelines*. (Q. 35)

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors. (Q. 36 and Q. 37)

AIRMIC, Alarm, IRM. 2002. *A Risk Management Standard*. (Q. 44)

Ernst & Young. 2013. *Value Creation – Background Paper for <IR>*. (Q. 45)

DOMAIN III: ASSURANCE ROLE OF THE INTERNAL AUDITOR

IIA. 2009. Position Paper. The Role of Internal Auditing in Enterprise-wide Risk Management. The Institute of Internal Auditors. (Q. 1)

IIA. Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures. The Institute of Internal Auditors. (Q. 1)

Mainelli, M. 2007. *Frontiers of Risk Management: Key Issues and Solutions*. (Q. 3)

IIA. 2009. Practice Guide, Formulating and Expressing Internal Audit Opinions. The Institute of Internal Auditors. (Q. 4)

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Q. 7, Q. 9, and Q. 18)

Sobel, Paul J. 2011. *Internal Auditing's Role in Risk Management*. The Institute of Internal Auditors Research Foundation. (Q. 8)

Corporate Executive Board. 2012. *Defining Internal Audit's Role in Mergers and Acquisitions: Adding Value for Successful Integration*. (Q. 8)

IIA. 2010. Practice Guide. Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors. (Q. 9, Q. 12, Q. 18, Q. 24, and Q. 25)

IIA. Practice Advisory 2050-2: Assurance Maps. The Institute of Internal Auditors. (Q. 10)

COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Coemmittee of Sponsoring Organizations of the Treadway

Commission. (Q. 11 and Q. 20)
Walker, Paul L., William G. Shenkir, and Thomas L. Barton. 2011. *Improving Board Risk Oversight Through Best Practices*. (Q. 14 and Q. 15)
IIA. Standard 2120: Risk Management. The Institute of Internal Auditors. (Q. 16)
IIA. Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning. The Institute of Internal Auditors. (Q. 16 and Q. 21)
IIA. Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity. The Institute of Internal Auditors. (Q. 17)
The IIA's CIA Learning System, Part 2, Section II, Chapters B and C. The Institute of Internal Auditors. (Q. 19)
IIA. Standard 2010: Planning. The Institute of Internal Auditors. (Q. 19)
Beasley, Mark S., Bruce C. Branson, and Bonnie V. Hancock. 2010. *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks*. Committee of Sponsoring Organizations of the Treadway Commission. (Q. 23)
Edmead, Mark. 2007. *Understanding the Risk Management Process. Internal Auditor*. (Q. 24)
Walker, David. 2009. *A review of corporate governance in UK banks and other financial industry entities*. http://corpgov.law.harvard.edu/2009/12/26/a-review-of-corporate-governance-in-uk-banks-and-other-financial-industry-entities/ (Q. 27)
International Organization for Standardization. ISO 31000:2009, *Risk Management – Principles and Guidelines*. (Q. 27)
IIA. Standard 2050: Coordination. The Institute of Internal Auditors. (Q. 28)
IIA. Practice Advisory 2050-2: Assurance Maps. The Institute of Internal Auditors. (Q. 29)
Ciorciari, Maria, and Peter Blattner. 2008. *Enterprise Risk Management Maturity-Level Assessment Tool*. The Society of Actuaries. (Q. 30)

DOMAIN IV: CONSULTING ROLE OF THE INTERNAL AUDITOR

IIA. Standard 2050: Coordination. The Institute of Internal Auditors. (Q. 2 and Q. 4)

IIARF. 2012. *Sawyer's Guide for Internal Auditors*, 6th Edition. The Institute of Internal Auditors Research Foundation. (Q. 3)

IIA. Standards 2120.C2, 2130.C1, 2010.C.1, and 1130.C2. The Institute of Internal Auditors. (Q. 4)

The IIA's CIA Learning System, Part 1, Section I, Introduction. The Institute of Internal Auditors. (Q. 5)

IIA. Standards 2220.A2, 2120.C2, and 2120.C1. The Institute of Internal Auditors. (Q. 6)

The IIA's CIA Learning System, Part 2, Section 1, Topics 8, 9. The Institute of Internal Auditors. (Q. 14 and Q. 15)

Maynard, Gregg R. 1999. Embracing Risk. *Internal Auditor*. (Q. 17)

The IIA's CIA Exam Learning System, Part I, Section II, Topic 3. The Institute of Internal Auditors. (Q. 21)

RIMS and IIA. 2012. *Risk Management and Internal Audit: Forging a Collaborative Alliance*. (Q. 23)

Pickett, K. H. Spencer. 2005. *Auditing the Risk Management Process*. John Wiley & Sons, Inc. (Q. 24)

IIA. Standard 2600: Communicating the Acceptance of Risks. The Institute of Internal Auditors. (Q. 25)

Leitch, Matthew. 2004. *Embedded Risk Management: The Auditors' Contribution*. (Q. 26)

GLOSSARY

NOTE: Many of the definitions in this glossary are taken from the glossary in The IIA's International Professional Practices Framework, or have been modified as appropriate to conform to the discussions in this textbook.

Add Value
Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

Adequately Designed — See Controls are Adequately Designed

Advocate
Inspire others to change their understanding, attitude, or behavior by promoting a particular viewpoint or position.

Appropriate Evidence
Any piece or collection of evidence gained during an engagement that provides relevant and reliable support for the judgments and conclusions reached during the engagement.

Assurance Layering
A technique of coordinating multiple assurance activities designed to mitigate a known risk to a needed or desired level within an established risk tolerance.

Assurance Map

A visual depiction of the different assurance activities and assurance functions within an organization. Such a depiction can help identify gaps or overlaps in assurance activities and help assess that risk is managed consistent with the board's and management's expectations.

Assurance Mapping
The process of coordinating and reviewing all assurance activities to identify and fill gaps and eliminate overlaps.

Assurance Services
An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Audit Engagement — See Assurance Services

Audit Observation
Any identified and validated gap between the current and desired state arising from an assurance engagement.

Audit Opinion
Internal audit's statement of the effectiveness of internal controls based on an independent and objective evaluation.

Audit Risk
The risk of reaching invalid audit conclusions and/or providing faulty advice based on the audit work conducted.

Audit Scope
The agreed span of an audit as defined by the purpose, planned activities, objectives, risks, and controls under review as well as any areas expressly excluded.

Audit Universe
A compilation of the subsidiaries, business units, departments, groups, processes, or other established subdivisions of an organization that exist

to manage one or more business risks.

Benchmarking
Systematic comparison of actual activity or performance with given standards of excellence or best practice.

Big Data
A term used to refer to the large amount of constantly streaming digital information, massive increase in the capacity to store large amounts of data, and the amount of data processing power required to manage, interpret, and analyze the large volumes of digital information.

Bottom-Up Approach
To begin by looking at all processes directly at the activity level, and then aggregating the identified processes across the organization.

Business Ethics
The moral principles and values used to inform organizational activities and decision making.

Business Process
The set of connected activities linked with each other for the purpose of achieving one or more business objectives.

Business Process Outsourcing (BPO)
The act of transferring some of an organization's business processes to an outside provider to achieve cost reductions, operating effectiveness, or operating efficiency while improving service quality.

CAE
Chief audit executive

Capabilities
Activities an organization is equipped to undertake given its resources (including staff expertise, technical knowhow, patents, reputation, equipment, facilities, customer base, and capital).

CEO

Chief executive officer

CFO
Chief financial officer

CGAP
Certified government auditing professional

CGFM
Certified government financial manager

Checklist (for Risk Identification)
A prepared set of common risks, usually classified under broad headings, used as a prompt or suggestions to help identify the actual risks that exist in a given activity or entity.

Chief Audit Executive
A senior position within the organization responsible for internal audit activities. When internal audit activities are obtained from external service providers, the chief audit executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, and follow-up of engagement results. The term also includes titles such as general auditor, head of internal audit, chief internal auditor, internal audit director, and inspector general.

CIA
Certified internal auditor

CIO
Chief information officer

CISO
Chief information security officer

Coaching
A process for helping others develop by enabling them to discover and grow.

Code of Ethics
The Code of Ethics of The Institute of Internal Auditors contains principles relevant to the profession and practice of internal auditing and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing. A code of ethics more generally is any set of guidelines designed to direct behavior.

Combined Assurance
Aligning various assurance activities within an organization to ensure assurance gaps do not exist and assurance activities minimize duplication and overlap but still manage risk consistent with the board's and management's expectations.

Compensating Control
An activity that, if key controls do not fully operate effectively, may help to reduce the related risk. Such controls also can back up or duplicate multiple controls and may operate across multiple processes and risks. A compensating control will not, by itself, reduce risk to an acceptable level.

Compliance
Conformity and adherence to applicable laws and regulations (COSO definition). May also include conformity and adherence to policies, plans, procedures, contracts, or other requirements.

Condition
The factual evidence that the internal auditor found in the course of the examination (what does exist).

Conflict of Interest
Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Consulting Services

Advisory and related services, the nature and scope of which are agreed to with the customer, are intended to improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Contingency Plan
A provisional plan prepared in advance for the purposes of recovering the situation if risks materialize or other things go wrong.

Continuous Auditing
Using computerized techniques to perpetually audit the processing of business transactions.

Control
Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. See also Internal Control and System of Internal Controls.

Control Environment
The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal controls. The control environment includes the following elements:

- Integrity and ethical values
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices
- Competence of personnel

Control Risk

The potential that controls will fail to reduce controllable risk to an acceptable level.

Control Risk Self-assessment (CRSA)
A structured process for identifying and analyzing risks, usually within a given framework, carried out by the risk owners, often with support from a facilitator.

Controllable Risk
The portion of inherent risk that management can reduce through day-to-day operations and management activities.

Controls are Adequately Designed
Present if management has planned and organized (designed) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks can be managed to an acceptable level.

Controls are Operating Effectively
Present if management has executed (operated) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

COO
Chief operations officer

COSO
Committee of Sponsoring Organizations of the Treadway Commission

Corruption
Acts in which individuals wrongfully use their influence in a business transaction to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another (for example, kickbacks, self-dealing, or conflicts of interest).

CPA

Certified Public Accountant

Criteria
The standards, measures, or expectations used in making an evaluation and/or verification of an observation (what should exist).

CRMA
Certification in Risk Management Assurance

CRO
Chief risk officer

CRSA
Control risk self-assessment

Customer
The subsidiary, business unit, department, group, individual, or other established subdivision of an organization that is the subject of a consulting engagement.

Data Analytics
A process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making.

Database
A large repository of data, typically contained in many linked files, and stored in a manner that allows the data to be easily accessed, retrieved, and manipulated.

Delegation
The passing of authority to a subordinate for certain tasks or roles while retaining the ultimate responsibility for their undertaking.

Democratic
A style of management or decision making that is highly decentralized and widely participative.

Detective Control
An activity designed to discover undesirable events that have already occurred. A detective control must occur on a timely basis (before the undesirable event has had a negative impact on the organization) to be considered effective.

Downside Risk — See Pure Risk

Effect
The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the consequence of the difference).

Emerging Risk
A previously unknown risk that may not yet be fully understood that has arisen due to changes in the internal or external environments or changes to the organization's objectives and activities.

Engagement
A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of objectives. See also Assurance Services and Consulting Services.

Engagement Work Program
A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

Entity-Level Control
A control that operates across an entire entity and, as such, is not bound by, or associated with, individual processes.

ERM
Enterprise risk management. See also Risk Management.

External Auditor — See Independent Outside Auditor

Framework
A body of guiding principles that form a template against which

organizations can evaluate a multitude of business practices. These principles are comprised of various concepts, values, assumptions, and practices intended to provide a yardstick against which an organization can assess or evaluate a particular structure, process, or environment or a group of practices or procedures.

Fraud
Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Fraudulent Financial Reporting
Acts that involve falsification of an organization's financial statements (for example, overstating revenues or understating liabilities and expenses).

GAAP
Generally Accepted Accounting Principles

GAIT-R
The IIA's *GAIT for Business and IT Risk* (part of the Guide to the Assessment of IT Risk [GAIT] methodology).

GAO
U.S. Government Accountability Office

General Information Technology Controls
Controls that operate across all IT systems and are in place to ensure the integrity, reliability, and accuracy of the application systems. Also represents a specific example of an "entity-level control."

Governance
The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

GRC
Governance, risk, and compliance

Groupthink
A tendency among groups to adopt a common position even where differences of opinion exist arising through peer pressure and an unwillingness to appear to be different or wrong.

Hard Controls
Controls that are effected by policies, processes, and structure.

Icebreaker
A group activity designed to familiarize individuals with each other and encourage greater collaboration.

Impairment to Independence or Objectivity
The introduction of threats that may result in a substantial limitation, or the appearance of a substantial limitation, to the internal auditor's ability to perform an engagement without bias or interference.

Independence
The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels. See also Organizational Independence.

Independent Outside Auditor
A registered public accounting firm, hired by the organization's board or executive management, to perform a financial statement audit providing assurance for which the firm issues a written attestation report that expresses an opinion about whether the financial statements are fairly presented in accordance with applicable Generally Accepted Accounting Principles.

Individual Objectivity
An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made.

Objectivity requires internal auditors not to subordinate their judgment on audit matters to that of others.

Information Technology Governance
The leadership, structure, and oversight processes that ensure the organization's IT supports the objectives and strategies of the organization.

Information Technology Operations
The department or area in an organization (people, processes, and equipment) that performs the function of running the computer systems and various devices that support the business objectives and activities.

Inherent Limitations of Internal Control
The confines that relate to the limits of human judgment, resource constraints and the need to consider the cost of controls in relation to expected benefits, the reality that breakdowns can occur, and the possibility of collusion or management override.

Inherent Risk
The combination of internal and external risk factors in their pure, uncontrolled state, or, the gross risk that exists, assuming there are no internal controls in place.

Insight
An end product or result from the internal audit function's assurance and consulting work designed to provide valued input or information to a client or customer. Examples include identifying entity-level root causes of control deficiencies, emerging risks, and suggestions to improve the organization's governance process.

Internal Audit Charter
A formal, written document that defines the internal audit function's purpose, authority, and responsibility. The charter should (a) establish the internal audit function's position within the organization, (b) authorize access to records, personnel, and physical properties relevant to the performance of engagements, and (c) define the scope of the internal audit function.

Internal Control
A process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

ISO 31000
A set of standards promulgated by the International Organization for Standardization designed to help organizations manage risk.

IT
Information technology

Key Control
An activity designed to reduce risk associated with a critical business objective.

Key Performance Indicator
A metric or other form of measuring whether a process or individual tasks are operating within prescribed tolerances.

Key Principles Approach
This approach to providing risk management assurance compares what is present within the entity under review with a given set of principles (from ISO, COSO, or other similar source), thus identifying areas that confirm and others that require further improvement.

Key Risk
A significant risk because of its ability to cause serious disruption to the organization's objectives or core activities.

Key Risk Indicator (KRI)
A measure used to indicate that certain trigger events or conditions likely to precipitate a risk event have occurred or arisen.

Lag Indicator
A signal of something (such as a risk incident) that has already occurred.

Laissez-faire
A style of management characterized by a lack of intervention and a tendency to allow things to happen.

Lead Indicator
A signal that something (such as a risk incident) is likely to occur in the near future.

Limited Assurance — See Negative Assurance

LoC
Letter of credit

Material Observation
An individual observation, or a group of observations, is considered "material" if the control in question has a reasonable possibility of failing and the impact of its failure is not only significant, but also exceeds management's materiality threshold.

Maturity Model
The principle underpinning the risk management maturity model is that over time, one would expect (and internal audit should encourage) a steady evolution in the maturity of risk management processes. Providing assurance on risk management processes on this basis involves identifying the current level of risk maturity and exploring with management the opportunities that exist for advancing maturity further.

Mission
Statement of an organization's purpose.

Monitoring
A process that assesses the presence and functioning of governance, risk management, and control over time.

Monte-Carlo Simulation

A problem-solving technique used to approximate the probability of certain outcomes by running multiple trial runs, called simulations, using random variables.

Negative Assurance
Assurance based on the absence of any evidence to the contrary.

Objectives
What an entity desires to achieve. When referring to what an organization wants to achieve, these are called business objectives, and may be classified as strategic, operations, reporting, and compliance. When referring to what an audit wants to achieve, these are called audit objectives or engagement objectives.

Objectivity — See Individual Objectivity

Observation
A finding, determination, or judgment derived from the internal auditor's test results from an assurance or consulting engagement.

Ongoing Assessments
Risk mitigation may be monitored routinely as part of the risk management processes themselves as a regular and systematic feedback in the cycle to check that actions are being taken as planned and controls are operating as expected. See also Separate Assessments.

Operating Effectively — See Controls are Operating Effectively

Operating System
Software programs that run the computer and perform basic tasks, such as recognizing input from the keyboard, sending output to the printer, keeping track of files and directories on the hard drive, and controlling various computer peripheral devices.

Operational Objective
A goal that is usually short- to mid-term (within a year or two) that is activity-focused and designed to enable the achievement of strategic objectives.

Opportunity
The possibility that an event will occur and positively affect the achievement of objectives.

Organizational Independence
The chief audit executive's line of reporting within the organization that allows the internal audit function to fulfill its responsibilities free from interference. See also Independence.

PESTEL
A mnemonic acronym that stands for **P**olitical, **E**conomic, **S**ocial, **T**echnological, **E**nvironmental, **L**egal. PESTEL analysis is a framework or tool used by marketers to analyze and monitor the macro-environmental factors that have an impact on an organization.

Porter's Five Forces Model
A model identifying five forces that shape industry competition (competitive rivalry, threat of new entrants, threat of substitutes, bargaining power of suppliers, and bargaining power of customers).

Porter's Value Chain Model
A model that helps to analyze specific activities through which firms can create value and competitive advantage.

Positive Assurance
Assurance based on a statement noting confirmed evidence of effective or ineffective controls.

Preventive Control
An activity designed to deter unintended events from occurring.

Probability-Proportional-to-Size (PPS) Sampling
A modified form of attribute sampling used to reach a conclusion regarding monetary amounts rather than rates of occurrence.

Process Elements Approach
This approach to providing assurance on risk management processes involves a validation of each of the key processes, looking for evidence

that they are working according to expectation and that as a whole the risk management framework is effective.

Process-Level Control
An activity that operates within a specific process to achieve process-level objectives.

Produce or Perish
A management grid model developed in 1964 by Robert R. Blake and Jane Mouton that balances task- and people-oriented leadership.

Professional Skepticism
The state of mind in which internal auditors take nothing for granted; they continuously question what they hear and see and critically assess audit evidence.

Psychology of Risk — See Risk Psychology

Pure Risk
A risk that is wholly negative with the potential to damage or constrain objectives without the possibility of creating positive opportunity.

RAG Rating
A system of colored indicators (red, amber, and green like traffic lights) to signify criticality. Red is used when urgent attention is needed, amber when caution is required, and green when conditions are as expected.

Reasonable Assurance
A level of assurance supported by generally accepted auditing procedures and judgments. Reasonable assurance can apply to judgments surrounding the effectiveness of internal controls, the mitigation of risks, the achievement of objectives, or other engagement-related conclusions.

Residual Risk
The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk).

Risk

The possibility that an event will occur and impact objectives, whether positively or negatively.

Risk Appetite
The amount of risk, on a broad level, an organization is willing to accept in pursuit of its business objectives. Risk appetite takes into consideration the amount of risk that management consciously accepts after balancing the cost and benefits of implementing controls.

Risk Assessment
The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed.

Risk Attitude
The aggregated risk appetite for an entity being the overall tendency to accept or avoid risk.

Risk Aware
A level of risk maturity where there is a scattered, silo-based approach to risk management across an entity.

Risk Capacity
The amount of risk an entity or activity is able to tolerate as a consequence of its capabilities.

Risk Capture
The ability to record and document a risk event when a risk materializes.

Risk Correlation
The association of two or more risks such that their likelihoods and impacts vary together in a direct relationship, being an example of a particular kind of interdependency.

Risk Criteria
Factors that may be used to analyze risk, the most common being likelihood (or probability) and impact (consequence), with other criteria

including volatility, velocity, and vulnerability.

Risk Culture
An organization's overall attitude and approach toward risk and risk management.

Risk-Defined
A middle-tier level of risk maturity in which risk appetite is defined and where there are defined risk management policies and strategies in place.

Risk-Enabled
The highest level of risk maturity where risk management processes and internal controls are enterprise-wide and fully embedded.

Risk Escalation
The process of reporting a risk event upwards in the management structure for the purposes of sharing the information and authorizing remedial action (including the implementation of contingency plans).

Risk Event (or Risk Incident)
The occurrence or materialization of a risk.

Risk Identification
The process of finding, recognizing, and describing risks.

Risk Incident — See Risk Event

Risk Interdependency
The relationships between two or more risks that, when combined, may precipitate a greater impact or additional consequences than when the risks arise on their own.

Risk Level (or Risk Severity)
The overall threshold of a risk, usually measured as the simple product of likelihood and impact, although organizations may choose to weight these factors and may take other factors such as vulnerability and velocity into account.

Risk Managed
A high level of risk maturity in which there is an enterprise-wide approach that is well communicated.

Risk Management
The process conducted by management to understand and deal with uncertainties (that is, risks and opportunities) that could affect the organization's ability to achieve its objectives. More generally, risk management can refer to any efforts made to address risk within a given endeavor.

Risk Management Framework
The overall arrangements for addressing risk within an organization.

Risk Map
A graphical depiction of risks, usually based on the two axes of likelihood and impact.

Risk Maturity
The degree to which an organization, its culture, and/or its risk management processes are robust, where robustness is a function of how embedded risk management processes are within the organization, and the extent to which a consideration of risk impacts decision making, planning, resource allocation, and other key activities.

Risk Mitigation
An action or set of actions taken by management to reduce the impact and/or likelihood of a risk to a lower, more acceptable level.

Risk Naive
A low level of risk maturity with very limited appreciation of the existence of risk in which risks are not addressed systematically.

Risk Prioritization
The ranking of risk according to severity to target attention and resources to the most significant risks.

Risk Profile

The overall picture of risk across a range of categories, showing the sum total exposures.

Risk Psychology
The subjective elements inherent in the identification and assessment of and attitude toward risk.

Risk Register
A structured record of all of the key risks within an organization or defined area of activity together with the analysis.

Risk Response
An action or set of actions taken by management to achieve a desired risk management strategy. Risk responses can be categorized as risk avoidance, reduction, sharing, or acceptance. Exploiting opportunities that, in turn, enable the achievement of objectives, is also a risk response. ISO 31000 refers to this step in risk management as risk treatment.

Risk Severity — See Risk Level

Risk Tolerance
The acceptable levels of risk size and variation relative to the achievement of objectives, which must align with the organization's risk appetite. It is also described as being the acceptable variation from risk appetite (i.e., by how much and for how long the entity can accept residual risk levels above appetite).

Risk Treatment — See Risk Response

Risk Universe
The sum total of all the relevant risks impacting a given entity or organization.

Sampling Risk
The risk that the internal auditor's conclusion based on sample testing may be different than the conclusion reached if the audit procedure was applied to all items in the population.

Sarbanes-Oxley
The U.S. Sarbanes-Oxley Act of 2002 is legislation passed by the U.S. Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures.

Secondary Control
An activity designed to either reduce risk associated with business objectives that are not critical to the organization's survival or success, or serve as a backup to a key control.

Scope — See Audit Scope

Separate Assessments
Risk management mitigation may be monitored by separate assessments, which are those that are not part of risk management processes themselves but are initiated and administered as required to gain assurance on their effectiveness. See also Ongoing Assessments.

Significant Observation
An individual observation or group of observations is considered "significant" if the control activity in question has a reasonable possibility of failing and the impact of its failure is significant.

SMART
A mnemonic acronym that stands for **S**pecific, **M**easurable, **A**chievable, **R**ealistic, **T**ime-limited and gives criteria to guide in setting objectives in project management, employee-performance management, and personal development.

Soft Controls
Controls that rely on the behavior and attitude of individuals.

Stakeholder
Individuals or parties with an interest (or stake) in a given project, enterprise, or organization.

Sufficient Evidence

A collection of evidence gained during an engagement that, in its totality, is enough to support the judgments and conclusions made in the engagement.

Sweet Spot
The optimal position used to refer to a number of different situations, including the optimal balance between risk and benefits.

System of Internal Controls
Comprises the five components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring that are in place to manage risks related to the financial reporting, compliance, and operational objectives of an organization. See also Internal Control.

Third-Party Service Provider
A person or firm, outside the organization, that provides assurance and/or consulting services to an organization.

Three Lines of Defense
A model of assurance whereby management control is the first line of defense in risk management; the various risk, control, and compliance oversight functions established by management serve as the second line of defense; and independent assurance is the third line of defense.

Tone at the Top
The entity-wide attitude of integrity and control consciousness, as exhibited by the most senior executives of an organization. See also Control Environment.

Top-Down Approach
To begin at the entity level with the organization's objectives, and then identify the key processes critical to the success of each of the organization's objectives.

Transparency
Communicating in a manner that a prudent individual would consider to be fair and sufficiently clear and comprehensive to meet the needs of the

recipient(s) of such communication.

Upside Risk
Risk with the potential for positive opportunity or gain.

Value Engineering (VE)
A systematic method to improve the “value” of goods or products and services by using an examination of function.

Vulnerability Assessment
The process of identifying and evaluating risks for a given venture or organization by examining the propensity for failure.

Walk-Through
A method of testing controls by following the control processes in operation from start to finish.

Work Program — See Engagement Work Program

SUGGESTED READING

DOMAIN I: ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGMENT

AIRMIC, Alarm, IRM. 2010. A *Structured Approach to Enterprise Risk Management (ERM)*. Available at http://theirm.org/ISO31000guide.htm (retrieved February 8, 2013).

Centre for Ethical Leadership. 2013. *Ethical Leadership*. Available at http://ethicalleadership.org/about-us/philosophies-definitions/ethical-leadership (retrieved February 3, 2013).

COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

Enterprise Risk Management: A Guide for Government Professionals, Karen Hardy, November 2014.

Institute of Business Ethics. 2013. What is business ethics? Available at www.IBE.org.uk (retrieved February 3, 2013).

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.

IIA. 2013. Position Paper, The Three Lines of Defense in Effective Risk Management and Control. The Institute of Internal Auditors.

Sobel, Paul J. 2011. *Auditor's Risk Management Guide: Integrating Auditing and ERM*. CCH Inc.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially chapters 1 and 2.)

DOMAIN II: PRINCIPLES OF RISK MANAGMENT PROCESSES

COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

COSO. 2012. *Risk Assessment in Practice*. Committee of Sponsoring Organizations of the Treadway Commission. ISO 31000:2009 Risk Management – Principles and Guidelines.

Deloitte. 2005. *Risky business? Managing Risk and Creating Value in a Volatile World*. London: Deloitte Research.

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.

Leitch, Matthew. 2008. *Intelligent Internal Control and Risk Management*. Gower Publishing Company. (Especially chapters 2 and 3.)

PwC. 2009. *Exploring Emerging Risks: Extending Enterprise Risk Management (ERM) to Address Emerging Risks*. PricewaterhouseCoopers. Available online at http://www.pwc.com/gx/en/research-publications/pdf/pwcglobalriskserm.pdf.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially Section 2, chapters 3–8.)

Kaplan, Robert S., and Anette Mikes. 2012. Managing Risks: A New Framework. *Harvard Business Review*, Vol. 90 Issue 6: 48–60.

DOMAIN III: ASSURANCE ROLE OF THE INTERNAL AUDITOR

Beasley, M., B. Branson, and B. Hancock. 2010. *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks*. Committee of Sponsoring Organizations of the Treadway Commission.

IIA. 2009. Position Paper, The Role of Internal Auditing in Enterprise Risk Management. The Institute of Internal Auditors. Available online at https://na.theiia.org/standardsguidance/Public%20Documents/PP%20Th (retrieved March 7, 2013).

IIA. 2009. Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes. The Institute of Internal Auditors.

IIA. 2011. Practice Guide, Reliance by Internal Audit on Other Assurance Providers. The Institute of Internal Auditors. Available online at https://na.theiia.org/standards-guidance/recommended-guidance/practiceguides/Pages/Reliance-by-Internal-Audit-on-Other-Assurance-Providers-Practice%20Guide.aspx.

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors. Available online at https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Assessing-the-Adequacy-of-Risk-Management-Practice-Guide.aspx (retrieved March 7, 2013).

IIA and RIMS. 2012. *Risk Management and Internal Audit: Forging a Collaborative Alliance*. The Institute of Internal Auditors and the Risk and Insurance Management Society. Available online at https://na.theiia.org/standards-guidance/Public%20Documents/RIMS%20and%20The%20IIA%20Execut

Protiviti. 2010. *Board Risk Oversight: A Progress Report*. Committee of Sponsoring Organizations of the Treadway Commission. Available online at http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf.

Sobel, Paul J. 2011. *Internal Auditing's Role in Risk Management*. The Institute of Internal Auditors Research Foundation. Available online at http://www.theiia.org/bookstore/product/internal-auditings-role-in-risk-management-1561.cfm.

Walker, P., W. Shenkir, and T. Barton. 2011. *Improving Board Risk Oversight Through Best Practices*. The Institute of Internal Auditors Research Foundation. (Especially chapter 9.)

DOMAIN IV: CONSULTING ROLE OF THE INTERNAL AUDITOR

IIA. 2009. Position Paper, The Role of Internal Auditing in Enterprise Risk Management. The Institute of Internal Auditors. Available online at https://na.theiia.org/standards-

guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%
(retrieved March 7, 2013).

IIA. 2012. Standard 2050: Coordination. The Institute of Internal Auditors.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially chapter 8, “Risk Management Reporting.”)

The *Certification in Risk Management Assurance® (CRMA®) Exam Practice Questions* is designed to be a helpful tool in preparing for the CRMA exam. Included are practical, scenario-based questions as well as those of a theoretical nature. Suggested solutions provide reference to specific sections of the *CRMA Exam Study Guide*. Additionally, a reference section offers sources for further study.

Within this comprehensive collection, there are 150 questions covering the four domains in the CRMA exam:

- Domain I: Organizational Governance Related to Risk Management
- Domain II: Principles of Risk Management Processes
- Domain III: Assurance Role of the Internal Auditor
- Domain IV: Consulting Role of the Internal Auditor

After reviewing the questions in each domain, you will have a clear understanding of the exam content. This analysis and reflection will help you determine whether you are ready to sit for the actual CRMA exam.

The IIA Research Foundation

ISBN 978-0-89413-914-7