# Contents

Foreword ................................................................. v
Acknowledgments .......................................................... vii
About the Authors ......................................................... ix

**DOMAIN I  Organizational Governance Related to Risk Management** ............................................. 1

Exam Practice Questions .................................................. 1
Solutions for Domain I ......................................................... 15

**DOMAIN II  Principles of Risk Management Processes** ............................................................ 31

Exam Practice Questions .................................................. 31
Solutions for Domain II ......................................................... 45

**DOMAIN III  Assurance Role of the Internal Auditor** ............................................................... 61

Exam Practice Questions .................................................. 61
Solutions for Domain III ......................................................... 69

**DOMAIN IV  Consulting Role of the Internal Auditor** ............................................................... 79

Exam Practice Questions .................................................. 79
Solutions for Domain IV ......................................................... 89
References ................................................................. 99
Glossary ................................................................. 103
Suggested Reading ......................................................... 117
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).
SOLUTIONS

DOMAIN I—ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

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

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.A

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

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

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.